2018

A framework for development of android mobile electronic prescription transfer applications in compliance with security requirements mandated by the Australian healthcare industry

Kyaw Kyaw Htat
Edith Cowan University

A framework for development of Android mobile electronic prescription transfer applications in compliance with security requirements mandated by the Australian Healthcare Industry

This thesis is presented for the degree of
Doctor of Information Technology

Kyaw Kyaw Htat

Master of Computer Science

Bachelor of Science (Computer Science)

Edith Cowan University

School of Science

Principal Supervisor: Professor Trish Williams

Associate Supervisors: Dr Vincent McCauley,

Dr Zubair Baig and Dr Krishnun Sansurooah

March 2018

USE OF THESIS

ABSTRACT

This thesis investigates mobile electronic transfer of prescription (ETP) in compliance with the security requirements mandated by the Australian healthcare industry and proposes a framework for the development of an Android mobile electronic prescription transfer application. Furthermore, and based upon the findings and knowledge from constructing this framework, another framework is also derived for assessing Android mobile ETP applications for their security compliance.

The centralised exchange model-based ETP solution currently used in the Australian healthcare industry is an expensive solution for on-going use. With challenges such as an aging population and the rising burden of chronic disease, the cost of the current ETP solution's operational infrastructure is certain to rise in the future. In an environment where it is increasingly beneficial for patients to engage in and manage their own information and subsequent care, this current solution fails to offer the patient direct access to their electronic prescription information. The current system also fails to incorporate certain features that would dramatically improve the quality of the patient's care and safety, i.e. alerts for the patient's drug allergies, harmful dosage and script expiration. Over a decade old, the current ETP solution was essentially designed and built to meet legislation and regulatory requirements, with change-averting its highest priority. With little, if any, provision for future growth and innovation, it was not designed to cater to the needs of the ETP process. This research identifies the gap within the current ETP implementation (i.e. dependency on infrastructure, significant on-going cost and limited availability of the patient's medication history) and proposes a framework for building a secure mobile ETP solution on the Android mobile operating system platform which will address the identified gap.

The literature review part of this thesis examined the significance of ETP for the nation's larger initiative to provide an improved and better maintainable healthcare system. The literature review also revealed the stance of each jurisdiction, from legislative and regulatory perspectives, in transitioning to the use of a fully electronic ETP solution. It identified the regulatory mandates of each jurisdiction for ETP as well as the security standards by which the current ETP implementation is

governed so as to conform to those regulatory mandates. The literature review part of the thesis essentially identified and established how the Australian healthcare industry’s various prescription-related legislations and regulations are constructed, and the complexity of this construction for eTP.

The jurisdictional regulatory mandates identified in the literature review translate into a set of security requirements. These requirements establish the basis of the guiding framework for the development of a security-compliant Android mobile ETP application. A number of experimentations were conducted focusing on the native security features of the Android operating system, as well as wireless communication technologies such as NFC and Bluetooth, in order to propose an alternative mobile ETP solution with security assurance comparable to the current ETP implementation. The employment of a proof-of-concept prototype such as this alongside / coupled with a series of iterative experimentations strengthens the validity and practicality of the proposed framework.

The first experiment successfully proved that the Android operating system has sufficient encryption capabilities, in compliance with the security mandates, to secure the electronic prescription information from the data at rest perspective. The second experiment indicated that the use of NFC technology to implement the alternative transfer mechanism for exchanging electronic prescription information between ETP participating devices is not practical. The next iteration of the experimentation using Bluetooth technology proved that it can be utilised as an alternative electronic prescription transfer mechanism to the current approach using the Internet. These experiment outcomes concluded the partial but sufficient proof-of-concept prototype for this research.

Extensive document analysis and iterative experimentations showed that the framework constructed by this research can guide the development of an alternative mobile ETP solution with both comparable security assurance to and better access to the patient’s medication history than the current solution. This alternative solution would present no operational dependence upon infrastructure and its associated, on-going cost to the nation’s healthcare expenditure. In addition, use of this mobile ETP alternative has the potential to change the public’s perception (i.e. acceptance from regulatory and security perspectives) of mobile healthcare solutions, thereby paving the way for further innovation and future enhancements in eHealth.

DECLARATION

I certify that this thesis does not, to the best of my knowledge and belief:

(i) incorporate without acknowledgment any material previously submitted for a degree or diploma in any institution of higher education;

(ii) contain any material previously published or written by another person except where due reference is made in the text; or

(iii) contain any defamatory material.

I also grant permission for the Library at Edith Cowan University to make duplicate copies of my thesis as required.

Signature: [redacted]

Date: 8th JUNE 2018

ACKNOWLEDGEMENTS

In science and in academic work there is no place for personal sentiment except in the acknowledgements and dedications of theses such as this. So much gratitude is owed to a number of special colleagues, friends and family. This has been a very long and strange journey which challenged not only my intellect but also my dedication to the cause and the unwavering support of these colleagues, friends and family. Despite the fact that life itself a very long journey of learning and we all are scholars of varying levels till the end, this has been a very rewarding one in which I have learnt so much more than I could ever have imagined.

First and foremost are my supervisors Professor Trish Williams and Dr Vincent McCauley. Trish, I am eternally grateful for your guidance, patience and understanding of the difficulties and competing priorities associated with doing a doctorate degree part-time whilst working full-time and raising a young family. I cannot thank you enough for your guidance through the theory and practice of information systems research which was unfathomable for me at first. It is your encouragement, humour and wise words that kept me on course when I felt despair and uncertainty during this long journey. I wouldn't have made it this far today without those. Vince, I sincerely appreciate your invaluable insight into the health IT universe. Your concrete expertise from both IT professional and clinician perspectives was an infinite fountain of knowledge for me. I am so thankful to you for being "Google" for all my inquisitive and sometimes challenging questions. Both of you amplify my enthusiasm and confidence to make a difference in the emerging health IT field. I also would like to express my sincere gratitude to A/Professor Donald McDermid for believing in me and taking me on as a doctoral candidate while the rest of the world disapproved of me for not having significant prior research experience.

To my clever boys, Caesar and Kaiser, I know this has been a terribly long time in the making, costing you countless weekends (a significant part of your childhood, which would otherwise have been much more fun). I hope that the determination and perseverance you witnessed in my pursuit of this goal sets an example for you in pursuing your passion in life. To my lovely wife, Khine Chaw

Su, I am eternally in your debt for your support and understanding through this journey, which I know has not been easy for you. I acknowledge your support and thank you from the bottom of my heart - and I promise that I will spend a lot more time being the test subject for your new recipes and helping you with publication of your next recipe books in the years to come. These acknowledgements would be partial without a dedication to my parents, Dr Soe Myint and Daw Pu Pu. I am thankful for your love and encouragement and the sacrifices that you have made. I am devastated that my father, Dr Soe Myint, passed away before seeing me achieve this milestone. I can’t imagine how happy and relieved he will be to see me finishing this doctorate. I hope that the black sheep of the family has finally done something notable.

Finally, I would like to thank my bosses, Andrew Hukin and Robyn Hukin, for allowing me to pursue my passion. The fortnightly time-off for study over the past seven plus years was crucial for my learning journey so thank you. I also would like to thank my colleague Takeshi Azumi for his help in finding relevant research materials originally written in Japanese. The “Google Translate” would not have been much help without your assistance and I wouldn’t have had a clue where to begin the investigation on eHealth solutions used in Japan without your help mate - thanks.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

GLOSSARY OF TERMS/ABBREVIATIONS

5CPA	Fifth Community Pharmacy Agreement
6CPA	Sixth Community Pharmacy Agreement
ADB	Android Debug Bridge
ADEs	Adverse Drug Events
ADHA	Australian Digital Health Agency
ADT	Android Developer Tools
AMA	Australian Medical Association
AMT	Australian Medicines Terminology
AOSP	Android Open Source Project
API	Application Programming Interface
AS	Australian Standard
ATS	Australian Technical Specification
CDA	Clinical Document Architecture
CDD	Compatibility Definition Document
CIS	Clinical Information System
CPA	Community Pharmacy Agreement
CTS	Compatibility Test Suite
DAK	Document Access Key
DoHA	Department of Health and Aging
EDS	Electronic Dispensing System
ELS	Endpoint Location Services
eMM	electronic Medication Management
EPS	Electronic Prescribing System
eTP	electronic Transfer of Prescriptions
GP	General Practitioner
GPS	Global Positioning System
HB	Handbook

HI	Health Identifiers
HL7	Health Level 7
IDE	Integrated Development Environment
IHE	Integrating the Healthcare Enterprise
IHTDSDO	International Health Terminology Standards Development Organisation
IoT	Internet-of-Things
ISO	Organisation for Standardisation
MA	Medicare Australia
MSIA	Medical Software Industry Association
NCTIS	National Clinical Terminology and Information Service
NDEF	NFC Data Exchange Format
NEHTA	National E-Health Transition Authority
NFC	Near Field Communication
NPDR	National Prescription and Dispense Repository
NPS	National Prescribing Service
OEM	Original Equipment Manufacturer
OTA	over-the-air
PBS	Pharmaceutical Benefits Scheme
PCEHR	Personally Controlled Electronic Health Records
PES	Prescription Exchange Services
PIP	Practice Incentives Program
PKI	Public Key Infrastructure
QUM	Quality Use of Medicines
RACGP	Royal Australian College of General Practitioners
RFID	Radio Frequency Identification
RK	Retrieval Key
RPC	Remote Procedure Call
SD	Secure Digital
SDK	Software Development Kit

SMD	Secure Message Delivery
VM	virtual machine
XDM	Cross-Enterprise Document Media Interchange
XML	Extensible Mark-up Language

CHAPTER 1. INTRODUCTION

During the last decade, the processing power and storage capacity of handheld computing devices has advanced exponentially. Today's smartphones and handheld computing devices such as tablet PCs possess a processing power and storage capacity far superior to those of desktop computers a decade ago. This advancement opens up a whole new territory in mobile computing platforms, both for the consumer and for industry partners such as social networking, health and fitness and banking. These industries are seizing the opportunity to extend their reach, while mobile computing devices are now ubiquitous in the consumer market.

This shift of focus enables mobile devices to become major candidates for integral roles within the evolving eHealth systems. Utilisation of mobile/handheld computing devices in healthcare systems will significantly alter how healthcare services are delivered, improve the quality of patient experience and reduce the cost of healthcare in general (West, 2012) by virtue of the better use of information technology in facilitating the electronic access, transmission and recording of health information. However, the adoption of mobile computing in healthcare inevitably transforms the ways in which health information is acquired, used, disclosed and stored. This transformation requires the establishment of sophisticated health information systems and governance frameworks within which to facilitate and dictate information sharing and exchange (Hodge, Gostin & Jacobson, 1999), explore opportunities and seek solutions to the current and potential issues associated with secure transmission and use of electronic data for health in a mobile environment. Among many other facets of eHealth, mobile computing can be adopted in the electronic Transfer of Prescriptions (eTP) for improved healthcare system outcomes and better cost-effectiveness of healthcare services. ETP creates a pathway of technological development from the current paper-based manual or web-based hybrid prescription processes to a fully electronic, mobile and paperless initiative. It is an important step towards an eHealth-enabled healthcare system which ensures medicines information is accurately and securely shared, providing a range of healthcare benefits to both prescribers and consumers (“NPS MedicineWise”, 2012). When fully implemented, this sharing of high quality patient medication information between the prescriber and dispenser enables quality use of medicine, thus enhancing the safety and quality of patient care (“AMA Position Statement”, 2009).

1.1 Background

Developed countries with digital health capabilities implement electronic prescribing systems to some extent, depending on their acts, regulations and the various levels (i.e. state and national) of their healthcare infrastructure. These systems play a crucial role in connecting prescribers and dispensers, and deliver indisputable benefits such as improved patient safety via reduced transcribing errors during dispense; increased workflow efficiency in dispensing at the pharmacy; reduced readmissions due to adverse drug events and preventable medication prescribing errors and the better coordination and management of care between doctors and pharmacists (“Boot”, 2011). An electronic prescribing system facilitates the secure and efficient management and sharing of a client’s/patient’s medication information and provides a wide range of benefits for all parties involved (i.e. prescribers, dispensers and consumers) ("AMA Position Statement", 2009; "NPS MedicineWise", 2012). The use of electronic prescription is also crucial in improving patients’ safety by reducing preventable adverse drug events through accurate medication information sharing and improved medication compliance. Since almost 70,000 hospital admissions per year are associated with adverse drug events, the decrease in these occurrences as the result of the employment of an electronic prescription would imply a significantly reduced demand on health funding. (“NEHTA Blueprint V2”, 2011). It is not an overstatement to say that electronic prescription is the key to enhanced patient safety, better medication compliance, improved accuracy and efficiency in medication information sharing between Clinical Information Systems (CIS) and reduced healthcare costs. However, these benefits do not come without a significant impact on Australian healthcare expenditure.

In Australia, the current electronic prescribing model for delivering electronic prescription details from the prescriber to the patient/user-selected prescription dispenser makes use of one of two Prescription Exchange Services (PES) – *Script Exchange* from eRx and *Script Vault* from MediSecure. Use of electronic prescription is cost-free for prescribers but each prescription downloaded from PES services by a pharmacy attracts an electronic prescription fee of fifteen cents. At present it is also cost-neutral to the pharmacies because the electronic prescription fee of fifteen cents for each eligible prescription is subsidised by the 6th Community Pharmacy Agreement (6CPA). Since December 2012, interoperability between the two PES operators allows prescribers to upload the electronic copy of their prescription to one PES service and the dispensers (i.e. pharmacies) to download from the other PES service. Prior to achieving interoperability between the two PES services the electronic prescription fees were as much as eighty-five cents per prescription (McDonald, 2015). There has been a considerable increase in the use of electronic prescriptions by pharmacies and doctors since the launch of eRX in 2009. A significant milestone in Australia's eHealth journey was achieved on 30th July 2015 when eRx, one of the two PES services, dispensed its one billionth prescription (*ibid*). When combined with the prescriptions dispensed by the other PES service operated by MediSecure (*Script Vault*), the numbers could be considerably higher. This indicates improved confidence in the use of electronic prescriptions and a substantial uptake by the pharmacies and doctors. On the other hand, eRx's announcement in August 2015 regarding the dispensing of its billionth electronic prescription also proves that electronic dispensing had cost the nation at least AU$150 million at that point in time (i.e. calculated using the current minimum fees, although it was much more expensive in the earlier years) (*ibid*). Since there are two PES services, the total cost of using both services will be considerably more, if not twice as much. A recent survey by eRx found that pharmacies using eRx are dispensing 753,000 electronic prescriptions per day, with up to twenty-five prescriptions per second during peak periods (*ibid*). The fees alone for 753,000 electronic prescriptions on just one day represent a cost to the nation of AU$112,950.

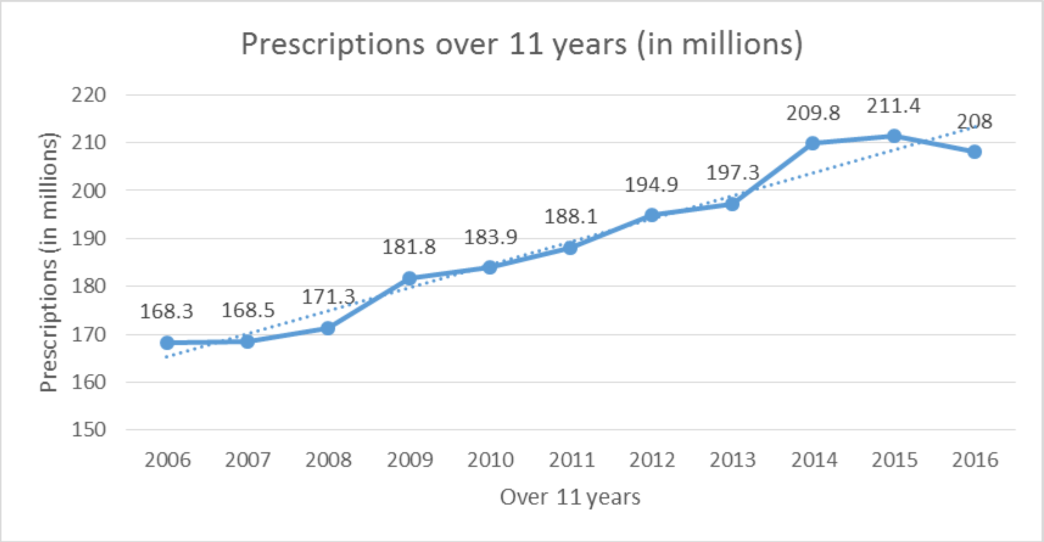


Figure 1.1: Number of prescriptions over an 11 year period (using PBS data)

Despite the decrease in the total number of prescriptions in 2016 compared to that of 2015, there has been an increase of 13.3% in electronic prescription fees for 2016 (i.e. AU$8,091,750 in 2015 and AU$9,164,954 in 2016) ("Expenditure and Prescriptions Twelve Months to 30 June 2016", 2016). Since there has been no change in the Electronic Prescription Fee for each prescription in recent years, this increase indicates that more electronic prescriptions are being used in 2016 compared to the previous year. Although this higher usage of electronic prescriptions perfectly aligns with the nation's eHealth initiatives, electronic prescriptions will continue to contribute to the nation's increasing healthcare expenditure unless more cost-effective, long term alternatives with comparable security measures are put in place.

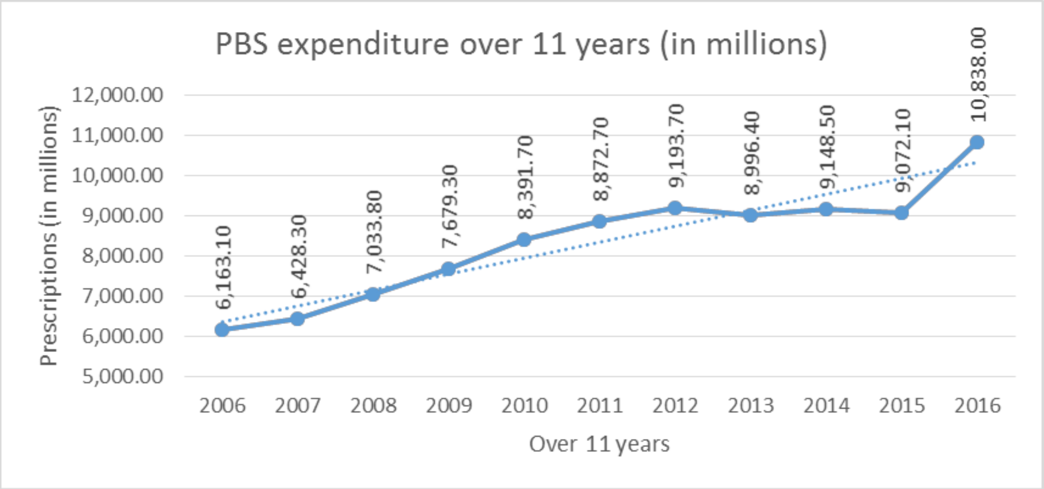


Figure 1.2: PBS expenditure over an 11 year period (using PBS data)

Using statistics from the Pharmaceutical Benefits Scheme website, Figures 1.1 and 1.2 show the PBS expenditure and number of prescriptions over an eleven years period, 2006 to 2016. It is evident that, although the PBS expenditure fluctuated slightly, the number of prescriptions increased steadily over the eleven years period. This indicates that unless cheaper alternatives are found, the ongoing cost associated with the current electronic prescription transfer model will continue to increase with the increasing volume of use. Although the Commonwealth subsidises the electronic prescription fee through a series of Community Pharmacy Agreements, the significant ongoing cost implied by these statistics prompted the exploration of cheaper or more cost-effective alternatives. Potential alternatives to using the current PES services for transferring electronic prescriptions include CD/DVD-ROM as used in Japan (“Japan Association for Medical Informatics”, 2014), Universal Serial Bus (USB) flash drives, smartcards, mobile smart phones and Health Level 7 (HL7) messaging via SMS or Secured Message Delivery (SMD) services.

Of these potential alternatives to using PES services, this research focuses on the use of the patient’s mobile device as the secure transfer media/mechanism for electronic prescriptions. Figure 1.3 illustrates the participants of the current electronic prescription model and its operation from a high-level perspective.

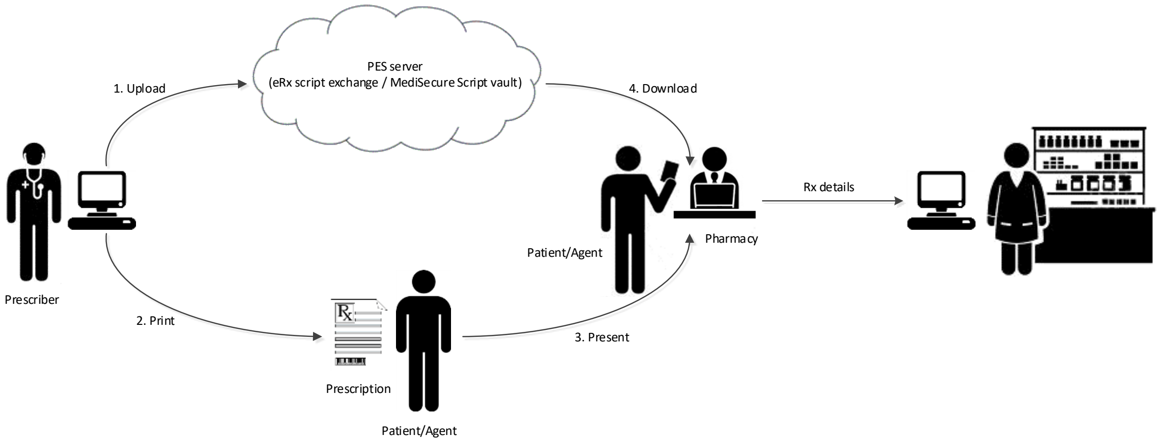


Figure 1.3: Current electronic prescription using PES services (overview)

This research examines the existing methods for the transfer of prescription information around current practices and legislative and regulatory constraints as well as enablers at Commonwealth, state and territory levels. Finally, it presents a framework for the development of a secure mobile application for prescription transfer which is compliant with those constraints. This research also assesses and then compares the security of prescription information in the current PES-based approach to that of mobile devices using the proposed secure mobile ETP application.

1.2 Significance of Study

This research offers potential financial, clinical and administrative benefits for all parties involved in the prescribing process (i.e. prescriber, dispenser and patient). Furthermore, it provides opportunities for future enhancements such as the implementation and integration of a Clinical Decision Support System component as part of the proposed mobile prescription solution. This component would require a study of its own within the ETP context and is outside the scope of this research.

1.2.1 Financial Benefits

Since this research is to explore the potential of using a mobile electronic prescription transfer mechanism as an alternative to the current approach which uses PES services, the fifteen-cent electronic prescription fee associated with using PES services might be eliminated. Although this fifteen cents sounds trivial for an individual prescription, its elimination would save tens of millions of dollars in annual healthcare expenditure. The savings on the 211.4 million prescriptions dispensed in 2015 alone would have been as much as AU$31.7 million (see Figure 1.1). This research, therefore, has the potential to significantly reduce the nation's healthcare budget. The current cost-neutrality of using electronic prescription (i.e. cost-free for all parties involved) is achieved via Commonwealth subsidy: the electronic prescription fee provided through a series of Community Pharmacy Agreements (i.e. 5CPA and 6CPA agreements). Whilst it is yet to be determined who will bear this cost when it is no longer subsidised by the Commonwealth – the prescriber, dispenser or patient – this research proposes a secure solution that allows the electronic prescription process to remain cost-free for all parties involved.

1.2.2 Clinical Benefits

This proposed alternative also opens up opportunities to incorporate certain useful features such as prescription expiration alerts and last repeat alerts. Currently the patient only receives this communication when a prescription is dispensed. More importantly, this proposed solution enables the implementation of alert features for drug allergies and harmful doses as part of the mobile electronic prescription transfer application. Whilst the implementation of these features is not part of the current study, opportunities for this are opened up, with potential to significantly improve patient safety and benefit all parties involved in the prescribing process.

Hospitals are also a major beneficiary of this solution. When the interface of the proposed application is implemented and integrated with the hospital information system, the application can directly transfer the full history of a patient's medication from the patient's mobile phone into the hospital's information system. Such access to the patient's complete medication history would be of inestimable clinical benefit both to the healthcare professionals in delivering better quality of care and the patient receiving it.

1.2.3 Administrative Benefits

Enabling the patient's smartphone as the secure transfer medium for electronic prescriptions allows the patient to be in control of their personal and sensitive information without negative impacts on public health initiatives and government recorded data such as the National Prescription and Dispense Repository (NPDR). It empowers the patient to take more responsibility for their health and places them in full control of personal, sensitive information, which in turn also controls the secondary use of such information by third parties (i.e. public health monitoring, program evaluation, research etc.). In addition to this, the proposed mobile solution has the potential to both reduce the complexity of the electronic prescription transfer process and remove the dependency on the current major supporting infrastructure (i.e. PES services) and Internet connectivity. Free from those dependencies, the proposed mobile solution will therefore function just as effectively in remote locations with poor or non-existent Internet connectivity, making it suitable for remote regions of Australia where the network availability is limited or unreliable.

From a wider perspective the proposed mobile electronic prescription transfer application is hypothetically suitable for the other countries and jurisdictions, for instance in Japan, where healthcare information is considered to be too sensitive to be transferred via the public Internet network.

Furthermore, without the requirement for the supporting network infrastructure and associated ongoing costs, this proposed solution has another, wider-reaching, facet: the potential to improve the quality of care in third world countries with limited resources, or indeed anywhere with network availability issues, by enabling the use of electronic prescriptions.

1.2.4 Conclusion

As an enabler for mobile electronic prescription and potential future innovations in the mobile ETP context, this research was conducted with a focus on the practicality of its outcomes both from development and utilisation perspectives. ETP plays a fundamental role in Australia’s eHealth initiative to improve its healthcare system. The mobile electronic prescription transfer solution proposed in this research offers an alternative to the continued use of the current costly and technologically constrained ETP implementation. The current ETP implementation has a significant ongoing operational cost (i.e. the Electronic Prescription Fee) and, while this represents only a small part of the nation’s overall healthcare expenditure, the funds could be invested in direct improvements in healthcare rather than spent on ongoing infrastructure.

1.3 Structure of the thesis

This research identified the relevant acts, regulations and standards governing the ETP implementation in the Australian healthcare industry at Commonwealth, state and territory levels. Further assessment and analysis of the relevant regulatory mandates determined each jurisdiction's readiness for the fully electronic ETP implementation, and established the mandatory security requirements for mobile ETP applications (in fact for any fully electronic ETP implementation in general).

The research outcomes were recorded in two tables: one table contains each jurisdiction's readiness for fully electronic ETP and the other lists the mandatory security requirements from the data at rest and data in transit perspectives. The table listing the mandatory security requirements will also serve as the security compliance matrix for ETP applications in accordance with the Australian healthcare industry's regulatory mandates. This security compliance matrix was used in determining whether mobile operating and wireless communication have sufficient security measures for ETP in the Australian healthcare industry.

Furthermore, this research proposed a fully electronic mobile ETP solution using a number of technologies which comply with the security requirements listed in the security compliance matrix. In order to propose said solution, a further series of research into the governing standards and experimentations was conducted on each candidate technology, assessing their compliance with the security requirements.

This research began with a preliminary study (Chapter 1) where the researcher explored the nature of electronic prescriptions and its usages and expenses over the past decade. Chapter 2 delved into the literature review on how the current implementation of ETP functions using the PES services and its governing standards, regulations and acts. This second chapter also examined the potential issues and shortcomings of current ETP implementation from various aspects, including availability and consistency of the patient’s medication information, its requirements for the supporting infrastructure and finally the associated ongoing expenses. It should be noted that before formulating the Research Questions – one primary question followed by two subsidiary questions – the researcher had previously investigated the functions of the current ETP in terms of infrastructure, security and its regulatory enablers and barriers. This research contributed to the publication of a paper titled, “***The hare and the tortoise: the potential versus the reality of ETP implementation***”.

Chapter 3 discussed the underlying principles (i.e. research methodology, methods and theoretical framework) and developed the research design and investigative approaches with which to answer the Research Questions devised in Chapter 2. Chapter 4 presented the research results and, based on those results, proposed an alternative mobile ETP solution using a number of potential candidate technologies in supporting comparable security assurances. Table 4.1 (*Analysis matrix of each jurisdiction's readiness for fully electronic ETP solution*) recorded each jurisdiction's readiness for the fully electronic prescription system from the regulatory perspective. The regulatory mandates were interpreted into a set of security requirements, the outcomes of which were recorded in section 2 and 3 of Table 4.2 (Analysis matrix of Security requirements for electronic prescription information).

Chapter 5's emphasis is on Android's security features from the data at rest perspective. Data at rest is information stored on a mobile device, PC hard drives or removable media (Hochmuth, n.d.). The experiment conducted was targeted towards the Android's encryption being able to handle and comply with the security requirements from the data at rest perspective. This is an output from a research paper titled "***Security of ePrescription: Security of data at rest in Prescription Exchange Services vs on mobile devices***", published as proceedings of the 4th Australian eHealth Informatics and Security Conference in 2015 (Htat, Williams, & McCauley, 2015b).

The emphasis of Chapter 6 was on the security aspects of data in transit, with a detailed study of NFC technology's security features and governing standards. The experiment in section 6.2 found that, due to development and portability issues, the use of NFC technology is not a practical solution. It was then decided to examine Bluetooth wireless technology as the alternative transfer mechanism. The in-depth study and experimentation on the Bluetooth technology's security features and governing standards proved it to be suitable for the proposed mobile ETP solution. The findings from this in-depth Bluetooth technology research was published in another paper titled "***Security of ePrescriptions: Data in Transit Comparison Using Existing and Mobile Device Services***", published as proceedings of the Australasian

Computer Science Week Multiconference 2017 (Htat, Williams, & McCauley, 2017).

Chapter 7 extended, from a more holistic perspective, the discussion built from the previous chapters, the literature review and the experimentation and research results. These discussions also reflect against the Research Questions devised in Chapter 2. Additional output from this research development phase yielded another publication titled "***Future of Australia's eTP: Script Exchange, Script Vault or secure mobile alternative***". This was published as proceedings of the 14th Australian Information Security Management Conference 2016. Note that the publication dates of the third and fourth papers are not in sequential order due to the difference in the lead time between their submission dates and publication dates. Figure 1.4 depicts the thesis structure reflecting on the research activities and published papers. Finally, Chapter 8 concluded the research by listing its potential impact and contribution towards the body of knowledge and identifying ways of extending this research.

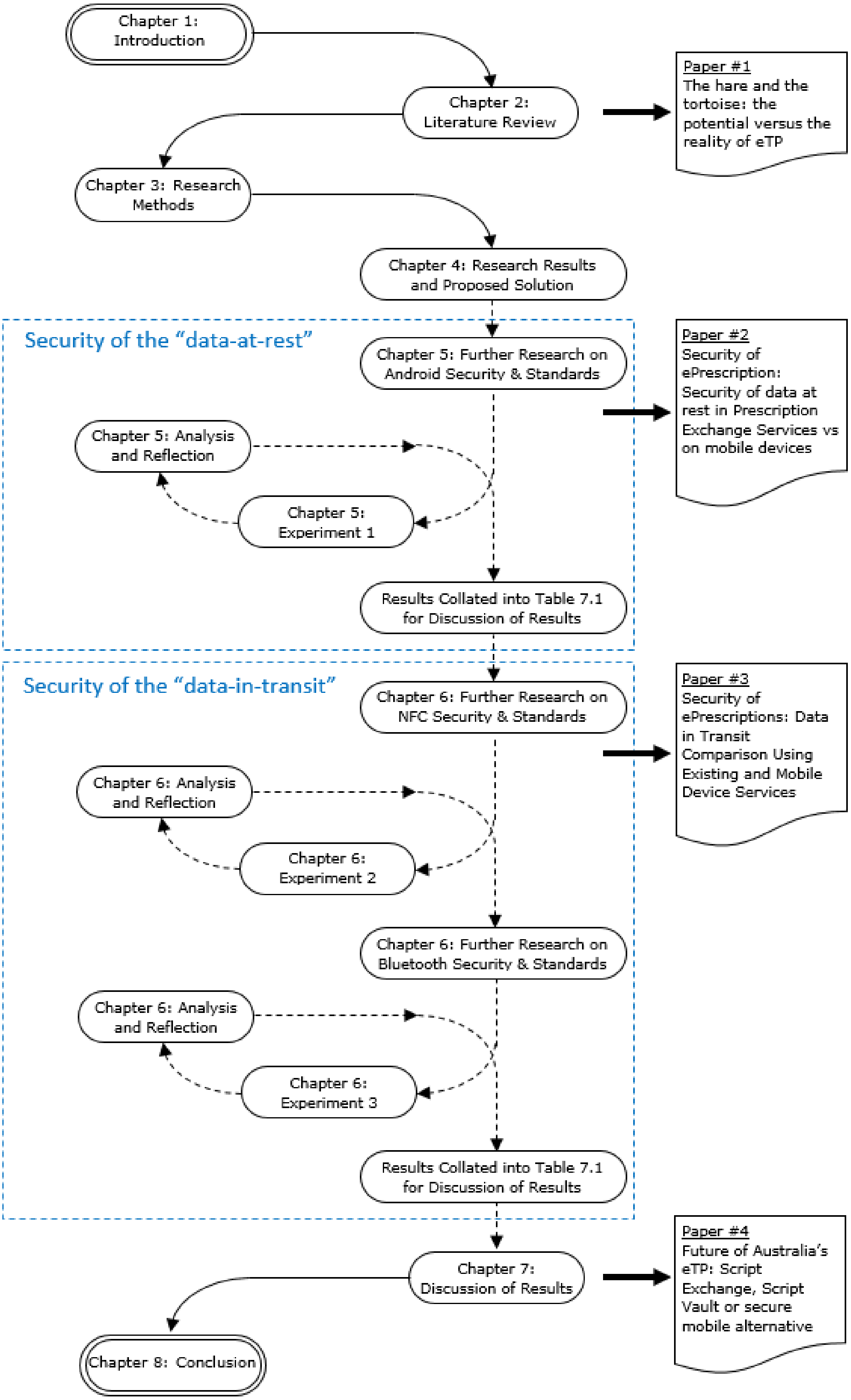

Chapter 1: Introduction
Chapter 2: Literature Review
Paper #1
The hare and the tortoise: the potential versus the reality of eTP
Chapter 3: Research Methods
Chapter 4: Research Results and Proposed Solution
Security of the "data-at-rest"
Chapter 5: Further Research on Android Security & Standards
Paper #2
Security of ePrescription: Security of data at rest in Prescription Exchange Services vs on mobile devices
Chapter 5: Analysis and Reflection
Chapter 5: Experiment 1
Results Collated into Table 7.1 for Discussion of Results
Security of the "data-in-transit"
Chapter 6: Further Research on NFC Security & Standards
Paper #3
Security of ePrescriptions: Data in Transit Comparison Using Existing and Mobile Device Services
Chapter 6: Analysis and Reflection
Chapter 6: Experiment 2
Chapter 6: Further Research on Bluetooth Security & Standards
Chapter 6: Analysis and Reflection
Chapter 6: Experiment 3
Results Collated into Table 7.1 for Discussion of Results
Chapter 7: Discussion of Results
Paper #4
Future of Australia's eTP: Script Exchange, Script Vault or secure mobile alternative
Chapter 8: Conclusion

Figure 1.4: Thesis structure reflecting the research activities and published papers

CHAPTER 2. LITERATURE REVIEW

2.1 Overview

The literature review explores the progression from the paper-based manual prescription process to the current implementation of the electronic prescription, with an emphasis on how it functions, its regulatory enablers and constraints at Commonwealth, state and territory levels and its limitations and issues as depicted in Figure 2.1.

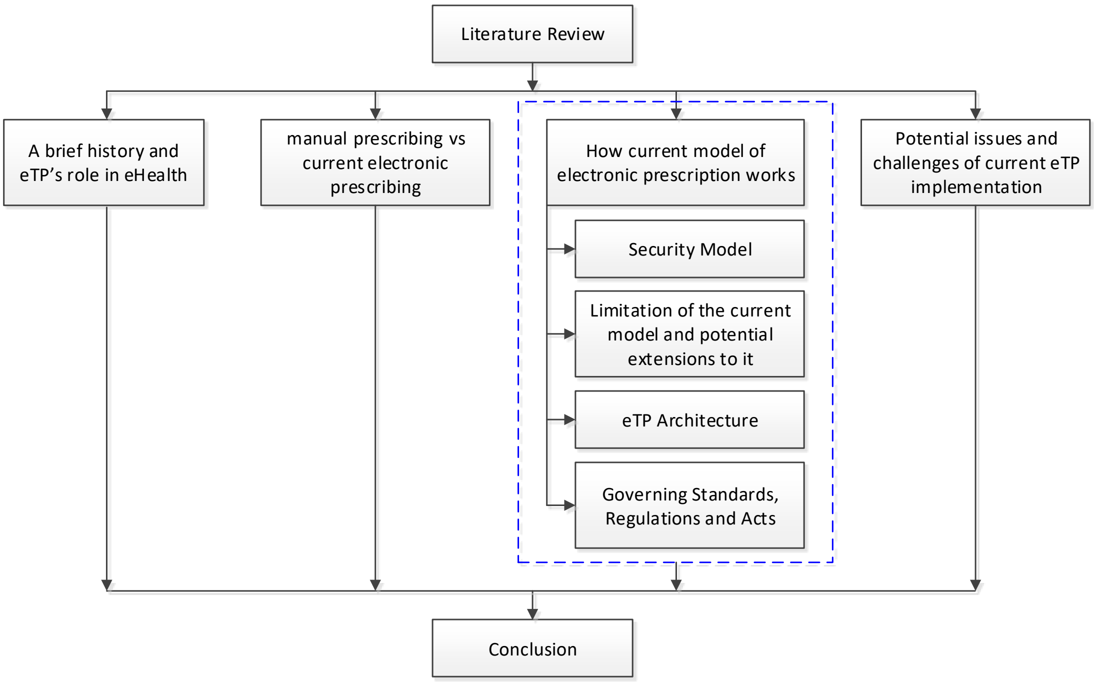

Literature Review
A brief history and eTP's role in eHealth
manual prescribing vs current electronic prescribing
How current model of electronic prescription works
Potential issues and challenges of current eTP implementation
Security Model
Limitation of the current model and potential extensions to it
eTP Architecture
Governing Standards, Regulations and Acts
Conclusion

Figure 2.1: Structure of ETP Literature Review

The literature review begins with the identification of the relevant acts, regulations, standards and specifications (such as Australian Technical Specification - ATS4888 series) governing ETP implementation in the Australian healthcare industry. The identification process commences at the Commonwealth level, gradually narrowing down to state and territory (jurisdictional) levels. Once the relevant Commonwealth and jurisdictional acts and regulations for ETP have been identified, a thorough analysis is conducted to document the security requirements mandated by those law and regulations. Further study is then conducted on the relevant standards and specifications governing the ETP implementation in order to document the security requirements imposed on the current ETP implementation.

These combined requirements define the minimal set of security measures for the Android mobile electronic prescription transfer application.

2.2 A brief history and ETP's role in eHealth

Although eHealth has many unique definitions from various perspectives, the World Health Organisation (WHO) defines it as the transfer of health resources and healthcare by electronic means ("eHealth", 2014). Despite its diverse definitions from various standpoints, eHealth's crucial involvement in improving the Australian healthcare system and making it a better maintainable system is irrefutable (Bennett, 2013). The National eHealth Transitioning Authority's (NEHTA) Electronic Medication Management (eMM) program is one of the first few critical phases in laying the foundation of eHealth for the Australian healthcare industry. The eMM program offers the promise of better healthcare services delivery via significant improvements in reduced medical errors (e.g. through the sharing of precise patient medication information between prescriber and dispenser), better compliance, time and cost savings and better drug safety ("AMA Position Statement", 2009; Ostergaard, 2011).

The eMM program primarily focuses on designing and developing eHealth specifications to improve medication-related outcomes through improving the quality and availability of medication-related healthcare information across the Australian health sector and supporting organisations in implementing these specifications. In fact, despite the significance of eHealth on eMM's agenda in recent years, improving medication management has been the objective of several national medicines policies, such as Quality Use of Medicines (QUM) and the APAC Guidelines (Ostergaard, 2011; "NEHTA Blueprint V2", 2011), for well over a decade.

In this eHealth journey, the implementation of ETP is the first step towards more efficient and effective medication management and it delivers several capabilities in realising the promise of eMM ("NEHTA Blueprint V2", 2011). In addition, since one of eMM's highest priority initiatives was to have the ETP process in place, an early opportunity was presented for connecting a significant group of healthcare providers (i.e. prescribers and dispensers) on a national scale (Ostergaard, 2011). With ETP in place, the client's/patient's medication information is accurately and securely shared, and a wide range of benefits are provided for all parties involved such as prescribers, dispensers and consumers ("AMA Position Statement", 2009; "NPS MedicineWise", 2012).

All of these benefits were made possible by the initial step taken in the prescription process: converting the conventional manual prescription process/model to a digital equivalent one. In Australia, the Commonwealth Government's Practice Incentive Program (PIP), introduced in the late 1990's to encourage desktop computing by General Practitioners (GPs), also contributed to the foundation which made this conversion a success. (Quinlan, 2000).

Developed countries around the world implemented their electronic prescribing systems depending on their acts, regulations and the various levels of healthcare infrastructure (i.e. government or private funded etc.). In United States of America, the electronic prescribing facilities are provided by various healthcare information exchange networks such as *Surescripts*, *RelayHealth*, *McKesson*, *ProviderPay*, *Truveris*, *AmerisourceBergen* and a few others. *Surescripts* is the dominant electronic prescription network used by the majority of all community pharmacies in the U.S (Gabriel and Swain, 2014) and similar to Australia's *Script Exchange*, half of the company is owned by the Pharmacy Associations (Moukheiber, 2014). Communication between the systems using different software, drug vocabularies and terminologies is mediated using *RxNorm*. *RxNorm* provides normalized names for clinical drugs and links them to the drug vocabularies commonly used in pharmacy management and drug interaction software (e.g. First Databank, Micromedex, Gold Standard Drug Database, and Multum) and terminology used in coding clinical drug properties sch as mechanism of action, physiologic effect, and therapeutic category ("RxNorm", 2018). Meanwhile, Canada's national e-prescribing service is called *PrescribeIT*™. At the national level, it enables prescribers to electronically transmit a prescription to a pharmacy of patient's choice ("PrescribeIT™", 2018). The programme is lead by *Canada Health Infoway*, a government funded not for profit organization, and offers three options to patients; *Directed*, *Deferred* and *Paper* ("Backgrounder", 2018). The "*Directed*" option securely delivers the electronic prescription directly to the pharmacy using the

PrescribeIT™ service if the patient has a pharmacy of choice at the time of prescribing. The "*Deferred*" option enables the prescriber to send the prescription electronically to the *PrescribeIT*™ service from which a pharmacy participating in *PrescribeIT*™ can retrieve it when the patient presents the prescription summary they have received from the prescriber. The "*Paper*" option allows the patient to request for paper prescriptions to be issued (*ibid*). In Spring 2018, *PrescribeIT*™ extended its functionalities to provide secure physician-pharmacy messaging, and to allow prescribers and pharmacists to create, receive, renew and cancel prescriptions ("PrescribeIT™", 2018). In Portugal, the Electronic Medication Prescription (PEM in Portugal), is a service implementing the electronic process of prescription, dispensing and reimbursement of ambulatory medication (Patrao, Deveza & Martins, 2013). It was developed by a Portuguese Government institution SPMS EPE with original intention of implementing additional safety and control in the medication circuit, as well as increases the potential to avoid fraud and to reduce costs. Access to prescription by pharmacy is authorized by the patient using the electronic personal/citizen identification card (i.e. with a chip) and prescription code. While prescriptions are integrated into the patient's electronic records within healthcare institutions and updated, it also allows access to chronic medicines, prescription history and alerts for interaction with allergies and adverse reactions registered on a nationwide electronic health records and conveyed to the national patient summary (*ibid*).

Despite all the differences in governing Laws and supporting infrastructures, all of these e-prescribing systems share the common objectives in improving the quality of the prescribing process (i.e. reduced fraud and abuse, and easier communication), increasing the safety of the patient (i.e. through greater accuracy with fewer errors and safer drug use with stronger medication compliance) and optimizing the health-related federal and territorial expenditures.

One critical aspect of electronic prescribing and eMM is how the prescription information and electronic health records are securely communicated between healthcare providers. Almost two decades ago, before the extensive use of smartphones, Chan (2000) proposed how to achieve a highly mobile health management framework by combining World Wide Web and smart card technologies. In this approach, using the SmartCard–Web Gateway Interface (SGI) as a common interface to communicate and access the medical records stored in a smart card, Chan (2000) demonstrated the feasibility of the concept in facilitating a truly mobile access of patient's medical records. After almost a decade later, Jürjens and Rumm (2008) proposed the use of model-based security analysis to address the risk associated with inherent vulnerabilities of such devices and the significant complexities of the architectures based on the study of the German Health Card. In their study, Jürjens and Rumm (2008) stated that the security analysis has to be embedded in the development and management of the systems.

2.3 Manual prescription vs current electronic prescription

Figure 2.2 demonstrates the conventional manual prescribing model with the prescriber writing on a pre-printed prescription pad. Once signed by the prescriber, the prescription is handed over to the patient/agent, who at later time will present it to the pharmacy. When the prescription is presented by the patient/agent at the pharmacy, the prescription details are transcribed into the pharmacy's Electronic Dispensing System (EDS) for dispensing. This collected and transcribed information is also used in subsequent processes such as Pharmaceutical Benefits Scheme (PBS) claiming and repeat dispensing processes. Before the dispensing occurs, the process mentioned above may include verification of the prescription details with the prescriber if any information is unclear or should the pharmacy have concerns about the validity of the prescription. This is usually carried out through a telephone call to the prescriber. However, this conventional model depicted in Figure 2.2 has numerous associated risks and vulnerabilities, including the loss of the prescription by the patient, transcription errors during the pharmacy data-entry process, illegible or misread script elements (especially with handwritten scripts) and fraudulent production or alteration of scripts.

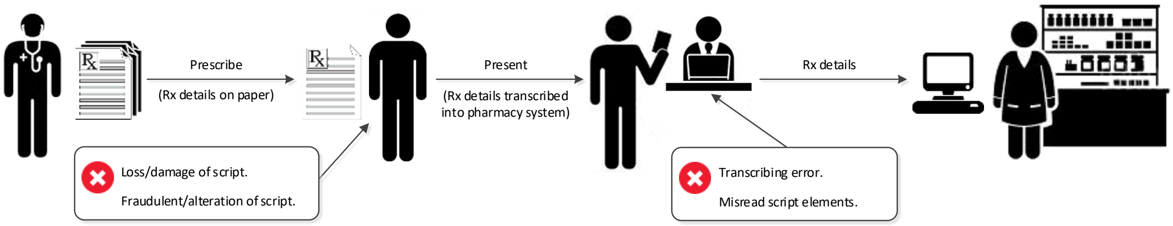


Figure 2.2: Manual prescribing process (Htat, Williams, & McCauley, 2015)

The current implementation of ETP addressed these issues by facilitating the electronic generation of a prescription by a prescriber, encryption of the generated electronic prescription using the prescriber's Commonwealth issued PKI certificates, its secure transmission to a dispenser along with the electronic authentication of the prescriber and dispenser access to the transmitted prescription using Commonwealth issued PKI certificates. Figure 2.3 describes the current electronic prescription model in Australia (Henderson, et al., 2014).

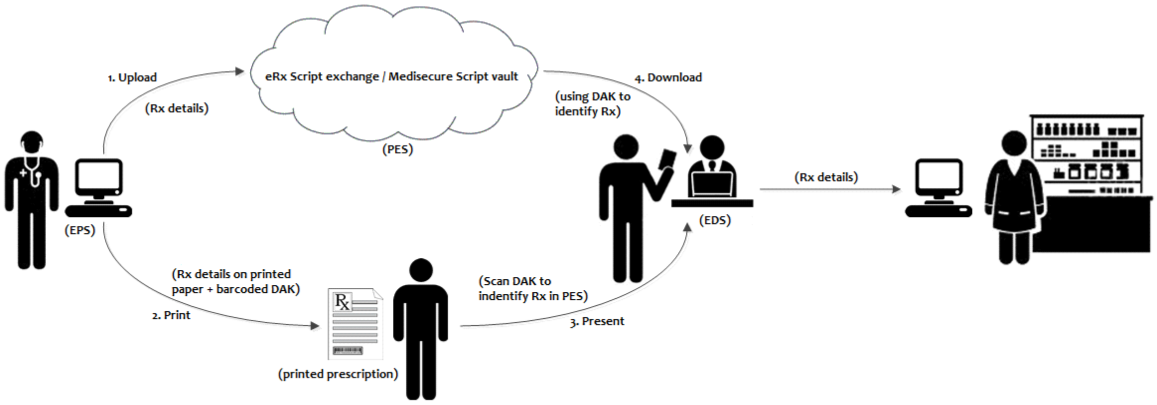

1. Upload
(Rx details)
eRx Script exchange / Medisecure Script vault
(PES)
4. Download
(using DAK to identify Rx)
(EPS)
(EDS)
(Rx details)
(Rx details on printed paper + barcoded DAK)
2. Print
(printed prescription)
(Scan DAK to indentify Rx in PES)
3. Present

Figure 2.3: Current electronic prescription transfer process (Htat, Williams, & McCauley, 2015)

This model makes use of the Prescription Exchange Service (PES), Electronic Prescribing System (EPS) and Electronic Dispensing System (EDS) as its fundamental components. The PES is an intermediary service which enables secure transmission of electronic prescription information between prescribers and dispensers ("ePrescriptions", 2012). It is mandatory for a PES system to meet the specified security and privacy standards approved by the Commonwealth ("Electronic Transfer of Prescriptions", 2016). To this day there are only two PES systems in Australia, *Script Exchange* from eRx and *Script Vault* from MediSecure ("Set up Electronic Transfer of Prescriptions", 2016). The EPS is a component of the prescriber's clinical software package for generating an electronic prescription, digitally signing it and finally uploading it to the PES ("ePrescriptions", 2012). The

EDS is another key component of pharmacy software which facilitates downloading the electronic prescription from the PES and submitting dispense records to the PES upon dispensing (“ePrescriptions”, 2012).

2.4 How current model of electronic prescription works

In this model, the EPS component of the prescriber’s clinical management software generates electronic copy of the prescription, encrypts it using the Public Key Infrastructure (PKI) certificate and then uploads it to one or both of the registered prescription exchange service (PES) whenever the prescriber prints a prescription (Standards Australia, 2013a).

Once uploaded, the prescription is stored securely on the PES to await download by the dispenser. In the meantime, the prescriber signs the prescription and hands it over to the patient/agent as per the manual prescription model. However, this printed prescription has one or more barcodes, depending on whether the prescriber is registered with one or both PES systems. Upon the patient/agent presenting the prescription, the pharmacy’s eTP-enabled pharmacy software scans the barcode on the prescription in order to download and decrypt the prescription details from the PES system. These downloaded prescription details provide the pharmacy’s EDS with the necessary information for dispensing and other subsequent operations such as PBS claiming and updating National Prescription and Dispense Repository (NPDR) (Standards Australia, 2013a).

Initially, prescriptions needed to be downloaded from the specific PES system to which the prescriber had uploaded it. This restriction not only imposed limitations on the prescription process but also added additional work load; having to register with both PES systems and upload the prescription to both systems upon prescribing. If this was not done and the pharmacy’s registered PES system was different to that of the prescriber, the prescription could not be downloaded (McDonald, 2012). This interoperability issue between the two PES systems not only disrupted the flow of the prescription process but also incurred a higher cost in delivering the service, costing eight-five cents (i.e. compared to thirty-five cents after achieving interoperability and later down to fifteen cents) in electronic prescription fees for each prescription downloaded from PES (*ibid*).

Furthermore, earlier studies on ETP revealed that despite the large number of prescriptions uploaded to PES by prescribers, the number of prescriptions being downloaded by dispensers was much lower. This was primarily due to the pharmacy at which the patient presents the prescription not being registered with the specific PES to which the prescription was uploaded by the prescriber (McDonald, 2012). The two PES systems became interoperable in December 2012 and the prescription process consequently became much more efficient, with prescribers able to upload to either PES system and dispensers to download from any PES system.

As part of this initiative for better interoperability between PES systems, the cost of downloading a prescription was reduced to fifteen cents per prescription. In addition to the interoperability, the two PES systems agreed to split the electronic prescription fees when a prescription was uploaded to one PES and downloaded or dispensed by the other (McDonald, 2012). At present, both PES systems are free of charge to prescribers (i.e. general practices and specialists etc.) and cost neutral to dispensers (i.e. pharmacies). There are no fees associated with registration or licensing for both prescribers and dispensers. However, whilst there is no transaction fee for prescribers for electronic prescriptions, pharmacies pay fifteen cents for each eligible transaction (i.e. an eligible prescription downloaded from PES). This fee has been offset as part of the two Community Pharmacy Agreements (CPA); 5th CPA for 1st July 2010 to 30th June 2015 and 6th CPA for 1st July 2015 to 30th June 2020 ("Electronic Transfer of Prescriptions (ETP)", 2013), which Agreements provide a mechanism by which the PES infrastructure is subsidised by the Commonwealth.

In the current prescription model, the printed prescription serves a dual purpose; firstly as a legal instrument when signed by the prescriber and secondly as a prescription notification slip (token) with one or more barcodes on it. In the current ETP system, each electronic copy of a prescription is identified by a set of alphanumeric characters that are unique in combination as mandated by the Section 6.2.2 of the ATS 4888.2-2013. This unique set of alphanumeric characters is called the Document Access Key (DAK). The barcode on the prescription is the printed representation of this unique DAK. As illustrated in Figure 2.3, when the pharmacy's eTP-enabled EDS scans this barcode from the printed prescription, the DAK enables the pharmacy software to download the prescription details from their PES system and decrypt it for dispensing and other secondary uses (Standards Australia, 2013a). This eliminates potential transcription errors, the need to verify prescription details with the prescriber and the ability to fraudulently alter prescriptions.

This electronic prescription model described in Figure 2.3 is, however, vulnerable to new potential issues such as incorrect medication code mapping between the prescriber's EPS and dispenser's EDS systems (e.g. the use of Pharmaceutical Benefits Scheme (PBS) coding, Australian Medicines Terminology (AMT) coding or other third-party product-specific coding systems), and other interoperability failures between the participating systems. After dispensing the medication, the EDS system provides a record of the dispensed medication to the PES (Standards Australia, 2013a). In the original implementation, upon receiving this dispensed record information the PES sent an automatic dispense notification back to the original prescriber. However, this automatic dispense notification service has been disabled at the request of the Royal Australian College of General Practitioners, due to potential implications for clinician duty of care (McDonald, 2013a).

In both PES systems the Cipher Key, a unique symmetric key generated using a one-way function from the DAK, is never disclosed to the PES operators so as to assure the security and privacy of confidential information such as patient and prescription details (Standards Australia, 2013a). NEHTA and Standards Australia released the first draft of ETP technical specifications in December 2010, ETP version 1.1 ("Electronic Transfer of Prescriptions v1.1", 2010). The *Script Exchange* from *eRx*, however, had been running live across Australia for seven months when this technical specification was released. *Script Exchange*, eRx's implementation of PES was therefore built using XML and Web Services technology based on the international and Australian standards ("ETP Standards", 2016). On the other hand, MediSecure's *Script Vault* was implemented in compliance with the HL7 Standards as set out in the Australian Technical Standards (ATS) 4888 series and has undergone the compliance audit process ("Frequently Asked Questions", 2015).

2.4.1 Security model

The security of electronic prescriptions on PES systems is primarily governed by the Australian Technical Specification (ATS) 4888 series, with 4888.2-2013 particularly emphasising the platform independent model. The security mechanism in ETP from a data at rest perspective revolves around the use of the Document Access Key (DAK), which is presented as a barcode on the paper prescription produced by any eTP-enabled electronic prescribing system (Standards Australia, 2013a).

In the current ETP implementation using PES systems, the DAK is used for encrypting the electronic prescription prior to uploading to the PES system, authorising access to the prescription stored on the PES system and decrypting it when downloaded from the PES system. In fact, the DAK is the primary pillar on which the entire ETP security model is built (*ibid*). Section 5.3 of ATS 4888.2-2013 provides an overview of the security mechanism using the DAK for securing the electronic prescription (i.e. in the form of Secured Clinical Documents) in the current ETP implementation and Figure 2.4 illustrates this operating mechanism.

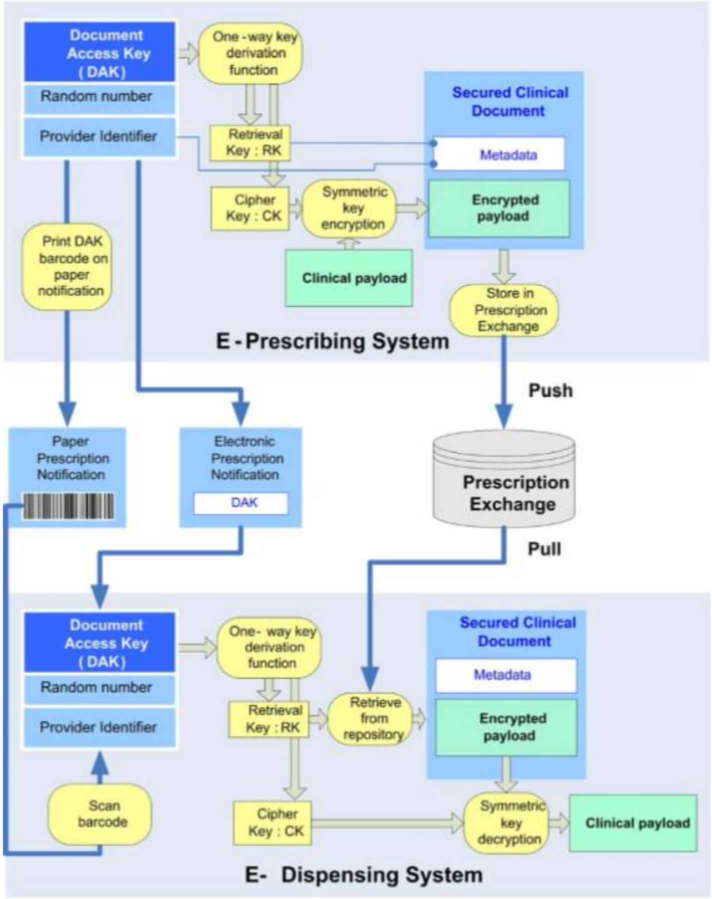


Figure 2.4: DAK usage for storage and retrieval of prescription with PES (Standards Australia, 2013a, Figure 19)

The DAK is the parent key from which all other keys such as Retrieval Key (RK), Cipher Key and DAK Holder Proof Key are derived using a published algorithm. Each DAK contains a Provider ID which uniquely identifies the operator/provider of the PES system and an entropic random value from which all other keys are derived. The RK is a random value which references a specific Secured Clinical Document (i.e. a prescription) from the PES system once it has been qualified with the Provider ID, hence it is called Qualified RK (Standards Australia, 2013a).

Because the DAK's random value has sufficient entropy, it is impractical for a party to have knowledge about it unless it is explicitly disclosed to that. Possession of a Qualified RK derived from the DAK therefore acts as a bearer's credential and thus grants the holder the right to retrieve the Secured Clinical Documents associated with that specific Qualified RK (*ibid*).

The Cipher Key is a unique symmetric key generated using a one-way function from the DAK and is used in encrypting and decrypting the payload/content of the Secured Clinical Document (i.e. the prescription). This encryption of the prescription by the electronic prescribing system is evident in Figure 2.4 prior to pushing/uploading it to the PES system. This Cipher Key is never disclosed to the PES operators, ensuring that the content of the Secured Clinical Document is not accessible and thereby keeping secure the individual's private-information. This process also eliminates the need to gain the consent of the prescription subject (i.e. patient) to PES operators having access to their private information (*ibid*).

The DAK Holder Proof Key is another important key derived from the DAK using a one-way function and is used by a dispensing pharmacy to prove to the PES system that it holds a DAK. Figure 2.5 shows the various data types portraying the implementation independent characteristics of a DAK (*ibid*).

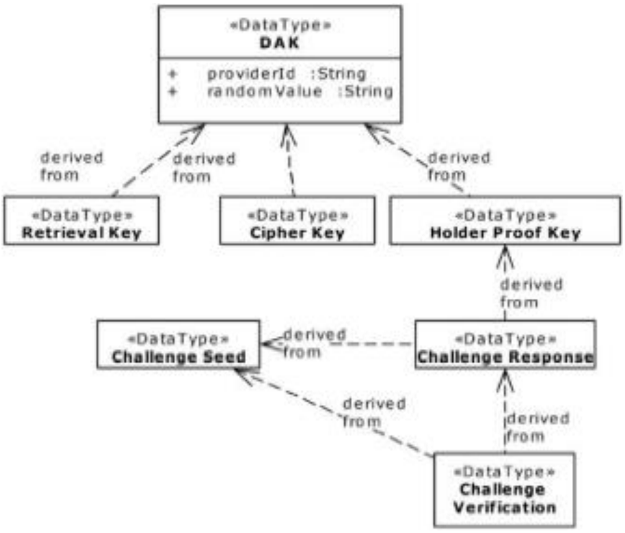


Figure 2.5: DAK and its constituent data types (Standards Australia, 2013a, Figure 21)

To ensure the security of electronic prescriptions stored in PES system, each of DAK's mandated characteristics is accompanied by a list of security conformance points. The security mechanism from the data at rest perspective makes use of the DAK for encryption mechanisms within the PES system. Storing the DAK or its derived Cipher Key on any stable storage (i.e. a permanent storage) requires a minimum of 128 bits encryption. In addition to this, derivation of any Cipher Key, Retrieval Key or DAK Holder Proof Key from a DAK by any system is strictly prohibited unless the user of that system is authorised to access the prescription subject's information from the Secured Clinical Document (i.e. the prescription) associated with that particular DAK (*ibid*).

The specification ATS 4888.2-2013 also prohibits sharing of a DAK Holder Proof Key as well as storing it in any non-transient recoverable form. Figure 2.6 depicts the structure and data types of an electronic prescription; the crucial piece of information upon which the entire ETP system is built (*ibid*).

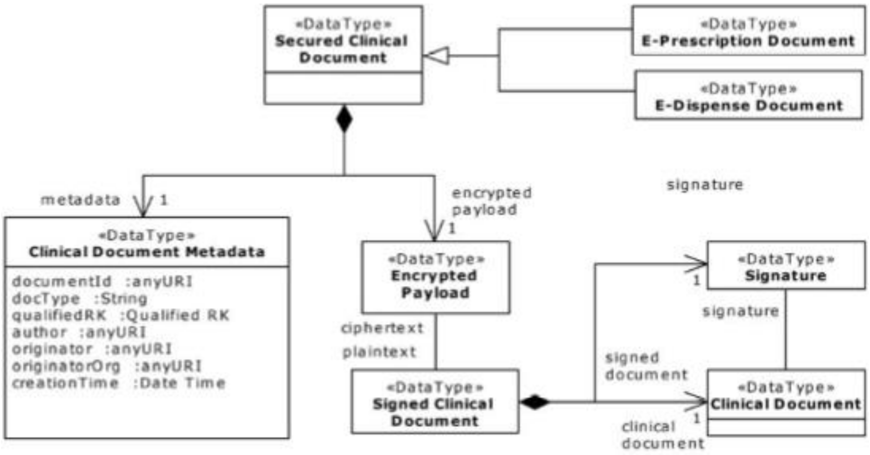


Figure 2.6: Electronic prescription and its constituent data types (Standards Australia, 2013a, Figure 23)

Despite being a platform specific implementation for web services, the technical specification ATS 4888.6-2013, section 3.4, outlines how the Secured Clinical Document is to be encrypted and decrypted for ETP or eHealth in general.

The way in which a Secured Clinical Document is created has no direct impact on the security of electronic prescriptions on the PES from a data at rest perspective. However, due to both the document type resulting from and the actions required during this creation process it is crucial in determining whether the use of mobile devices for transferring electronic prescription is achievable. The technical specification ATS 4888.6-2013 mentions that the Secured Clinical Document is a Signed Clinical Document encoded as Base64 binary data within the Message Payload element in compliance with clause 7.3.1 of the specification ATS 5822-2010. In turn, the Signed Clinical Document is indeed an IHE's Cross-Enterprise Document Media Interchange (XDM) representation of an HL7 CDA form as defined in the specification ATS 4888.3-2013 (Standards Australia, 2013b; Standards Australia, 2013c).

In summary, the security and integrity of prescription information within the PES system from the data at rest perspective is governed by a set of specifications and standards such as ATS 4888.2-2013, HL7 CDA and IHE, while facilitating the national transition towards eHealth. On the other hand, the specification states that the security of electronic prescription from the data in transit aspect is specific to the implementation platform (Standards Australia, 2013a). This research found that the security of the data in transit between ETP participants (i.e. Prescriber, Prescription Subject, Prescription Exchange and Dispenser) relies principally on the encryption mechanism of the specific implementation platform (*ibid*).

2.4.2 Limitation of the current model and potential extensions to it

The primary limitation of the current ETP model in our progress towards more effective medication management is the availability of the patient's medication history. Despite the existence of the National Prescription and Dispense Repository (NPDR), availability of patients' medication history is limited and generally acknowledged to be an issue for healthcare professionals. Moreover, the medication information stored in NPDR has varying levels of clinical value and usefulness since not all the information stored in NPDR is coded as per the Australian Medication Terminology (AMT) coding system. Depending on where the information was collected/submitted (i.e. the source of information), the medication information stored in NPDR can be in image form, uncoded text or coded text using medication coding systems other than AMT. The AMT system delivers unique codes to unambiguously identify trade products and medicines approved for use in Australia (McDonald, 2014; "Australian Medicine Terminology", 2016).

In response to this, as a second step towards more effective medication management, pharmacy software vendor FRED IT rolled out the first phase of MedView Medicines Workspace during the later stages of the Northern Queensland trial for the opt-out model of the My Health record (MyHR). This is a secured web application to enable doctors, pharmacists, hospitals and patients to have shared access to a patient's critical medicines information in a summary form (McDonald, 2016a, 2016b). The following figure, Figure 2.7, depicts the various sources from which MedView will retrieve medication information in order to compile a consolidated list of a patient's medication history. Because it is still in early trial stage, its practical usefulness and benefits to the healthcare industry are yet to be witnessed.

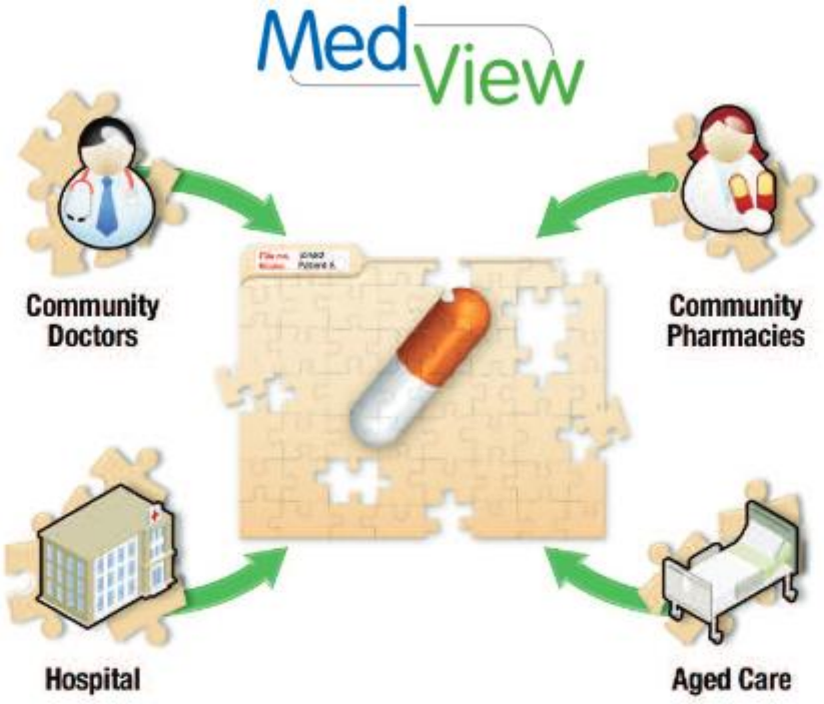


Figure 2.7: MedView for consolidated patient's medication history ("MedView and eRx", 2012)

Another area yet to be explored to improve healthcare services is mobile health or mHealth ("M-HEALTH", n.d.). Along with both hardware and software advancements in mobile technologies, the term "going mobile" is a recent trend in digital transformation, affecting many industries such as retail, social networking, banking and the legal industry. This even includes such highly regulated fields as the public healthcare sector. The first instance of this assimilation into Australian healthcare is the child health extension of the Commonwealth's Personally Controlled Electronic Health Records (PCEHR), which allows parents to enter information such as immunisations, growth parameters and developmental milestones for children up to the age of 14 years (McDonald, 2013b).

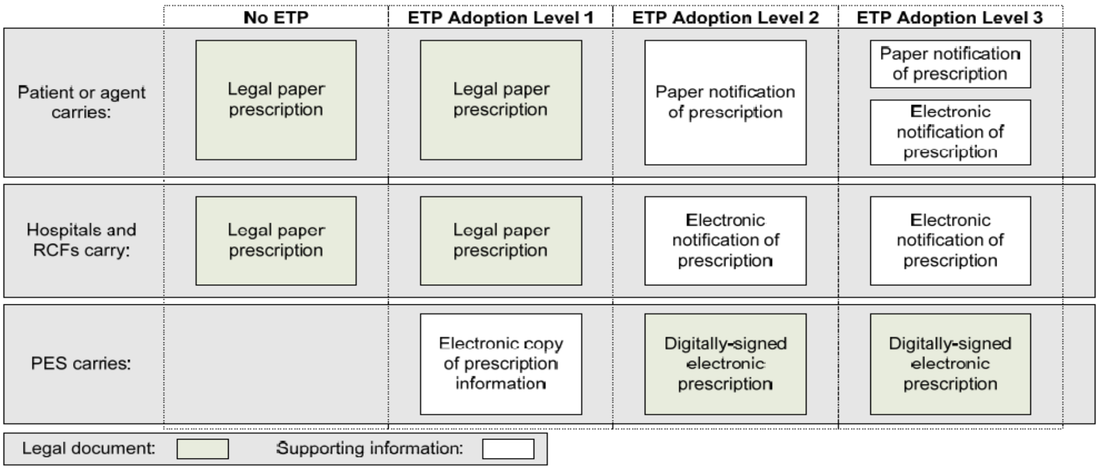
In the pursuit of better medication management, the mobile health option was explored. As a result, a mobile application called *eRx Express* was released by eRx in 2014 to enhance the current electronic prescription process model described in

Figure 2.3. It enabled patients to scan the DAK barcode from the prescription to their mobile phone and securely submit it to their choice of pharmacy for a scheduled pickup at later time (“Express Scripts”, n.d.). However, this application still requires the printed prescription notification from which the DAK barcode was scanned before being transmitted to a specific pharmacy. As a result, the prescriber’s signature on the printed prescription is still mandatory as it is mandated by relevant acts/regulations in each state and territory (e.g. Poison Regulation 1965 Regulation 51 (1B) in Western Australia). This requirement will only be replaced once the use of digitally signed electronic prescriptions has legislative approval.

2.4.3 eTP Architecture

Over the past a few years, the healthcare industries in developed countries have witnessed a significant increase in adopting electronic prescribing systems (Monegain, 2013). The majority of these ETP adoptions were initially led by the Government to improve the quality of healthcare and reduce Adverse Drug Events (ADEs), while significantly reducing long-term costs via better prevention of ADEs and readmissions (Reeve & Sweidan, 2011; Roughead, Semple & Rosenfeld, 2013). However, once eHealth components are in place, even if partially operational, the improved healthcare infrastructure, such as electronic healthcare records, will increase the demand for electronic prescribing systems and unlock massive potential for future growth. The level of ETP adoption in various countries, states and jurisdictions varies based on diverse interpretations and implementations of data protection as well as confidentiality laws, availability of required infrastructure and resistance to embrace the change by the stakeholders at various levels (Jolly, 2011).

Figure 2.8 depicts the levels of ETP adoption, the extent to which ETP is implemented, its influence on the information workflow and the form in which the information is communicated (Gregory, 2013). Despite being a key government initiative to improve the delivery and quality of healthcare, the level of ETP adoption varies across the different sectors of the healthcare industry such as primary care clinics, aged care facilities and hospitals.



	No ETP	ETP Adoption Level 1	ETP Adoption Level 2	ETP Adoption Level 3
Patient or agent carries:	Legal paper prescription	Legal paper prescription	Paper notification of prescription	Paper notification of prescription Electronic notification of prescription
Hospitals and RCFs carry:	Legal paper prescription	Legal paper prescription	Electronic notification of prescription	Electronic notification of prescription
PES carries:		Electronic copy of prescription information	Digitally-signed electronic prescription	Digitally-signed electronic prescription

Legal document: 🟩 Supporting information: □

Figure 2.8: Level of ETP adoption (Gregory, 2013)

According to Figure 2.8, the printed prescription is both the legal prescription for dispensing and the transfer medium for delivering the DAK identifier to the dispenser in Level 1 ETP adoption. Having the prescription details printed with the DAK benefits the patient because the printed prescription details may be used for dispensing if the pharmacy's EDS system is not eTP-enabled or access to PES is not available (Gregory, 2013; "Electronic Transfer of Prescriptions", 2016). However, this requires the prescriber's handwritten signature on the printed prescription as mandated by the s. 51(1B) of the Poisons Regulations 1965 in WA and similar legislation in other states.

On the other hand, using a data storage device as the transfer media for the electronic prescription rather than the printed paper version eliminates the requirement for the prescriber's written signature, as this is exempted by the s. 51 (1A) and s. 51(1C) of the WA's Poisons Regulations 1965 and s. 9(1) and s. 9(3) of the Commonwealth's Electronic Transaction Acts 1999.

In Level 2 ETP adoption, represented in Figure 2.8, the printed prescription notification is used as a transfer medium for delivering the identifying DAK to the dispenser. The printed prescription notification also contains the same prescription details as the electronic prescription thereby facilitating dispensing if access to PES system is not available (Gregory, 2013; "Electronic Transfer of Prescriptions", 2016). Nonetheless, due to this potential alternative use, the same principles and restrictions apply to the prescriber's handwritten signature as in Level 1 ETP adoption.

In the current electronic prescription transfer process, upon receiving the printed prescription or the prescription notification submitted by the patient/agent, the pharmacy's eTP-enabled EDS system downloads the prescription details from the PES system using the DAK. Finally, the Level 3 ETP adoption replaces the paper notification with a fully-electronic notification thereby eliminating the requirement for handwritten signature by the prescriber (Gregory, 2013).

However, since the digitally-signed electronic prescription is the legal document in both level 2 and 3 of the ETP adoption, legislative approval for the use of digitally signed electronic prescription is necessary. According to Figure 2.8, the current implementation of ETP in Australian healthcare can be categorised as between level 1 and 2 because, despite having the ability to use the electronic prescription notifications in certain sectors of the healthcare industry, the printed paper prescription remains the legal document and the legislative approval for the use of digitally signed electronic prescription is yet to occur.

2.4.4 Governing Standards, Regulations and Acts

In order to remove the legislative barriers to the electronic communication of health information and the consequent facilitation of an improved healthcare system, numerous standards have been adopted and/or developed by various national programs and authority bodies over the past decade, with the Commonwealth and state governments repealing and/or amending acts and regulations for the same purpose. The Australian Commonwealth government, for instance, has removed Commonwealth legislative barriers to electronic prescribing and dispensing of PBS medicine by implementing changes to the National Health (Pharmaceutical Benefits) Amendment Regulations 2006.

However, state and territory legislative barriers remain unchanged despite being identified for necessary changes. Alignment with Commonwealth amendments is occurring slowly and this will provide rules for electronic prescribing and dispensing in the respective jurisdictions. The following table briefly lists the Commonwealth, state and territory acts and regulations which have been repealed and amended to accommodate the implementation of ETP for Australian healthcare.

Table 2.1: Commonwealth, State and Territory Acts enabling ETP implementation

Jurisdiction	**Acts/Regulation**
Commonwealth	Electronic Transactions Act 1999
Commonwealth	National Health Act 1953; National Health (Pharmaceutical Benefits) Regulations 1960
NSW	Poisons and Therapeutic Goods Regulation 2008
VIC	Drugs, Poisons and Controlled Substances Regulations 2006
QLD	Health (Drugs and Poisons) Regulation 1996
WA	Poisons Act 1964; Poisons Regulations 1965
SA	Controlled substances Act 1984; Controlled substances (Poisons) Regulations 2011
TAS	Poisons Act 1971; Poisons Regulations 2008
ACT	Medicines, Poisons and Therapeutic Goods Act 2008; Medicines, Poisons and Therapeutic Goods Regulations 2008
NT	Medicines, Poisons and Therapeutic Goods Act 2012

Table 2.1 lists the acts and regulations which govern the implementation of ETP at Commonwealth, state and territory levels. Figure 2.9 shows how these governing acts and regulations fit together at Commonwealth, state and territory levels in order to accommodate current nationwide ETP implementation. Figure 2.9 also demonstrates the relationship between legislation and regulations in Australia, along with the complexity of this construction for eTP.

The outermost circle represents the encompassing regulation for the entire nation. The next inner circle defines the regulations for each state and territory amended as per jurisdictional legislative requirements. These two circles enable the use of electronic transactions at national, state and territory levels, making the use of ETP and other electronic transactions possible. The third circle lists acts and regulations governing the poisons and therapeutic goods for each jurisdiction, which play a key role in enabling the use of ETP system. The centre circle contains various standards and specifications developed in compliance with those national and jurisdictional legislative requirements. Because the closer the circle to the centre of the diagram the more ETP specific it becomes, this diagram is named “Dante’s 4 circles of eTP”; its concept analogous to 14th century poet Dante Alighieri’s Nine

Circles of Hell from Divine Comedy, where the lower circles are for more severe sins.

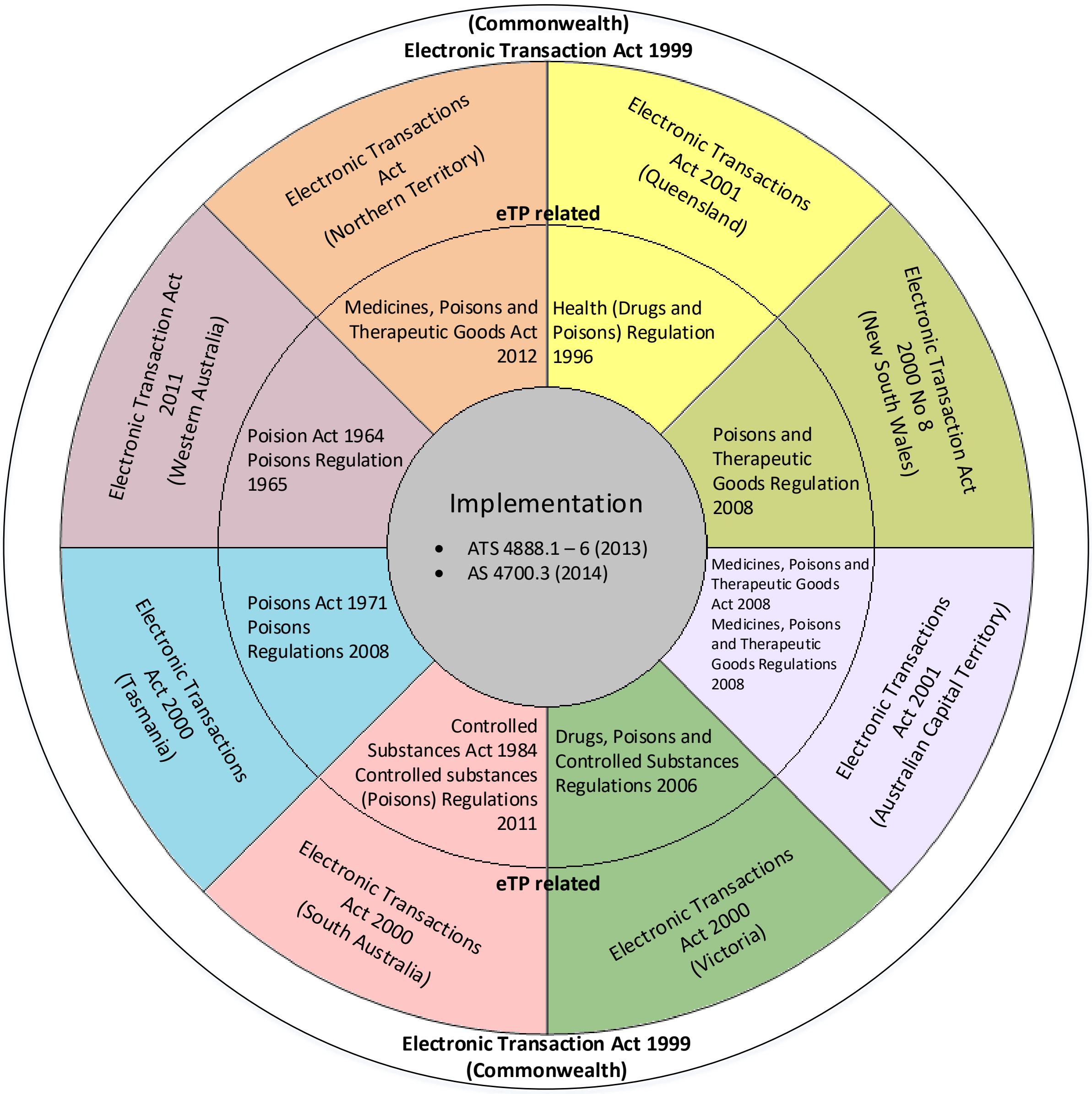

(Commonwealth)
Electronic Transaction Act 1999
Electronic Transactions Act (Northern Territory)
Electronic Transactions Act 2001 (Queensland)
eTP related
Medicines, Poisons and Therapeutic Goods Act 2012
Health (Drugs and Poisons) Regulation 1996
Electronic Transaction Act 2011 (Western Australia)
Electronic Transaction Act 2000 No 8 (New South Wales)
Poision Act 1964 Poisons Regulation 1965
Poisons and Therapeutic Goods Regulation 2008
Implementation
• ATS 4888.1 – 6 (2013)
• AS 4700.3 (2014)
Medicines, Poisons and Therapeutic Goods Act 2008 Medicines, Poisons and Therapeutic Goods Regulations 2008
Poisons Act 1971 Poisons Regulations 2008
Electronic Transactions Act 2000 (Tasmania)
Electronic Transactions Act 2001 (Australian Capital Territory)
Controlled Substances Act 1984 Controlled substances (Poisons) Regulations 2011
Drugs, Poisons and Controlled Substances Regulations 2006
eTP related
Electronic Transactions Act 2000 (South Australia)
Electronic Transactions Act 2000 (Victoria)
Electronic Transaction Act 1999
(Commonwealth)

Figure 2.9: Dante's 4 circles of eTP

The *Electronic Transaction Act 1999* (Commonwealth) facilitates the use of electronic means and enables the use of electronic communications in dealings with government, business and community for future economic and social prosperity of Australia. Various states and territories amended and adopted this overarching act according to their jurisdictional legislative requirements. These jurisdictional Electronic Transaction Acts, along with various acts and regulations governing the poisons and therapeutic goods for each jurisdiction, dictate the requirements for ETP implementation in that jurisdiction. Additionally, various standards and specifications have been developed reflecting those requirements. The ATS4888 series and AS4700.3, which primarily govern the implementation of eTP, are examples of those standards and specifications. Table 2.2 briefly describes the constituent standards and specifications in Figure 2.9, Dante's 4 circles of eTP, and their usages and applications in ETP implementation.

Table 2.2: Standards and specifications governing the ETP implementation

Standards/Specification	Usages/Applications in implementing eTP
ATS 4888.1-2013 Electronic transfer of prescriptions - Platform independent (logical) information model to support electronic transfer of prescriptions	Specifies the essential clinical data groups and elements required in an e-prescription exchange for prescriptions that are generated by registered medical practitioners and dispensed by pharmacists, and the constraints that should be applied. In addition to specifying the requirements it also identifies how the data elements of a typical printed prescription are recorded in the structure of an e-prescription.
ATS 4888.2-2013 Electronic transfer of prescriptions - Platform independent (logical) services model to support electronic transfer of prescriptions	Describes a technology platform independent model which describes the constituent primary functionalities, processes and their interactions. Implementing those functions allows conceptualizing and synthesizing of a new model using mobile storage devices.
ATS 4888.3-2013 Electronic transfer of prescriptions - Platform implementation specific e-prescription HL7 Clinical Document Architecture implementation guide	Defines the representation of a prescription using HL7 Clinical Document Architecture (CDA) Release 2 for the electronic exchange of e-prescriptions between healthcare providers as per Electronic Transfer of Prescriptions (eTP) Specification. This document guides implementers step by step through mapping each data component of ATS 4888.1 to a corresponding CDA attribute or element and specifies the descriptions of constraints on the CDA and custom extensions to the CDA in order to fulfil the requirements for Australian implementations of an electronic prescription (e-prescription). It also contains conformance requirements against which implementers can attest the compliance of their systems.
ATS 4888.4-2013 Electronic transfer of prescriptions - Platform implementation specific dispense record HL7 Clinical Document Architecture	Describes the Dispense Record for Electronic Transfer of Prescriptions (eTP). Dispense Record is primarily used in current ETP specification for updating the Dispensing State, issuing Dispense Notifications to the prescriber and sending the dispense information to the National Prescription and Dispense Repository (NPDR).

Standards/Specification	Usages/Applications in implementing eTP
implementation guide	
ATS 4888.5-2013 Electronic transfer of prescriptions - Platform implementation specific prescription request HL7 Clinical Document Architecture implementation guide	Describes the Prescription Request Electronic Transfer of Prescriptions (eTP). This would primarily be used by a dispenser for requesting a formal prescription to legitimate the dispensing of therapeutic goods following an instruction from a prescriber to supply a therapeutic good without a prescription.
ATS 4888.6-2013 Electronic transfer of prescriptions - Platform implementation specific web service	Defines a platform-dependent technical services specification for an Electronic Transfer of Prescriptions (ETP) package using web services. It defines the roles, behaviours and service interfaces for the implementation of an interoperable E-prescribing, E-dispensing, Prescription Exchange, Facility Based Supply Manager and Last Supply Notification Agent system. Compliance with ATS 4888.2 (i.e. platform independent Specification) is implied by conformance with this Technical Specification.
AS 4700.3-2014 Implementation of Health Level Seven (HL7) Version 2.5 - Electronic messages for exchange of information on medicines prescription	It is based on AS 4700.3-2005 and supersedes AS 4700.3(Int)-2007. It covers the implementation of the Health Level Seven (HL7) Version 2.5 protocol for communication between prescribers, dispensers and their healthcare trading partners in Australia and is an alternative approach to the use of HL7 Clinical Document Architecture Release 2 (CDA) as described in ATS 4888.x. The Standards Australia Working Group IT-014-06-04, Prescription Messaging, has reviewed and interpreted data segments and data elements as either mandatory, conditional or optional, and provided relevant usage notes in the Australian health environment.

In addition to these standards and specifications listed in Table 2.2, the following standards and technical specifications listed in Table 2.3 may also be useful to support and govern various aspects of ETP implementation in the Australian healthcare industry.

Table 2.3: Additional standards and specifications governing the ETP implementation

Standards/Specification	Usages/Applications in implementing eTP
AS 5550-2013 E-health web services profiles	Specifies a Standard for interconnectivity between implementations using Web services toolkits. Three profiles are specified - a base Web services profile, and profiles for securing Web services using either TLS or WS-Security. These can be used to secure Web services using existing toolkits instead of bespoke approaches.

Standards/Specification	Usages/Applications in implementing eTP
AS 5551-2013 E-health XML secured payload profiles	Describes a standard method for securing an XML document and defines mechanisms for representing signed and/or encrypted XML fragments using digital signatures, cryptographic encryption, or a combination of these at multiple levels as required. Unlike theW3C recommended XML structure where the signature and encryption contains optional and implementation defined/specific features, this standard only defines four XML elements for representing secured XML fragments. One or more of these XML elements can be used to secure the data as long as they are in XML fragments and the signature and the XML fragment being signed, or the encryption keys and cipher text, are represented together in the same XML document.
AS 5552-2013 E-health secure message delivery	This standard defines an interoperable mechanism, a set of roles and their associated interfaces and behaviour, for clinical messaging between software systems at two distinct organizations over the Internet using the industry-standard Web services protocols. Clinical messaging requires a network infrastructure, broad interconnectivity, end-to-end privacy and assurance of delivery. Organisations which cannot rely on significant infrastructure or technology expertise within the organization are accommodated by the standard interfaces that cater for hosted services while retaining end-to-end privacy and delivery assurance. Key constraints/characteristics are (a) its only intended for use for transmission of message payloads from an identified sender organization to an identified receiver organization (b) Does not constrain the message payload content. Only the control and routing information necessary for transmission in a safe and secure manner is defined (c) Business processes or business services are not included. Only the externally visible behaviour necessary to implement interconnected messaging is defined.
ATS 5546-2013 E-health endpoint location service	Provides a scalable and easily maintainable discovery mechanism for an information sender to dynamically locate a relevant known target recipient in the national e-health environment where communications between different healthcare organizations is facilitated through the use of various kinds of service invocation. This document defines the technical service specification for the Endpoint Location Service (ELS) and contains the requisite data types, interfaces and their behaviours for unambiguous operation between clients and service providers. It also provides the sender with technical information required to invoke the instance.
HB 308 2011 Location of digital signatures in	Despite not being a comprehensive guide to the security concerns of digital signatures, it proposes a method for creating and storing digital signatures in HL7 V2 messages that meet Medicare Australia (MA)

Standards/Specification	Usages/Applications in implementing eTP
HL7 V2 Messages	requirements for a healthcare sector electronic transaction. It enables paperless digitally signed documents to be implemented in place of physically signed paper documents.

The Standards and Technical Specifications listed in both Table 2.2 and Table 2.3 are neither complete nor comprehensive as only those relevant to this research are shown. Also listed, however, are the applicable standards and specifications; for the future implementation of digital signature usage in electronic prescriptions, for instance, or for a different implementation such as replacing the simple Subscriber-Provider architecture used in current ETP systems with Endpoint Location Services (ELS). Their applicability varies depending on both the design and the architecture of their implementation such as development of a web service or a client-server application.

Whilst Table 2.2 and Table 2.3 list the relevant eHealth standards for implementation of ETP and secure communication for healthcare information, as well as the clinical documents in general, the Figure 2.10 depicts how some of these eHealth standards fit together with other existing industrial standards from various areas such as Extensible Mark-up Language (XML), Web services, cryptography and communication protocols. While Figure 2.9 focused on the Acts and Regulations specific to ETP implementation, Figure 2.10 emphasises how eHealth standards and specifications sit within the existing industrial standards and protocols from a more generic perspective of communicating healthcare information securely. Figure 2.10 was constructed by studying the relationship and dependencies between AS5550-2013, AS5551-2013, ATS5546-2013 and AS5552-2013.

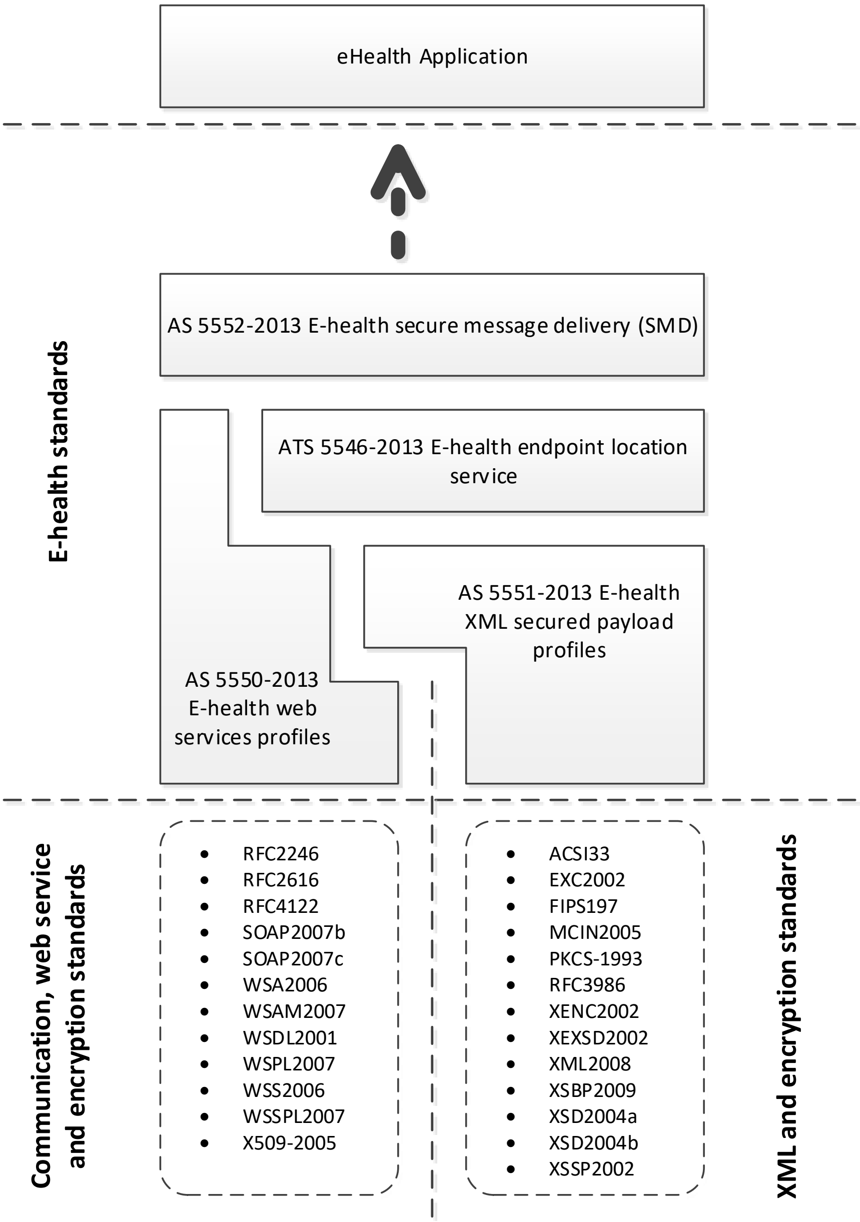

eHealth Application
AS 5552-2013 E-health secure message delivery (SMD)
ATS 5546-2013 E-health endpoint location service
AS 5551-2013 E-health XML secured payload profiles
AS 5550-2013 E-health web services profiles
E-health standards
Communication, web service and encryption standards
XML and encryption standards
RFC2246
RFC2616
RFC4122
SOAP2007b
SOAP2007c
WSA2006
WSAM2007
WSDL2001
WSPL2007
WSS2006
WSSPL2007
X509-2005
ACSI33
EXC2002
FIPS197
MCIN2005
PKCS-1993
RFC3986
XENC2002
XEXSD2002
XML2008
XSBP2009
XSD2004a
XSD2004b
XSSP2002

Figure 2.10: eHealth standards and industrial standards

2.5 Potential issues and challenges of current ETP implementation

Current ETP implementation using PES has enabled us to progress forward according to the national strategy for improving Australian healthcare system outcomes in a sustainable manner. However, the current implementation is not without significant issues.

Current ETP implementation requires a supporting infrastructure and involves an ongoing cost. Due to this dependency on the supporting infrastructure (i.e. the Internet connection), current ETP implementation is not suitable for remote regions of Australia where network availability is limited or unreliable. Moreover, the associated ongoing fee of fifteen cents for each prescription downloaded, whilst negligible for an individual prescription, represents a substantial amount nationwide and will have a significant impact on the nation's healthcare expenditure in the long run.

The announcement by eRx in August 2015 regarding the dispense of their first billionth electronic prescription indicated that this approach had cost the nation at least $150 million at that point in time (McDonald, 2015). When combined with the figures of the only other PES service in Australia, the total electronic prescription fees incurred so far was significantly more. According to eRx's survey outcomes, eRx is currently dispensing approximately 22.5 million electronic prescriptions each month, resulting in AU$3.3 million dollars for electronic prescription fees alone ("One billion eRx electronic scripts", 2016).

Predictably, an annual increase of at least five percent in the number of PBS prescriptions is shown in Figure 1.1. This increase will eventually lead to an increase in cost over time while making use of the current PES implementation, and this cost will continue to rise significantly over time unless a more cost-effective alternative approach is implemented.

Another challenge with the current PES infrastructure is the availability of the patient's medication history (Productivity Commission, 2015; "MedView Medicines Workspace", 2016). Since the medication information stored in the NPDR is not coded according to the AMT coding protocols, it has varying levels of clinical value and usefulness for the healthcare professionals (McDonald, 2014). In fact, this shortcoming resulted from another issue which was the failure to adhere to a single, consistent coding system (*ibid*). The Jurisdictions require that the AMT coding be used in medication-related clinical activities such as prescribing, recording, medication review, prescription dispensing, medication administration and transfer of medicines information between and within healthcare organisations. Despite this requirement, however, getting all the stakeholders to conform to this practice has proved very challenging ("Electronic Medication Management Systems", 2012).

For instance, although PBS data should match AMT data in most cases, some AMT codes in PBS distribution are different to those in the AMT distribution from the National Clinical Terminology and Information Service (NCTIS) ("AMT PBS FAQs", 2016). This is due to PBS system creating its own description and using its own namespace identifier – the 7 digit ID which appears within the full identifier string – where a product needs to be described differently for legislative and reimbursement purposes, or even where the AMT concept does not meet PBS requirements, for example the PBS description requires more or less detail than the associated AMT description provides ("AMT PBS FAQs", 2016).

In addition, AMT and PBS have different release cycles, making the change incorporation more difficult and increasing the chances localised changes being required (i.e. non-AMT PBS codes). Both the NEHTA, which is now known as Australian Digital Health Agency (ADHA), and PBS have been working together to ensure quality mapping processes and alignment between both the AMT and PBS releases ("Answers to questions on notice", 2016).

This inconsistent use of coding systems nonetheless has the potential to create interoperability issues between the stakeholders, which would represent significant delays in reaching eTP's full potential. Furthermore, this potential interoperability issue discouraged the EPS and EDS software vendors from adopting the AMT coding system ("MSIA Issues presented at the eHealth ICT meeting", 2013). In any case, adoption of AMT coding by EPS and EDS software vendors may not be an issue in the future as AMT coding has been provided as a formal subset of the SNOMED CT-AU release since late 2015 ("Australian Medicine Terminology", 2016).

Another inconvenience of the current ETP implementation is the remaining legislative requirement for a handwritten signature by the prescriber in most jurisdictions. While awaiting the legislative changes supporting the use of digital signature in electronic prescriptions, the printed, paper-based prescription remains the legal document, requiring the prescriber's signature as per current acts and regulations. Because the current ETP implementation uses a printed, paper-based prescription to transfer the identifying DAK to the dispenser, the necessity of a paper token from the prescriber remains active and in place, along with all the legislative and regulatory constraints. This requirement for prescriber's handwritten signature impedes the adoption of the electronic prescription process and its full potential such as remote prescription.

Compared to the prior challenges such as the ongoing operation cost, the inability to assist in recording the patient's medication history and the requirement for the prescriber's hand-written signature, the following two issues are specifically from the technical and implementation perspectives. Despite interoperability between the two PES systems, further information sharing is unlikely to be straightforward, as their implementation and governing standards differ from one another; MediSecure's *Script Vault* complies with HL7 standards as mandated in ATS 4888 series, while eRx's *Script Exchange* is built using XML and Web Services technology drawn from different International and Australian standards ("ETP Standards", 2016; "Frequently Asked Questions", 2015).

This being the case, unless significant modifications are made to both systems for better information flow, further interaction or information sharing is more likely to require a third-party tool/utility such as a protocol translator or integration engine, for instance Orion Health's Rhapsody, NextGen Healthcare's Mirth Connect or Infor's Cloverleaf. This introduction and utilisation of third-party tools would produce not only an additional cost to the system but also the considerable associated risks and vulnerabilities.

One definition of vulnerabilities is "weaknesses in a computer's makeup that allows it to be exploited by cybercriminals" ("Vulnerabilities", 2017). Since tools and programs are written by humans, they are inherently imperfect and are not free of errors and therefore have the potential to create avenues for would-be attackers

(Holt, 2017). The current PES implementations do not utilise the established eHealth infrastructures for transferring prescription information. Over the course of the eHealth journey, a tremendous amount of time, effort and funding has been expended on putting in place various eHealth specifications and infrastructures such as the Health Identifiers (HI) Services, Secure Message Delivery (SMD) and Endpoint Location Services (ELS).

However, the PES prescription exchange model uses none of these features. Instead of making use of HI and ELS services, PES implements a simple Subscriber-Provider pattern. Use of SMD is also irrelevant for PES prescription exchange model as it is not a dedicated point-to-point transmission; the prescriber's submitted prescription is stored on PES to await its download by a subscribed dispenser (i.e. pharmacies). Therefore, these costly eHealth services are of little use for current PES implementation although they could have been utilised for better security and consistency.

2.7 Summary

The literature review presents and discusses the issues and shortcomings surrounding the current implementation of ETP in the Australian healthcare industry from a number of aspects including availability and consistency of the patient's medication information and the nation's healthcare expenditure.

Beginning the literature review on ETP is a brief history of Australia's eHealth journey under the guidance of NEHTA, which signifies a crucial step towards Electronic Medication Management and many other programs on the eHealth agenda. This is followed by an outline of the transition from manual prescribing to the current implementation of ETP using two PES services. The functioning of ETP implementation is briefly and clearly described, along with its interactions with external systems such as NPDR and the PBS online claiming system. The technical details of ETP are explored next, including its security measures using DAK and the requirement for the prescriber's signature on printed prescriptions.

The ongoing associated cost of a fifteen-cent electronic prescription fee and its current subsidisation by the Commonwealth is briefly discussed before emphasising the inability of ETP to provide patients' complete medication history to the clinician and other healthcare provider despite the existence of the National Prescription and Dispense Repository (NPDR). The fact that NPDR's varying levels of clinical value and usefulness is primarily due to the use of different coding such as AMT coding and non-AMT PBS coding is highlighted. Following this is a description of FRED IT's current attempt, using MedView Medicines Workspace, to facilitate shared access of critical medicines information among healthcare service providers such as doctors, pharmacists, hospitals and patients.

The current "going mobile" trend in the Australian healthcare sector is highlighted by a brief mention of the release and use of the child health mobile application extension of the Commonwealth's Personally Controlled Electronic Health Records (PCEHR) and the *eRx Express* mobile application. This is followed by an explanation, from the architectural perspective, of the various levels (i.e. Level 1-3) of ETP adoption and its influence on the information flow, the form in which the information is communicated and the legal document format (i.e. printed or electronic form) in each ETP adoption level.

The next section identifies and examines the relevant Acts, regulations, standards and specifications governing the ETP implementation at Commonwealth, state and territory levels in terms of their influence on current ETP process and the security measures they mandate. How they fit together and form a complex legislative and regulation construct for ETP is depicted by Figure 2.9 (Dante's 4 circles of eTP), whilst Tables 2.2 and 2.3 briefly describe each of the eTP-related standards and specifications relevant to this research. Figure 2.10 helps to explain the positioning of eTP- and eHealth-specific standards within the existing industrial standards from contexts such as communication, web services, XML and encryption. The literature review concludes by highlighting the shortcomings of the current ETP implementation such as its reliance on the supporting infrastructure and associated ongoing cost, its inability to provide a patient's complete medication history and its requirement for the prescriber's handwritten signature, which presents an obstacle to becoming a fully electronic process.

The literature review also contributes by providing a clear awareness of the fact that, despite being a crucial development in eHealth initiatives towards a safer and better outcome in Australian healthcare, current ETP implementation has some significant and costly flaws in terms of availability and consistency of the patient's medication information and an ongoing expense which can only rise with the increase in population. Given the advancements in security and widespread user acceptance of mobile computing, it is imperative to explore a viable alternative electronic prescription transfer mechanism with comparable security assurance at a cheaper cost, if not completely cost-free.

From the legislative and regulatory perspectives, the Commonwealth and the states and territories have repealed and amended Acts and Regulations and developed and/or adopted numerous standards and specifications in order to pave the way for implementing eTP. However, legislative approval for the legal use of digitally-signed electronic prescriptions is still pending, thereby impeding one of the final processes supporting the efficient use of electronic information communication in electronic prescribing. While awaiting further legislative changes supporting ETP implementation to the next level, it is therefore necessary to explore alternatives which can be implemented within the existing legislative framework - alternatives with reduced complexity, comparable security measures and controls and without the need for major supporting infrastructure and its associated ongoing costs.

2.8 Research Questions (RQs)

2.8.1 Main Research Question

The primary research question is:

Can a technical framework be constructed to serve as a guide for development of ANDROID mobile electronic prescription transfer applications in compliance with the security requirements mandated by Australian healthcare laws, regulations and standards?

The Primary Research Question was addressed through the exploration of two supporting Research Questions. Based upon the findings from the supporting questions, this research determined whether a technical framework can be constructed for development of an Android mobile electronic prescription transfer applications in compliance with the relevant laws, regulations, standards and specifications governing the Australian healthcare industry.

Based on the outcomes and preliminary analysis of the Primary Research Question in the creation of such technical framework, an associated series of procedures was then developed to validate and verify a functional, practical and implementable solution, which could potentially serve as an alternative approach in the adoption of a mobile electronic prescription transfer mechanism for the Australian healthcare industry. The first supporting question relates to the security requirements for electronic prescription transfer applications in the Australian healthcare industry.

2.8.2 Subsidiary Research Question 1

How can the security requirements imposed by the relevant laws, regulations and standards in the Australian healthcare system be integrated into a framework for the assessment of mobile electronic prescription transfer applications?

Answering this Subsidiary Research Question involved analysing the acts, regulations, standards and publications related to the security requirements and the electronic prescription transfer specifications for prescribing in the Australian healthcare context. The publications included those produced by the Australian

Digital Health Agency (formerly NEHTA), Standards Australia, the Department of Health, the Pharmacy Guild and other relevant authorities. The resultant analysis formed the assessment criteria for the next phase of the research: further investigation of and experiments on the candidate technologies such as operating system platform, encryption and wireless communication.

2.8.3 Subsidiary Research Question 2

How can the assessment criteria framework developed in Subsidiary Research Question 1 be used in assessing the native security features and third-party tools on the Android for the security compliance of mobile electronic prescription transfer applications?

This second supporting question required a detailed study of the capability of the Android's native security features, other third-party security tools/frameworks and wireless communication technologies, to fulfil the security requirements identified by the previous Research Question. Through a series of experiments, potentially some in an iterative manner, this research identified the candidate technologies and studied their relevant security measures/mechanisms which address the security requirements specified in the outcome of Subsidiary Research Question 1. The experiment outcomes were assessed for technical viability and practicality in the development and deployment of potential solutions for the Australian healthcare industry.

2.9 Learning from the Research

This study of the current implementation of ETP emphasises on how it functions, its regulatory enablers and constraints at Commonwealth, state and territory levels as well as its limitations and issues. This study states the vital role of ETP in improving the Australian healthcare system and its future maintainability. It examines the security model of current ETP implementation, which revolves around the use of DAK for securing prescription information. It investigates the levels of ETP implementation/adoption and subsequently categorises the current ETP implementation in Australia as between level 1 and 2, according to Gregory's (2003) *levels of ETP adoption*. The limitations of the current ETP implementation are discussed, along with its potential extensions for improvements. Next it identifies the relevant laws, regulations, standards and specifications governing the ETP implementation at Commonwealth, state and territory (i.e. jurisdictional) levels. These findings establish the minimal security requirements for Android mobile ETP applications.

This study concludes with the construction of the Primary Research Question and two Subsidiary Research Questions, which in turn lead to the next stage of the research. The paper produced at the end of this stage (i.e. Research Paper 1 in Appendix A) firstly briefly describes these findings and secondly contrasts the current ETP implementation with its full potential as a mobile implementation. The research findings published in the paper produced were verified by the “triple-blinded peer review” process.

Htat, K. K., Williams, P. A. H., & McCauley, V. (2015). The Hare and the Hortoise [*sic*]: The Potential Versus the Reality of eTP Implementation. In *Proceedings of the 23rd Australian national Health Informatics Conference 2015*, Brisbane, Australia (pp. 114-120).

Contributions: Htat (65%), Williams (25%) and McCauley (10%)

CHAPTER 3. RESEARCH METHODS

3.1 Overview

This chapter begins by exploring some qualitative research methods relevant to this research and is followed by a discussion of the underlying principles, designs and investigative approaches employed in endeavouring to answer the Research Questions.

3.2 Methodological Approach

Denzin and Lincoln (1994) suggest that there are three essential components to understanding the nature of qualitative research. The first component declares that qualitative research is interpretive, the second states that it is multimethod and the third articulates that it is conducted in the field or in the person's natural setting and surroundings.

Christensen et al (2011) refer to the use of several methods (i.e. multimethod) as triangulation because it is believed that "the use of several methods provides better understanding of the phenomenon being investigated". Whilst Moore (2002) defines research methods as the tools selected by researchers to provide the data that explores research questions (i.e. subsequently analysis conducted, and conclusions are drawn upon), Williamson (2002) stresses their importance by suggesting that the selection of an appropriate methodology is crucial to the success and applicability of the research. Pickard (2007) supports the importance of selecting an appropriate method, as well as the researchers' understanding of the methods in establishing the validity of the research findings. Williamson then cites that "truth value", "applicability", "consistency" and "neutrality" are the four concepts with which to gauge the value of the research. In qualitative research such concepts are mapped to "credibility", "transferability", "dependability" and "confirmability" respectively (Pickard, 2007).

In order to establish such value and credibility for the research, the following section explored and investigated different research methods selected for their apparent relevance to the nature of this research.

3.2.1 Hermeneutics

Initial investigation of the hermeneutics approach was conducted, since answering Subsidiary Research Question 1 required deciphering the true meaning of what the legal texts imply and interpreting them into a set of security requirements. The name hermeneutics comes from the Greek word “hermeneuein”, meaning “to interpret or translate”, and it offers a theoretical framework for interpretive understanding, or meaning, with an emphasis on context and original purpose. It originally provided guidelines for scholars in interpreting biblical texts into actual explanation (Crotty, 1998).

Ree & Urmson (1991) point out the radical redevelopment of hermeneutics by modern thinkers from a method used by theologians to investigate the inner meanings of sacred texts to a reflective practice of unmasking hidden meanings beneath apparent ones. In 2003, Laverty described the data generation and analysis processes conducted in a Hermeneutical Circle method as being comprised of reading, reflective writing and interpretation with rigour. Laverty also depicted these processes as shown in the Figure 3.1.

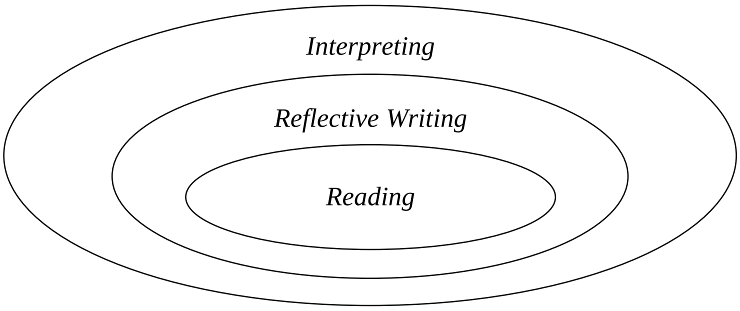


Figure 3.1: Hermeneutical Circle (Laverty, 2003)

The initial intent of this research was to utilise the hermeneutics approach to derive a set of acceptance criteria (i.e. security requirements) from the applicable legislations, regulations and standards for the security of electronic prescription information in the Australian healthcare industry. However, further investigation revealed that hermeneutics was not a suitable method, since this research is seeking neither the transcendental interpretations of the text nor the meaning determined by the researchers using their interpretation for further discussion and understanding (Crotty, 1998; Cole & Avison, 2007). This research simply needed to interpret the legal texts and standards in order to create a set of technical and security requirements.

3.2.2 Document Analysis

Bowen (2009) defines document analysis as "a systematic procedure for reviewing or evaluating documents - both printed and electronic (computer-based and Internet-transmitted) material". He also mentions that it is a low-cost, unobtrusive and non-reactive way to obtain empirical data. Although it has been used primarily as a complement to other research methods for triangulating and theory building, its uses as a stand-alone method have increased considerably within the public health research environment, especially in evaluating the impact of initiatives such as a committee-led venture to increase immunisation uptake in an area or a Board-led approach to reduce sexual ill-health ("Document Analysis", n.d.; Bowen, 2009).

In the document analysis approach, documents containing texts and images produced without the researcher's intervention are examined and interpreted in order to elicit meaning, to gain a more in-depth understanding and to develop empirical knowledge (*ibid*). The documents can be in a variety of forms retrieved from various sources such as libraries, newspaper archives and organisational or institutional files. Researchers using this approach would normally review prior literature as part of their studies and then incorporate that information in their reports (Bowen, 2009).

According to Bowen (2009), document analysis is an iterative process which combines elements of content analysis and thematic analysis involving skimming (superficial examination), reading (thorough examination) and interpretation. In this approach, the use of content analysis organises the information into categories related to the phenomena of interest and entails a first-pass document review which identifies the meaningful and relevant passages of texts or other data (Corbin & Strauss, 2008). Through a more in-depth and focused re-reading and review, thematic analysis in this approach identifies patterns within the data, as well as emerging themes, as the basis for further analysis, coding and category construction based on the data's characteristics (Fereday & Muir-Cochrane, 2006).

Like other research methods, document analysis is not without inherent limitations (Bowen, 2009). However, limitations such as “insufficient detail” and “low retrievability” were not applicable to the documents used in this research, and the benefits of the method outweighed its limitations. Based on these findings, this research employed the document analysis method for evaluating documents (i.e. the applicable legislations, regulations and standards) in such a way that empirical knowledge was produced.

Through document analysis an understanding was developed to derive a set of acceptance criteria (i.e. security requirements) from those documents with the aim of securing electronic prescription information in the Australian healthcare industry. The value and credibility of this particular research was strengthened by the use of triangulation. Whilst Angers and Machtmes (2005) stress the necessity of triangulation to minimise bias and establish credibility of the data obtained during the research, Patton (1990) claims that the use of triangulation helps in preventing the introduction of vulnerabilities due to the research findings being an artefact of a single method or source, or influenced by a single investigator's bias. The research findings are corroborated by the supervisory review at the end of each research stage.

3.2.3 Experimental Research

Pickard (2007) defined experiment as “a controlled research situation” in which the researcher can establish the experimental conditions down to the smallest details, where the experimental environment can be isolated from the unwanted variables and external influences. The extent of error (i.e. experimental error) must be identified when these conditions cannot be met entirely (Pickard, 2007). Pickard also stresses that understanding the nature of experimentation and experimental error is crucial in establishing the value and significance drawn from the research.

The basic model of the true experiment not only demonstrates that “If X then Y” but also “If no X then no Y” (Pickard, 2007). The inherent difficulties in measuring the extent of error and identifying the variables responsible for it classify many studies which claim to be “experimental research” as “quasi-experimental research”. Whilst the true experiment aims towards covariance between the identified variables, with deliberate manipulation of the independent variables, the quasi-experiment aims to establish levels of correlation between observable variables without any intervention and temporal restrictions (Pickard, 2007; Field & Hole, 2002).

Christensen et al (2011) describe experimental research as an attempt to identify cause-and-effect relationship by conducting controlled experiments. From the most simplistic perspective, cause is something that produces something else and effect is the difference between what would have happened without the manipulation of the independent variables and what did happen with the manipulation of those (*ibid*). Christensen et al (2011) also state that it is impossible to obtain the true measure of an effect as it requires the situation to both be X and Y at same time, when they are in fact mutually exclusive (i.e. impossible).

Before developing enough understanding of the experimental research method, it was initially assumed that answering Subsidiary Research Question 2 would follow the quasi-experimental research method. With better understanding of the method, however, and since Subsidiary Research Question 2 only sought “how to use the findings from Subsidiary Research Question 1 in assessing security compliance of an Android electronic prescription transfer application” rather than pursuing the “cause-and-effect” of using those findings in such a security compliance assessment, it was concluded that the use of the experimental research method was not an appropriate approach for this particular research.

3.2.4 Action Research

Seale (2007) state that action research is “grounded in the belief that research with human brings should be participative democratic”. Reason and Bradbury (2001) second this by declaring that “A primary purpose of action research is to produce practical knowledge that is useful to people in the everyday conduct of their lives”. It is more often used in the fields of information and communication research due to its value in improving service provision, encouraging reflective practice and structuring and disseminating experience to the wider community (Pickard, 2007).

Kurt Lewin, who first used the term “action research”, believes that some form of action/change has to be part of the research design from the beginning in order to make a difference (Pickard, 2007). Therefore, an investigation leads to some form of action and it is then followed by an evaluation (*ibid*). However, Williamson (2002) calls this design the “most basic action research cycle” and describes it as in Figure 3.2.

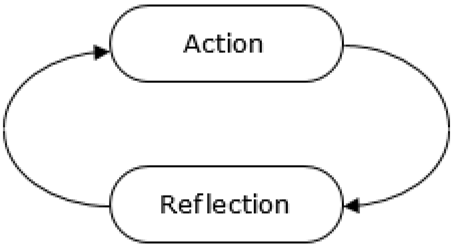


Figure 3.2: The most basic action research cycle (Williamson, 2002)

Williamson states that the “reflection is based on experiences of action” and describes the whole practice as a learning process. She portrays it iterative nature of action research’s thusly: “Action research is usually carried out in discrete cycles, where later cycles are used to challenge, support and refine insights and results from previous cycles” (Williamson, 2002). The Action Research cycle, with multiple elements for more complex scenarios, is depicted in Figure 3.3.

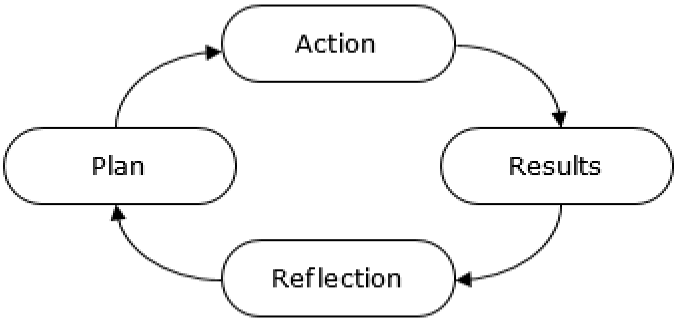


Figure 3.3: A typical action research cycle (Williamson, 2002)

Whilst participation in the research context leads to the thorough understanding of the problem, the action/change introduced and the outcome of that action/change, the researcher actually being part of the context being researched and having such tacit knowledge of the situation posed the greatest challenge for this research method, which calls into question the credibility or validity of the outcome because it relies on the researcher's notion of objectivity. Nevertheless, Herr and Anderson (2005) point out that it is irrelevant to use the same validity criteria used in judging the positivistic and naturalist researches, and provided "democratic validity", "outcome validity", "process validity", "catalytic validity" and "dialogue validity" as the five criteria applicable in measuring the credibility of action research.

Although this research is not a perfect candidate for the use of the action research method, better understanding of this method enabled the researcher to derive from it an iterative experimentation and reflection approach for this particular research. This derived approach still agreed with Williamson's (2002) brief description of the action research cycles as "mini-experiments in practice".

In each cycle of research, the reflection on the experimentation result indicated whether or not the candidate technology complied with the mandated security requirements, that is to say whether or not it could be used in the proposed mobile ETP solution, and whether or not the experimentation needed iteration with a different technology.

3.3 Theoretical Framework for the Research

Williamson (2002) uses the architect's house-plan metaphor to depict a theoretical framework; a theoretical framework describes the key ideas underpinning the research and how they are related in the same way in which a house plan describes the rooms of the house and how they are interconnected. Crotty (1998) says that the starting point in developing a research proposal is to identify the methodologies and methods that will be utilised in the research and consequently justifying the choice. Therefore, this section identifies and describes the relevant theoretical framework to be employed in addressing the Research Questions.

This research falls into the realm of mixed methods, these being qualitative and iterative experimentation and reflection. It used qualitative data from the document analysis research followed by iterative experimentation to explore and verify potential solutions and subsequently derive a framework to answer the main Research Question.

Miles and Huberman (1994) mention that the qualitative aspects are based on observation, interviews or reading documents, whilst Wolcott (1992) describes it as “watching, asking or examining”. The objective of this study is to interpret the requirements mandated by acts, regulations and standards into a set of acceptance criteria (i.e. security requirements) to be fulfilled by such potential candidate technologies as Android’s native security features and third-party tools and short-range wireless communication technologies such as NFC and Bluetooth.

Williamson (2002) categorises research as basic research, primarily concerned with deriving new knowledge and focusing on theory building and/or hypothesis testing, and applied research, which concerns solving specific problems in real-life situations and is immediately usable as solutions to actual problems. While basic research mainly contributes to the advancement of the general knowledge of society, applied research intends to help practitioners to be better informed about their work environment and to do their job better (Williamson, 2002). According to Williamson’s categorisation, this particular research is of applied research type with exploratory nature.

Despite qualitative research being a widely used approach and offering many ways of being conducted, there are some pervasive issues associated with qualitative research such as labour-intensive data collection, the distinct possibility of researcher bias, time demands for processing and coding data and the credibility and quality of conclusions (Miles & Huberman, 1994). The reliability and validity of the qualitatively derived findings in particular can be seriously in doubt (Dawson, 1979, 1982; Ginsberg, 1990; Kirk & Miller, 1986; Kvale, 1989a; LeCompte & Goetz, 1982) as it is mainly dependent on the competence of the analysis process. Williamson (2002) suggests the use of triangulation, which encourages validation of interpretivist research findings by adding rigour, breadth and depth to the amalgamation, analysis and writing up of the data. This is achieved by using multiple methods and theoretical constructs; (1) the use of data triangulation which allows the researcher to access variety of data sources for the study, (2) the use of several different researchers and/or evaluators, (3) the adoption of multiple theories and/or perspectives to interpret a single set of data and (4) undertaking multiple methods to study a single problem or phenomenon.

May (2002) also states that the relationship of the researcher to the research is important since the researcher's ability to interpret data sensibly and avoid reading too much or not enough into a situation will depend on firsthand experiences. Moreover, Liamputtong (2009) adds that it is crucial for qualitative researchers to have a good understanding of the methodology so that they can interpret data sensibly and with insight and not simply interpret data in the light of preconception and prejudice which has the potential to perpetrate unsatisfactory or inappropriate understandings of the phenomenon of interest.

As this research was conducted in eHealth, an emerging field at the intersection of medical informatics and public health and information security, there was little literature about theoretical frameworks for use in this integrated field. Since this study was designed to decipher the true meaning of the legal texts, interpret them into a set of security requirements and build a framework to guide the development of a mobile ETP application in compliance with those security requirements, a combination of document analysis and repetitive/cyclic experimentation research approaches was employed.

Bowen (2009) describes document analysis as a systematic procedure for reviewing or evaluating documents in textual or graphical forms that have been recorded without the researcher's intervention. Similar to other analytical methods in qualitative research such as hermeneutics, document analysis method examines and interprets documents in various forms in order to elicit meaning, gain understanding and develop empirical knowledge (Bowen, 2009). However, unlike the hermeneutics approach, the interpretation using document analysis did not reflect the researcher's perception of the phenomena transcending its textual meaning. Instead, using document analysis, the artefacts were examined and interpreted by the researcher to derive their genuine meaning relevant to the context of interest.

In this study the document analysis research approach was used to derive the acceptance criteria (i.e. security requirements) via analysis and interpretation of the existing artefacts, namely the applicable laws, regulations and standards related to electronic prescribing and dispensing, together with information security in the Australian healthcare industry.

The data generation/collection phase involved extensive study and analysis of the applicable legislations, regulations and standards. However, this research extended the interpretation of artefacts to construct the relationships between the legal explanations and a practical understanding for real-life application. Manen (1990) suggests that there is no fixed set of methods to perform this type of study. Both the data generation and analysis processes used a document analysis circle method which mainly comprised skimming, reading and interpretation (Bowen, 2009). By adding the process of "knowing the research context and finding relevant artefacts" to Bowen's (2009) description of the document analysis method, Figure 3.4 portrays the Document Analysis Circle for this particular research and is adopted from the Laverty's (2003) depiction of the Hermeneutical Circle.

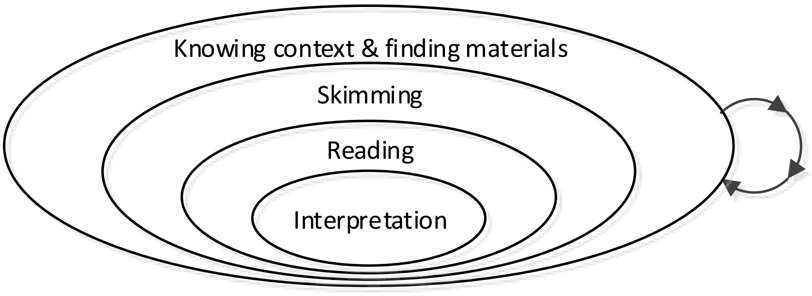


Figure 3.4: Document Analysis Circle derived from Laverty's (2003) Hermeneutical Circle

Initially, the interpretations and conclusions drawn from this study were to be reviewed by the expert panel as part of the source triangulation process, involving cross-checking, for better reliability and validity, for consistency of information derived at different times and from different people. After much deliberation however, the use of the expert-panel for the triangulation and verification process was considered redundant since firstly, all the significant findings of the research were published in a series of four double-blinded peer-reviewed papers during the course of the research and secondly, because the research findings were reviewed by the internal supervisory panel of domain experts who were actively involved in the research context.

The data collection and analysis phases for exploring the native security features and third-party tools on Android in fulfilling the security requirements were designed using the iterative experimentations and reflection approach. Once the interpretation of the legal texts had been sufficiently conducted using the document analysis approach to identify the security requirements and construct the acceptance criteria, the rest of the research mainly involved a series of experimentations and reflection based upon the experimentation outcomes as to whether they satisfied the identified security requirements.

In agreement with Maxwell (2005), who says “Sequential models are not a good fit for qualitative research, in which any components of the design may need to be reconsidered or modified during the study in response to new development or to changes in some other component”, the iterative experimentation and reflection approach employed for the rest of the research was very similar to the action research approach. For each security requirement identified, a series of potentially repetitive experimentations were conducted to explore and determine which candidate technology fulfilled the security requirement and complied with the constructed acceptance criteria. In a similar way action research is used to bring about change of practice while creating knowledge at the same time (Williamson, 2002) the selected iterative experimentation and reflection approach is employed for the exploratory research to bring about improvement of practice or to propose new solutions to practical problems. Figure 3.5 depicts the constituent elements of each experiment iteration for this research in a detailed form.

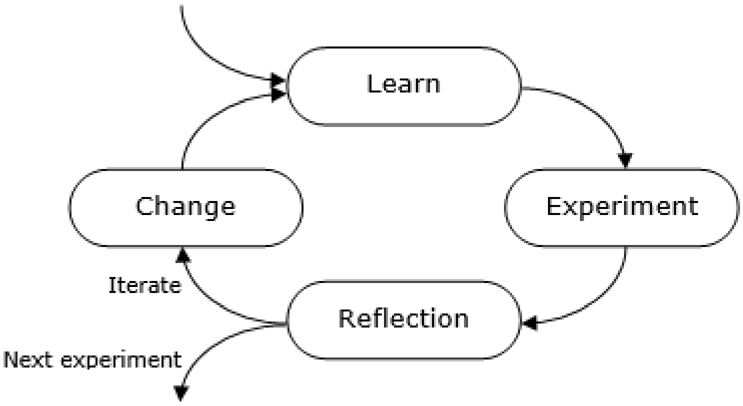


Figure 3.5: Iterative Experimentation and Reflection Cycle

McNiff and Whitehead (2002) define action research not as a set of concrete steps but as a process of learning from experience: a dialectical interplay between practice, reflection and learning. In a similar way, each iteration of the experimentation for this research explored the available options by learning further details about the tools, technologies and features, conducting an experiment to verify its viability and finally reflecting whether the outcome is a suitable one for the specific security requirement, before proceeding to the next experimentation for another legislative/security requirement or repeating the iteration with necessary changes based on the lessons learnt and the experience gained. Similar to Williamson’s (2002) description of the typical action research cycles, these repetitive experimentations are employed in this research as a process through which findings and insight are generated in an explorative manner, since details of each iteration are seldom planned up-front and new insights and experience gained through experimentation and reflection may necessitate repeating the iteration.

This approach is designed to be critically reflective, the need for reflection existing in times when current action did not produce the desired results and the change was needed (Williamson, 2002). However, unlike the extensive version of the action research approach, not much rigour was anticipated to be utilised in these iterations. All the research findings and conclusions drawn from this stage were also subject to review by the experts as part of the triangulation process (i.e. reviewed by the supervisory panel of domain experts).

Every step of the analysis and derivation of conclusion from this entire research was designed and carried out with the utmost care as the strength of qualitative data mainly relies on the competence of the analysis process and iterative experimentation process. The analysis process was performed using the analysis matrix populated from answering the two Subsidiary Research Questions.

Although referred to as analysis, the process actually consisted of three integrated activities: data reduction, conclusion-drawing and verification. Data reduction itself generally consisted of selecting, focusing, simplifying, abstracting and transforming the data to assemble into the information required for conclusion-drawing and other necessary actions. It also allowed the researcher to understand what was happening and enabled further actions based on that understanding. Conclusion-drawing and verification followed data analysis. Triangulation process was used to ensure the validity of qualitative data by means of experts testing its plausibility, sturdiness and conformability. Reviewing may take as little as a few seconds, while extensive conclusion-drawing required replicating the findings in another data set. In all the expert review activities of the triangulation process the dialectics action research technique was exercised by welcoming disagreement as a way to generate better information and by achieving consensus through focusing on disagreement and its resolution (Williamson, 2002).

3.4 Research Design

This research focused on a specific facet of mobile health, that being the security of electronic prescription data on Android mobile devices, which in turn is a segment of the national eHealth program. Marshall and Rossman (1995) suggest that the Research Questions in qualitative research should be general enough to permit exploration but focused enough to delimit the study. Accordingly, the two supporting Research Questions were carefully designed so that they clearly defined the boundary of this research context while allowing exploration from different perspectives. In addition, for better segregation of the emphasis and in-depth understanding of the findings, all the studies and experimentations for this research were conducted from two perspectives: security of the prescription information from the perspectives of both data at rest and data in transit.

As a result of the document analysis, the first supporting question derived a set of security requirements from the applicable national as well as eHealth-specific standards, laws and regulations for security of prescription information in Australia. This document analysis process also developed the practical understanding of the security requirements for real-life application from the legal explanation. The preliminary study identified that standards and publications such as “AS 4700.3-2014”, “ATS 4888.1-2013 ~ ATS 4888.6-2013”, “AS 5550-2013”, “AS 5551-2013”, “AS 5552-2013”, “ATS 5546-2013”, “ATS 5822-2010” and “HB 308 2011” by Standards Australia will be emphasised in answering the first Subsidiary Research Question. In addition, other standards and publications from organisations and authority bodies such as the Australian Digital Health Agency (ADHA, previously NEHTA), International Organisation for Standardisation (ISO), Health Level 7 (HL7), Integrating the Healthcare Enterprise (IHE) and the International Health Terminology Standards Development Organisation (IHTDSDO) will also be considered for their relevance to ETP implementation in the Australian healthcare industry.

Subsequently, through a series of experimentations the second supporting question explored and verified the native encryption features of Android which could potentially fulfil the security requirements for the electronic prescription information from a data at rest perspective. The later iterations of the experiment explored and verified the candidate short-range wireless communication technologies such as NFC and Bluetooth for security assurance from the data in transit perspective while transferring the electronic prescriptions between the ETP participating devices (i.e. between the patient's smart phone, prescriber's EPS and pharmacy's EDS).

Despite an initial plan to use a panel of domain experts (i.e. external expert-panel) for triangulation and verification of the research findings, the significant findings from different stages of the research were in fact published as a series of four double-blinded peer-reviewed papers. The first paper, published at the end of the preliminary study of the research, portrayed the current implementation of ETP and compared it against its full potential. It was published as the proceedings of the 23rd Australian National Health Informatics Conference 2015. The second paper revealed the research findings on securing the electronic prescription information from the perspective of data at rest and compared how it is achieved in the current implementation using PES services against the proposed mobile alternative. This paper effectively covered the research findings of Experiment 1 and was published as the proceedings of the 4th Australian eHealth Informatics and Security Conference 2015. The third paper focused on the security of electronic prescription information from the data in transit perspective and the comparison of how it was implemented in current ETP versus its implantation in the proposed mobile solution (i.e. using the potential candidate wireless communication technologies such as NFC and Bluetooth). This paper is in fact a summary of the research findings from Experiments 2 and 3. It was published as the proceedings of the Australasian Computer Science Week Multiconference 2017. The final published paper from this series presented the comparison between the current ETP and the proposed mobile alternative from a more holistic perspective, basically reflecting the "Discussion of Results" and "Conclusion" sections of this thesis. This last paper was published as the proceedings of the 14th Australian Information Security Management Conference 2016.

Based on these research findings, the Primary Research Question was formulated to determine whether it is possible to create a framework for the development of an Android mobile electronic prescription transfer application in compliance with security requirements mandated by relevant standards, laws and regulations.

This study reveals that such a framework can be built from the legislative and security perspectives and, as such, this developed framework could be used to guide the development of an Android mobile ETP application for the Australian healthcare industry, thereby creating a significant contribution towards the national eHealth program. The following diagram graphically depicts the scope and context of this research.

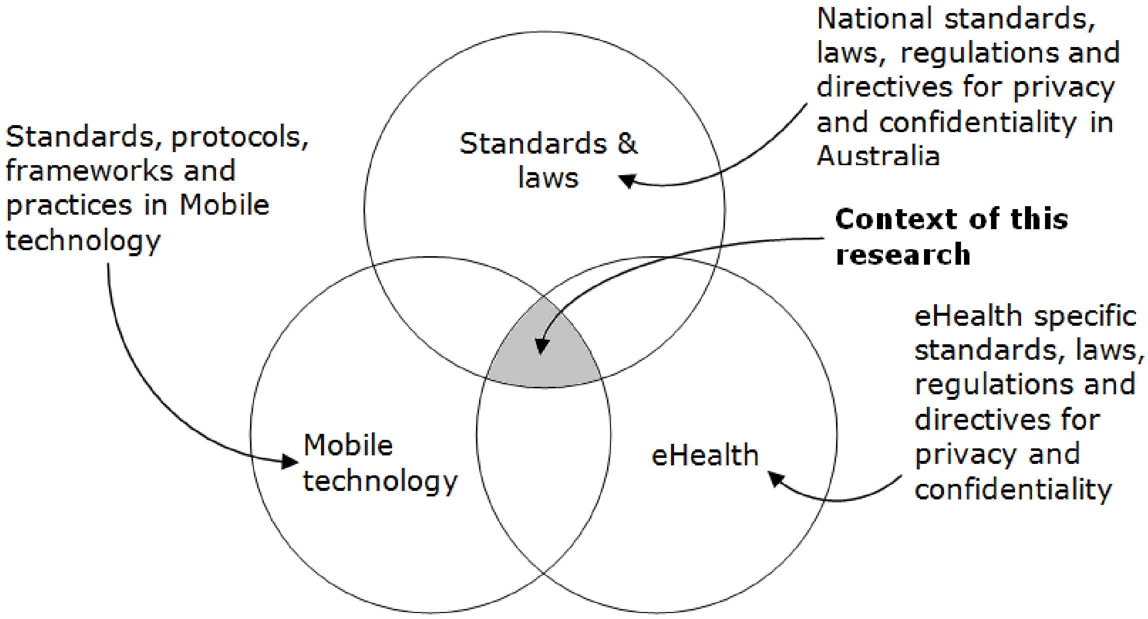

National standards, laws, regulations and directives for privacy and confidentiality in Australia
Standards, protocols, frameworks and practices in Mobile technology
Standards & laws
Context of this research
eHealth specific standards, laws, regulations and directives for privacy and confidentiality
Mobile technology
eHealth

Figure 3.6: Scope and context of the research

The extensive document analysis and rigorous iterative experimentation and reflection derived from Williamson's action research cycle were used for data collection and analysis processes, in conjunction with the triangulation process employing the dialectic action research method for verification and scrutiny from different perspectives before progressing further to the next step, iteration or final conclusion (Williamson, 2002). The document analysis emphasised on the current established acts, regulations and standards and publications mainly produced by the Department of Health and Aging, NEHTA and Standards Australia. Data collection populated the analysis matrix with applicable security requirements and the candidate technologies (i.e. Android's security features, NFC and Bluetooth) which would potentially fulfil those requirements.

Data analysis surveyed the collected information against the essential criteria and measured the outcomes accordingly for synthesis and conclusion. The synthesis and conclusion process derived a framework to guide the development of an Android mobile ETP application in compliance with the security requirements or drew a conclusion as to why it cannot be achieved. The conclusions made from the previous iteration become part of the input for the next iteration. A rigorous internal review was conducted by the researcher and the thesis supervisors after every stage to ensure that the data collection, analysis and synthesis processes were carried out appropriately and that any necessary adjustments were applied.

These data collection, analysis, synthesis and conclusion and review processes continued in an iterative manner within the defined context until the research had produced the final report. The following figure graphically depicts these iterative processes.

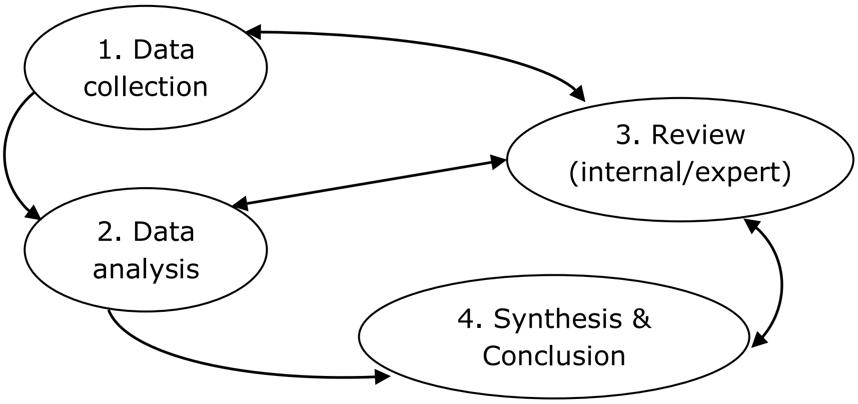


Figure 3.7: Conceptual framework derived from the iterative data collection and analysis model of Miles & Huberman (1994)

Table 3.1 briefly describes how the data collection and analysis were performed for each research question during the iterative processes of the entire research. The principal supervisor's active involvement with national and international digital health systems and eHealth standards, as well as the associate supervisor's extensive experience and knowledge in the clinical and health IT industry provided the researcher invaluable guidance, support and critical review throughout the learning journey.

With access to such extensive knowledge and guidance the internal review process was effectively a triangulation and verification process for the research findings at every stage.

Table 3.1: Data collection and analysis for each research question

Subsidiary Research Question 1	*How can the security requirements, imposed by the relevant laws, regulations and standards in the Australian Healthcare system, be integrated into a framework for the assessment of mobile electronic prescription transfer applications?* The procedures to be followed in this study are crudely depicted in Figure 3.9.
Data collection method	Analysis and synthesis of the applicable laws, regulations, standards and interpretations of those for the desired context.
Participants in data collection	Researcher
Data analysis method	Extensive reviews and research by researcher and then followed by an internal review by the thesis supervisors who are also domain experts.
Participants in data analysis and review (triangulation process)	Researcher and then followed by an internal review by the thesis supervisors (domain/area experts).
Recruitment process	Not applicable/necessary.
Subsidiary Research Question 2	*How can the assessment criteria framework (from subsidiary research question 1) be used in assessing the native security features and third-party tools on the ANDROID for the security compliance of mobile electronic prescription transfer applications?* The procedures to be followed in this study are roughly depicted in Figure 3.10.
Data collection method	Conduct the experiment with knowledge from reading books, research papers and technical discussion forums of relevant areas.
Participants in data collection	Researcher
Data analysis method	Performing experiments using appropriate tools for each security requirements documented then followed by an internal review by the thesis

	supervisors who are also domain experts.
Participants in data analysis and review (triangulation process)	Researcher and then followed by an internal review by the thesis supervisors (domain/area experts).
Recruitment process	Not applicable/necessary.
Main research question	*Can a technical framework be constructed to serve as a guide for development of ANDROID mobile electronic prescription transfer applications in compliance with security requirements mandated by the Australian Healthcare laws, regulations and standards?* The procedures involved in this study are roughly depicted in Figure 3.8.
Data collection method	Populating the analysis matrices (i.e. Table 4.1, 4.2 and 7.1) with the research findings from subsidiary question #1 and #2.
Participants in data collection	Researcher
Data analysis method	Analyse the contents of the analysis/compliance matrices collated by the two subsidiary research questions.
Participants in data analysis and review (triangulation process)	Researcher and then followed by an internal review by the thesis supervisors (domain/area experts).
Recruitment process	Not applicable/necessary.

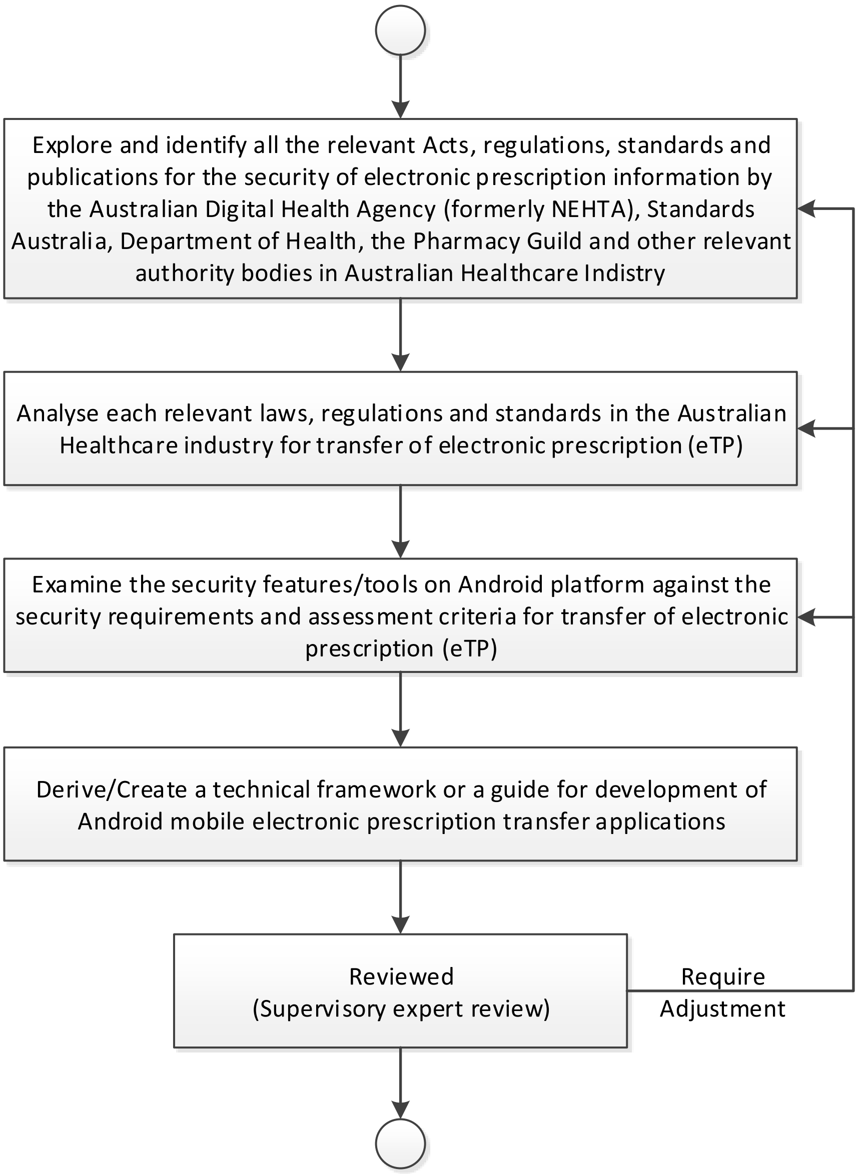

Explore and identify all the relevant Acts, regulations, standards and publications for the security of electronic prescription information by the Australian Digital Health Agency (formerly NEHTA), Standards Australia, Department of Health, the Pharmacy Guild and other relevant authority bodies in Australian Healthcare Indistry
Analyse each relevant laws, regulations and standards in the Australian Healthcare industry for transfer of electronic prescription (eTP)
Examine the security features/tools on Android platform against the security requirements and assessment criteria for transfer of electronic prescription (eTP)
Derive/Create a technical framework or a guide for development of Android mobile electronic prescription transfer applications
Reviewed (Supervisory expert review)
Require Adjustment

Figure 3.8: Building a framework for examining Android mobile electronic prescription transfer applications for compliance with security requirements

Figure 3.8 is a high-level depiction of the overall process of the entire research. It began with a preliminary study which explored and identified the relevant acts, regulations and standards of and publications by the relevant authority bodies in the Australian healthcare industry for the security of electronic prescription information. The draft of the analysis matrix template, which was later finalised and populated by the studies answering the supporting questions 1 and 2 (Figure 3.9 and Figure 3.10), was also designed as part this stage. The first study (Figure 3.9) translated the acts, regulations and standards into security requirements and its findings populated the analysis matrices. Through a series of repetitive experiments and reflections, the second study explored and examined the security features of the candidate technologies (i.e. Android platform's encryption, security of NFC and Bluetooth) for security requirements translated from a plethora of acts, regulations and standards in the previous study. The outcomes of this examination were recorded in the analysis matrices for the final assessment. Based on the content of these matrices, the final research conclusion was drawn and a framework was derived if the study revealed that it was viable as well as practical. The review process at the end of this stage may also result in additional iterations, potentially starting from any stage of the study.

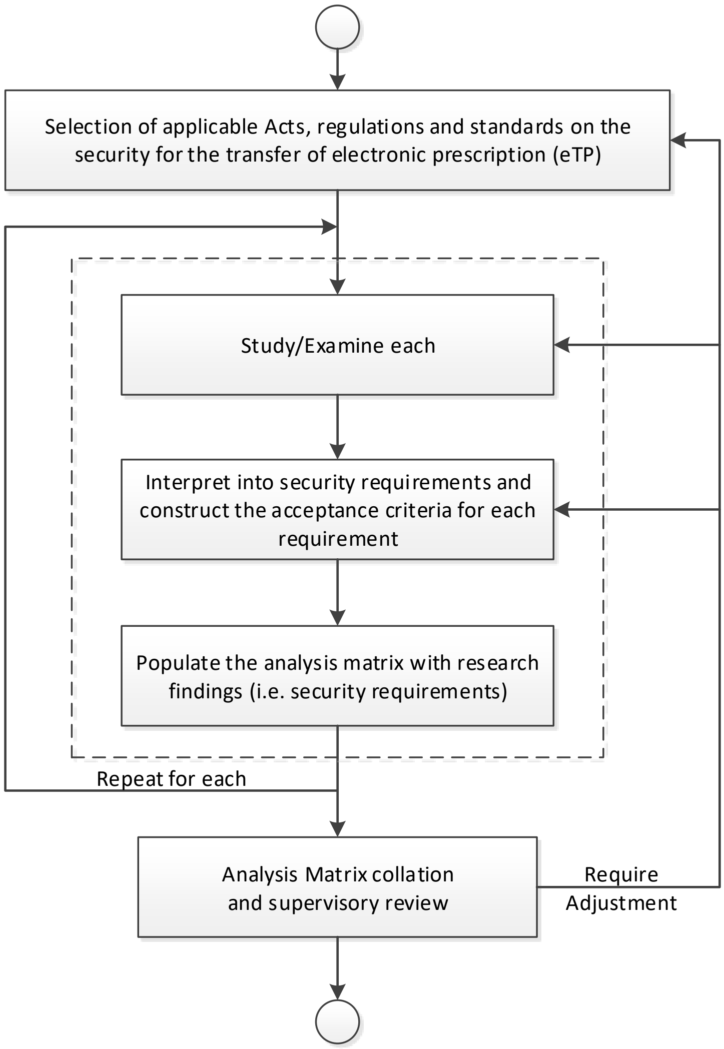

Selection of applicable Acts, regulations and standards on the security for the transfer of electronic prescription (eTP)
Study/Examine each
Interpret into security requirements and construct the acceptance criteria for each requirement
Populate the analysis matrix with research findings (i.e. security requirements)
Repeat for each
Analysis Matrix collation and supervisory review
Require Adjustment

Figure 3.9: Constructing the technical/security requirements and acceptance criteria

As depicted in Figure 3.9, this study began with the selection of applicable acts, regulations and standards related to the security for the transfer of electronic prescription in the Australian healthcare industry. Each selected act, regulation and standard was examined in detail and interpreted into a set of security requirements, which in turn formed the acceptance criteria for later experimentation and analysis stages. This study populated the analysis matrices with its findings, and the same process was repeated for all the rest of the selected acts, regulations and standards. The review process at the end of this study could potentially lead to further iterations with certain adjustments. Based on the required adjustment and the ground for the repetition, the next iteration may start from any step within this stage of the study.

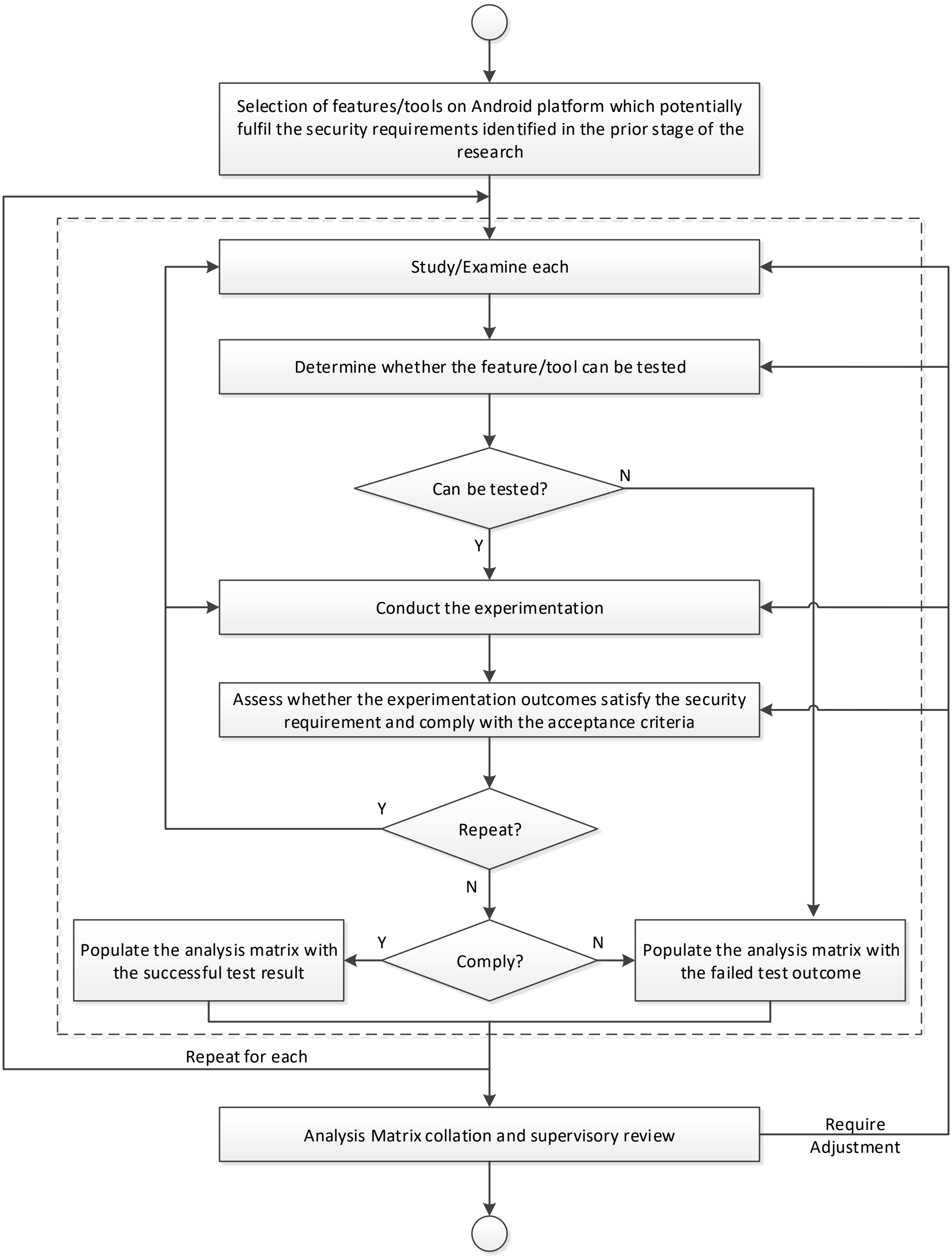

Selection of features/tools on Android platform which potentially fulfil the security requirements identified in the prior stage of the research
Study/Examine each
Determine whether the feature/tool can be tested
Can be tested?
N
Y
Conduct the experimentation
Assess whether the experimentation outcomes satisfy the security requirement and comply with the acceptance criteria
Y
Repeat?
N
Y
Comply?
N
Populate the analysis matrix with the successful test result
Populate the analysis matrix with the failed test outcome
Repeat for each
Analysis Matrix collation and supervisory review
Require Adjustment

Figure 3.10: Examining the security and privacy features/tools on Android platform

This study started with the selection of security features of the candidate technologies (i.e. Android’s encryption capability and security of NFC and Bluetooth) which would potentially fulfil the security requirements for the transfer of electronic prescription as identified in the previous study. Each feature was then studied for further details to determine whether it could be tested. When the study revealed that it could not be tested, this failed outcome was recorded in the analysis matrices. When the study proved that it was testable, an experimentation was conducted to verify whether the selected feature satisfied the security requirement (i.e. complied with the acceptance criteria) and whether its application was practical for the industry. Depending on the experimentation outcome from both viability and practicality perspectives, another iteration of the investigation was repeated with the necessary changes. At the end of the potentially iterative experimentation the outcome was recorded in the analysis matrices for later analysis and derivation of the framework.

This process was repeated for each security requirement identified in the prior study. As previously, the review process at the end of this study would potentially lead to further iterations with certain adjustments.

3.5 Equipment or Apparatus

Internet access was critical for the research, as was unlimited access to the related standards and regulations and local and federal laws of the Government and relevant authority bodies. This included access to the departmental libraries, document archives and repositories.

As part of the hardware requirements, experiments conducted for this research required a computer running Windows 8.1 with decent hardware configuration (e.g. Intel i5 or equivalent processor, 4 GB RAM with 256 GB HDD), and a smartphone with Android OS version 4.0 or higher with NFC and Bluetooth capabilities. In addition, a generic (i.e. no manufacturer-specific) NFC card reader with USB connection and a generic (i.e. no manufacturer-specific) Bluetooth USB dongle or a laptop with Bluetooth capabilities were also mandatory for the experiments involved.

At this point in time, no other associated cost anticipated such as licenses and subscription fees.

3.6 Procedure

The research to address Subsidiary Research Question 1 commenced after research ethics was granted. This was followed by a supervisory expert review to verify and validate the outcome from this phase. Similarly, for Subsidiary Research Question 2, the outcome was subjected to review a by supervisory expert panel to ensure the outcome was relevant and appropriate for progression to the next phase of the research. Based on these outcomes, the assessment was performed against the acceptance criteria as part of the iterative experimentation and reflection, and the conclusion drawn on whether it was possible to build a framework for development of electronic prescription transfer applications on Android platform in compliance with the security requirements of the Australian healthcare industry. This conclusion was also reviewed and validated by the supervisory expert panel for necessary adjustments. If the final conclusion, verified by supervisory expert panel, reveals that such a framework can be built, a working framework will be produced, representing substantial contribution towards the national eHealth program.

During the course of the study, these supervisory expert panel reviews and feedback processes were planned as part of the fortnightly meeting. The materials and outcomes were reviewed and emailed to the supervisors prior to the scheduled meeting. When any disagreement occurred as part of the meeting's dialectic triangulation process, it was decided that the supervisors' feedback was to be incorporated back into the study before the next round of experiment.

For each stage, a set of applicable acceptance criteria for assessing the outcome was prepared prior to the data collection and analysis. Where applicable, the assessment metrics and mechanisms were measured and defined, as they have significant impact on the outcomes and accuracy of the analysis and review processes. During the study, each review process could result in further repetitions and this iterative process was governed using the methodology of repetitive experimentation and reflection.

In each repetition of the experiment, the necessary adjustments were applied before continuing with another round of iteration and review. Depending on the context of the experimentation and the required adjustments, some repetitions took different approaches to those in prior repetitions and were not pre-planned or designed up front (as in Williamson's description of the typical action research cycles in 2002). These reviews were designed to examine not only the collected data and synthesised product but also the assessment metrics and criteria within the context, such as the legislative and regulatory requirements and mobile security.

In order to divide the research into manageable components, investigations for both Subsidiary Research Questions 1 and 2 were carried out from two different security perspectives: (1) security of the electronic prescription information at rest and (2) security of the electronic prescription information in transit. All the research outcomes from exploring and identifying the mandatory security requirements (i.e. derived from a plethora of acts, regulations and Standard) and how to fulfil them (i.e. technically on the Android platform) were assessed from these two security perspectives. Figure 3.11 shows how the security measures for prescription information in the current electronic prescription transfer model were categorised into these two security perspectives.

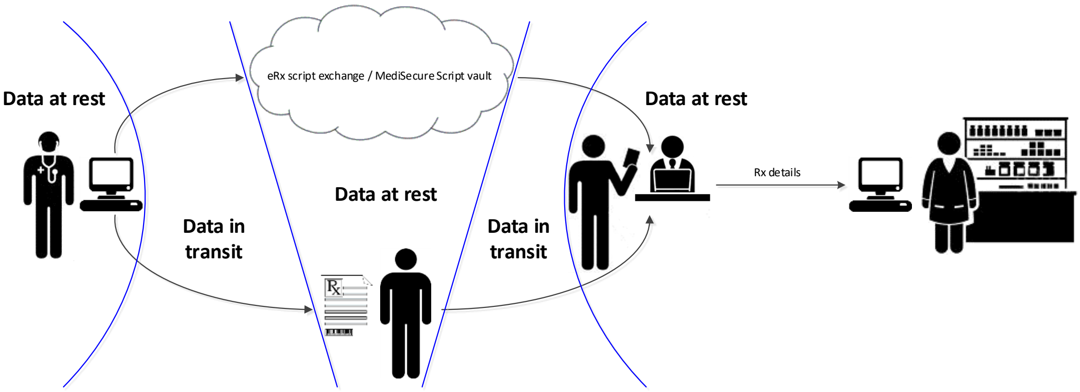


Figure 3.11: Current ETP model from security of data at rest and in transit perspectives

Given that the research context is not only highly regulated but also highly proprietary, this research investigated how these two aspects of security are implemented in the existing implementation, for example how acts and regulations are complied with, how standards are implemented and how security mechanisms are employed. The research then explored and verified how these implementations could be achieved on the proposed Android platform (i.e. using its native security features, existing technologies and third-party tools) with a short-range wireless communication technology. Figure 3.12 depicts the roadmap of this research, its results, the papers produced from the research findings and the frameworks constructed.

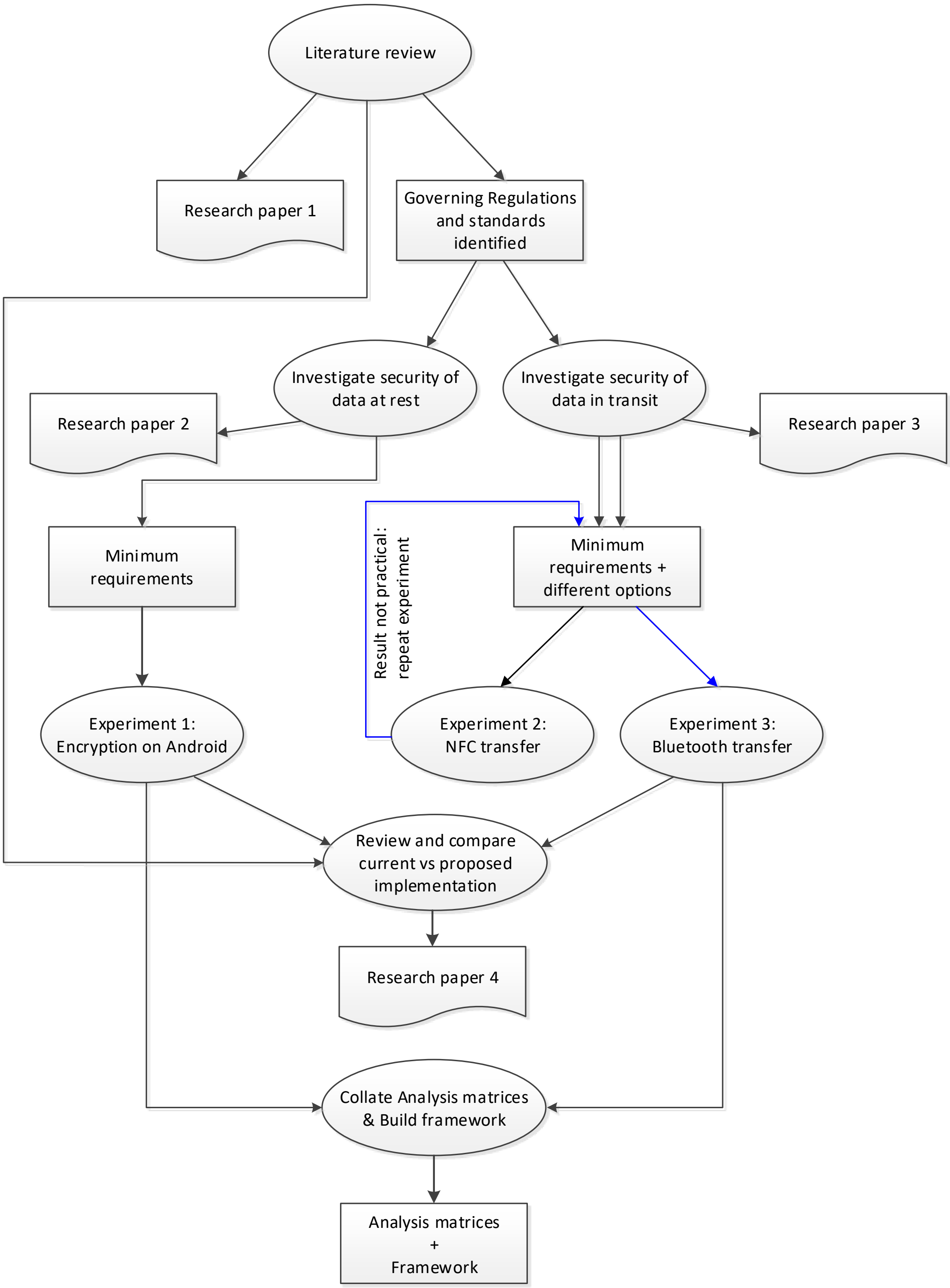

Literature review
Research paper 1
Governing Regulations and standards identified
Investigate security of data at rest
Investigate security of data in transit
Research paper 2
Research paper 3
Minimum requirements
Minimum requirements + different options
Result not practical: repeat experiment
Experiment 1: Encryption on Android
Experiment 2: NFC transfer
Experiment 3: Bluetooth transfer
Review and compare current vs proposed implementation
Research paper 4
Collate Analysis matrices & Build framework
Analysis matrices + Framework

Figure 3.12: Research roadmap

3.7 Data analysis

Using qualitative research methods, a significant amount of analysis activity was implicitly involved in the data collection for both Subsidiary Research Questions. The study for Subsidiary Research Question 1 analysed the applicable acts, regulations and standards and transformed these legal explanations into a set of practical understanding and security requirements.

The second Subsidiary Research Question involved analysing the experimentation outcomes on the Android's native security features and short-range wireless communication technologies (i.e. NFC and Bluetooth) which potentially fulfil the security requirements. The review process validated the study outcomes by triangulation at the end of each study. During the triangulation process (i.e. expert supervisory review) for each study, the collected data, applicable assessment metrics and derived essential criteria were reviewed. The feedback from this review was then incorporated back into the study, which resulted in either making necessary adjustments prior to the next iteration of experiment or proceeding to the next stage of the study.

Table 3.1 depicted the generic template format of the analysis matrices (i.e. Table 4.1, 4.2 and 7.1) which were populated by the research findings from the two studies involving Subsidiary Research Questions 1 and 2. The “Feature or usage”, “Jurisdiction”, “Governing regulations, standards & specifications” columns of the Table 4.1, 4.2 and 7.1 were populated by the research findings from answering Subsidiary Research Question 1. In addition, findings from Subsidiary Research Question 1 also populated the "Requirements mandated and impact on proposed fully electronic prescribing process" and "Jurisdiction’s readiness for the fully electronic ETP solution" columns of the Table 4.1, and “Security requirements mandated” column of the Table 4.2.

Investigations for Subsidiary Research Question 2 were then conducted for each of these security requirements recorded in Table 4.2. The “Technology conforming to the mandated requirement” column of the Table 7.1 contains the research findings from a series of iterative investigations, as well as experimentation outcomes fulfilling the mandated requirements identified in the prior stage of the research (i.e. the investigation to answer the Subsidiary Research Question 1). These iterative investigations and experimentations also examined the practicality of the outcomes from development, deployment and operational perspectives.

The researcher then performed the analysis based on the holistic knowledge and understanding acquired from these studies. Once the supervisory expert review panel had verified the analysis outcome and the conclusion drawn, a framework was constructed to guide the development of an Android mobile ETP application in compliance with security requirements of the Australian healthcare industry. Once again, this synthesised product was also subjected to review by the supervisory expert panel for further adjustment.

Table 3.2: Template of the Analysis matrix

No	Feature or usage	Jurisdiction	Governing regulations, standards & specifications	Requirements mandated and impact on proposed fully electronic prescribing process (or) Security requirements mandated	Jurisdiction's readiness for the fully electronic ETP solution (or) Technology conforming to the mandated requirement
	(1) Legislative and regulatory requirements				
1	…	…	…	…	…
2	…	…	…	…	…
	Section (1): Security requirements for electronic prescription from data at rest perspective				
3	…	…	…	…	…
4	…	…	…	…	…
	Section (2): Security requirements for electronic prescription from data in transit perspective				
5	…	…	…	…	…
6	…	…	…	…	…

3.8 Limitations

Conducted in fulfilment of the requirements for the Professional Doctorate Degree in Information Technology (DIT), this thesis inherently focuses less intensely on the research aspect so as to emphasise making a difference in the workplace and/or profession via directing and informing change (“Difference between Academic and Professional Doctorate Degrees”, 2017; “Professional Doctorates”, n.d.), as well as the practicality of the research outcome. The shorter allocated timeframe for the research element in the DIT course (i.e. 1.5 years for DIT compared to 4 years for PhD) certainly imposed some limits on various aspects of the research process as a whole compared to those of the PhD research thesis.

Another limitation is the precision of the research outcomes, which can only be as accurate as the assessment metrics allows. If the research conclusion had showed that a framework cannot be built to guide the development of an Android mobile ETP application in compliance with security requirements, synthesising a custom security mechanism was not within the scope of this research. Moreover, this research was not designed to be flexible enough to accommodate provision for future changes in the technologies used in the proposed model or amendments in the relevant laws, regulations and standards. Another significant limitation of this research is that it provides no insight into the potential use of iOS despite its large consumer base comparable to Android OS.

This research did not explore its potential impacts and usefulness beyond the Australian Healthcare Industry despite its prospective applicability in countries with ETP capability. The research findings of Subsidiary Research Question 1 only concerned the current acts, regulations, standards and publications issued by the Department of Health and Aging (DoHA), the Australian Digital Health Agency (ADHA previously NEHTA) and Standards Australia. Although the research findings of Subsidiary Research Question 1 are generally applicable to any fully electronic prescription transfer applications in the Australian healthcare industry, both Subsidiary Research Question 2 and the Primary Research Question strictly intended to explore the Android’s native security features and other candidate technologies which were currently available on the market, and to build a framework using those features and technologies. Despite the widespread use of the prior versions of Android Operating System (OS) on the market, the exploration and experimentations for Subsidiary Research Question 2 were only concerned with the Android OS version 4.0 or later.

In addition to the abovementioned limitations specific to this particular study, there were also limitations inherited from the chosen research methodology. Some inherent limitations due to being a qualitative research are:

- The credibility and quality of the research findings may be limited by the competence of the analysis process (Dawson, 1979, 1982; Ginsberg, 1990; Kirk & Miller, 1986; Kvale, 1989a; LeCompte & Goetz, 1982).
- The relationship of the researcher to the research may limit the researcher’s ability to interpret data meaningfully (May, 2002).
- The credibility and quality of the research conclusions may be influenced by the distinct possibility of researcher bias (Miles & Huberman, 1994).

This research was initially designed to address these limitations by employing the triangulation process using a panel of external/independent domain experts at the end of each stage. However, having two research supervisors with active involvement in the research context (i.e. one actively involved with both national and international digital health systems and eHealth standards, the other with extensive experience and knowledge in clinical and health IT industry) rendered the need for such expert panel redundant.

The research findings at the end of each stage were therefore verified by the internal “supervisory expert review” process before proceeding to the next stage. Furthermore, the final outcomes were also reviewed by the supervisory panel of domain experts in order to strengthen the credibility or value of the research’s outcomes.

CHAPTER 4. RESEARCH RESULTS AND PROPOSED SOLUTION

4.1 Overview

This chapter begins by presenting the research findings from the analysis of the various jurisdictions' legislation and standards conducted for Subsidiary Research Question 1. Subsequently, and based upon the knowledge gathered from the second chapter, Literature Review, this fourth chapter proposes a potential alternative solution to the current ETP implementation (i.e. the mobile electronic prescription transfer application on Android smartphone) and, more so, sought additional details on the technologies involved in the proposed solution for further assessment.

This chapter presents the research findings in an extended form, although a significant part of the chapter's content has been published in a more concise form through four papers listed in Appendix-A (i.e. published in chronological order).

4.2 Research Results

This research found that although the Commonwealth Electronic Transaction Acts 1999 and those jurisdictional Electronic Transaction Acts at the various state and territory levels enable the use of electronic means in general, they do not directly impose or mandate any specific requirements on the electronic prescribing process. Both Table 4.1 and 4.2 list the research outcomes in a consolidated form for verification via potentially iterative experimentations.

The analysis of the experiments subsequently promoted the derivation of a conclusion and ultimately led to the development of the framework. All the research outcomes listed in these two matrices were categorised into three groups as listed below:

(1) Each jurisdiction's readiness for the fully electronic ETP solution (Table 4.1)

(2) Security requirements for electronic prescription from the data at rest perspective

(3) Security requirements for electronic prescription from the data in transit perspective (Table 4.2)

Based on the research findings for Subsidiary Research Question 1, various acts, regulations and standards influencing the use of electronic prescription and how they affected the use of a fully electronic prescribing system (i.e. jurisdictions' regulatory readiness for fully electronic prescription) were listed in the Table 4.1.

The research findings from Subsidiary Research Question 1 also populated the first four columns (from left to right) of Table 4.2. In fact, the fourth column of Table 4.2 recorded the security requirements for electronic prescription information translated from those regulatory mandates by this research. Fundamentally, this defined the acceptance criteria or the minimal security requirements for the proposed mobile prescription transfer model. The last column of Table 4.2 documents the outcomes from the further research and iterative experimentations conducted for answering Subsidiary Research Question 2.

Effectively, these documented experimentation outcomes were to indicate which candidate technology and third-party tools would comply with the security requirements listed in the fourth column of Table 4.2 (i.e. security requirements translated/derived from the regulatory mandates).

Table 4.1: Analysis matrix of each jurisdiction's readiness for fully electronic ETP solution

No.	Feature or usage	Jurisdiction	Governing regulations, standards & specifications	Requirements mandated and impact on proposed fully electronic prescribing process	Jurisdiction's readiness for the fully electronic ETP solution
1	Use of electronic prescription	Western Australia	***Poisons Regulation 1965*** 32A, 32B and Appendix K	This enables the use of fully electronic prescribing process	Ready for proposed fully electronic solution
2	Use of electronic prescription	Queensland	***Health (Drugs and Poisons) Regulation 1996*** 82 (1)(b), 193 and 197 (2)	This enables the use of fully electronic prescribing process	Ready for proposed fully electronic solution
3	Use of electronic prescription	New South Wales	***Poisons and Therapeutic Goods Regulation 2008*** 35 (2)(b) and 80 (2)(b)	This enables the use of fully electronic prescribing process	Ready for proposed fully electronic solution
4	Use of electronic prescription	Australian Capital Territory	***Medicines, Poisons and Therapeutic Goods Regulation 2008*** The "Note" part of the section 40	No special mention on the use of electronic system	Ready for proposed fully electronic solution
5	Use of electronic prescription	Victoria	***Drugs, Poisons and Controlled Substances Regulations 2006*** 26 (1)(b)	This enables the use of fully electronic prescribing process	Ready for proposed fully electronic solution

No.	Feature or usage	Jurisdiction	Governing regulations, standards & specifications	Requirements mandated and impact on proposed fully electronic prescribing process	Jurisdiction’s readiness for the fully electronic ETP solution
6	Use of electronic prescription.	South Australia	***Controlled Substances (Poisons) Regulations 2011*** 33 (5)	This enables the use of fully electronic prescribing process	Ready for proposed fully electronic solution
7	Use of electronic prescription	Northern Territory	***Medicines, Poisons and Therapeutic Goods Regulation*** The section “*Note for Division 1*”	This enables the use of fully electronic prescribing process	Ready for proposed fully electronic solution
8	Use of electronic prescription.	Tasmania	***Poisons Regulations 2008*** 16 (1) and (2)	This enables the use of fully electronic prescribing process	Ready for proposed fully electronic solution
9	Implies prescriber's hand-written signature not required in electronic prescription	Western Australia	***Poisons Regulation 1965*** Schedule 4: 37. (1A) (1B) Schedule 8: 51. (1A) (1B) and (1C)	This enables the use of fully electronic prescribing process	Ready for proposed fully electronic solution
10	Implies prescriber's hand-written signature is not required in electronic prescription	Queensland	***Health (Drugs and Poisons) Regulation 1996*** 79 (7) and 190 (5)	This enables the use of fully electronic prescribing process	Ready for proposed fully electronic solution

No.	Feature or usage	Jurisdiction	Governing regulations, standards & specifications	Requirements mandated and impact on proposed fully electronic prescribing process	Jurisdiction’s readiness for the fully electronic ETP solution
11	Implies prescriber's hand-written signature is not required in electronic prescription	South Australia	***Controlled Substances (Poisons) Regulations 2011*** 33 (5) and 34 (3)	This enables the use of fully electronic prescribing process	Ready for proposed fully electronic solution
12	Implies prescriber's hand-written signature is not required in electronic prescription	Tasmania	***Poisons Regulations 2008*** 16 (5)	This enables the use of fully electronic prescribing process	Ready for proposed fully electronic solution
13	Prescriber’s signature is required.	New South Wales	***Poisons and Therapeutic Goods Regulation 2008*** 35 (2) and 80 (2)	Unless there is regulatory change for the use of electronic/digital signature in prescriptions, this requirement prevents the use of fully electronic prescription	May require regulatory change as the regulation requires prescriber’s signature. But it neither explicitly approves the use electronic/digital signature nor exempt electronic prescription from requiring written signature.
14	Prescriber’s signature is required.	Australian Capital Territory	***Medicines, Poisons and Therapeutic Goods Regulation 2008*** 40 (a) and the “Note” part of the	Unless there is regulatory change for the use of electronic/digital signature in prescriptions, this requirement prevents the use of	May require regulatory change as the regulation requires prescriber’s signature. But it neither explicitly approves the use electronic/digital signature

No.	Feature or usage	Jurisdiction	Governing regulations, standards & specifications	Requirements mandated and impact on proposed fully electronic prescribing process	Jurisdiction's readiness for the fully electronic ETP solution
			section 40 (a)	fully electronic prescription	nor exempt electronic prescription from requiring written signature.
15	Prescriber's signature is required.	Victoria	***Drugs, Poisons and Controlled Substances Regulations 2006*** 26 (3)(d)	Unless there is regulatory change for the use of electronic/digital signature in prescriptions, this requirement prevents the use of fully electronic prescription	May require regulatory change as the regulation requires prescriber's signature. But it neither explicitly approves the use electronic/digital signature nor exempt electronic prescription from requiring written signature.
16	Prescriber's signature is required.	Northern Territory	***Medicines, Poisons and Therapeutic Goods Regulation*** 8. (m)	Unless there is regulatory change for the use of electronic/digital signature in prescriptions, this requirement prevents the use of fully electronic prescription	May require regulatory change as the regulation requires prescriber's signature. But it neither explicitly approves the use electronic/digital signature nor exempt electronic prescription from requiring written signature.

Table 4.2: Analysis matrix of Security requirements for electronic prescription information

No.	**Feature or usage**	**Jurisdiction**	**Governing regulations, standards & specifications**	**Security requirements mandated**	**Technology conforming to the mandated requirement**
	Section (1): Security requirements for electronic prescription from data at rest perspective				
1	Encryption of the electronic prescription	Nationwide	***ATS 4888.2-2013*** section 5.3.6	The electronic prescription is to be encrypted using a symmetric key derived from DAK	**?**
2	Saving the DAK and any of its derived keys on any permanent storage	Nationwide	***ATS 4888.2-2013*** section 7.3.3	Minimum of 128 bit encryption for storing DAK or any of its derived keys on any stable storage	**?**
3	HL7 message structure for electronic prescription	Nationwide	***AS 4700.3-2014***	Mandated HL7 message structure for the electronic prescription	**?**
	Section (2): Security requirements for electronic prescription from data in transit perspective				
4	Security of electronic prescription	Nationwide	***ATS 4888.2-2013*** section 5.3.5	Security of data in transit between ETP service participants are specific to the implementation ‘platform’	**?**

From the legislative and regulatory perspectives, this research revealed that although the use of electronic prescription was supported in all jurisdictions, the use of electronic/digital signature for the electronic prescription in place of prescriber's written signature was neither explicitly approved nor prohibited in ACT, NSW, VIC and NT.

These states' regulations mandated that the prescriber's signature be present on the prescription but did not specify whether it has to be a handwritten signature or electronic/digital signature of the prescriber. Since the current ETP implementation also produces the printed prescriptions, serving dual-purpose as a legal prescription document as well as a transfer mechanism for DAK from the prescriber to the dispenser (i.e. serving as the printed prescription notification), the presence of the prescriber's written signature on the printed prescription also legalises it by complying with these regulatory requirements. However, once it has been converted to a fully electronic prescribing process it would be impossible to accommodate the prescriber's written signature, necessitating minor amendments/modification to the regulation before transitioning to the fully electronic prescribing process.

Despite the mixed results obtained (i.e. non-definitive outcomes for the presence of prescriber's signature in written/digital format) from Subsidiary Research Question 1 (i.e. from the legislative and regulatory perspectives), the experimentations conducted for Subsidiary Research Question 2 revealed that the proposed mobile solution complied with all the security requirements mandated by the existing standards and specifications governing the current ETP implementation.

In addition, while the proposed mobile solution (any fully electronic prescribing process in this case) does not fully adhere to some jurisdictions' regulatory mandates for the presence of the prescriber's signature, the Electronic Transaction Act recognises and approves alternative ways to use written signature in identifying a person and indicating the approval of the information contained/communicated ("The Electronic Transactions Act 1999", n.d.).

Therefore, this research was justified and hence proceeded further by proposing a cheaper, if not completely cost-free, fully electronic prescription transfer solution with comparable security assurance (i.e. comparable to the current ETP implementation using PES systems) which utilised the patient's Android smartphone as an alternative secured transfer medium.

4.3 The proposed alternative solution using Android smartphones

The Electronic Transactions Act 1999 primarily supports the creation, transfer and storage of the electronic prescription, amendments 51(1A), 51(1B) and 51(1C) of the Poisons Regulations 1965 for Western Australia effectively allows an electronic prescription to be a legal document without the prescriber's written signature when issued electronically. These two amendments, combined with other changes in the governance of the Commonwealth, states and territories to enable eHealth, are sufficient to support an ETP Level 3 model.

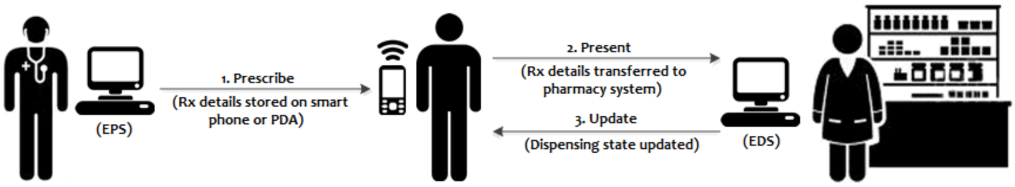

(EPS)
1. Prescribe
(Rx details stored on smart phone or PDA)
2. Present
(Rx details transferred to pharmacy system)
3. Update
(Dispensing state updated)
(EDS)

Figure 4.1: Proposed fully-electronic mobile prescription transfer process (Htat, Williams, & McCauley, 2015)

In the proposed fully electronic mobile prescription transfer model, the EPS generates an electronic prescription, encrypts it using the DAK as per the data security conformance guidelines in ATS4888.2, encrypts the DAK with the 128-bit symmetric encryption and then transfers it to the patient's mobile device (i.e. Android smartphone) through a wireless connectivity using either NFC or Bluetooth.

The encrypted electronic prescription is stored on the mobile device (i.e. the patient's or agent's Android smartphone) in the same way in which it is stored within the PES in the current prescribing model. When the mobile device is presented at the pharmacy by the patient/agent, the encrypted prescription, together with the DAK, is transferred to the pharmacy system. The prescription is then decrypted by the pharmacy system using the DAK. This proposed fully electronic mobile ETP transfer model bypasses the PES entirely by using the mobile device as the transfer medium for the electronic prescription.

Once the medication has been dispensed, the pharmacy's EDS uploads the dispensing information into the NPDR. In this proposed mobile ETP model the prescription is issued and transferred in fully-electronic form, thus being exempted from the requirement to have the prescriber's written signature in accordance with the various acts and regulations governing the Poisons and Therapeutic Goods for each jurisdiction (e.g. section 51(1A), 51(1B) and 51(1C) of the Poisons Regulations 1965 in Western Australia).

This proposed ETP transfer model supports ETP adoption Level 3 as long as there is a fully electronic mechanism to securely transfer the electronic prescription from the prescriber's EPS to the mobile storage device and from the mobile storage device to the dispenser's EDS. This proposed mobile ETP model is envisaged to use Near Field Communication (NFC) or Bluetooth technology as the alternative prescription transfer mechanism.

NFC was designed for use in close proximity (i.e. up to a few centimetres) for secure data transfer and supports strong security features that facilitate the highly secure transfer and storage of data. The NFC technology's reliability and practicality is evident by its use in the banking industry, including its use by the Commonwealth Bank for its product, Tap & Pay. Nevertheless, this preference of employing NFC for data transfer was not solely based on the technical viability but also on the consumer acceptance of and confidence in the technology. NFC's simplicity from a user perspective enables easy information sharing and NFC is now enabled on the majority of recent model mobile phones by various manufacturers ("NFC phones: The definitive list", 2016).

Bluetooth, on the other hand, is a mature, short-range wireless communication technology with widespread support from almost all mobile phone manufacturers and with many applications in the healthcare industry ("Medical & Health", 2017; "Mobile Phones & Smart Phones", 2017). With the advent of Bluetooth Low Energy (Bluetooth LE) in recent years, it has extended its application to millions of medical devices and countless Internet-of-Things (IoT) devices ("Bluetooth", 2016). As the global standard enabling the IoT by assuring the connectivity between various devices from various industries (*ibid*), it is also a strong candidate technology for the proposed mobile ETP model.

In the current hybrid ETP model, the PES makes uploaded prescriptions available to dispensers and also prevents access to prescriptions which have been cancelled, expired or fully dispensed. For the latter purpose, PES updates the dispensing state of each prescription after each dispense.

In the proposed model, the smartphone utilised as the mobile storage device makes the prescription available to the dispenser and then the dispensing state of the prescription is updated by the dispenser's EDS directly to the mobile storage device. Due to the connectionless nature of the proposed model, cancelling the prescription by the prescriber will require use of an additional service such as SMS to remotely update the dispensing state of the prescriptions stored on the smartphone.

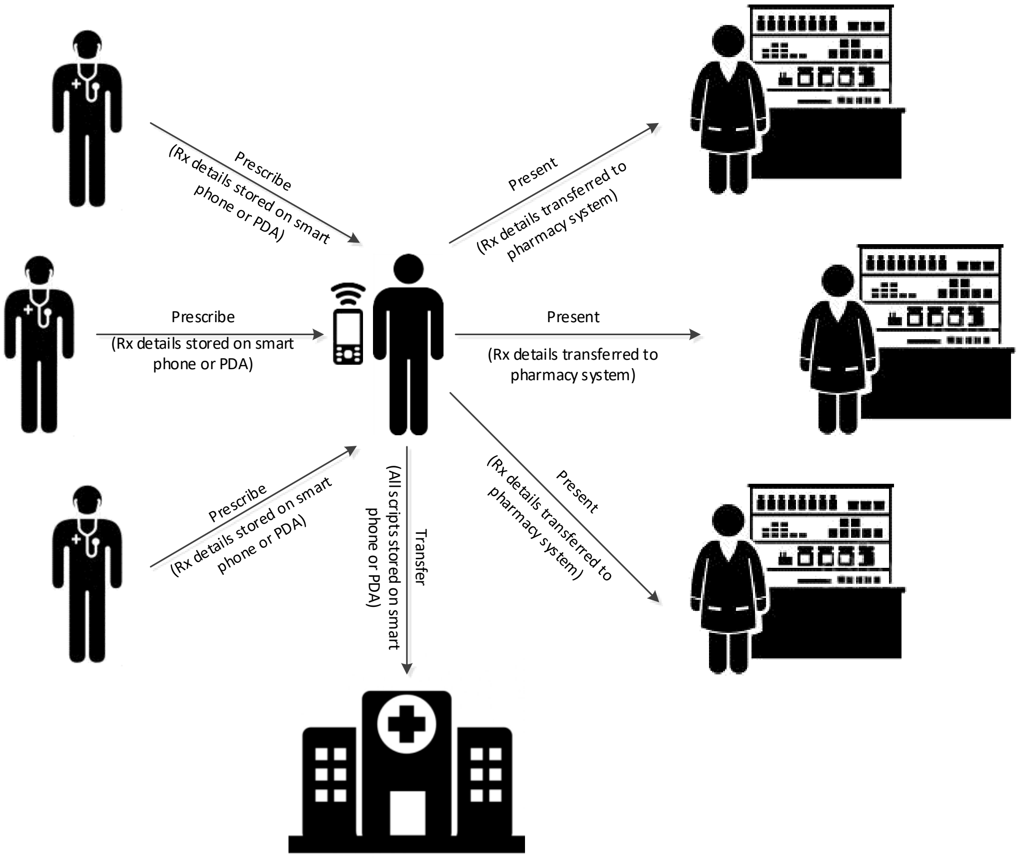

Prescribe
(Rx details stored on smart phone or PDA)
Prescribe
(Rx details stored on smart phone or PDA)
Prescribe
(Rx details stored on smart phone or PDA)
Present
(Rx details transferred to pharmacy system)
Present
(Rx details transferred to pharmacy system)
Present
(Rx details transferred to pharmacy system)
Transfer
(All scripts stored on smart phone or PDA)

Figure 4.2: Sharing of patient's medication history in proposed solution

As described in Figure 4.2, this proposed mobile ETP application also functions as a mobile repository of the patient's medication history, thus making it available to hospitals and other healthcare service providers once the interface for integrating this mobile solution with the hospital information systems and clinical information systems has been implemented. This interface will allow direct transfer of the patient's full medication history from the patient's smartphone to the hospital/clinical information system. Such access to the patient's complete medication history would be of tremendous clinical advantage to the healthcare professionals in delivering better quality of care, substantially benefiting both patients and the healthcare providers.

Further assessments to determine whether this proposed mobile ETP solution complies with the mandated security requirements for electronic prescription will require further detailed investigations and potentially iterative experimentations on the security measures and the governing standards of the potential candidate technologies such as the Android operating system's encryption capability (Chapter 5), NFC (sections 6.1~2 of Chapter 6) and Bluetooth wireless communication (sections 6.4~6 of Chapter 6).

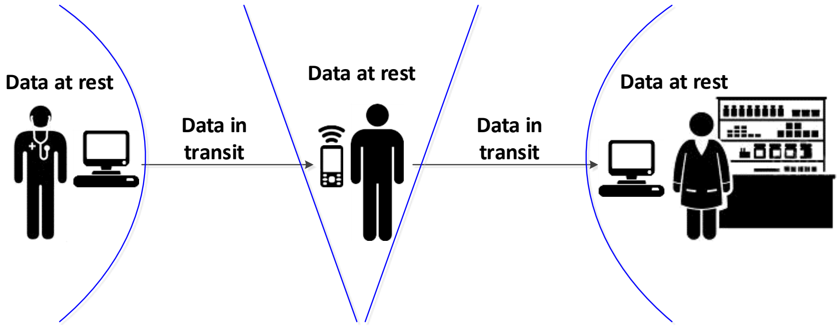


Figure 4.3: Proposed solution from security of data at rest and in transit perspectives

Whilst Table 4.2 of this chapter listed the mandatory security requirements constructed from answering Subsidiary Research Question 1 and section 4.3 proposed an alternative mobile ETP solution, the two subsequent chapters (Chapter 5 and Chapter 6) assess the technologies used in the proposed solution against those identified security requirements and will determine whether it complies with the same regulatory requirements as the current ETP implementation. In the same way that the security of the prescription information in the current ETP implementation was assessed, security of the prescription information in the proposed solution will also be evaluated from the very same security perspectives; the security of the prescription information at rest and the security of the prescription information in transit.

Figure 4.3 depicts how the proposed solution can be divided into different sectors and assesses the security measures from the perspectives of both data at rest and data in transit.

CHAPTER 5. SECURITY OF THE DATA AT REST

5.1 Android Native Security

The investigation conducted in this section studied details of the Android OS's architecture, process and security model and its potentials as a candidate technology for the proposed mobile ETP solution. This section also identified the possible issues associated with Android for the proposed mobile ETP solution.

5.1.1 A brief history and overview

Android is arguably the world most popular mobile operating system platform, rapidly taking the world by storm from its first release in 2009. It is the OS which oddly names each release after sweets and tasty desserts in an alphabetical order. Its market share in Australia from 2013 to 2017 is depicted in Figure 5.1.

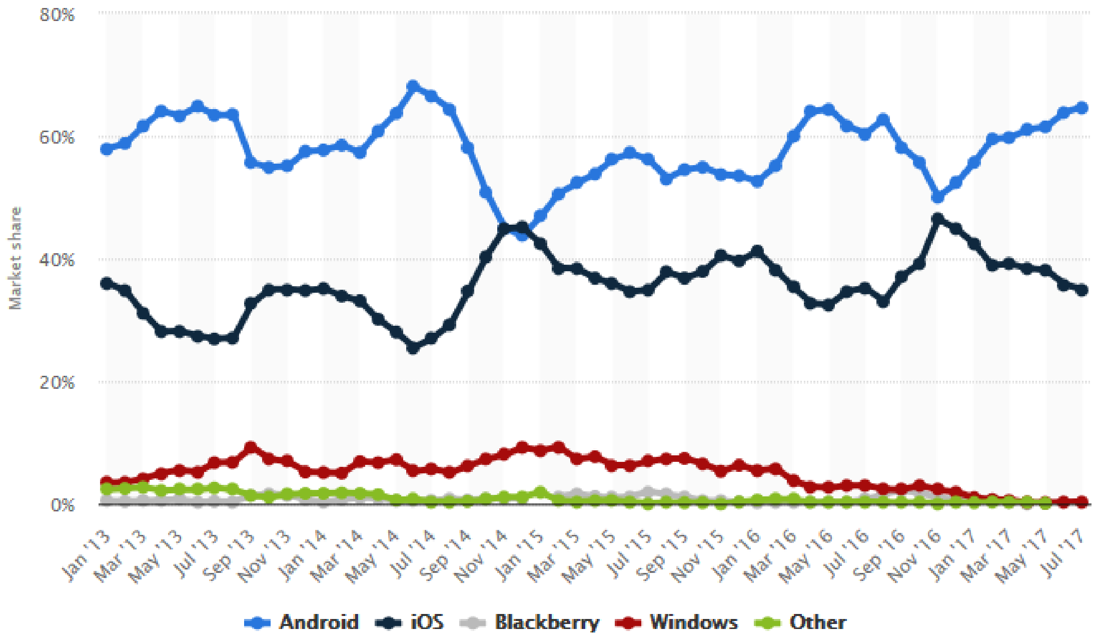


Figure 5.1: Market share by smartphone OS in Australia 2013-2017 ("Market share held by smartphone operating systems in Australia from 2013 to 2017", 2018)

Despite its choice of sweet names for each release, Android ruthlessly conquered the world of mobile operating systems with rigour, as is evident in Figure 5.1.

The Android Inc. of Palo Alto, California, was founded in 2003 by four young computing experts, Andy Rubin, Rich Miner, Nick Sears and Chris White, with the initial intention to develop an operating system for mobile devices, such as digital cameras, which would be aware of both a user's location and their personal preferences (Callaham, 2017). The focus was later shifted to cellular phones as they realised that only targeting digital cameras would have a potentially low demand (Brachmann, 2014).

In 2005, Android Inc. was procured by Google as part of its venture into mobile operating platforms (*ibid*). Foundation of the Open Handset Alliance (OHA) by Google in 2005 was one of the primary forces behind Android's rapid success and dominance of the mobile computing world. The OHA is a consortium of technology manufacturers working together to create open mobile device standards (*ibid*). Wireless telecommunications providers such as T-Mobil, mobile handset manufacturers such as Motorola and High Tech Computer (HTC) and chipset manufacturers such as Texas Instruments and Qualcomm were among the constituent 34 companies when the consortium was founded (*ibid*). Being a product from a coalition of various technology manufacturers dedicated to creating open mobile device standards, compatibility plays a crucial role in Android's ecosystem.

The Android community believes that "Android ecosystem thrives with device compatibility" and this is depicted in Figure 5.2 ("Android Compatibility", n.d.).

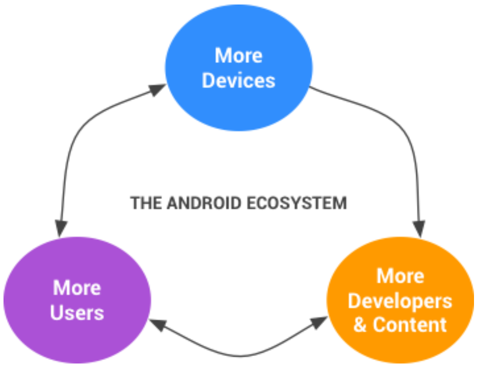


Figure 5.2: Android ecosystem ("Android Compatibility", n.d.)

Before its world dominance, HTC Dream's debut in late 2008 with Android version 1.0 was the Android's first appearance as a commercial smartphone operating system. Then, in April 2009, with HTC Magic, Android introduced its tasty name series to the world with the release of Android version 1.5, more commonly known as Cupcake (Brachmann, 2014; Callaham, 2017). In September 2009, Android version 1.6 (Donut) was released with various significant updates and began its course of dominating the mobile operating system world with the highest adoption rate (*ibid*). Android's rapid popularity and adoption rate is well matched by the pace of development of the operating system itself (Brachmann, 2014).

The fledgling work commenced in 2009 has transformed repeatedly over the past few years and has been refined into the feature-packed suite we see today on many devices of various sizes and shapes (*ibid*). However, despite being the most widely adopted mobile operating system with frequent updates and rapid improvements, it is a far-from-perfect OS with a number of vulnerabilities. In fact, until the release of Android version 5 (Lollipop) it was vulnerable to privilege escalation attack (Avkash, 2014) and it still has numerous vulnerabilities associated with varying levels of complexity and risks ("Android Security Bulletin", 2017). These vulnerabilities do not, however, prevent the Android OS from being one of the best candidates for this research's proposed mobile electronic prescription transfer application.

Among many sources of information, the full extent of the Android's publicly-known vulnerabilities can be found in vulnerabilities databases such as AndroidVulnerabilities.org (AVO) and Varutra's Mobile Vulnerabilities Database (MVD). These vulnerabilities databases and additional information can be linked together by the Common Vulnerabilities and Exposures List (CVE), sponsored by the United States Computer Emergency Readiness Team (US-CERT) ("All vulnerabilities", n.d.; "MVD: Mobile Vulnerability Database", 2013; "Android: Security Vulnerabilities", n.d.). Further information such as the fixes for these vulnerabilities can be found at the U.S. National Vulnerability Database (NVD) (*ibid*).

5.1.2 Architecture and Security

From an architectural perspective, the Android OS was designed to be truly open for developers to build innovative applications whilst offering an application environment with security assurance for users, data, applications, the device and the network ("Security", n.d.). Whilst providing the freedom to implement own/custom device specifications, drivers, interfaces and enhancements, each Android device must pass the Compatibility Test Suite (CTS) to ensure the compatibility, reliability and a high level of quality with consistent user experience ("Android Interfaces and Architecture", n.d.). Figure 5.3 roughly depicts the Android software stack and their core nature/functionalities.

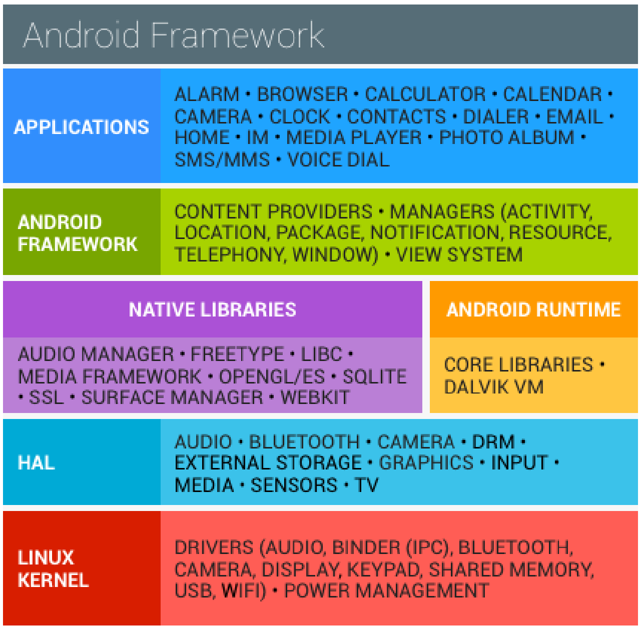

Android Framework
APPLICATIONS
ALARM • BROWSER • CALCULATOR • CALENDAR • CAMERA • CLOCK • CONTACTS • DIALER • EMAIL • HOME • IM • MEDIA PLAYER • PHOTO ALBUM • SMS/MMS • VOICE DIAL
ANDROID FRAMEWORK
CONTENT PROVIDERS • MANAGERS (ACTIVITY, LOCATION, PACKAGE, NOTIFICATION, RESOURCE, TELEPHONY, WINDOW) • VIEW SYSTEM
NATIVE LIBRARIES
AUDIO MANAGER • FREETYPE • LIBC • MEDIA FRAMEWORK • OPENGL/ES • SQLITE • SSL • SURFACE MANAGER • WEBKIT
ANDROID RUNTIME
CORE LIBRARIES • DALVIK VM
HAL
AUDIO • BLUETOOTH • CAMERA • DRM • EXTERNAL STORAGE • GRAPHICS • INPUT • MEDIA • SENSORS • TV
LINUX KERNEL
DRIVERS (AUDIO, BINDER (IPC), BLUETOOTH, CAMERA, DISPLAY, KEYPAD, SHARED MEMORY, USB, WIFI) • POWER MANAGEMENT

Figure 5.3: Android software stack ("Security", n.d.)

Over the past decade, the consumer focus has shifted from desktop to mobile computing devices (West, 2012). Nowadays, mobile phones are so much more than mere telecommunication devices: they have become an essential part of our lives for many other purposes such as social networking, health and fitness and performing financial transactions.

However, in a similar way to security on the Internet of Things (IoT) devices, these mobile devices were not originally designed and built with security as a top priority requirement, despite becoming an integral part our daily life in various aspects including such security sensitive contexts as personal banking and healthcare (Maddox, 2016). In addition to this inherent nature (i.e. security not being a high priority feature by design), the strengths and vulnerabilities of the OS platforms used also contribute significantly to the security factors of the device. In its early days, Android OS was created based on the Linux Kernel version 2.6 with adapted security mechanisms for the mobile and flash memory environment ("Tutorial: Understanding Android's Security Framework", 2010; "Which Android runs which Linux kernel?" 2013). It utilised component-based framework for application development where each of them is made of different types of components, such as Activity, Service, ContentProvider and BroadcastReceiver ("Tutorial: Understanding Android's Security Framework", 2010). This openness is one of Android's most attractive features over other OS platforms, and it also has the least restricted application deployment strategy, which allows applications to be published easily ("Publish Your App", n.d.).

On the other hand, however, this openness also allows publication of malicious applications without scrutiny (*ibid*). Android permits the developers to self-sign their applications for the ease of upgrading or patching their own software, and the applications signed with the same key can request to run with the same user identifier (UID). This mechanism also allows developers to copy data from existing versions without creating complicated interfaces and permissions.

5.1.3 Process and Security Model

In Android OS architecture, just a small amount of Android OS code runs as root (i.e. superuser with unrestricted control over the device) and all the rest of the OS code above the Linux Kernel is restricted by the Application Sandbox ("Security", n.d.). Then, all the applications are isolated from each other by individually running in separate processes under distinct low-privileged UID. Each of these UIDs has a distinct set of permissions limiting them from accessing other's data or code (Felt, Chin, Hanna, Song & Wagner, 2011).

Handling of the Application Programming Interface (API) calls are carried out in three steps through the layers of the Android's OS architecture (see Figure 5.4

for details), and each call consists of a permission check determining the caller's privileges to access that particular API prior to the actual invocation. In the Android version 2.2, there were 134 permissions categorised into four different levels, such as Normal, Dangerous, Signature and SignatureOrSystem, according to their associated risks/threats, and security was primarily achieved by enforcing these permissions at various points (Felt, Chin, Hanna, Song & Wagner, 2011). Figure 5.4 explains the Android's process and security architecture.

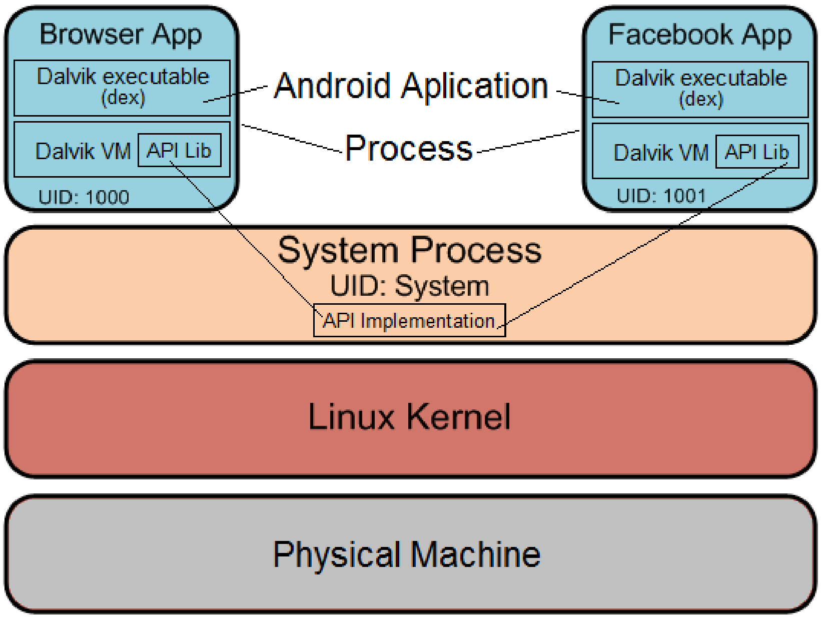


Figure 5.4: Android's Security and Process Model

The Android API framework consists of two parts: a library that resides in each application's virtual machine and the implementation of the API that runs in the system process (Felt, Chin, Hanna, Song & Wagner, 2011). It handles all the API calls in three steps as mentioned below:

1. The application invokes the API library in its virtual machine (VM)
2. The library then invokes the private interface, which is a Remote Procedure Call (RPC) stub in the same library
3. The RPC stub finally initiates an RPC request with the system process that asks a system service to perform the desired operation

Another simple yet effective mechanism supplementing the process isolation method is the use of manifest permissions assigned to applications during the installation-time ("Application Fundamentals", n.d.). This demands that every application declare upfront which permissions it requires, and then during the installation the user is notified which permissions the application will be granted. These permissions/privileges determine what the application can perform such as taking pictures, using Global Positioning System (GPS) or making phone calls.

The user permits or denies the requested permissions during the installation of the application via a dialog and the application's permissions are then stored in the AndroidManifest.xml file, which cannot be changed after the installation process. A user's denial to grant permission to the application will result in cancellation of that installation process. This security mechanism allows users to have control over their privacy and helps reduce the impact of bugs, as well as vulnerabilities in the applications. These permissions are also used in controlling access to privacy-related and security-related parts of API invocations (*ibid*).

However, this mechanism would be ineffective if the application request more permissions than it actually requires, or the user does not recognise the importance of this notification and its consequences (Felt, Chin, Hanna, Song & Wagner, 2011).

5.1.4 Reasons for being a good candidate for the proposed solution

Since one of the intentions of this research was to find a viable alternative transfer mechanism for the electronic prescription with minimal infrastructural requirements and associated cost, the Android's huge market base (see Figure 5.1) enables it to be the top potential candidate for this research. Once this research has proven the suitability and practicality of the proposed mobile electronic prescription transfer model on Android mobile devices, Android's huge consumer base will create enough traction in the Australian healthcare industry for the major players to give their attention to this alternative approach, ultimately becoming an alternative transfer mechanism for electronic prescription.

Android's assurance for compatibility is another good reason for Android being an excellent candidate for this research's proposed solution. It is impossible for any device manufacturer to speculate all the software that users could ever conceivably need and provide them as pre-installed applications with their products.

Therefore, Android was designed as an open and secure environment for running the aftermarket applications developed by the third-party developers to write the application users wanted. The Android Open Source Project (AOSP) aims at making the application development as easy and open as possible (“Security”, n.d.; “Android Compatibility”, n.d.; Hildenbrand, 2017). At the same time, the necessity to comply with the Android Compatibility Definition Document (CDD) and pass the Compatibility Test Suite (CTS) ensures the compatibility among various devices and operating system platforms. This assurance guaranteed the compatibility and it was a significant incentive for the choice of the Android platform (“Security”, n.d.; “Android Compatibility”, n.d.) for this research’s proposed solution.

As the most popular mobile operating system, with the highest adoption rate and largest consumer base, the Android inevitably has extensive developer community support. This support was another viable reason for choosing the Android platform to be a candidate for this research. Last but not the least, the Android’s developer friendliness, its open architecture and its availability of abundant tools and frameworks in the market made it a very natural and easy choice.

5.1.5 Potential issues of Android for the proposed solution

Despite its numerous benefits, the Android’s openness also attracted individuals and organisations which had malicious intent. Despite other potential vulnerabilities, the following ones could pose serious impacts on the security of the mobile ETP application’s data and hence require the devising of counter measures for securing against them.

5.1.5.1 Vulnerabilities as of 2013

As previously mentioned, the vulnerabilities listed below had significant impacts on the sensitive data stored by the mobile ETP application. However, this assessment was initially performed at the early stage of the research in 2013, and the following findings are those of that time.

Lack of device level data encryption: Device level encryption mainly protects data from unauthorised access via Android Debug Bridge (ADB) port, dumped device image or booting from the SD card. Until 2014, Android stored data unencrypted both on the internal file system and on the removable mass storage media such as Secure Digital (SD) memory card (“Encryption”, n.d.; Raphael, 2017). Whilst the data stored on the internal file system of the device received little protection by the process isolation and permission control mechanisms, the data on the removable media was unprotected due to the use of Virtual File Allocation Table (VFAT) file system for the ease of data transfer between different devices (“Mobile Application Security on Android”, 2009). However, the device level encryption feature was supported in some devices running Android version 2.3.4 (“Gingerbread”) such as Samsung Galaxy S II and Motorola Droid Bionic, tablets running Android 3.0 (“Honeycomb”) and Android 4.0 devices (“Ice Cream Sandwich”) (“Android 4.0 Platform Highlights”, n.d.). In the Android 4.0, the encryption of the removable storage such as SD card was not supported natively.

User rooting the device: Rooting offers freedom or power at the expense of security. It allows side-loading, bypassing the restrictions imposed by the carrier, use of third-party software and custom Read-Only Memory (ROM). Despite the user becoming more powerful locally, rooted Android devices are likely to have a few or all of the following vulnerabilities:

- Rooted device may no longer receive over-the-air (OTA) updates from the carrier, exposing the devices’ vulnerabilities to new threats due to being left unpatched (Kassner, 2011).
- On a rooted Android phone the hardware is the only limitation for an application with root access. For instance, the mobile OS boot-loader, other programs' private data, system settings and files and SMS are all at the mercy of an application with the root access.
- A rooted application can also hide itself from the system and user, or pretend to be uninstalled while being perfectly well and alive. (“What are the security disadvantages of rooting an Android phone?”, 2011)
- The rooting process of a device usually leaves the ADB port open, providing an open invitation to all other perpetrators to bypass security measures like screen lock. (“Issue 17918: Device can be accessed via ADB when encryption is enabled”, 2011)

- On a rooted android phone device, the mobile OS system is more vulnerable to malware due to a weakened overall security and integrity of the device.

Privilege Escalation: All Android versions so far are still subject to this vulnerability. This vulnerability enables an infected but seemingly harmless application to install additional applications with a lower level of permission, allowing operations such as accessing call records, texts, Web browsing history and storage media without the user's install-time approval for those permissions (Chavez, 2011; Webster, 2011).

5.1.5.2 Vulnerabilities as of 2016

Android's vulnerabilities and their impacts on research were revised in 2016 during the experimentation and analysis stage of the research thesis. Most of the findings were fairly different to those from the initial investigation and therefore their impacts on this research have been updated accordingly.

The full-disk encryption was supported in Android version 4.0+ and, since the number of the devices running prior to Android version 4.0 is only 2.3% in total, the impact of the vulnerability due to the lack of device level data encryption is now significantly low. In the Android version 6.0, the removable storage such as the SD card can be treated as internal storage and is therefore encrypted by default. In prior versions, however, it was up to the device manufacturer building the firmware to enable the encryption feature for the SD card, although Android provided the capability for filesystem encryption ("Does Android's Full Filesystem Encryption also encrypt the SD card?", 2012).

Despite the various changes in the Android operating system platform over the past a few years, the vulnerabilities associated with user rooting the Android device remains the same and still pose serious security risks for its data and applications.

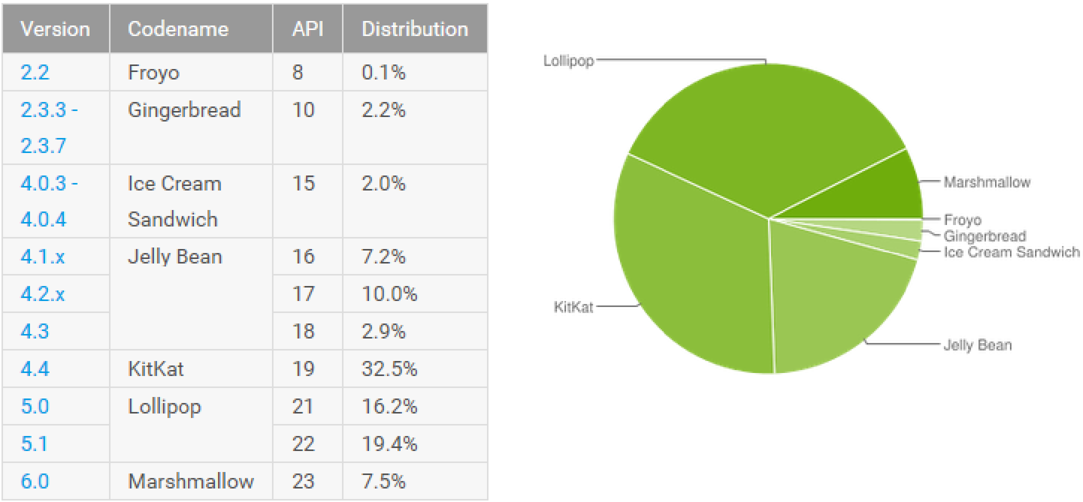
Many privilege escalation vulnerabilities have been identified and rectified either as a patch for the current version or in the later version. At the time of this research, the most recent privilege escalation vulnerability patched up in Android version 5.0 (Lollipop) was the one due to the flaw resided in the java.io.ObjectInputStream (Avkash, 2014). However, since these vulnerabilities originated from various sources such as logic bugs in the applications, bugs in the Original Equipment Manufacturer (OEM) frameworks or in the Kernel drivers, it is impossible to say that privilege escalation vulnerabilities are a thing of the past even though it would appear there are none at large at present.

Another important factor in Android security is the Linux Kernel version on which the Android was built. Linux Kernel sits at the bottom of the Android software stack as shown in the Figure 5.4 and generally Android inherits its strength and weaknesses from the Linux Kernel on which it was built. Table 5.1 lists which Android versions make use of which Linux Kernel version for further investigation. However, there is no hard and fast rule defined in the association or dependency between Android and Linux Kernel versions since devices from different manufacturers running the same Android version can run on different Linux Kernels. Table 5.1 merely lists the common association or dependency between Android and Linux Kernel versions.

Table 5.1: Android version and Linux Kernels (“Which Android runs which Linux kernel?”, 2013)

Android Version	**Name**	**API Level**	**Linux Kernel in AOSP**
1.5	Cupcake	3	2.6.27
1.6	Donut	4	2.6.29
2.0/1	Éclair	5-7	2.6.29
2.2.x	Froyo	8	2.6.32
2.3.x	Gingerbread	9, 10	2.6.35
3.x.x	Honeycomb	11-13	2.6.36
4.0.x	Ice Cream Sandwich	14, 15	3.0.1
4.1.x	Jelly Bean	16	3.0.31
4.2.x	Jelly Bean	17	3.4.0
4.3	Jelly Bean	18	3.4.39
4.4	Kit Kat	19, 20	3.10
5.x	Lollipop	21, 22	3.16.1
6.0	Marshmallow	23	3.18.10

In addition, the Figure 5.5 shows the distribution of various Android versions currently being used. This information is vital in estimating the impact of certain vulnerabilities based on a specific version of Android.



Version	Codename	API	Distribution
2.2	Froyo	8	0.1%
2.3.3 - 2.3.7	Gingerbread	10	2.2%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	2.0%
4.1.x	Jelly Bean	16	7.2%
4.2.x		17	10.0%
4.3		18	2.9%
4.4	KitKat	19	32.5%
5.0	Lollipop	21	16.2%
5.1		22	19.4%
6.0	Marshmallow	23	7.5%

Figure 5.5: Distribution among Android versions (“Dashboards”, n.d.)

5.1.6 Conclusion

Since one of this research’s objectives was to eliminate the requirement of the special supporting infrastructure along with its associated costs, the Android’s existing strong consumer community made it a suitable candidate for this research. Android’s openness in its architectural design and its firm support for the development of innovative applications by the third-party developers was another major driving force behind the selection of Android for this research. Its well-established development community with widely supported compatibility among various devices from different manufacturers and its assurance for the security of data and application whilst providing a consistent user experience with a high level of quality are the added benefits of using the Android platform. Therefore, the vulnerabilities identified did not prevent Android OS from being selected as the candidate OS because the strength/benefits it offers outweighs its vulnerabilities for this research.

All the research findings so far indicate that the use of Android as the OS platform for the proposed mobile ETP application will benefit both the healthcare industry and its already-established large consumer base. Whether it has the necessary encryption capability for securing electronic prescriptions is yet to be determined by the experiments in the following section (section 5.2).

5.2 Experiment 1: Android's Encryption – Security of the data at rest

5.2.1 Overview

The "Confidentiality of data at rest" section of the ATS4888.2-2013 (i.e. section 5.3.6 of ATS4888.2-2013) mandates that the payload of the Clinical Document managed by the Prescription Exchange is to be encrypted using a symmetric key derived from the Document Access Key (DAK). In addition, the "Data security conformance points ETP 22-2" section of the ATS4888.2-2013 also mandates that DAK and any of its derived cipher keys need to be encrypted with a secret cipher key of at least 128 bits before being stored on any stable storage.

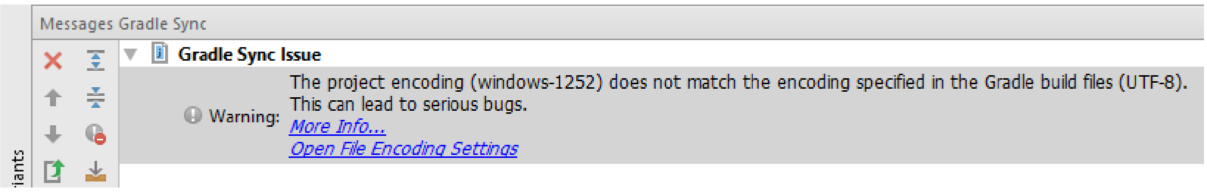
Therefore, the aim of this experiment was to verify that the Android OS platform can support the required encryption capabilities with adequate performance. The prototype developed to test the Android's encryption was initially executed using the Android device emulator. Then, in order to verify how it performs on the actual Android smartphones, it was deployed and tested on two Android phones from two different manufacturers, HTC One and Samsung Galaxy A3 model smartphones.

5.2.2 Experiment details

The prototype application for this experiment was developed using the Android Studio package, which was downloaded from the official Android Studio website ("Android Developers", n.d.), and the development environment was configured to use the Android version 5.0.1 with API 21. The installation and configuration process for this experiment went seamlessly compared to the researcher's prior experience with earlier versions of Eclipse Integrated Development Environment (IDE) bundled with Android Developer Tools (ADT).

Initially, the development environment for this experiment was set up using a laptop with 64-bit Windows 7 Operating System, 16 GB of RAM and 200 GB of free storage space on the disk drive. The researcher verified the setup of the development environment by writing a simple "Hello World" application and executing it within the emulator. During the early stage of this experiment it became necessary, due to work requirements, to upgrade the operating system of the laptop to 64-bit Windows

8.1. When this experiment was resumed after the Windows upgrade, the Android Studio failed to compile even the simplest “Hello World” application, showing the following compile-time error.



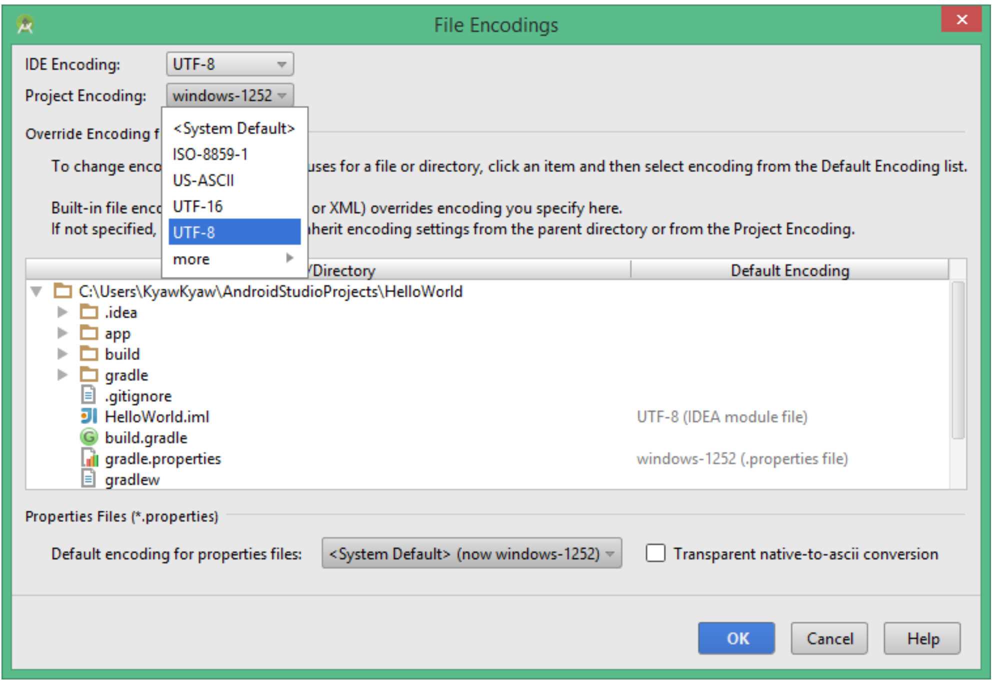
Messages Gradle Sync

Gradle Sync Issue

Warning: The project encoding (windows-1252) does not match the encoding specified in the Gradle build files (UTF-8).
This can lead to serious bugs.
More Info...
Open File Encoding Settings

Figure 5.6: Compilation error after OS upgrade from Windows 7 to Windows 8.1

The encoding issue shown in Figure 5.6 was resolved by the setting the project’s encoding and the build’s encoding to the same encoding system as shown in Figure 5.7.



File Encodings

IDE Encoding: UTF-8

Project Encoding: windows-1252

Override Encoding f

To change enco uses for a file or directory, click an item and then select encoding from the Default Encoding list.

Built-in file enc or XML) overrides encoding you specify here.
If not specified, herit encoding settings from the parent directory or from the Project Encoding.

/Directory	Default Encoding
C:\Users\KyawKyaw\AndroidStudioProjects\HelloWorld	
.idea	
app	
build	
gradle	
.gitignore	
HelloWorld.iml	UTF-8 (IDEA module file)
build.gradle	
gradle.properties	windows-1252 (.properties file)
gradlew	

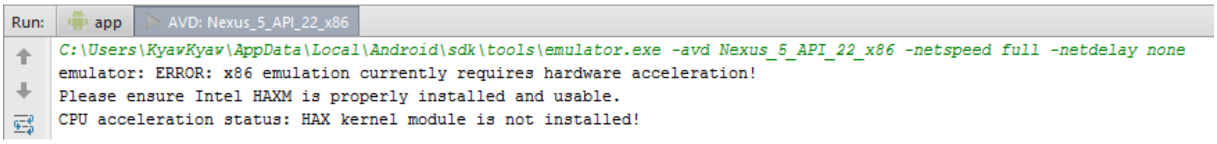
Properties Files (*.properties)

Default encoding for properties files: <System Default> (now windows-1252)

□ Transparent native-to-ascii conversion

Figure 5.7: Project encoding (Android Studio)

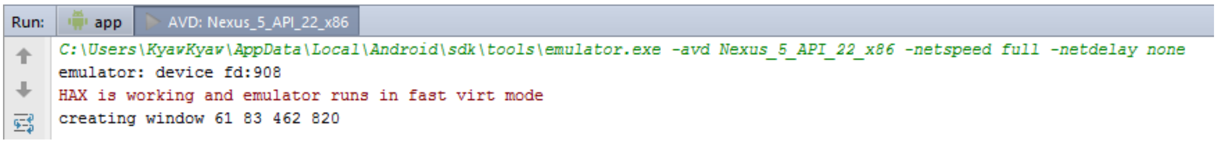
Although rectifying the encoding issue fixed the prototype’s compilation error, the execution of the Android emulator threw more errors, depicted in Figure 5.8, and failed to start up.



```
C:\Users\KyawKyaw\AppData\Local\Android\sdk\tools\emulator.exe -avd Nexus_5_API_22_x86 -netspeed full -netdelay none
emulator: ERROR: x86 emulation currently requires hardware acceleration!
Please ensure Intel HAXM is properly installed and usable.
CPU acceleration status: HAX kernel module is not installed!
```

Figure 5.8: Emulator start-up error (Android Studio)

Further investigation and research for this issue discovered that it was due to the Hyper-V feature, Microsoft's virtualisation technology introduced by the Windows 8.1, and found a range of workarounds on technical forums and discussion pages on the Internet. The approach taken by the researcher to overcome this situation was to create a dual boot option without Hyper-V feature. Once the Windows OS was loaded with this "No Hyper-V" option, the Android emulator executed well without any issue as shown in Figure 5.9.

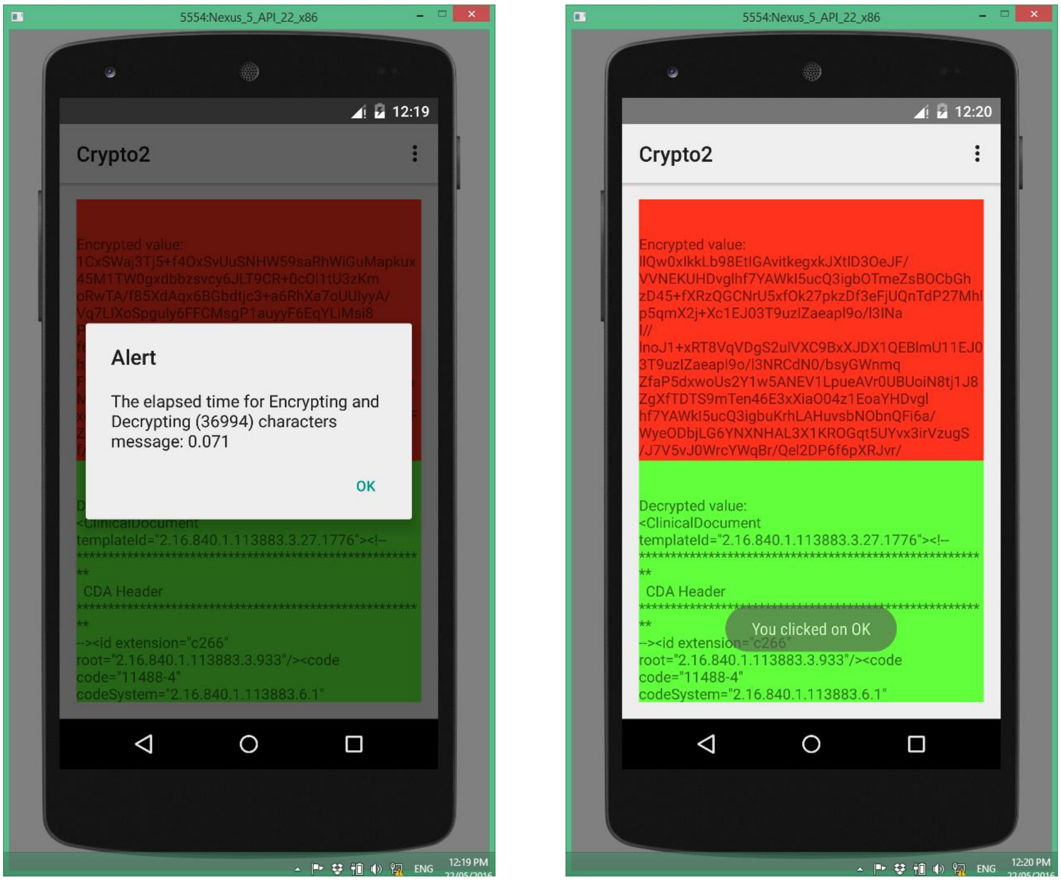


```
C:\Users\KyawKyaw\AppData\Local\Android\sdk\tools\emulator.exe -avd Nexus_5_API_22_x86 -netspeed full -netdelay none
emulator: device fd:908
HAX is working and emulator runs in fast virt mode
creating window 61 83 462 820
```

Figure 5.9: Successful emulator start-up with "No Hyper-V"

In fact, this "No Hyper-V" option not only enabled execution of the Android emulator but also other virtualisation technologies such as VMWare and Oracle's VirtualBox. With this approach, the experiment progressed and the prototype application to test the encryption on Android platform was created using the Android's "javax.crypto" libraries.

This prototype used the sample HL7 CDA (Clinical Document Architecture) document, which was downloaded from the Gleaning Resource Descriptions from Dialects of Languages (GRDDL) Primer section of the W3C website for its encrypting and decrypting operations, in order to reflect the file size and complexity of the actual electronic prescriptions. However, to avoid the unnecessary technical complexity in the development of the prototype for this experiment, it stored the entire content of the CDA file into a literal string variable and performed the encryption and decryption operations using this string variable instead of reading and writing to/from the Android file system. An illustration of how the prototype operated and how it was executed in the Android emulator is depicted in Figure 5.10.



Encrypted value:
1CxSWaj3Tj5+f4OxSvUuSNHW59saRhWiGuMapkux
45M1TW0gxdbbzsvcy6JLT9CR+0cOl1tU3zKm
oRwTA/f85XdAqx6BGbdtjc3+a6RhXa7oUUlyyA/
Vq7LIXoSpguly6FFCMsgP1auyyF6EqYLiMsi8

Alert

The elapsed time for Encrypting and Decrypting (36994) characters message: 0.071

<ClinicalDocument
templateId="2.16.840.1.113883.3.27.1776"><!--
****
**
CDA Header
****
**
--><id extension="c266"
root="2.16.840.1.113883.3.933"/><code
code="11488-4"
codeSystem="2.16.840.1.113883.6.1"

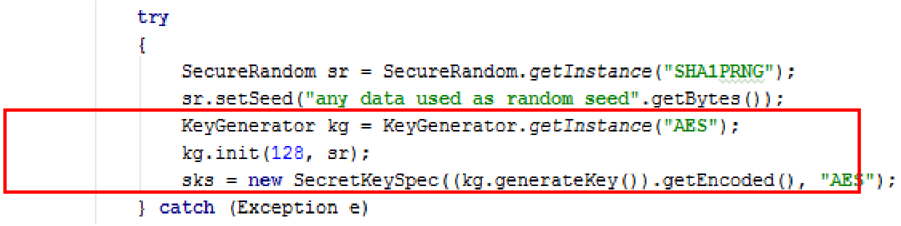
Encrypted value:
lIQw0xIkkLb98EtIGAvitkegxkJXtlD3OeJF/
VVNEKUHDvglhf7YAWkI5ucQ3igbOTmeZsBOCbGh
zD45+fXRzQGCNrU5xfOk27pkzDf3eFjUQnTdP27Mhl
p5qmX2j+Xc1EJ03T9uzIZaeapl9o/l3INa
l//
lnoJ1+xRT8VqVDgS2ulVXC9BxXJDX1QEBlmU11EJ0
3T9uzIZaeapl9o/l3NRCdN0/bsyGWnmq
ZfaP5dxwoUs2Y1w5ANEV1LpueAVr0UBUoiN8tj1J8
ZgXfTDTS9mTen46E3xXiaO04z1EoaYHDvgl
hf7YAWkI5ucQ3igbuKrhLAHuvsbNObnQFi6a/
WyeODbjLG6YNXNHAL3X1KROGqt5UYvx3irVzugS
/J7V5vJ0WrcYWqBr/Qel2DP6f6pXRJvr/

Decrypted value:
<ClinicalDocument
templateId="2.16.840.1.113883.3.27.1776"><!--
****
**
CDA Header
****
**
--><id extension="c266"
root="2.16.840.1.113883.3.933"/><code
code="11488-4"
codeSystem="2.16.840.1.113883.6.1"

You clicked on OK

Figure 5.10: Prototype running in Android emulator

Since this prototype used the 128-bit AES encryption as shown in Figure 5.11 for encrypting and decrypting the CDA content, it proved that the Android satisfied the technical requirements mandated by the ATS4888.2-2013 for security of data at rest for electronic prescription.



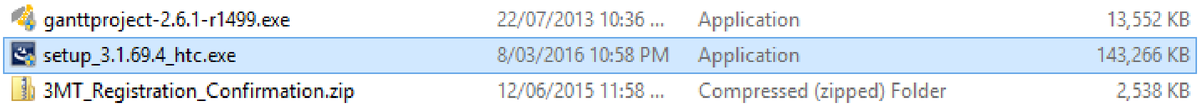
```
try
{
    SecureRandom sr = SecureRandom.getInstance("SHA1PRNG");
    sr.setSeed("any data used as random seed".getBytes());
    KeyGenerator kg = KeyGenerator.getInstance("AES");
    kg.init(128, sr);
    sks = new SecretKeySpec((kg.generateKey()).getEncoded(), "AES");
} catch (Exception e)
```

Figure 5.11: Use of AES 128-bit encryption

However, since all the development and testing so far were conducted only within the development environment using an emulator, the prototype needed to be deployed onto an actual Android device to test the performance of the operating system and device in performing these encryption and decryption operations in reality. The first device to be tested on was the research's HTC One handset running Android version 5.0.2.

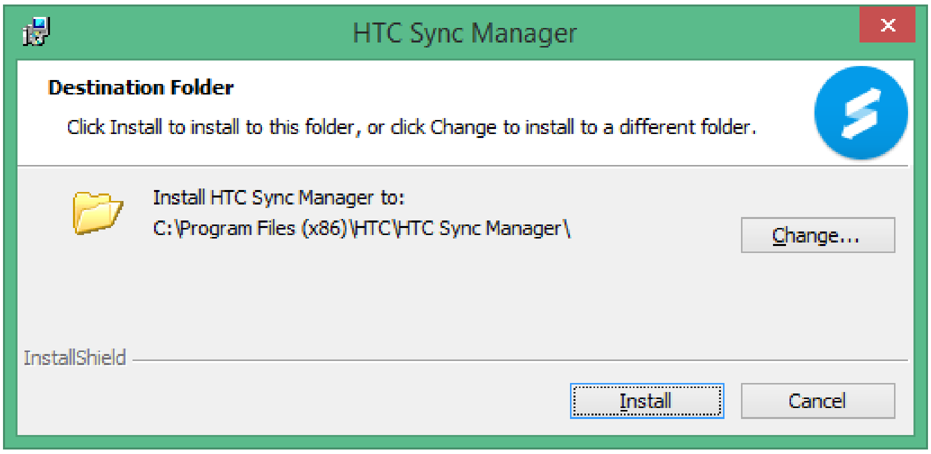
The first issue encountered in the attempt to repeat this test on HTC One handset was that the Android Studio did not recognise the HTC One handset and therefore it was not possible for the prototype to be deployed and tested on that particular HTC One device.

This was due to not having the USB driver for the HTC One device on the development machine, and, after several hours of investigation and analysis, it was found that the USB driver for the HTC One phone only came as part of the HTC Sync Manager utility program. Therefore, the HTC Sync Manager was downloaded from the HTC Support web site (HTC, 2016) and successfully installed as shown in the following figures: Figure 5.12, 5.13 and 5.14.



ganttproject-2.6.1-r1499.exe	22/07/2013 10:36 ...	Application	13,552 KB
setup_3.1.69.4_htc.exe	8/03/2016 10:58 PM	Application	143,266 KB
3MT_Registration_Confirmation.zip	12/06/2015 11:58 ...	Compressed (zipped) Folder	2,538 KB

Figure 5.12: The HTC Sync Manager downloaded from HTC Support web site



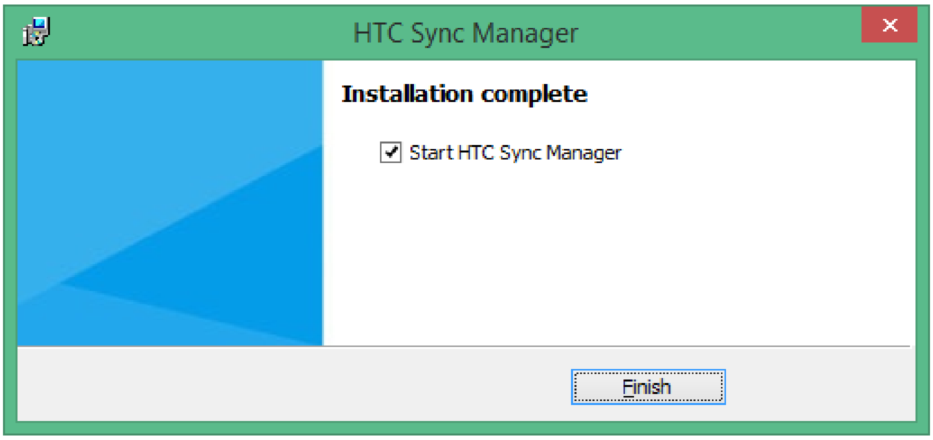
HTC Sync Manager

Destination Folder

Click Install to install to this folder, or click Change to install to a different folder.

Install HTC Sync Manager to:
C:\Program Files (x86)\HTC\HTC Sync Manager\

Figure 5.13: HTC Sync Manager (installation step 1)


HTC Sync Manager

Installation complete

☑ Start HTC Sync Manager

Figure 5.14: HTC Sync Manager (installation step 2)

Once the HTC Sync Manger was installed, both the Windows Device Manager and the Control Panel's "Programs and Features" section displayed its presence as illustrated in Figure 5.15 and 5.16 respectively.

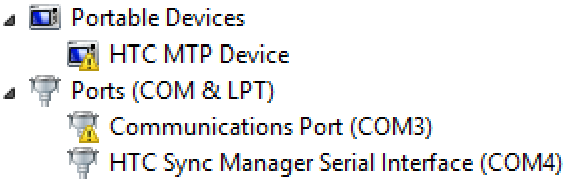
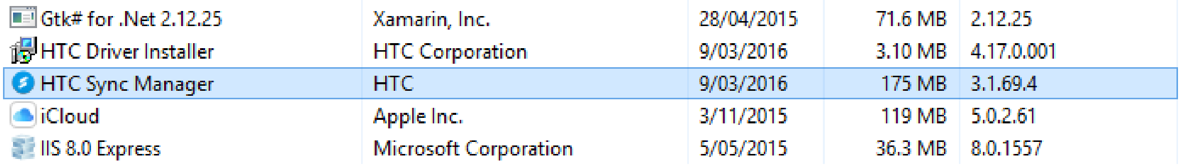

- Portable Devices
  - HTC MTP Device
- Ports (COM & LPT)
  - Communications Port (COM3)
  - HTC Sync Manager Serial Interface (COM4)

Figure 5.15: Windows Device Manager



Gtk# for .Net 2.12.25	Xamarin, Inc.	28/04/2015	71.6 MB	2.12.25
HTC Driver Installer	HTC Corporation	9/03/2016	3.10 MB	4.17.0.001
HTC Sync Manager	HTC	9/03/2016	175 MB	3.1.69.4
iCloud	Apple Inc.	3/11/2015	119 MB	5.0.2.61
IIS 8.0 Express	Microsoft Corporation	5/05/2015	36.3 MB	8.0.1557

Figure 5.16: Windows Program and Feature

However, the Android Studio and its Android Device Monitor utility still did not recognise the HTC One device correctly in order to deploy and execute the prototype application on it. Figure 5.17 demonstrated that the Android Device Manager detected the presence of the HTC One device but its status was showing as being offline.

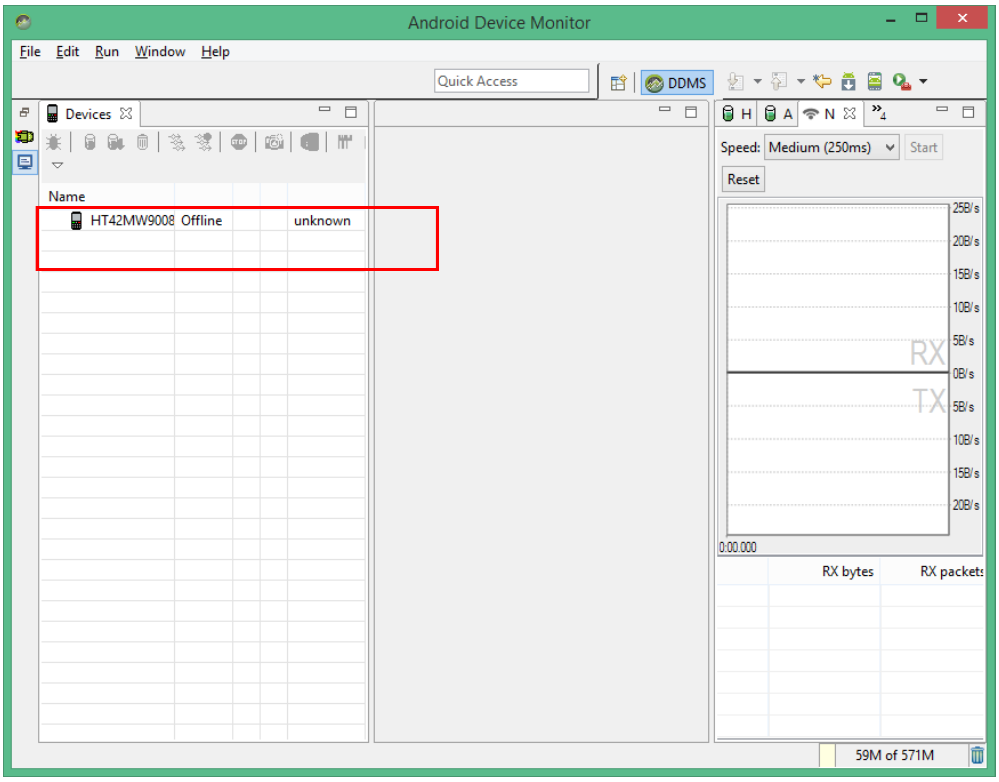


Figure 5.17: Android Device Monitor (Android Studio)

The USB connection from the laptop to the HTC One device seemed to be only responsive to the HTC Sync Manager alone and not to any other programs at all. Further investigations on this issue revealed that after the installation of the HTC Sync Manager, it was necessary to uninstall the HTC Sync Manager from the system so that it will leave only the HTC USB driver on the system. The following Figure 5.18 and 5.19 depicted how the Windows Device Manager and the Control Panel's Programs and Features section looked like once the HTC Sync Manager had been uninstalled from the system.

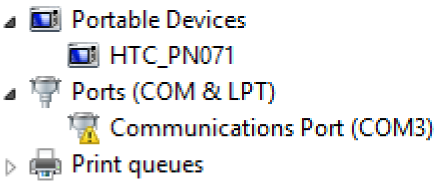
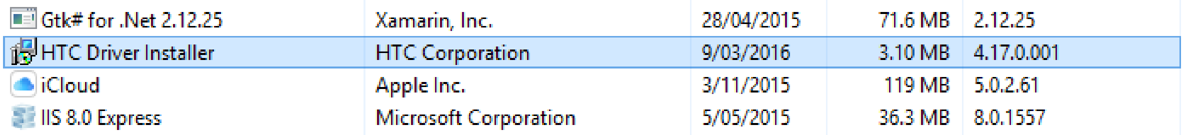


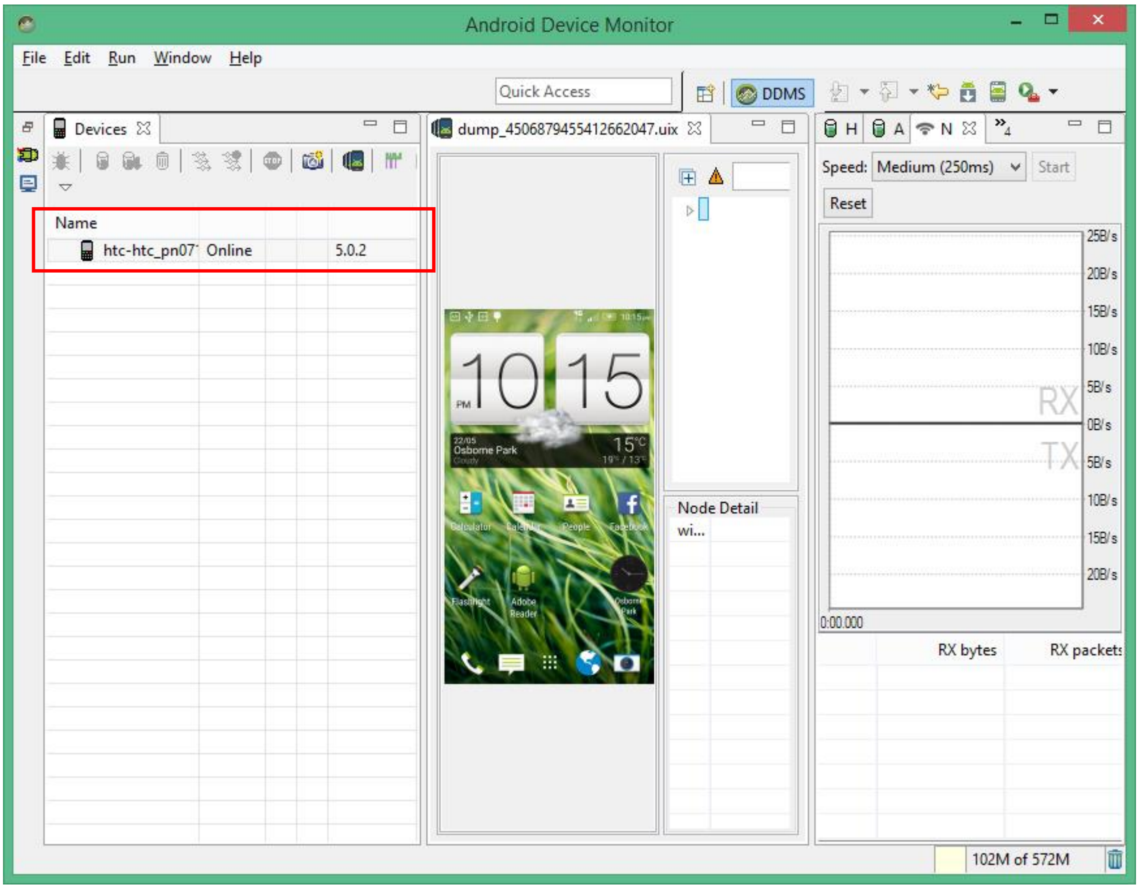
Figure 5.18: Windows Device Manager (after HTC Sync Manager uninstalled)



Gtk# for .Net 2.12.25	Xamarin, Inc.	28/04/2015	71.6 MB	2.12.25
HTC Driver Installer	HTC Corporation	9/03/2016	3.10 MB	4.17.0.001
iCloud	Apple Inc.	3/11/2015	119 MB	5.0.2.61
IIS 8.0 Express	Microsoft Corporation	5/05/2015	36.3 MB	8.0.1557

Figure 5.19: Windows Program and Feature (after HTC Sync Manager uninstalled)

Once the HTC Sync Manager was removed from the system, the HTC One device started working correctly with the Android Studio as shown in Figure 5.20.



Name		
htc-htc_pn07'	Online	5.0.2

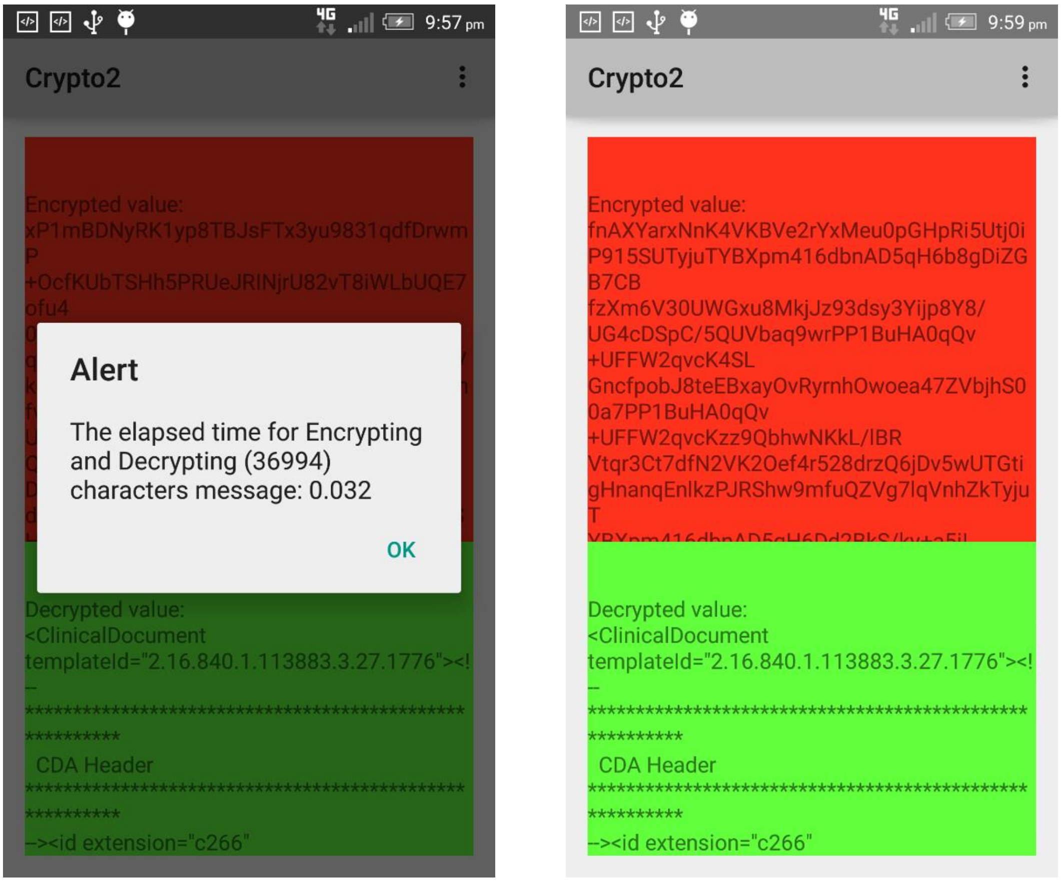
Speed: Medium (250ms)

102M of 572M

Figure 5.20: Android Device Manager (after HTC Sync Manager uninstalled)

Figure 5.21 showed the prototype application deployed and executed on the actual Android device. This experiment also revealed that the encryption and decryption operations took less time when the prototype was executed on the actual device compared to the time taken when it was executed in the emulator. On the actual device, it took between approximately 0.05 to 1 second to decrypt or encrypt the HL7 CDA document which is 36.2 KB in size.

Subsequently, the experimentation was repeated on the Samsung Galaxy A3 handset without any changes or reconfiguration.



```
Encrypted value:
xP1mBDNyRK1yp8TBJsFTx3yu9831qdfDrwm
P
+OcfKUbTSHh5PRUeJRINjrU82vT8iWLbUQE7
ofu4
```

Alert

The elapsed time for Encrypting and Decrypting (36994) characters message: 0.032

```
Decrypted value:
<ClinicalDocument
templateId="2.16.840.1.113883.3.27.1776"><!
--
************************************************
**********
 CDA Header
************************************************
**********
--><id extension="c266"
```

```
Encrypted value:
fnAXYarxNnK4VKBVe2rYxMeu0pGHpRi5Utj0i
P915SUTyjuTYBXpm416dbnAD5qH6b8gDiZG
B7CB
fzXm6V30UWGxu8MkjJz93dsy3Yijp8Y8/
UG4cDSpC/5QUVbaq9wrPP1BuHA0qQv
+UFFW2qvcK4SL
GncfpobJ8teEBxayOvRyrnhOwoea47ZVbjhS0
0a7PP1BuHA0qQv
+UFFW2qvcKzz9QbhwNKkL/IBR
Vtqr3Ct7dfN2VK2Oef4r528drzQ6jDv5wUTGti
gHnanqEnlkzPJRShw9mfuQZVg7lqVnhZkTyju
T
YBXpm416dbnAD5qH6Dd2BkS/ky+a5iI
```

```
Decrypted value:
<ClinicalDocument
templateId="2.16.840.1.113883.3.27.1776"><!
--
************************************************
**********
 CDA Header
************************************************
**********
--><id extension="c266"
```

Figure 5.21: Prototype executed on actual Android device

5.2.3 Experiment 1: Results/Outcomes.

From this experiment, it was found that security features available on Android platform were more than sufficient to ensure the security of data at rest as it was mandated by the ATS4888.2-2013 with adequate performance. This experiment outcome indicated that the use of an Android device as the alternative data transfer mechanism for exchanging the electronic prescription between prescriber’s EPS system and pharmacy’s EDS system will provide comparable security assurance to that of the current mechanism using the Prescription Exchange Services.

5.2.4 Experiment 1: Lessons learnt

During the experiment, the deployment of the prototype application from the Android Studio development environment to the HTC One device encountered the HTC USB driver related issue. However, this issue was only associated with a specific scenario where the application was directly deployed to an actual device from the Android Studio development environment and it is completely irrelevant when the application is deployed via the Google PlayStore.

Some of the issues encountered during this experiment, such as the Android emulator issue on Windows 8.1 with Hyper-V feature and the HTC Sync Manager issue, would have taken a much longer time with a lot more effort and frustration without the combined knowledge and support from various online communities, technical forums and discussions web pages. The researcher spent many hours researching, investigating and rectifying through these digital resources in search of any relevant information on the issues encountered, and they provided crucial information and potential solutions for resolving those issues over the course this experiment.

5.2.5 Experiment 1: Modifications.

Neither additional modification nor another round of experimentation was required as this experiment successfully proved that the Android operating system platform has sufficient encryption capabilities to satisfy the security requirements mandated by the ATS4888.2-2013 for storing electronic prescription.

5.2.6 Conclusion

Experiment 1 successfully proved that the Android operating system platform has sufficient encryption capabilities to satisfy the security requirements mandated by the ATS4888.2-2013 for storing electronic prescription.

5.3 Learning from the Research

The analysis of the relevant regulations and standards allowed this research to determine the readiness of each jurisdiction for a fully electronic prescription system, and established that the use of DAK and 128-bit symmetric encryption were the minimal requirements for securing electronic prescriptions from the data at rest perspective. These findings were collated in Table 4.1 and Section (1) of Table 4.2.

Subsequently, Experiment 1 verified that the proposed Android operating system has sufficient encryption capability for securing electronic prescriptions by complying with the requirements mandated by ATS4888.2-2013. The experiment which encrypted and decrypted the sample HL7 CDA document not only proved that it does not require any third-party utility or tools for performing the 128-bit symmetric encryption, but also exhibited the fact that such encryption can be done with a decent performance (i.e. between 0.2-1 seconds for encrypting the HL7 CDA document of 36k).

The experimentation outcomes indicated that the proposed Android mobile ETP application offered the security assurances equivalent to that of the current ETP implementation from the data at rest perspective. This stage was therefore concluded, leading to the next phase of the research. The paper produced at the end of this stage (i.e. Research Paper 2 in Appendix A) briefly describes the current security mechanisms for ETP from the data at rest perspective, how these can be achieved on Android OS platform and proposes an Android mobile ETP application with NFC as the alternative transfer mechanism for electronic prescriptions between ETP participants. The research findings published in the paper were verified by the double-blinded peer review process at the time of publication.

Htat, K. K., Williams, P. A. H., & McCauley, V. (2015). Security of ePrescription: Security of data at rest in Prescription Exchange Services vs on mobile devices. In *Proceedings of the 4th Australian eHealth Informatics and Security Conference 2015*, Perth, Australia. (pp. 15-22). doi: 10.14221/aeis.2015.2

Contributions: Htat (80%), Williams (15%) and McCauley (5%)

CHAPTER 6. SECURITY OF THE DATA IN TRANSIT

The “Confidentiality of data in transit” section of the *ATS4888.2-2013* states that “The mechanisms used to ensure the confidentiality of data in transit between ETP service participants are specific to the implementation ‘platform’”. However, as much as the *ATS4888* series mentions the implementation details on securing prescription information from the data at rest perspective, there was no further information on what the recommended approach is or how it should be implemented to secure prescription information from the data in transit perspective.

In addition, the research context turned out to be not only highly regulated but also highly proprietary. This made it impossible to investigate how the electronic prescriptions were transferred in the current implementation and search for an alternative transfer mechanism with comparable security measures. Therefore, using more of a “black-box” approach, this research endeavoured to find a transfer mechanism (i.e. a short-range wireless communication technology) that is comparable in security measures to using the Internet.

This chapter studied the details of the NFC and Bluetooth wireless communication technologies followed by experimentation determining their suitability for the proposed mobile ETP solution.

6.1 Near Field Communication

The investigation conducted in this section studied details of the NFC technology’s architecture, security model and its potentials as a candidate technology for the proposed mobile ETP solution. This section also identified the possible issues associated with NFC for the proposed mobile ETP solution.

6.1.1 A brief history and how it works

As the name suggests, near field communication (NFC) is a short-range, high frequency and low bandwidth wireless communication technology which enables secure two-way interactions between NFC enabled devices in a ubiquitous manner

(Coskun, et al., 2013). This new technology, which is now supported by majority of the smartphone manufacturers (“NFC phones: The definitive list”,2016), was invented in 2002 by Franz Amtmann, Philippe Maugars and researchers working at NXP Semiconductors and Sony ("Winners the European Inventor Award 2015", 2015).

Various industries’ widespread acceptance and support of this NFC technology became evident at an early stage when it was adopted as a standard by the European Computer Manufacturers Association (ECMA) International in December 2002 (Coskun, et al., 2013). The International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) adopted NFC technology in December 2003, and in 2004 the NFC Forum was founded by NXP Semiconductors, Phillips and Sony to further promote the technology and its interoperability among devices and services (Coskun, et al., 2012).

Technically, NFC is a subset of Radio Frequency Identification (RFID) technology (“The Difference between RFID and NFC”, 2011) which was extended by using smart card technologies’ interfaces (Coskun, et al., 2013). The NFC devices communicate at a frequency of 13.56 MHz, which is that originally used by RFID, and so the communication occurred only when the devices are in close proximity (*ibid*).

In a way, NFC is an evolution of RFID, influenced by the synergy of several technologies including wireless communications, mobile devices, mobile applications and smart cards ("Winners the European Inventor Award 2015", 2015). Being a descendent of the RFID technology, NFC’s evolution dates back to 1940s with the use of Barcode technology, and its ancestry is roughly depicted by Coskun et al. (2013) as in Figure 6.1.

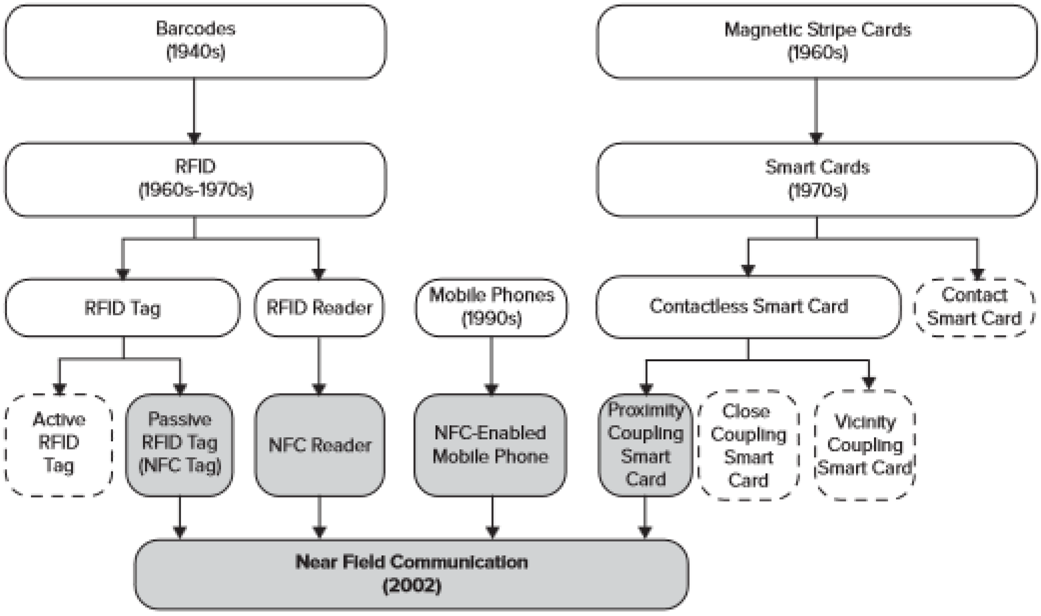


Figure 6.1: Evolution of NFC (Coskun, et al., 2012)

NFC restricted its communication range to maximum of 4cm, with the data transfer rate of up to 424 Kbps (Coskun, et al., 2013). While Figure 6.2 presents a broad comparison of NFC's communication range and data transfer rate against other wireless communication technologies, further details such as operating frequency, data rate and range of each technology are listed in Table 6.1.

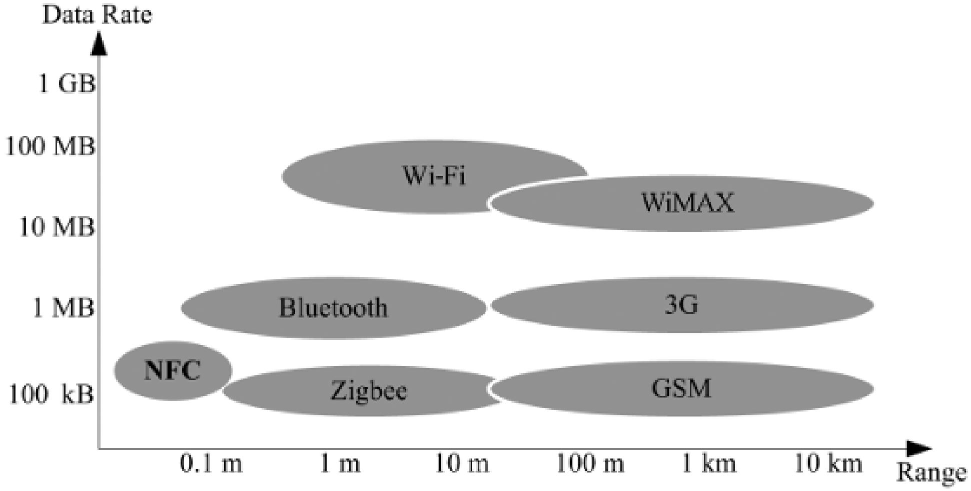
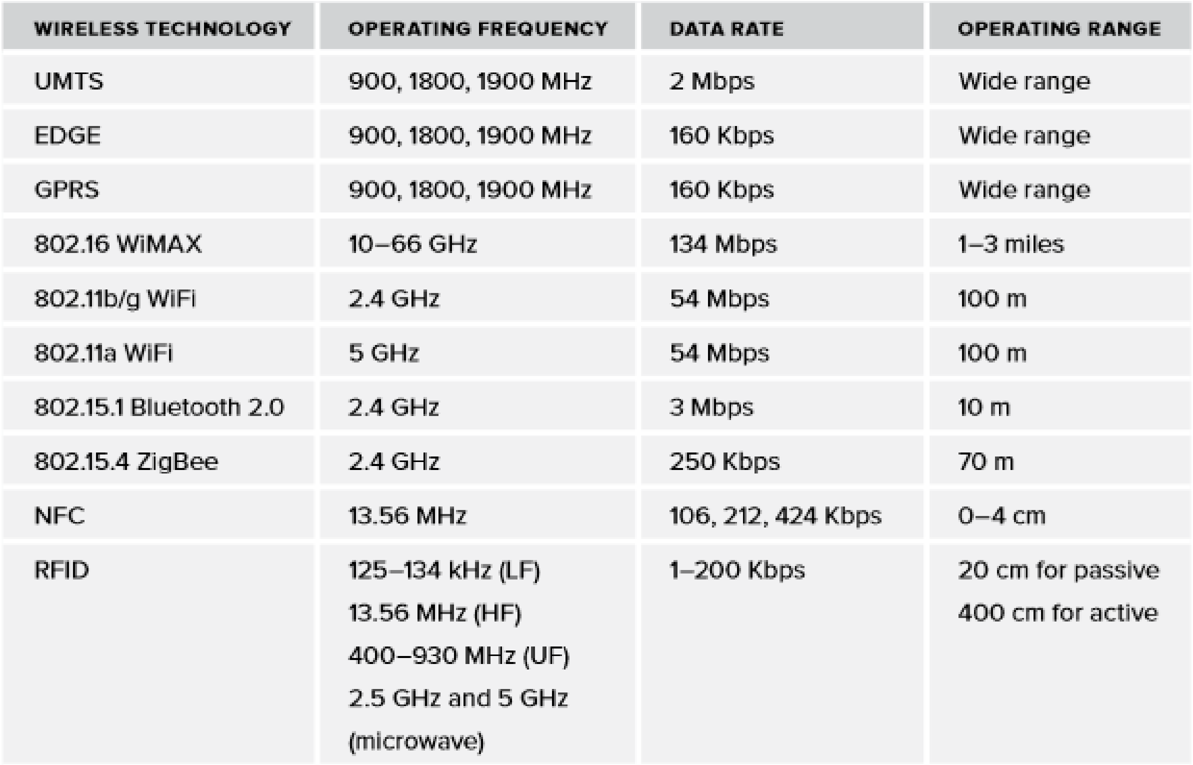


Figure 6.2: NFC's communication range in comparison with other wireless communication technologies (Coskun, et al., 2012)

Table 6.1: Frequency, data rate and range of wireless technologies (Coskun, et al., 2013)



WIRELESS TECHNOLOGY	OPERATING FREQUENCY	DATA RATE	OPERATING RANGE
UMTS	900, 1800, 1900 MHz	2 Mbps	Wide range
EDGE	900, 1800, 1900 MHz	160 Kbps	Wide range
GPRS	900, 1800, 1900 MHz	160 Kbps	Wide range
802.16 WiMAX	10–66 GHz	134 Mbps	1–3 miles
802.11b/g WiFi	2.4 GHz	54 Mbps	100 m
802.11a WiFi	5 GHz	54 Mbps	100 m
802.15.1 Bluetooth 2.0	2.4 GHz	3 Mbps	10 m
802.15.4 ZigBee	2.4 GHz	250 Kbps	70 m
NFC	13.56 MHz	106, 212, 424 Kbps	0–4 cm
RFID	125–134 kHz (LF) 13.56 MHz (HF) 400–930 MHz (UF) 2.5 GHz and 5 GHz (microwave)	1–200 Kbps	20 cm for passive 400 cm for active

This new technology's success (i.e. widespread usages) and the emergence of its ecosystem evolved around its simple and ubiquitous nature (Coskun, et al., 2013). Just as personal computers (PCs) have changed the way users interact with a computer using keyboards and monitors instead of punch cards, and touch screens have drastically changed the human-computer interactions, NFC has changed the way connection is established between devices by simply requiring very close proximity, also known as "touching" (*ibid*). Instead of users having to perform the various pairing and authentication steps required by the technology such as Bluetooth and WiFi, NFC technology adjusts to normal human behaviour in performing activities. From a higher perspective, NFC's seamless pairing and communication nature takes us a step further toward ubiquitous computing where human-computer interaction is integrated into our everyday life to the highest level with little effort in using them (Reisenhofer, et al., 2016; Coskun, et al., 2012).

An NFC device is categorised as either an active or a passive device, based on whether it has its own power source (Coskun, et al., 2013). An active device has its own power/energy source whereas a passive device is powered using the energy created by an electromagnetic field generated by an active device (*ibid*).

In a similar way to RFID data exchange and other existing client-server communication paradigms, NFC communication involves two parties: (1) the initiator and (2) the target. The initiator, an active device, initiates the communication with the target device and this responds to the initiator's request (*ibid*). In the case of the target being a passive device, it uses the initiator's power/energy in responding to the initiator's communication request. On the other hand, the initiator always needs to be an active device as it requires a power source to initiate the communication even if it does not have to power the target (i.e. in scenarios where the target is also an active device) (*ibid*).

In addition to these active or passive device types and communication modes (i.e. being an initiator or target), NFC has three operating modes: (1) reader/writer mode which reads data from and writes to a target, (2) card emulator mode which acts like an RFID tag when they are within communication range of another NFC or RFID device and (3) peer-to-peer mode where data exchange occurs in both directions (Igoe, et al., 2014). Coskun et al. (2012) depict these operating modes and the governing standard for each in Figure 6.3.

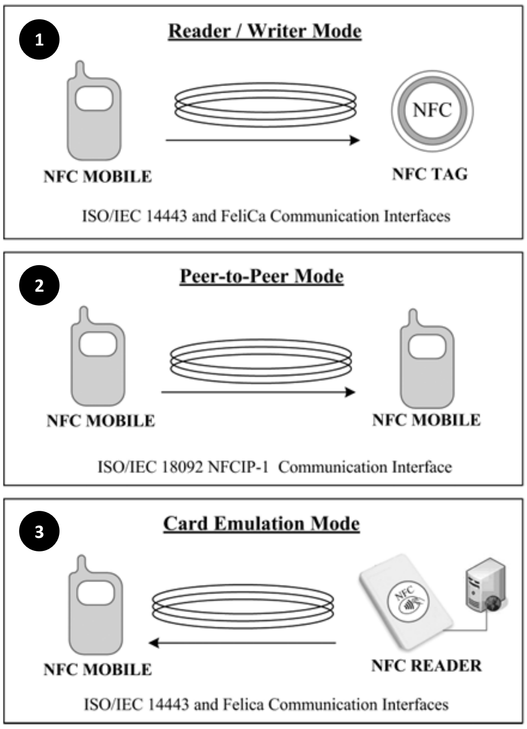

1
Reader / Writer Mode
NFC
NFC MOBILE
NFC TAG
ISO/IEC 14443 and FeliCa Communication Interfaces
2
Peer-to-Peer Mode
NFC MOBILE
NFC MOBILE
ISO/IEC 18092 NFCIP-1 Communication Interface
3
Card Emulation Mode
NFC
NFC MOBILE
NFC READER
ISO/IEC 14443 and Felica Communication Interfaces

Figure 6.3: Three operation modes of NFC (Coskun, et al., 2012)

At present, despite being governed by myriad standards and specifications, this research found that the NFC ecosystem is mainly made up of action components belonging to the following three categories: NFC mobiles, NFC readers and NFC tags.

- NFC mobiles: These are NFC-enabled mobile phones or smartphones. The integration of NFC technology with these devices was the primary enabler which unlocked vast opportunities for various innovative uses and widespread acceptance of the NFC ecosystem (Coskun, et al., 2012)
- NFC readers: These perform data transfer with an NFC component/device. Some real life uses would be the contactless POS (Point of Sale) terminal which supports contactless NFC payments such as ***CommBank Tap & Pay*** and ***ANZ Mobile Pay***. ("COMMBANK Tap & Pay", 2016; "ANZ Mobile Pay", 2015)
- NFC tags: Technically, these are classified as passive RFID tags that have no integrated power source of their own. During the communication, a small amount of power is taken by the NFC tag from the reader/writer in order to power the tag's electronics and perform the data transfer to the reader/writer (i.e. NFC enabled device) (Poole, n.d.)

The category to which an NFC device belongs dictates how security will be implemented and which standards and specifications it will be governed by.

6.1.2 Architecture and Security

Security is NFC's most critical concern as its primary motivation being integrating personal and private information such as credit/debit card data into mobile devices. Like many other information systems, NFC's vulnerability to attacks and its defence mechanisms are mostly subject to different use cases (Coskun, et al., 2012). Due to the context of this research thesis, this section will only emphasise on NFC's generic security features and those security features specific to the NFC smartphones operating in peer-to-peer mode and card emulation mode.

Similar to the 7 Layers Model by Open System Interconnection (OSI), the mental model of NFC architecture (i.e. Figure 6.4) by Igoe et al. (2014) helps in visualising and understanding each layer of the NFC stack. Figure 6.4 also maps each layer of the NFC stack with their specific governing standards. Further details on those governing standards will be discussed in the next section, “Governing Standards”.

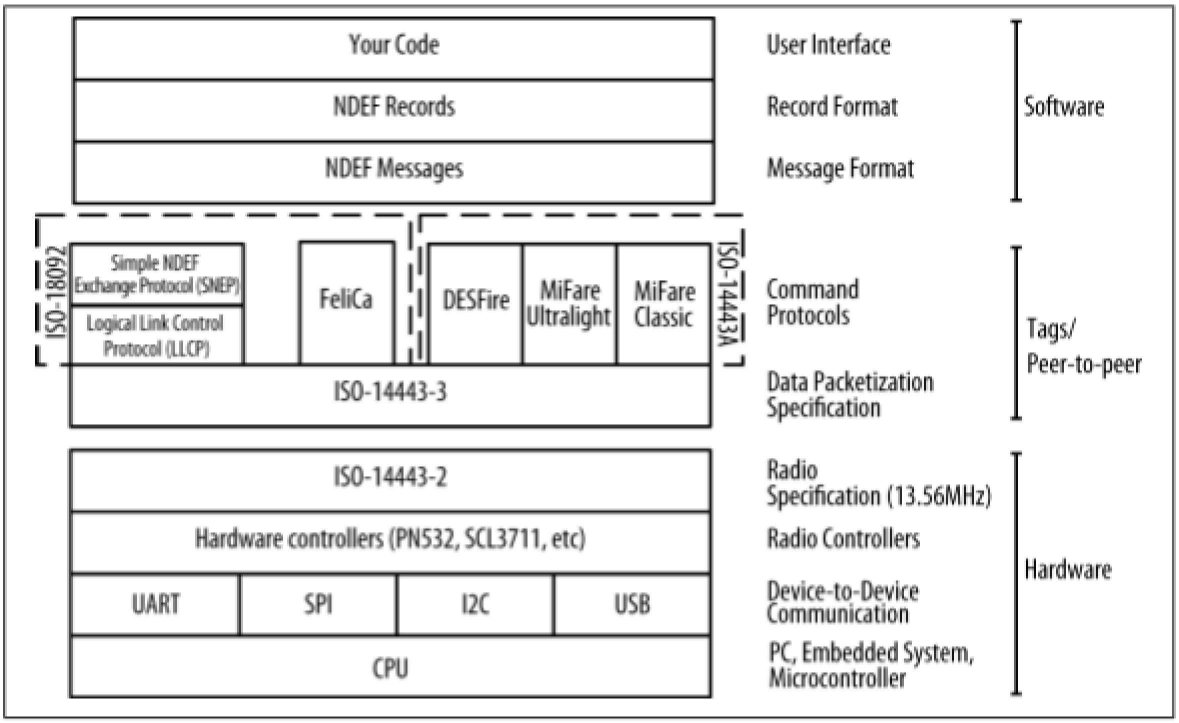


Figure 6.4: NFC protocol stack (Igoe, et al., 2014)

From the NFC’s security perspective, RFID technology’s wireless communication range was considered too far, and this long communication range exposed the radio signal to signal-interception. Therefore, NFC technology significantly shortened its communication range to a maximum distance of 4 cm between devices. This requirement for device proximity strengthens security as the chances of the devices’ radio signals being intercepted is significantly reduced over such a short distance (Hamblen, 2012).

Another security feature of NFC is its native support for encryption. As per NFC Forum’s specification, the secure element (SE) or secure access module was designed to be programmable and capable of running small programs on its own (Coskun, et al., 2013). It can generate hashes and verify codes/values using public key encryption and decryption (Igoe, et al., 2014). Any NFC-enabled smartphone has at least one SE for performing secure proximity transactions with external NFC devices (Coskun, et al., 2013). The SE also enables secure storage of data such as users' credit card information and the secure execution of NFC-enabled services such as contactless payments (*ibid*). Despite SE being a combination of hardware, software, interfaces and protocols, a variety of modules such as Universal Integrated Circuit Cards (UICC), secure memory cards or embedded chip/hardware can serve as SEs (Coskun, et al., 2012). These various types of SEs and their interaction with other components of the NFC technology are depicted in Figure 6.5 by Coskun, et al. (2012).

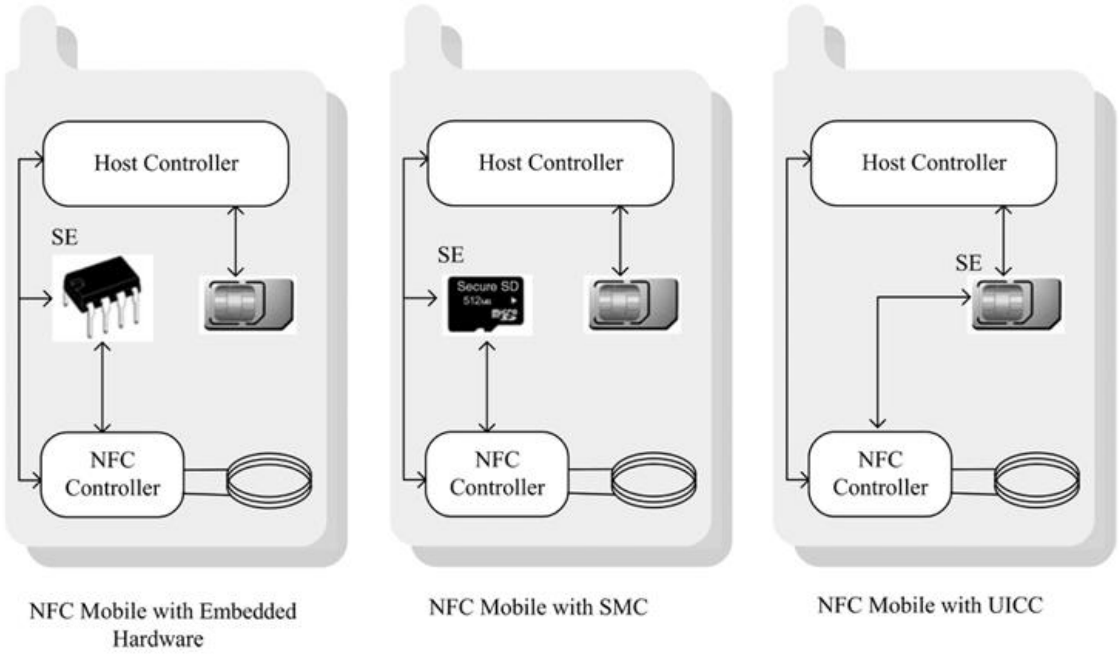


Figure 6.5: Various SE configurations in NFC (Coskun, et al., 2012)

Among these various SE types, the use of UICC based SEs is ideal for current use as they are portable and easily manageable via Over-the-Air (OTA) technology, while ensuring the secure execution of transactions (Coskun, et al., 2013). OTA is the standard for exchanging applications and application related information via wireless communication.

Even with all of these security features, NFC is not without security vulnerabilities. NFC has inherent security issues which can be categorised into reader/writer related issues, smart card related issues and communication related issues. However, these issues are being addressed using many standardised security protocols developed and maintained by organisations such as ECMA International, International Organization for Standardization (ISO), International Electrotechnical

Commission (IEC) and NFC Forum founded by Nokia, Philips, and Sony (Coskun, et al., 2013). Further details on each standard are given in the next section, “Governing Standards”, as well as information such as which security issue that standard is addressing, and which organisation is governing it.

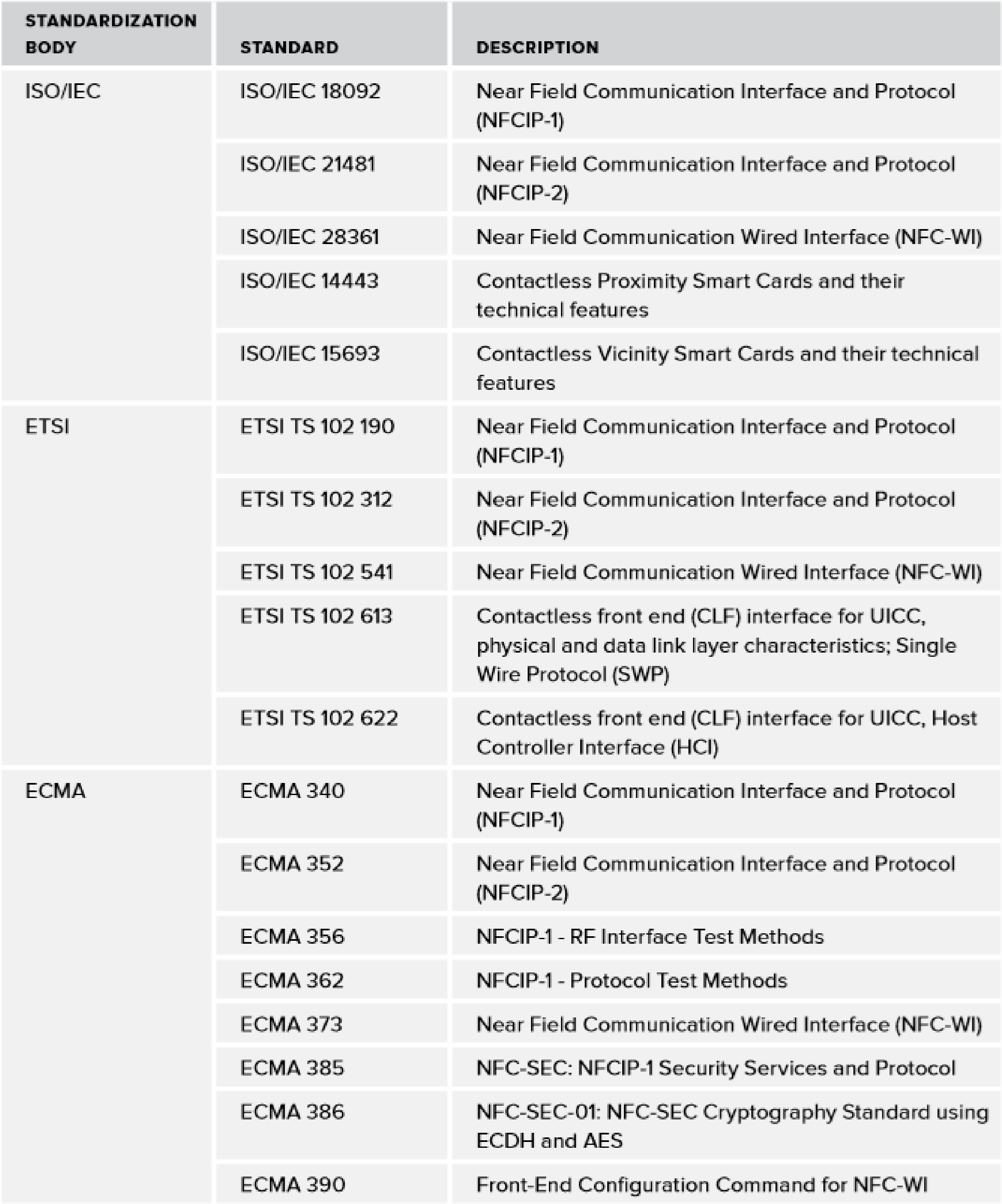
6.1.3 Governing Standards

This research found that many device manufacturers currently support NFC and its uses are promoted by many organisations. Due to its origin involving a few technologies (i.e. such as smart cards, mobile phones and card readers etc.) and complex use cases such as mobile wireless payment systems, several standards were developed and governed by numerous respective organisation bodies.

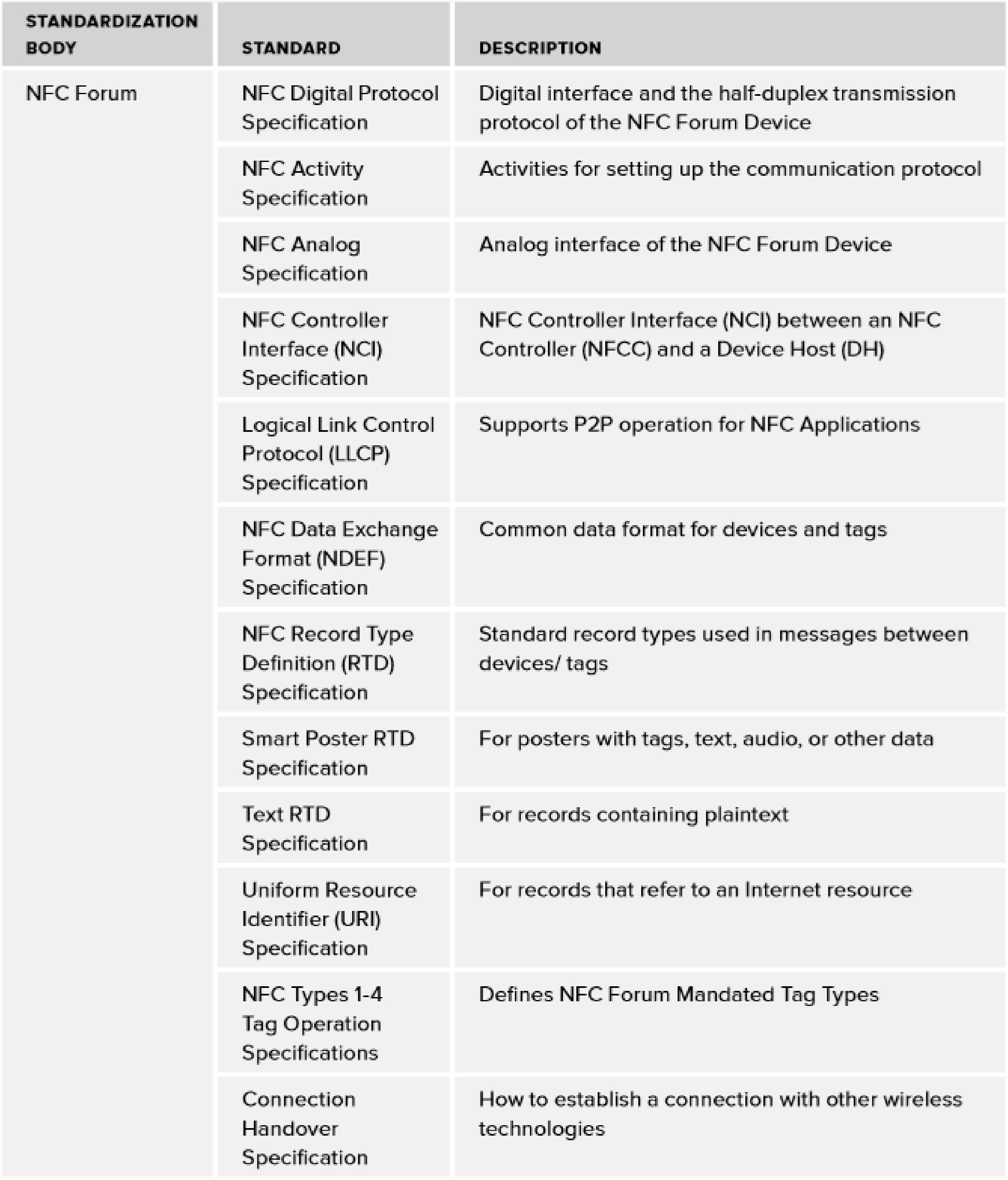
Among many organisations with influence over NFC, the principal standardisation bodies are: NFC Forum, GlobalPlatform, GSM Association (GSMA), International Organisation for Standardisation/International Electrotechnical Commission (ISO/IEC), European Computer Manufacturers Association (ECMA) International European Telecommunications Standards Institute (ETSI) and ETSI Smart Card Platform (ETSI SCP), Java Community Process (JCP), Open Mobile Alliance (OMA), 3rd Generation Partnership Project (3GPP), and EMVCo.

Whilst interoperability is essential to the functionality of the technology, security is another mandatory aspect as Coskun et al (2013) stated “a service is useful only when it is both functional and secure enough”. Integration and implementation of these standards is to be secure while remaining functional. Some major standards for NFC technology were briefly listed in the following table, Table 6.2.

Table 6.2: NFC standards (Coskun, et al., 2013)



STANDARDIZATION BODY	STANDARD	DESCRIPTION
ISO/IEC	ISO/IEC 18092	Near Field Communication Interface and Protocol (NFCIP-1)
	ISO/IEC 21481	Near Field Communication Interface and Protocol (NFCIP-2)
	ISO/IEC 28361	Near Field Communication Wired Interface (NFC-WI)
	ISO/IEC 14443	Contactless Proximity Smart Cards and their technical features
	ISO/IEC 15693	Contactless Vicinity Smart Cards and their technical features
ETSI	ETSI TS 102 190	Near Field Communication Interface and Protocol (NFCIP-1)
	ETSI TS 102 312	Near Field Communication Interface and Protocol (NFCIP-2)
	ETSI TS 102 541	Near Field Communication Wired Interface (NFC-WI)
	ETSI TS 102 613	Contactless front end (CLF) interface for UICC, physical and data link layer characteristics; Single Wire Protocol (SWP)
	ETSI TS 102 622	Contactless front end (CLF) interface for UICC, Host Controller Interface (HCI)
ECMA	ECMA 340	Near Field Communication Interface and Protocol (NFCIP-1)
	ECMA 352	Near Field Communication Interface and Protocol (NFCIP-2)
	ECMA 356	NFCIP-1 - RF Interface Test Methods
	ECMA 362	NFCIP-1 - Protocol Test Methods
	ECMA 373	Near Field Communication Wired Interface (NFC-WI)
	ECMA 385	NFC-SEC: NFCIP-1 Security Services and Protocol
	ECMA 386	NFC-SEC-01: NFC-SEC Cryptography Standard using ECDH and AES
	ECMA 390	Front-End Configuration Command for NFC-WI



STANDARDIZATION BODY	STANDARD	DESCRIPTION
NFC Forum	NFC Digital Protocol Specification	Digital interface and the half-duplex transmission protocol of the NFC Forum Device
	NFC Activity Specification	Activities for setting up the communication protocol
	NFC Analog Specification	Analog interface of the NFC Forum Device
	NFC Controller Interface (NCI) Specification	NFC Controller Interface (NCI) between an NFC Controller (NFCC) and a Device Host (DH)
	Logical Link Control Protocol (LLCP) Specification	Supports P2P operation for NFC Applications
	NFC Data Exchange Format (NDEF) Specification	Common data format for devices and tags
	NFC Record Type Definition (RTD) Specification	Standard record types used in messages between devices/ tags
	Smart Poster RTD Specification	For posters with tags, text, audio, or other data
	Text RTD Specification	For records containing plaintext
	Uniform Resource Identifier (URI) Specification	For records that refer to an Internet resource
	NFC Types 1-4 Tag Operation Specifications	Defines NFC Forum Mandated Tag Types
	Connection Handover Specification	How to establish a connection with other wireless technologies

6.1.4 Reasons for being a good candidate for the proposed solution

Nowadays almost everyone carries a smartphone, and the majority of the smartphone manufacturers support NFC. The use of NFC technology is therefore a very practical solution for short-range data transfer. Another reason for the candidacy of NFC technology is its implicit security feature, the very short and restricted communication range providing a very low probability of signal-interception (Coskun, et al., 2012).

In addition to its functionalities and security, NFC, unlike other wireless communication technology such as Bluetooth and WiFi, does not require much human intervention in establishing connection between devices. Intuitively, the touching action was considered as the triggering condition, and establishing communication or launching an installed application occurred as soon as two NFC devices were touched. From a higher perspective, this behaviour not only simplifies the communication process but also enables and promotes ubiquitous computing (Coskun, et al., 2012).

Last but not the least is its well supported interoperability. The integration and application of the NFC technology is well governed by various standards and specifications with support from the international standardisation bodies and industry entities (Coskun, et al., 2013). This assures the interoperability of the NFC technology and its functionalities despite having many stake holders in its ecosystem (Clark, 2015). For example, any two devices compliant with version 1.3 of the Logical Link Control Protocol (LLCP) specification are able to establish peer-to-peer unauthenticated secure connection and exchange AES encrypted LLCP messages as soon as they are brought together (*ibid*).

6.1.5 Potential issues of NFC for the proposed solution

With all these governing standards and specifications, NFC’s interoperability at the end-user level is excellent. Tap virtually any two NFC-enabled smartphones and they will establish a connection and exchange data almost instantaneously, requiring nothing more than being kept very closely together. However, NFC’s interoperability at the software development level is not so seamless. Among various NFC card reader/writer devices produced by many manufacturers, only the Sony FeliCa card readers/writers are recognised as proximity devices and operate well for application development for Windows 8+ (i.e. Windows 8 or higher) platforms using Windows Proximity APIs, a set of classes in the Windows operating system runtime that support connections between devices within close distance.

This is the result of the joint venture between Sony (i.e. the FeliCa technology) and XNP Semiconductors (i.e. Mifare technology) to enable the global adoption of contactless smart card applications in mobile phones (“NXP and Sony announce joint venture”, 2006). At present, NXP Semiconductors is the only hardware vendor that made Windows 8+ (i.e. Windows 8 or higher) compatible proximity drivers publicly available (Sharief, 2013). For the rest of the NFC card reader/writer devices, application development for Windows 8 or higher had to resort to using other, less generic, approaches such as low-level socket programming, instead of making use of the Windows Proximity APIs provided by the Windows Runtime.

6.1.6 Conclusion

Use of NFC for the electronic prescription transfer is likely to be well accepted by users as they have already been introduced to using the same technology in ticketing, loyalty card programmes and even in performing more mission-critical operations such as financial transactions (i.e. mobile payments).

NFC is widely supported by most device manufacturers and it has an excellent end-user level interoperability. However, this pre-experiment study of the technology found that there is room for improvement in software development on Windows platform to make use of the Window Proximity APIs provided by the Windows Runtime.

This shortcoming was likely to result in having to use a less generic approach such as low-level socket programming, and the solution ended up being less interoperable and portable. Nonetheless, whether NFC technology has the necessary security measures and is practical (i.e. from development and deployment of the solution perspectives) to be an alternative secured transfer mechanism for electronic prescriptions in the Australian healthcare industry is yet to be determined by the experimentation in the following section (Experiment 2: NFC – Security of the data in transit).

6.2 Experiment 2: NFC – Security of the data in transit

6.2.1 Overview

Since the preliminary study in section 6.1 found the NFC technology to be the potential secured transfer mechanism for the proposed mobile ETP solution from various aspects (i.e. widespread support by various smartphone manufacturers, excellent interoperability and convenience of use), this experimentation began with the NFC technology verifying its suitability for the proposed mobile ETP solution.

6.2.2 Experiment details

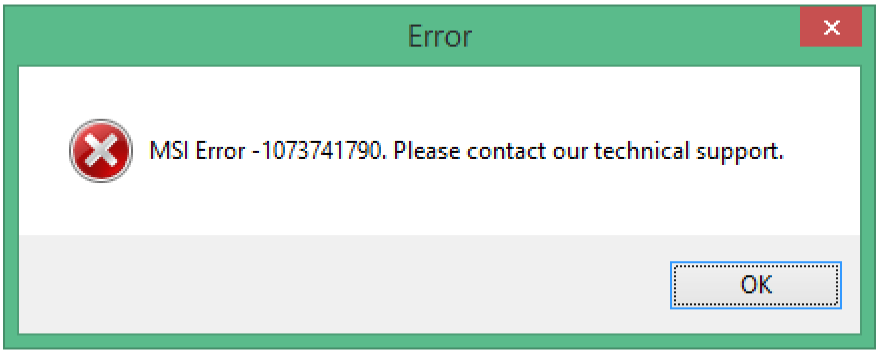
NFC was selected as the transfer mechanism for exchanging electronic prescription data between the prescriber's electronic prescribing system (EPS), the client's/patient's smartphone and the electronic dispensing system (EDS) at the pharmacy because of its widespread support by the majority of the smartphone manufacturers, excellent interoperability between devices, adequate support for security and its ease of use in establishing communication with another device as long as both devices are NFC enabled.

Since the majority of both the Clinical Management Systems used at the primary care clinics and the Pharmacy Management Systems in Australia run on Windows operating system platform, it is envisaged that the transfer of the electronic prescription from the prescriber's electronic prescribing system to the client's/patient's smartphone, and from the client's/patient's smartphone to the pharmacy's electronic dispensing system, will be NFC communications between Windows machines/PCs and Android smartphone.

Therefore, the proposed solution envisioned that this communication will occur between a NFC reader/writer device attached to the prescriber's EPS or dispenser's EDS and the client's/patient's Android smartphone, as the use of an NFC reader/writer device is more practical than acquiring a new computing device, laptop or tablet with NFC capability. An experimental prototype was developed using the C# .NET programming language, taking full advantage of the Windows Proximity

APIs supported by the Windows Runtime (WinRT) to leverage its efficiency, reliability, portability and security.

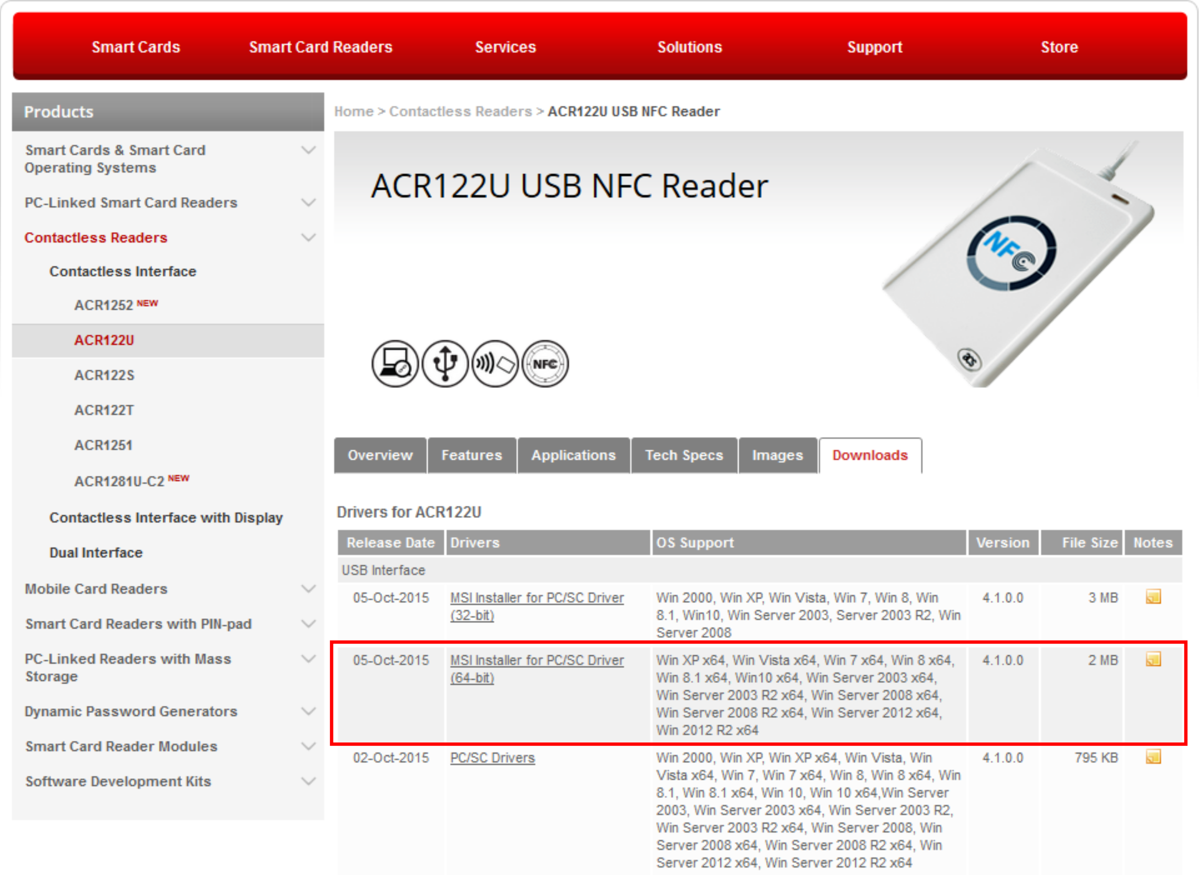
Among many generic NFC card reader/writer devices produced by various manufacturers, the researcher procured a USB ACR122U contactless RFID smartcard reader/writer from Advanced Card Systems (ACS) due to its widespread use in various industries. The NFC reader/writer device was shipped with an installation CD containing the device driver software and Software Development Kit (SDK). However, the following error occurred when the device driver software was installed from the provided installer CD.



MSI Error -1073741790. Please contact our technical support.

Figure 6.6: NFC device driver installation error on Windows 8.1

After some investigation and analysis, the researcher discovered that some discussion forums suggested that the error is likely to be resolved by using a newer version of the driver software than the one shipped with the device. Therefore, as shown in the following Figure 6.7, a newer version of the installer was acquired and installed from the ACR122U's Product page (i.e. "http://www.acs.com.hk/en/products/3/acr122u-usb-nfc-reader/") of the ACS website and then successfully installed.


Smart Cards
Smart Card Readers
Services
Solutions
Support
Store
Products
Smart Cards & Smart Card Operating Systems
PC-Linked Smart Card Readers
Contactless Readers
Contactless Interface
ACR1252 NEW
ACR122U
ACR122S
ACR122T
ACR1251
ACR1281U-C2 NEW
Contactless Interface with Display
Dual Interface
Mobile Card Readers
Smart Card Readers with PIN-pad
PC-Linked Readers with Mass Storage
Dynamic Password Generators
Smart Card Reader Modules
Software Development Kits
Home > Contactless Readers > ACR122U USB NFC Reader
NFC
Overview
Features
Applications
Tech Specs
Images
Downloads

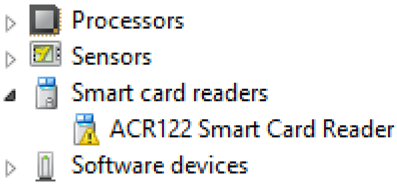
ACR122U USB NFC Reader

Drivers for ACR122U

Release Date	Drivers	OS Support	Version	File Size	Notes
USB Interface					
05-Oct-2015	MSI Installer for PC/SC Driver (32-bit)	Win 2000, Win XP, Win Vista, Win 7, Win 8, Win 8.1, Win10, Win Server 2003, Server 2003 R2, Win Server 2008	4.1.0.0	3 MB	
05-Oct-2015	MSI Installer for PC/SC Driver (64-bit)	Win XP x64, Win Vista x64, Win 7 x64, Win 8 x64, Win 8.1 x64, Win10 x64, Win Server 2003 x64, Win Server 2003 R2 x64, Win Server 2008 x64, Win Server 2008 R2 x64, Win Server 2012 x64, Win 2012 R2 x64	4.1.0.0	2 MB	
02-Oct-2015	PC/SC Drivers	Win 2000, Win XP, Win XP x64, Win Vista, Win Vista x64, Win 7, Win 7 x64, Win 8, Win 8 x64, Win 8.1, Win 8.1 x64, Win 10, Win 10 x64,Win Server 2003, Win Server 2003 x64, Win Server 2003 R2, Win Server 2003 R2 x64, Win Server 2008, Win Server 2008 x64, Win Server 2008 R2 x64, Win Server 2012 x64, Win Server 2012 R2 x64	4.1.0.0	795 KB	

Figure 6.7: ACR112U device's product page

On Windows 8.1 systems, the ACR122U NFC reader/writer was correctly detected even before the device driver installation. However, Figure 6.8 indicated that it will not function properly as the Windows operating system could not determine the right driver software for it.



Processors
Sensors
Smart card readers
ACR122 Smart Card Reader
Software devices

Figure 6.8: Windows Device Manager (no driver for NFC reader/writer)

Installing the newer version of the driver software downloaded from the ACS website rectified this issue and the following Figure 6.9 showed that the correct driver software for the NFC reader/writer was detected by the Windows operating system and the device was ready to function.

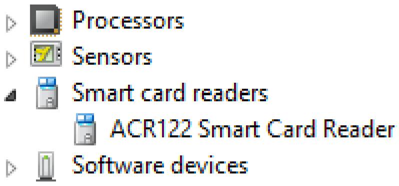
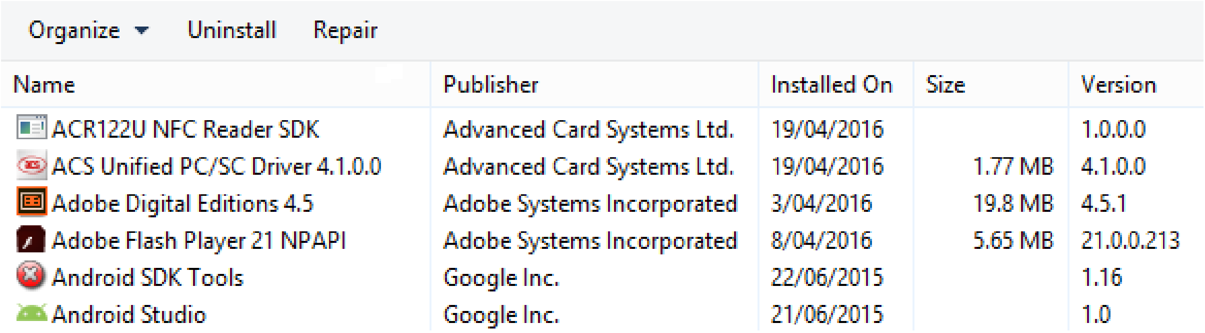


Figure 6.9: Windows Device Manager (driver found for NFC reader/writer)

Once the driver issue was resolved, the Software Development Kit (SDK) for the device was installed from the provided CD. The SDK installation process was simple and successfully completed after following on-screen prompts. The researcher's verification of the installed components from "Programs and Features" windows of the "Control Panel" is displayed as in the Figure 6.10.

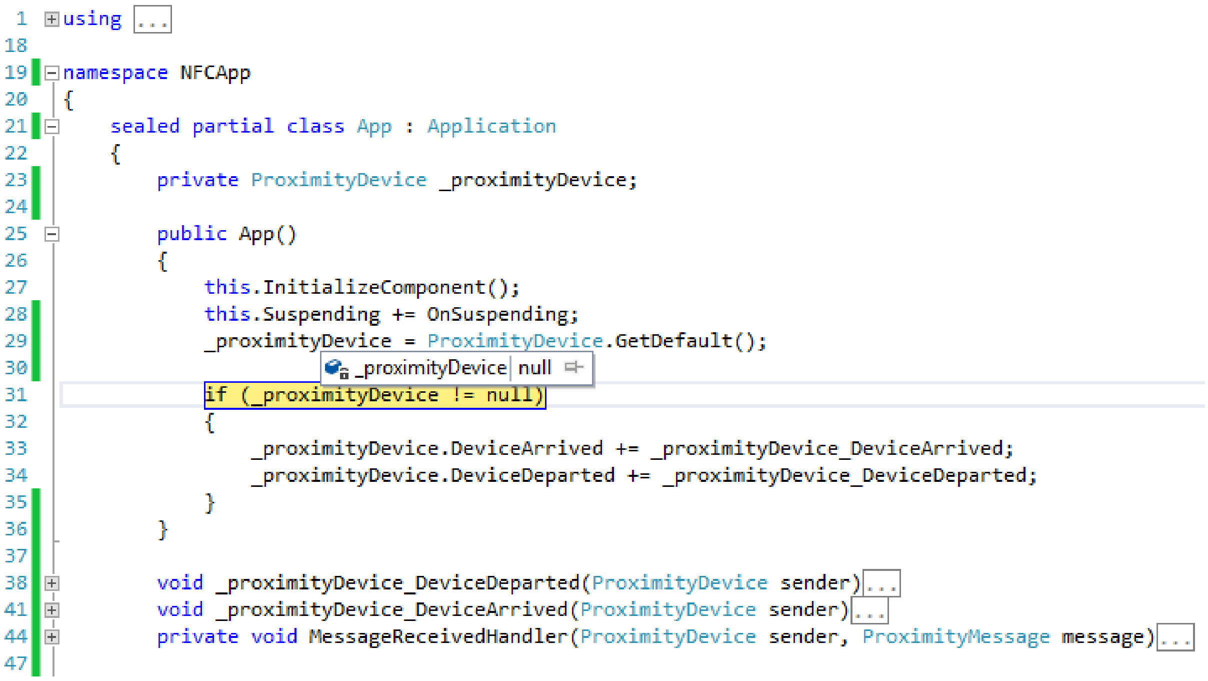


Name	Publisher	Installed On	Size	Version
ACR122U NFC Reader SDK	Advanced Card Systems Ltd.	19/04/2016		1.0.0.0
ACS Unified PC/SC Driver 4.1.0.0	Advanced Card Systems Ltd.	19/04/2016	1.77 MB	4.1.0.0
Adobe Digital Editions 4.5	Adobe Systems Incorporated	3/04/2016	19.8 MB	4.5.1
Adobe Flash Player 21 NPAPI	Adobe Systems Incorporated	8/04/2016	5.65 MB	21.0.0.213
Android SDK Tools	Google Inc.	22/06/2015		1.16
Android Studio	Google Inc.	21/06/2015		1.0

Figure 6.10: Programs and Features (after ACR122U SDK installed)

With the researcher's limited knowledge of NFC application development at that point in time, the setup of the NFC reader/writer was considered to be successfully completed and the development of the prototype had commenced. According to the research plan, the prototype was developed as a Window Store App in Visual Studio 2013 using C# .NET framework and Window Proximity API. Instead of creating a Windows Desktop application, the prototype was created as a Windows Store App because access to the WinRT Features such as Proximity APIs is more seamless and less restricted from Windows Store Apps (Xavier, 2012).

Using WinRT in C# .NET framework, accessing the NFC devices began with instantiating a ProximityDevice object using the ProximityDevice class. This instantiation was done by invoking the "GetDefault" static method of the ProximityDevice class in the Windows.Networking.Proximity package. Once a ProximityDevice object was instantiated, it was used by the application in handling events such as an NFC device getting within the communication range and leaving the communication range by subscribing to DeviceArrived and DeviceDeparted events. However, as shown in the following Figure 6.11, the GetDefault static method of the ProximityDevice class always returned a null object in this prototype, preventing any further development.



```
using ...

namespace NFCApp
{
    sealed partial class App : Application
    {
        private ProximityDevice _proximityDevice;

        public App()
        {
            this.InitializeComponent();
            this.Suspending += OnSuspending;
            _proximityDevice = ProximityDevice.GetDefault();
                          _proximityDevice null
            if (_proximityDevice != null)
            {
                _proximityDevice.DeviceArrived += _proximityDevice_DeviceArrived;
                _proximityDevice.DeviceDeparted += _proximityDevice_DeviceDeparted;
            }
        }

        void _proximityDevice_DeviceDeparted(ProximityDevice sender)...
        void _proximityDevice_DeviceArrived(ProximityDevice sender)...
        private void MessageReceivedHandler(ProximityDevice sender, ProximityMessage message)...
```

Figure 6.11: Issue in using Proximity Library

After some in-depth research it was found that “FeliCa” NFC card readers/writers from Sony were the only devices that could be recognised as Proximity devices by the WinRT on Windows 8 and higher versions. Figure 6.12 presents how a Sony’s FeliCa NFC card reader/writer appeared as a proximity device in the Windows Device Manager panel.

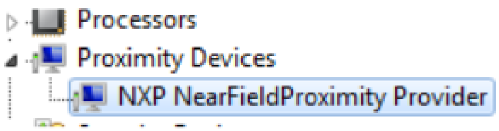


Figure 6.12: FeliCa NFC device in Windows Device Manager (“NFC Troubleshooting Guide”, n.d.*)*

The reason for this is that NXP Semiconductors, Sony’s joint venture partner in enabling the global adoption of contactless smart card applications on mobile phones (“NXP and Sony announce joint venture”, 2006), is the only provider of proximity driver software compatible with Windows 8 and above (Sharief, 2013). Therefore, application development using any other NFC card reader/writer devices for Windows 8 or higher versions required resorting to less generic approaches, such as low-level socket-based connection, instead of making use of Windows Proximity

APIs, the more abstract and portable approach provided by the WinRT. Use of socket-based connections required reserving certain IP addresses and ports for the communication purpose between the devices. Such requirement could result in imposing some issues, such as IP and port conflict etc., as the application could be interacting with multiple devices dynamically.

Unlike Electronic Funds Transfer at Point of Sales (EFTPOS) systems, where both hardware and software are provided by the same vendor, usually by a financial institution, this research does not picture that a specific brand of NFC reader/writer devices, pre-configured to use certain IP address and port, will be provided by the software vendor of the Electronic Prescribing System (EPS) or Electronic Dispensing System (EDS) for the mobile electronic prescription transfer.

In addition, there may be various applications and peripherals devices installed at the prescriber's or dispenser's facility, potentially resulting in some of those required IP addresses and ports already being occupied. Therefore, in order to be a vendor agnostic solution in this primary health care environment, use of low-level socket-based connections in implementing the mobile electronic prescription transfer application is likely to be impractical in reality.

Despite the fact that the prototype development was deterred by the lack of a publicly available proximity driver for the NFC card reader/writer being used, this experiment found another aspect of limitation in NFC's interoperability. The NFC Data Exchange Format (NDEF) is the most widely supported format by various manufacturers and it was the format in which most NFC devices and applications exchange data with one another.

According to the NDEC specification, the capacity of the NDEF payload was 232-1 (i.e. approximately 4GB) but it was mostly limited by the storage capacity of the NFC tag or device participating in the data exchange. However, if the data to be exchanged was in a non-NDEF format, the interoperability would be severely limited because defining the protocol stack for exchanging data was entirely up to the application developer ("Advanced NFC", n.d.). This not only severely impacted the application's interoperability but also inherently introduced security-, reliability- and efficiency-related risks.

6.2.3 Experiment 2: Results/Outcomes.

Despite how it initially appeared, this experiment found that interfacing with the NFC readers/writers (i.e. except for the FeliCa NFC card readers/writers) required the use of the software development kit (SDK) provided by the hardware manufacturer. This severely limited the solution's portability (i.e. interfacing with different NFC readers/writers by various manufacturers) and interoperability (i.e. integration with EPS and EDS developed by various software vendors). On the other hand, the necessity to use a specific brand of NFC reader/writer (i.e. the FeliCa NFC card readers/writers) for all the Electronic Prescribing Systems (EPS) and all the Electronic Dispensing Systems (EDS) was too limiting and impractical for the Australian healthcare industry. In fact, this experiment discovered that use of NFC technology failed to be both device manufacturer agnostic and EPS and EDS software vendor agnostic from the perspectives of application development, portability and interoperability.

Therefore, this experiment deemed that the NFC technology was not a suitable alternative transport mechanism for transferring electronic prescriptions between the EPS, the EDS and the client's/patient's smartphone.

6.2.4 Experiment 2: Lessons Learnt.

The tools and sample applications provided by the manufacturer were primarily designed for configuring the security settings of the NFC cards and the device itself and for reading/writing the data to and from the NFC cards at the block and segment levels.

NFC has the best interoperability at the end-user level for exchanging photographs, contacts and web URLs. However, this experiment found that development of NFC application in C# for the non-mobile environment, such as Desktop or Windows Store App environments, was not as efficient and portable as its mobile counterparts. The NFC application development was the most efficient and best supported in the mobile environment where the driver software, along with the hardware, is provided by the manufacturer. Essentially, any issues between the hardware and the driver software were taken care when the device was manufactured with inbuilt NFC capability. However, application development for NFC in the Windows desktop environment, including the Windows Store Apps, is yet to mature and still has room for improvement.

Although the exchange of NDEF-type data between various NFC devices and applications are widely supported among various NFC devices and applications, exchanging the non-NDEF data requires defining the protocol stack and thus has very limited interoperability compared to the NDEF data.

6.2.5 Experiment 2: Modifications.

Since this experiment proved that the NFC technology is not suitable for transferring electronic prescriptions between the EPS, the EDS and the client's/patient's smartphone, the researcher has commenced the next iteration by conducting a detailed literature review on Bluetooth, the rival technology in short range radio communication. The next section (Section 6.4) describes the detailed literature review on Bluetooth technology and is followed by Section 6.5 in which its suitability for transferring electronic prescription information in the proposed fully electronic mobile ETP solution is verified through an experimentation.

6.2.6 Conclusion

Despite the findings from the preliminary study, this experiment proved that use of NFC technology is not suitable (see sections 6.2.2 and 6.2.3 for details) for the proposed mobile ETP solution. The experiment found that only the Sony's FeliCa NFC reader/writer can be programmed using C# .NET and Windows Proximity API, and the rest of the NFC reader/writer devices required the use of SDK from their device manufacturers. This is mainly due to the hardware manufacturers not making the proximity driver of their devices publicly available for software development and integration.

This experiment concluded as a failure because, if developed using any of these vendor-specific SDK, the solution would work only for those specific devices, thereby introducing a portability issue that invalidates the use of NFC technology as a practical solution for the Australian healthcare industry.

6.3 Learning from the Research

Despite NFC technology's widespread support from most mobile device manufacturers, excellent end-user level interoperability and explicit acceptance by users even in mission critical operations such as financial transactions (i.e. mobile payments), this experimentation found that it has much room for improvement in the software development from the perspectives of interoperability and portability.

The NFC application development was best supported in the mobile environment where the driver software and libraries were provided by the manufacturer alongside with the hardware. However, application development to interact with NFC devices in Windows environment (i.e. as extensions of EPS and EDS to communicate with its mobile counterpart) was yet to mature and still has much room for improvement.

The tools and utilities provided by the NFC device manufacturers are mainly designed to configure the security settings of the NFC cards/devices and to perform the read/write operations at the block and segment levels (i.e. low-level data access operations). At present, only the FeliCa NFC readers/writers are recognised as proximity devices on Windows 8.1 and later operating system platforms in order to leverage the use of Window Proximity API for software development. Application development for the other NFC devices necessitated resorting to using less generic/portable approaches such as low-level socket programming and vendor provided SDKs. Therefore, the application ends up being less interoperable and portable. These experiment outcomes have a severe impact on the practicality of the proposed mobile ETP solution for the Australian healthcare industry, where it was intended to be device manufacturer (i.e. NFC reader/writer) agnostic as well as EPS and EDS software vendor agnostic.

Furthermore, in this environment it is impractical to have an application which requires certain IP addresses and ports reserved solely for its communication purpose, as these may potentially be occupied by various other applications and peripherals installed at the prescriber’s or dispenser’s facility. Therefore, the use of NFC technology is deemed not suitable as the alternative transport mechanism for the proposed mobile ETP solution and hence the researcher commenced another iteration of experimentation on the next potential candidate rivalling NFC in short range radio communication; Bluetooth.

6.4 Bluetooth

6.4.1 A brief history and how it works

Bluetooth, named after the 10th century King Harald Blåtand (i.e. Harold Bluetooth in English) of Denmark, is a low-power, short-range radio communication technology for point-to-point and point-to-multipoint communications (“Bluetooth fact or fiction”, 2016). The men behind this technology were Sven Mattisson and Jaap Haartsen from Lund Ericsson Lab in 1998. It was initially called Multi-Communicator (MC) Links and was conceived as a low-cost wireless solution to replace RS-232 standard cables.

Bluetooth technology was the first low-power radio communication technology to wirelessly connect various accessories (i.e. devices such as wristband, headset and portable speaker etc.) from different industries (i.e. telecommunication, entertainment, health, sports and fitness etc.) (“Bluetooth fact or fiction”, 2016) enabling the building of Wireless Personal Area Networks (WPAN).

This technology unlocked many new opportunities for various devices and changed the consumer perspective permanently. In fact, Bluetooth has transcended its usual/intended applications by permeating various other devices across all industries and markets such as smart home, wearables and location-based technologies. Emergence of Bluetooth version 4, also known as Bluetooth Low Energy (BLE), enabled this permeation even further and its market growth can be witnessed in the following two figures (Kaye, 2014).

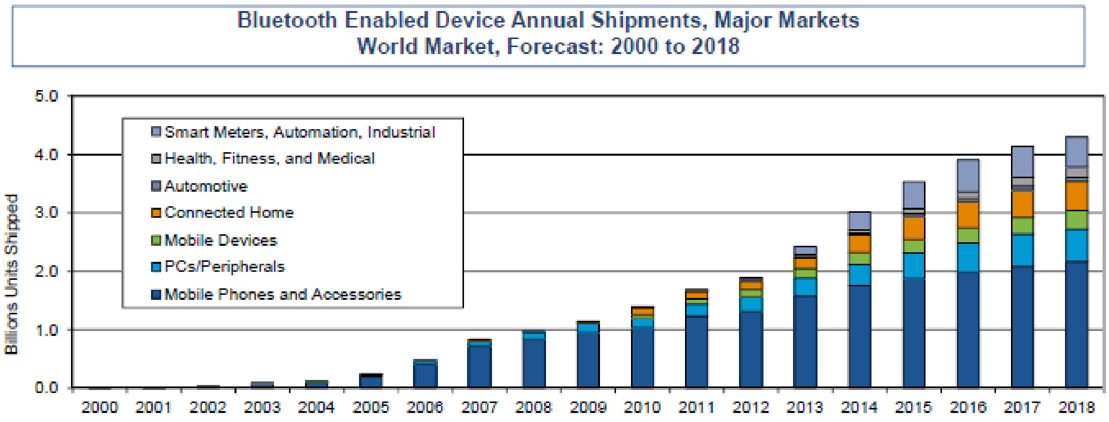


Figure 6.13: Bluetooth's market growth (Kaye, 2014)

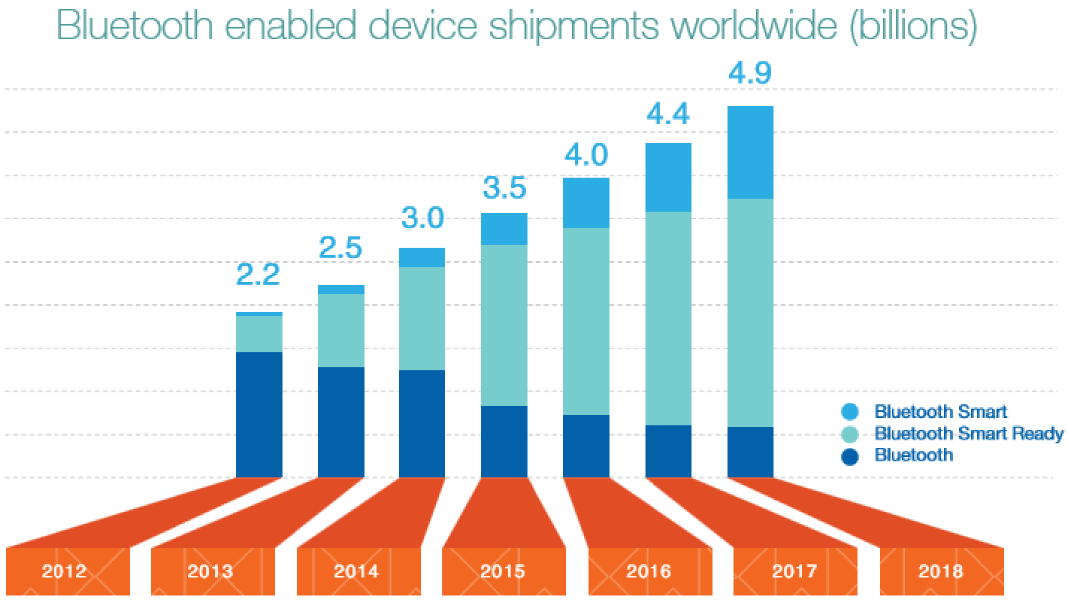


Figure 6.14: Bluetooth devices worldwide ("Bluetooth SIG 2014 Annual Report", 2015)

Bluetooth makes use of the spread spectrum frequency-hopping technology and shares the same frequency band, 2.4 GHz, with Wi-Fi and many other household appliances such as microwave oven and cordless phone ("What can an attacker do", 2013).

From its very early days, Bluetooth technology was governed and guided by the Bluetooth Special Interest Group (SIG). Bluetooth SIG was initially founded with five companies (i.e. Ericsson, IBM, Intel, Nokia, and Toshiba) and now it has over 33,000 members worldwide ("Wireless History Timeline", 2016; "Member Directory", 2016). Bluetooth version 3 (i.e. not the latest version but the most widely used version in current market) supports a data transfer rate up to 24 megabits per second (Mbps) and has three connection types: Asynchronous Connection-Less

(ACL), Synchronous Connection-Oriented (SCO) and extended Synchronous Connection-Oriented (eSCO). The ACL connection is used for both asymmetric and symmetric data transfer and the integrity of data is ensured by the packet retransmission (IEEE, 2005). SCO connection is symmetric and used for real-time two-way voice communication. The voice can be distorted when the Bit Error Rate (BER) is high as SCO does not use packet retransmission. The eSOC is symmetric and is also used for real-time two-way voice transmission. However, it ensures the data integrity by using retransmission packets. This assurance of data integrity enables eSOC connection to carry data packet as well (*ibid*).

When Bluetooth devices communicate with one another, the connection initiator becomes the piconet master and the remaining devices become slaves. A piconet is a tiny network composed of two or more Bluetooth devices occupying the same physical channel (i.e. synchronised to a common clock and hopping sequence) (Haataja, et al., 2013; "Communications Topology", 2016). Each Bluetooth-enabled device may participate in more than one piconet simultaneously and a slave in one piconet can be a master in another piconet. Within a piconet all communications go through the piconet master, and the piconet master is also in charge of the frequency hopping and synchronisation with the slave devices. When piconets share a common device between them, the common device relays the data between the different piconets and together they form a scatternet. These common piconet members are called scatternet members and it is how Bluetooth extends its data transmission range restriction (*ibid*). This network topology and how it works is roughly depicted in the following diagram, Figure 6.15.

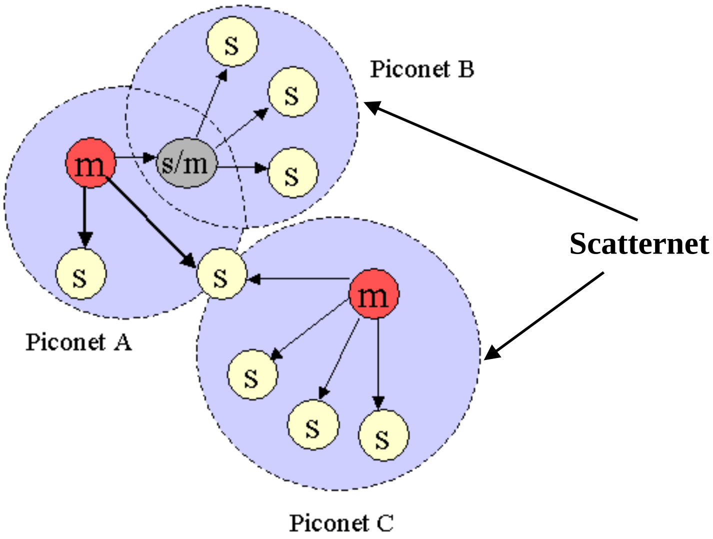


Figure 6.15: Bluetooth network topology (Mahmoud, 2003)

Current Bluetooth architecture allows up to seven active slaves in a piconet, with many more connected in parked state in which slaves enter reduced power mode but remain synchronised with the master, ready to be active and part of the piconet again ("Baseband Architecture", 2016; Blankenbeckler, 2010; "Communications Topology", 2016).

6.4.2 Architecture and Security

Bluetooth architecture consists of the core system and specific profiles based on the intended use case or application. Each Bluetooth profile states possible applications and defines the general behaviours of how it will communicate with other devices in order to achieve its function. Therefore, a Bluetooth-enabled device must be able to interpret certain Bluetooth profiles to perform its intended functions.

Fundamentally, Figure 6.16 depicts the Bluetooth core system specified by both Bluetooth SIG and IEEE Std 802.15.1-2005. The diagram also shows that the lowest three layers (i.e. Link Manager, Baseband and Radio layers) of the Bluetooth core system are grouped into a subsystem called Bluetooth Controller.

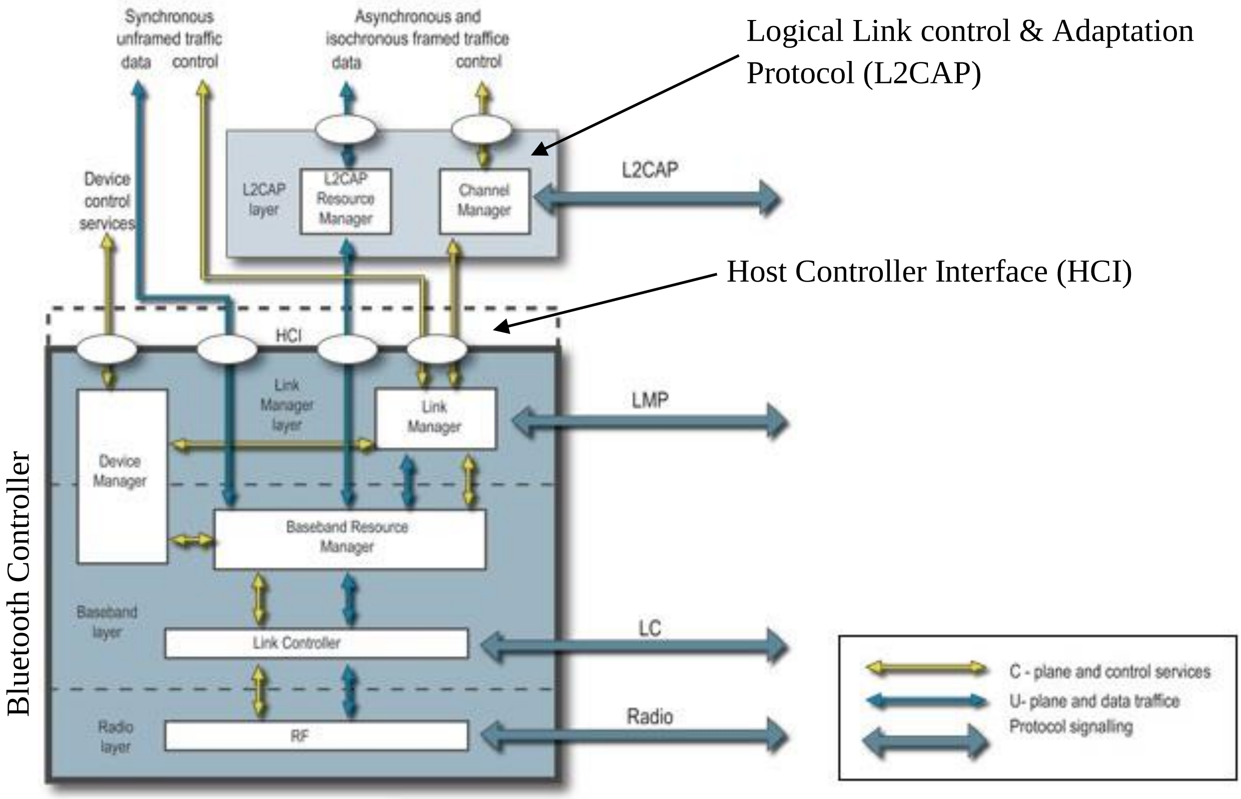


Figure 6.16: Bluetooth core system ("Core System Architecture", 2016)

Just as the lowest three layers of the Bluetooth stack are grouped into the Bluetooth Controller subsystem, the rest of the layers, except the Application Layer, are grouped together as the Bluetooth Host subsystem. The interoperability between the two subsystems, Bluetooth Controller and Bluetooth Host, is supported by defining the common interface (“Core System Architecture”, 2016).

There is a wide range of Bluetooth profiles, each describing many different types of applications or use cases for devices, and the Bluetooth-adopted specification section of the Bluetooth SIG website lists a wide range of supported profiles for each specific Bluetooth core specification version. Interoperable or compatible applications are to be designed and developed by following the guidance provided by these specifications and profiles ("Adopted specifications", 2016). Figure 6.17 provides a high-level perspective on how the Bluetooth profiles and the core system fits together to form the entire Bluetooth protocol stack.

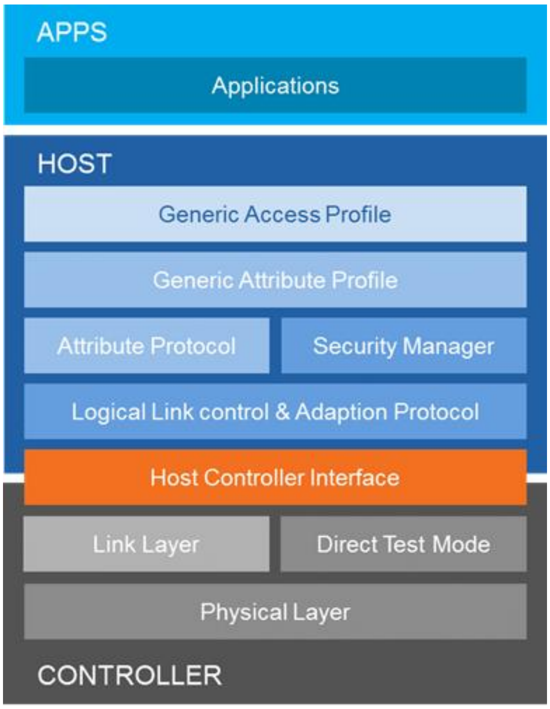


Figure 6.17: Bluetooth protocol stack ("Bluetooth core specification", 2016)

Due to the way they are illustrated, the prior two diagrams (Figure 6.16 and 6.17) do not clearly show how they fit together. Therefore, Figure 6.18 emphasises on showing how they are related and integrated.

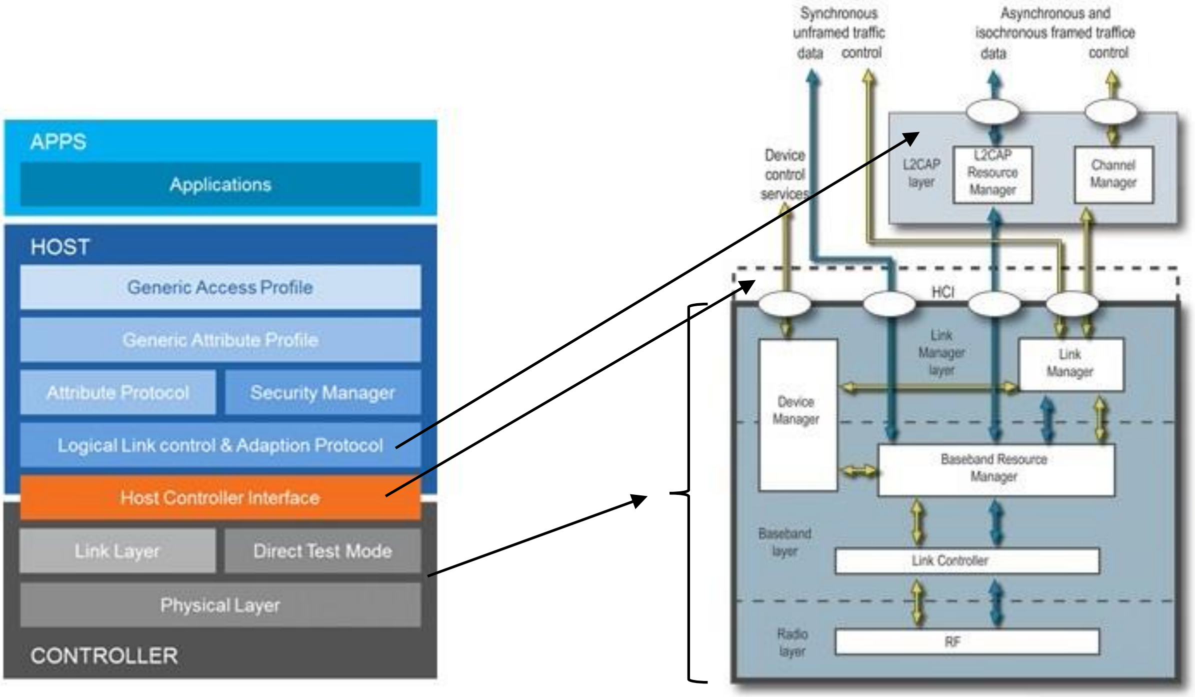


Figure 6.18: Bluetooth protocol stack and core system mapping ("Bluetooth core specification", 2016; "Core System Architecture", 2016)

In Figure 6.19, the IEEE Std 802.15.1 compares the OSI 7 layers model with the Bluetooth's protocol stack. The diagram also includes IEEE 802.2 as a transitioning step between the two models as it shows the division of Data Link layer of the OSI model into MAC and LLC layers.

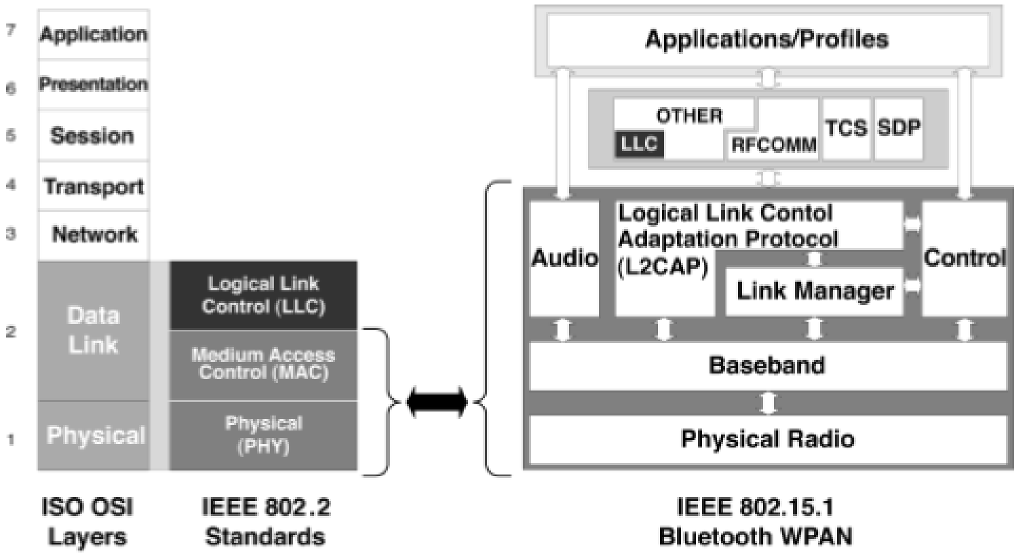
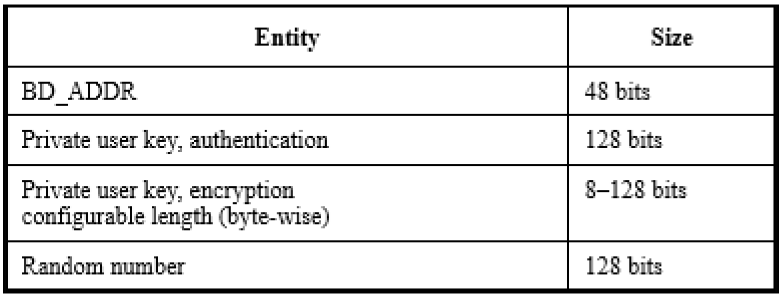


Figure 6.19: OSI layers and Bluetooth protocol stack mapping (IEEE, 2005)

The IEEE Std 802.15.1 specified Bluetooth's security in terms of encryption, authentication and key generation schemes. In order to support usage protection and information confidentiality, security measures are provided at both Application Layer and Link Layer. Although user information is protected by encrypting the packet payload using a stream cipher called E_0 which is resynchronized for every payload, the IEEE Std 802.15.1 dictates that the access code and packet header shall never be encrypted (IEEE, 2005).

Bluetooth's security fundamentals are Bluetooth Device Address (DB_ADDRESS), two secret keys and a pseudo-random number which will be generated for each new transaction. Table 6.3 summarises each of those entities and their sizes (*ibid*).

Table 6.3: Bluetooth security entities and their sizes (IEEE, 2005)



Entity	Size
BD_ADDR	48 bits
Private user key, authentication	128 bits
Private user key, encryption configurable length (byte-wise)	8–128 bits
Random number	128 bits

The Bluetooth Device Address (BD_ADDR) is the primary identifier of a Bluetooth device, similar to Ethernet Media Access Control (MAC) address, and is acquired by the user interactions or via the automatic enquiry routine by a device. This 48-bit number uniquely identifies a Bluetooth device among peers in the piconet. Both secret keys, the authentication key and encryption key, are derived during the initialisation. The authentication key is often referred to as the link key, underlining its importance to the link/connection.

As described in Table 6.3, the authentication key is a 128-bit random number shared between two or more parties as the base of all security transactions between these parties. The link key is not only used in the authentication routine but is also one of the parameters in deriving the encryption key. Whilst the encryption key and authentication are completely different keys, the encryption key is derived from the authentication key during the authentication process and each time encryption is activated. The piconet master can use separate encryption keys for each slave device in a point-to-multipoint configuration with ciphering activated. The random number is generated by a random or pseudo-random process in the device as a nonrepeating (i.e. it is highly unlikely that the value will repeat within the lifetime of the authentication key) and randomly generated (i.e. the chances of predicting its value is not significantly greater than zero) number (“Baseband Architecture”, 2016; Blankenbeckler, 2010; "Communications Topology", 2016; IEEE, 2005).

Utilising these fundamental security components, Bluetooth Security Manager (SM) provides the Bluetooth protocol stack to generate and exchange security keys to create encrypted link for secure communication among peers. It defines two roles, Initiator and Responder, and supports three security procedures: Pairing, Bonding and Encryption Re-establishment. The Pairing procedure generates a temporary security key or short-term key (STK) and creates an encrypted link.

However, the generated security key is not stored and thus cannot be reused for later connections. The Bonding procedure on the other hand, which also includes the pairing step, creates a permanent association by sharing the security key which will be used for later connections until deleted by either side of the connection. Once bonded, the Encryption Re-establishment procedure defines how to re-establish a secure encrypted connection without having to go through the Bonding (i.e. Pairing and Bonding) procedure (IEEE, 2005; Townsend, et al., 2014). These Pairing and Bonding processes are depicted in the Figure 6.20.

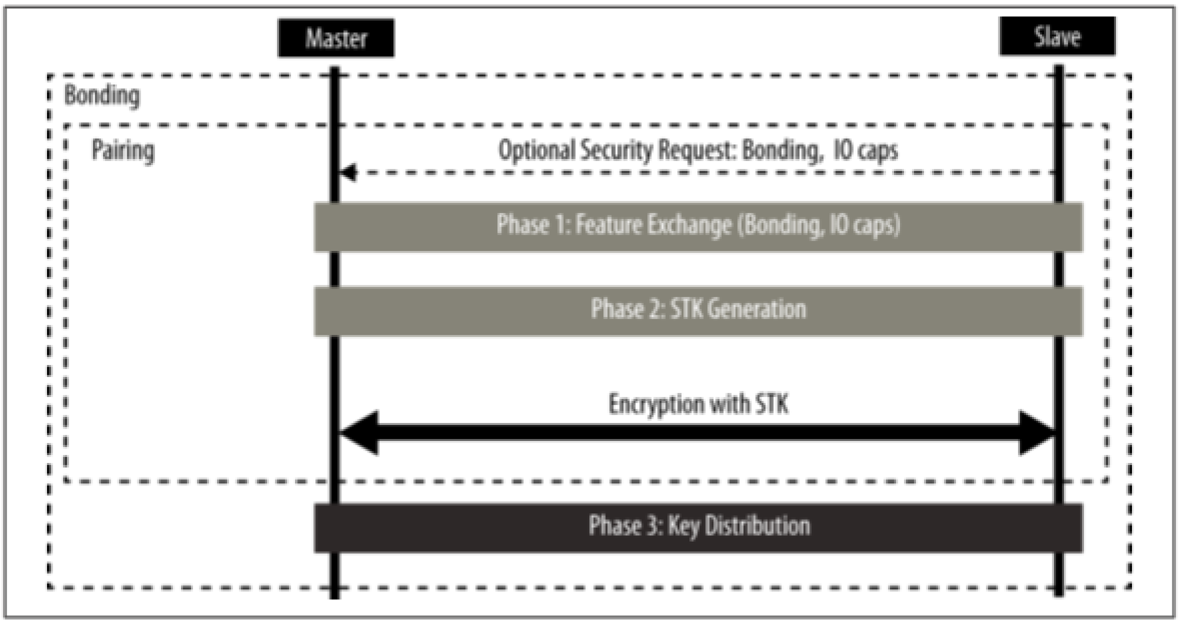

Master
Slave
Bonding
Pairing
Optional Security Request: Bonding, IO caps
Phase 1: Feature Exchange (Bonding, IO caps)
Phase 2: STK Generation
Encryption with STK
Phase 3: Key Distribution

Figure 6.20: Bluetooth pairing and bonding (Townsend, et al., 2014)

6.4.3 Governing Standards

All the Bluetooth specifications were formalised by the Bluetooth SIG upon its establishment in 1998. Soon after that, in early 1999, Bluetooth was also adopted as IEEE Std 802.15 by the Working Group for Wireless Personal Area Networks within IEEE ("Wireless History Timeline", 2016; IEEE, 2005).

6.4.4 Reasons for being a good candidate for the proposed solution

Although this research could not find a consolidated list of mobile smartphones that support Bluetooth technology, the support for Bluetooth on mobile smartphones is no less than that of NFC ("iOS: Supported Bluetooth profiles", 2015; "Any Android phones that do not support Bluetooth", 2012).

Bluetooth technology has a longer communication range compared to NFC and this exposes the radio signal to signal interception attacks. However, its spread spectrum frequency-hopping behaviour, in addition to encryption, provides extra security against such threat. Using Adaptive Frequency Hopping (AFH), Bluetooth hops 1600 times per second between 79 channels within 2.4 GHz and 2.48 GHz ISM band (i.e. Industrial, Scientific and Medical radio bands) (“What can an attacker do”, 2013).

Using the Bluetooth technology, establishing connection between devices is less seamless, requiring extra steps to be performed manually, compared to using the NFC technology. However, from the perspective of mobile electronic prescription transfer application, this requirement to pair the devices (i.e. between prescriber’s device, client/patient’s smartphone and dispenser’s device) can be considered an additional security measure. Moreover, this pairing is not required for subsequent operations once the devices have been paired and bonded.

From its early days, implementation and compliance of the Bluetooth technology has been closely governed and guided by the Bluetooth SIG. With manufacturers strictly adhering to the relevant profile specification of the device type, the interoperability between devices by different manufacturers from various industries is well supported. Moreover, with the release of version 4.x, Bluetooth also helped change the face of the healthcare industry as its increased use in many medical devices enables consumers to control and manage their own health.

6.4.5 Potential issues of Bluetooth for the proposed solution

Like any other wireless communication technology, Bluetooth is vulnerable to some security threats inherently. First of all, although Bluetooth’s standard communication range is 10 metres, it is not guaranteed that the radio signal is not accessible beyond that distance. This characteristic exposes Bluetooth’s signals to be easily interceptable by would-be attackers.

Along with its popularity and widespread uses, there are malware and worm programs exploiting Bluetooth design and/or implementation vulnerabilities. The Caribe worm and Bluejacking would be the less harmful form of these whilst Bluebugging can be more dangerous as it allows the attacker to remotely access the compromised phone and use its features, such as making/forwarding/listening calls and text messages.

The Caribe (also known as Cari and Cabir.B) is the world's first wireless worm which runs on the Symbian Operating System (Millard, 2004). Whilst most Internet-delivered content (i.e. primary source of various malware) is filtered by the telecommunication carrier for security, the Caribe worm replicates over Bluetooth connections in the form of a file called "caribe.sis" in the phone's messaging inbox. When the user clicks the file and chooses to install it, the worm infects the device and starts looking for other Bluetooth-enabled devices to infect over Bluetooth connection (*ibid*). The worm scans for other Bluetooth-enabled devices and attempts to send itself onto the first device found every time the device is powered off and back on (i.e. propagation is triggered by the device activation). Setting a device to non-discoverable mode protects the device from being infected by the Cabir worm. However, once compromised, even disabling Bluetooth does not stop an infected device from infecting the other devices ("Bluetooth-Worm:SymbOS/Cabir", 2017; "SymbOS.Cabir", 2017).

Bluejacking, also known as Bluespamming, allows the sending of unsolicited messages to other Bluetooth-enabled devices via Bluetooth. Despite the name, it neither hijacks nor steals information from the device. This technique uses the basic Object Exchange Stack that was used for "beaming" business cards and applications via Infrared on Palm OS and exploits the discoverability feature of Bluetooth devices. Whilst it generally poses minimal security risk, it can be extremely bothersome because the message alerts the recipient to take action such as reading, responding or deleting it (Leyden, 2003; Tan, 2007).

Bluebugging on the other hand is taking full control of the device without the owner's knowledge by exploiting the outdated firmware with faulty/vulnerable Bluetooth implementation. This attack begins by first gaining the trusted device status, potentially using the business-card transfer process, and then establishing a connection with the targeted device by tricking it into believing that the attacker's device is a harmless peripheral such as a Bluetooth headset. Once this is achieved, the compromised device and the data within are at the mercy of the attacker since most functions of the device can be controlled by the attacker via the AT command codes (i.e. the ATtention command set, also known as the Hayes command set, which is typically used by developers and service technicians). Fortunately, the vulnerability to Bluebugging attack was addressed in the later firmware upgrades (Doherty, 2015).

Essentially, just as Doherty (2015) mentioned, Bluetooth presents a trade-off between convenience and security, and it will always be vulnerable to the limitations of user education and user risk awareness. Since this research is not about Bluetooth's security, it relies on the relevant authorities producing security patches and necessary firmware upgrades, white-hat hackers exposing the vulnerabilities before the black-hat ones exploiting them. The experiment in Section 6.5 is to determine whether Bluetooth is a suitable electronic prescription transfer mechanism alternative to using the Internet for the proposed fully electronic mobile ETP solution.

6.4.6 Conclusion

Bluetooth is the first widely used radio technology for wireless peer-to-peer connection and with its constant advancements over the time, such as the advent of Bluetooth Low Energy (BLE), it is still going strong after almost two decades. Basically, Bluetooth technology is the global standard enabling the Internet-of-Things (IoT) by assuring the connectivity between various devices from various industries ("Bluetooth", 2016). Its widespread uses in various applications familiarises consumers with how the technology works, its security and reliability. Based on this familiarity and trust, built over a period of almost two decades, use of Bluetooth technology for mobile electronic prescription transfer is likely to be well accepted by the users.

Bluetooth is well supported by most mobile smartphone manufactures and has an excellent interoperability between devices, which is assured by the Bluetooth SIG ("iOS: Supported Bluetooth profiles", 2015; "Any Android phones that do not support Bluetooth", 2012). It is strongly supported by a large development community, with a variety of frameworks and tools/utilities on various hardware and/or software platforms.

Compared to NFC, Bluetooth also has better support from the device manufacturers and software vendors. The research findings so far indicate that among all the current wireless communication technology Bluetooth is likely to be the most suitable transfer mechanism for the mobile electronic prescription transfer application. Nevertheless, whether it actually possesses adequate security measures to be an alternative secured transfer mechanism for electronic prescriptions and its practicality (i.e. from development and deployment of the solution perspectives) is yet to be determined by one of the experimentations in the next section (Experiment 3: Bluetooth – Security of data in transit).

6.5 Experiment 3: Bluetooth – Security of the data in transit

6.5.1 Overview

Prior experiment was conducted using NFC technology as the transfer mechanism for exchanging electronic prescription data between devices. Despite its widespread support and excellent interoperability between devices at the end-user level, support for software development by the product manufacturers, such as availability of software drivers and software development frameworks, are still fairly limited. An example of this limitation is the fact that only the Sony FeliCa NFC card readers/writers are recognised as proximity devices by the Windows 8 and later versions, due to unavailability of the proximity driver for the products manufactured by other vendors.

The necessity to use a specific brand of NFC reader/writer devices for both the primary care's Electronic Prescribing System (EPS) and the pharmacy's Electronic Dispensing System (EDS) is too limiting and this research does not deem it practical in reality for the Australian healthcare industry.

Therefore, to come up with a more vendor agnostic and practical solution in this primary healthcare environment, another experiment for transferring the electronic prescription data between the PCs (i.e. primary care's EPS and pharmacy's EDS systems) and the mobile smartphone (i.e. client's/patient's phone) is conducted using a more mature short-range wireless communication technology, Bluetooth.

6.5.2 Experiment details

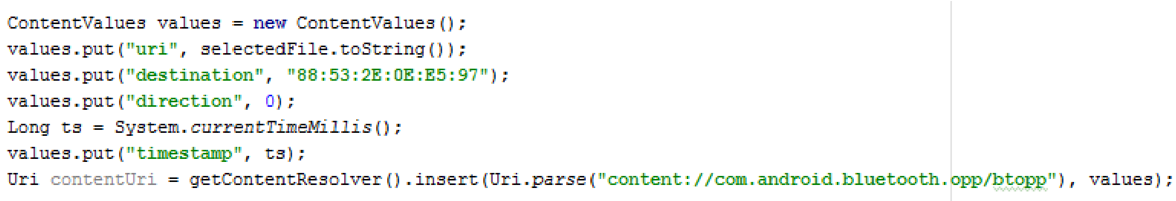
In this experiment, Bluetooth technology was used in transferring electronic prescription data between the prescriber's electronic prescribing system (EPS), the client's/patient's mobile smartphone and the pharmacy's electronic dispensing system (EDS). It is a mature technology with widespread support by almost all mobile smartphone manufacturers, an excellent interoperability among supported devices and adequate support for security. Although establishing connection between supported devices is not as seamless as using NFC since it requires manual pairing, this can also be considered an additional security feature in this application.

As per the prior experiment, this experiment was conducted using Windows 8 operating system platform since the majority of the Clinical Management Systems used at primary care clinics and Pharmacy Management Systems in Australia run on Windows operating system platform. Therefore, despite the change of technology in transferring the electronic prescription data, both the desktop application and its mobile counterpart will remain using the same operating system platforms, Windows 8 and Android. However, instead of using a desktop PC with external USB Bluetooth adaptor/dongle, similar to using the USB NFC card reader/writer as in the prior experiment, this experiment was conducted using a laptop with inbuilt Bluetooth capability to communicate with the mobile smartphone.

The Windows metro application for the transfer of the electronic prescription from the prescriber's electronic prescribing system (i.e. most likely a desktop PC or a laptop) to the client's/patient's mobile smartphone via Bluetooth can be implemented using various frameworks such as 32feet.NET open-source library from *CodePlex* or the *PeerFinder* class from the "Windows.Networking.Proximity" class library of the .NET framework. *CodePlex* is Microsoft's open-source project hosting website where people from various professions and industries share projects and ideas. Since many resources and support can be found from various sources for utilising these libraries and frameworks, implementation of the Windows 8 metro application was not the focus of this proof of concept prototyping experiment. On the other hand, due to the limited processing power, storage space and supported features on mobile devices compared to those of PCs, encryption/decryption of the prescription may not actually be practical even if transferring the electronic prescription via Bluetooth is achievable. Therefore, this experiment will focus on the development of the application prototype for transferring the electronic prescription from the client's/patient's Android smartphone to the pharmacy's electronic dispensing system (EDS) from achievability and practicality perspectives. As a result, an experimental prototype is to be developed for Android platform utilising full capacity of Android's native support for the transfer of electronic prescription via Bluetooth communication with encryption for adequate levels of efficiency, reliability, portability and security.

The Android application development environment on Windows 8 platform was completed as part of Experiment 1 (i.e. experiment for 128-bit symmetric encryption on Android for security of prescriptions from the data at rest perspective), and therefore allows this experiment to begin straight after Experiment 2 (i.e. experiment on transferring electronic prescription via NFC connection from a Windows 8 metro application to Android phone). Initially, based on prior experience in programming for Android, the researcher attempted to suppress the Bluetooth pairing dialog screen in order to make the connection establishing process as seamless as it was in NFC.

As shown in the following Figure 6.21, an attempt was made to suppress the Bluetooth pairing dialog screen by directly writing the destination device's address into to the content provider.



```
ContentValues values = new ContentValues();
values.put("uri", selectedFile.toString());
values.put("destination", "88:53:2E:0E:E5:97");
values.put("direction", 0);
Long ts = System.currentTimeMillis();
values.put("timestamp", ts);
Uri contentUri = getContentResolver().insert(Uri.parse("content://com.android.bluetooth.opp/btopp"), values);
```

Figure 6.21: Suppressing the Bluetooth pairing step on Android

At runtime, however, the above program code (Figure 6.21) generated the error shown in Figure 6.22. Despite having the correct access permission as illustrated in Figure 6.23, the debugging process (see Figure 6.24) identified that the error originated from accessing the Bluetooth share. Furthermore, the investigation revealed that, despite the application being granted the appropriate permissions to access the Bluetooth share, direct manipulation (i.e. writing) of the content provider is now protected for better security since Android version 4.1 ("Android Bluetooth print stopped working on 4.1", 2012). In Bluetooth 4.1 and later versions, sharing of file over Bluetooth was achieved as shown in Figure 6.25.

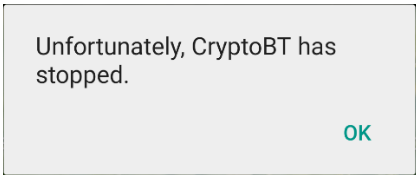

Unfortunately, CryptoBT has stopped.

Figure 6.22: Android runtime error (suppressing Bluetooth pairing)

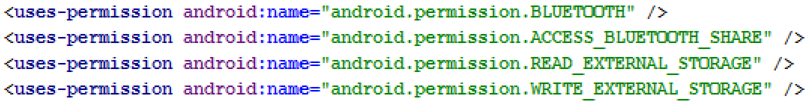

```
<uses-permission android:name="android.permission.BLUETOOTH" />
<uses-permission android:name="android.permission.ACCESS_BLUETOOTH_SHARE" />
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
```

Figure 6.23: Android permission for Prototype

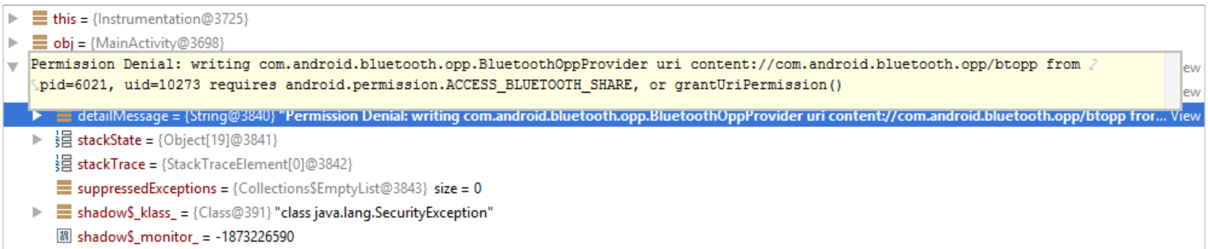

```
▶ this = {Instrumentation@3725}
▶ obj = {MainActivity@3698}
▼ Permission Denial: writing com.android.bluetooth.opp.BluetoothOppProvider uri content://com.android.bluetooth.opp/btopp from
  pid=6021, uid=10273 requires android.permission.ACCESS_BLUETOOTH_SHARE, or grantUriPermission()
  ▶ detailMessage = {String@3840} "Permission Denial: writing com.android.bluetooth.opp.BluetoothOppProvider uri content://com.android.bluetooth.opp/btopp fror... View
  ▶ stackState = {Object[19]@3841}
    stackTrace = {StackTraceElement[0]@3842}
    suppressedExceptions = {Collections$EmptyList@3843} size = 0
  ▶ shadow$_klass_ = {Class@391} "class java.lang.SecurityException"
    shadow$_monitor_ = -1873226590
```

Figure 6.24: Debugging the Bluetooth error

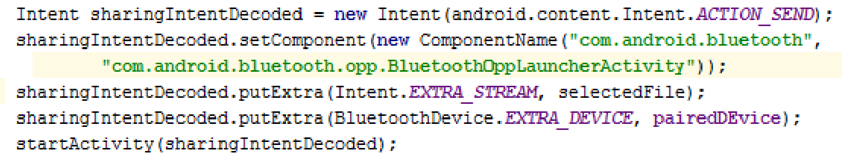
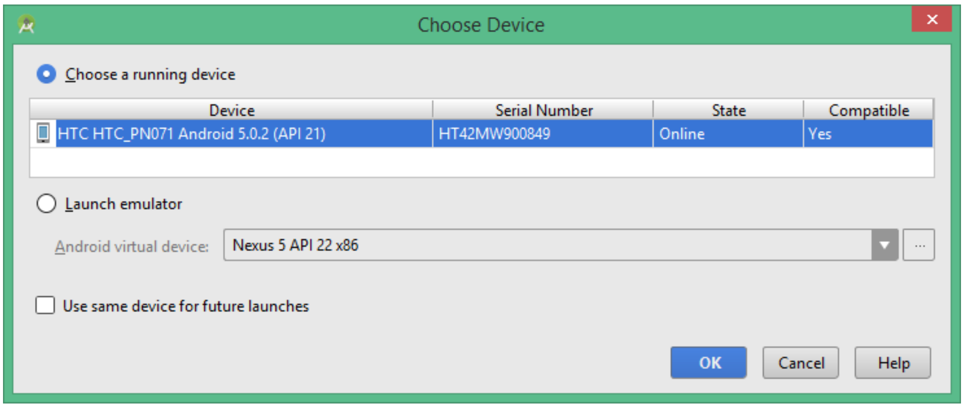

```
Intent sharingIntentDecoded = new Intent(android.content.Intent.ACTION_SEND);
sharingIntentDecoded.setComponent(new ComponentName("com.android.bluetooth",
        "com.android.bluetooth.opp.BluetoothOppLauncherActivity"));
sharingIntentDecoded.putExtra(Intent.EXTRA_STREAM, selectedFile);
sharingIntentDecoded.putExtra(BluetoothDevice.EXTRA_DEVICE, pairedDEvice);
startActivity(sharingIntentDecoded);
```

Figure 6.25: Sharing file over Bluetooth (Bluetooth 4.1 and later versions)

However, when approach shown in Figure 6.25 was taken, a dialog box popped up listing all the devices paired with the mobile phone in order to pick one for the destination. In favour of more seamless operation, the researcher attempted to suppress this dialog box by overriding the "android.bluetooth.devicepicker.action.LAUNCH" intent and broadcasting the "android.bluetooth.devicepicker.action.DEVICE_SELECTED" message in response to it. Unfortunately, it was found that broadcasting these messages has been internal since Android 4.1 and thus only the Android system itself can send those intent ("Caused by: java.lang.SecurityException: Permission Denial", 2014).

Aside from these two failed attempts by the researcher in making the use of Bluetooth more seamless as if using the NFC, the development of the prototype went well and the selected sample CDA file was successfully sent via Bluetooth to the paired laptop. Figure 6.26 shows where the selection was made for the use of the attached device (i.e. via a USB cable) or the emulator when the prototype was executed in the Android Studio.


Choose Device

● Choose a running device

Device	Serial Number	State	Compatible
HTC HTC_PN071 Android 5.0.2 (API 21)	HT42MW900849	Online	Yes

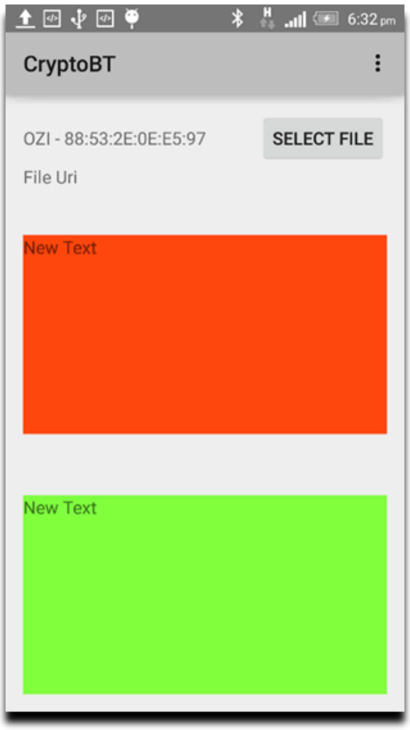
○ Launch emulator

Android virtual device: Nexus 5 API 22 x86

□ Use same device for future launches

Figure 6.26: Device selection in Android Studio

Except for a few preliminary steps, all the testing in this experiment was conducted using an actual Android device connected via USB connection instead of the software emulator. Once the selection was made to use the connected Android device, the prototype was executed on that device as shown in the figure 6.27.



OZI - 88:53:2E:0E:E5:97

File Uri

New Text

New Text

Figure 6.27: The prototype running on an Android device

In the prototype, the textbox with the red background is to display the encrypted content of the select CDA file and that with the green background will show the decrypted content of the previously encrypted file shown in the red textbox. Clicking on the “Select File” button will invoke a list of applications, as depicted in Figure 6.28, for selecting a file from various sources such as the Android file system or the Dropbox. However, before any file is selected from the Android mobile prototype application to be sent to the paired laptop via Bluetooth, the laptop needs to be set to receive the file via the Bluetooth connection as shown in Figure 6.29. This step is only required in this experiment because the prototype application does not have the desktop/PC/laptop side counterpart representing the application operating at the pharmacy's electronic dispensing system (EDS) end with which to receive the electronic prescription file from the client's/patient's mobile smartphone. The dialog shown in Figure 6.30 will be displayed once the "Receive a File" selection is made in Figure 6.29.

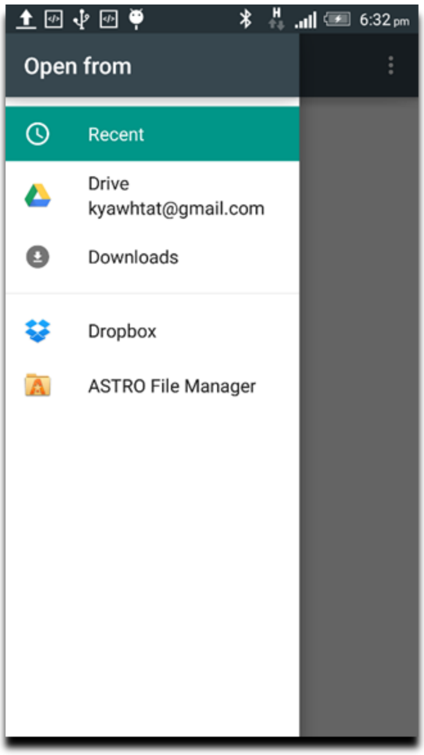


Figure 6.28: Selecting the file

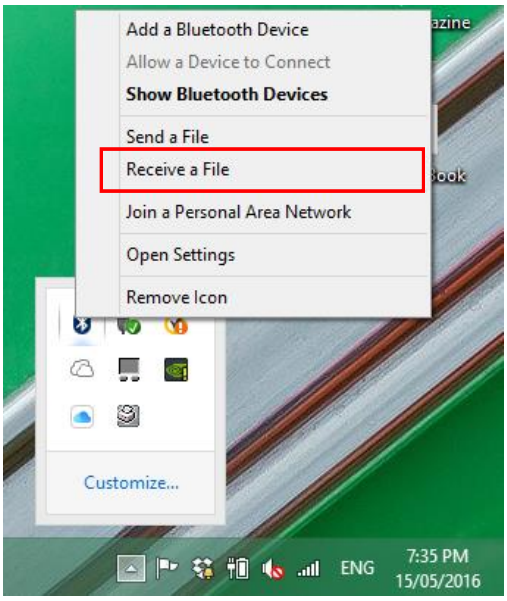


Figure 6.29: Receiving the file

The dialog displayed on the laptop in Figure 6.32 indicates that it is ready to receive the transmission so that the prototype running on the Android phone can transmit the CDA file via the Bluetooth connection to the laptop. Once the file to be sent is selected in the mobile prototype application, a dialog box will be displayed listing all the devices paired with phone (i.e. as the researcher's attempt to broadcast the message has failed) as shown in Figure 6.30.

When a destination is selected from the list, the prototype will commence encrypting the selected file. It will then save the encrypted content on the Android file system, display the encrypted content in the UI's red textbox and then decrypt the same content, to be displayed in the green textbox. The encrypted file written to the Android file system will then be sent to the selected destination via Bluetooth connection. Figure 6.31 depicts the prototype application after a file has been sent to the paired laptop.

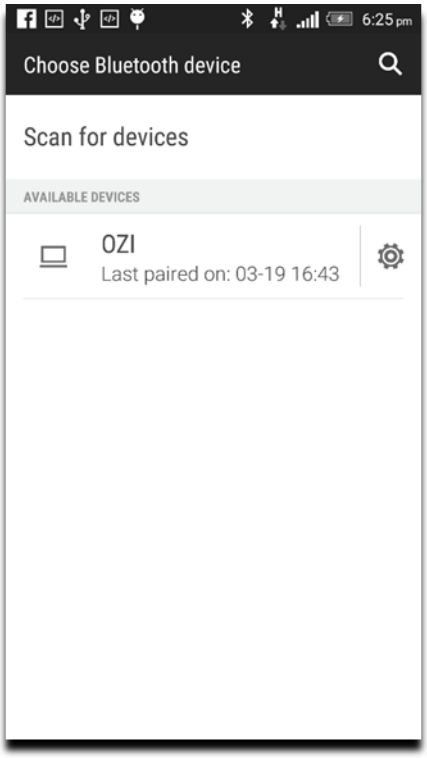
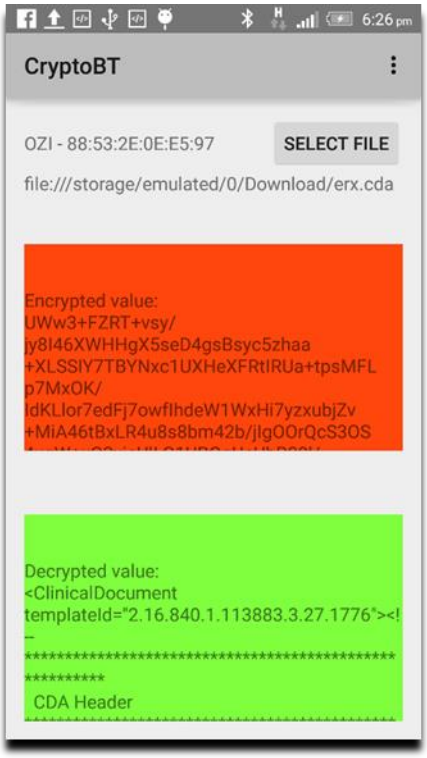


Figure 6.30: Selecting destination device



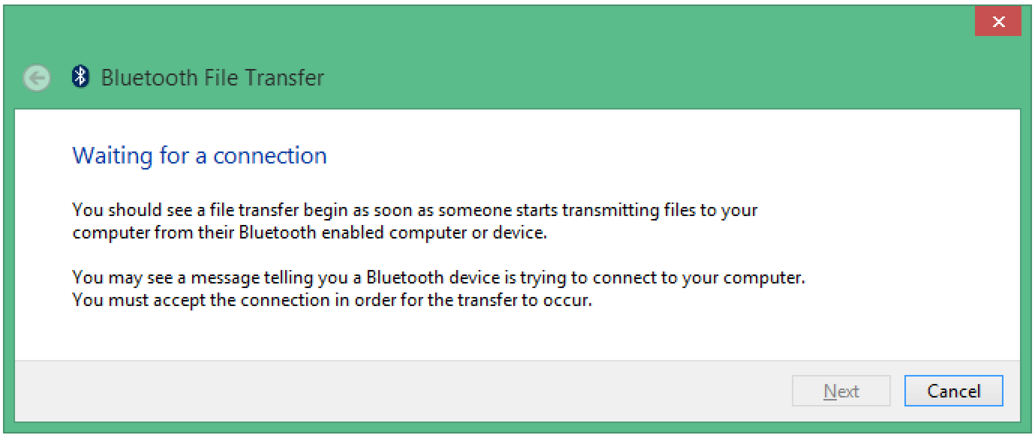
OZI - 88:53:2E:0E:E5:97

file:///storage/emulated/0/Download/erx.cda

```
Encrypted value:
UWw3+FZRT+vsy/
jy8I46XWHHgX5seD4gsBsyc5zhaa
+XLSSIY7TBYNxc1UXHeXFRtIRUa+tpsMFL
p7MxOK/
IdKLlor7edFj7owflhdeW1WxHi7yzxubjZv
+MiA46tBxLR4u8s8bm42b/jlgOOrQcS3OS
```

```
Decrypted value:
<ClinicalDocument
templateId="2.16.840.1.113883.3.27.1776"><!
–
*********************************************
**********
 CDA Header
```

Figure 6.31: Encrypted and decrypted content



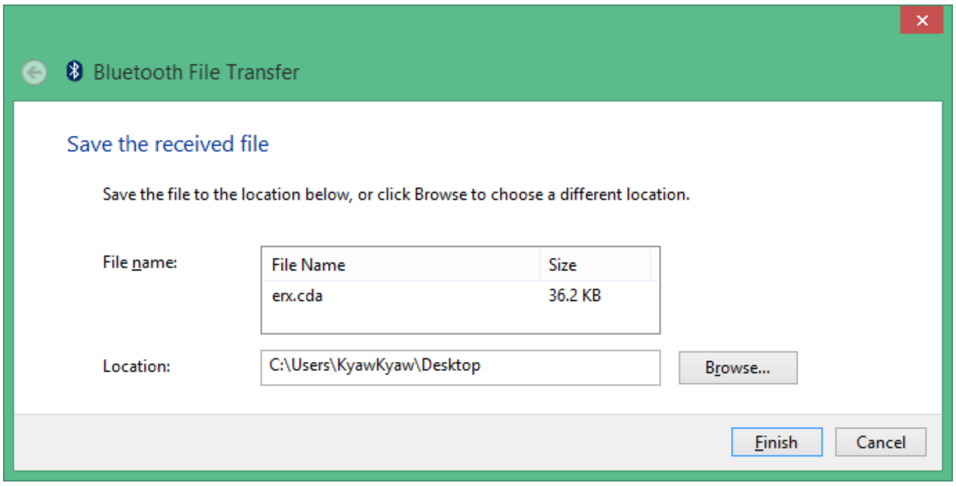
Waiting for a connection

You should see a file transfer begin as soon as someone starts transmitting files to your computer from their Bluetooth enabled computer or device.

You may see a message telling you a Bluetooth device is trying to connect to your computer. You must accept the connection in order for the transfer to occur.

Figure 6.32: Awaiting the file transfer

At this point in time, the laptop will have received the file and a dialog box similar to the one shown in Figure 6.33 will be displayed awaiting user's input on where to save the received file.


Bluetooth File Transfer

Save the received file

Save the file to the location below, or click Browse to choose a different location.

File name:

File Name	Size
erx.cda	36.2 KB

Location: C:\Users\KyawKyaw\Desktop

Figure 6.33: File received via Bluetooth (Windows 8.1)

Despite the fact that the process of establishing connection using Bluetooth is not as seamless as using NFC, the development of the prototype application went well without any issue. In addition to that, the prototype developed using the HTC One mobile works well on the Samsung Galaxy A3, with no changes or reconfiguration required. This experiment had no software driver related issue, and no special or vendor specific Software Development Kit (SDK) was required for using Bluetooth during the development of this prototype. Some modifications for improved security in the Android version 4 and later versions, such as making intents and messages protected, had an impact on the user-friendliness of the prototype; however, it was more of a nuisance in the connection establishing process than a critical deal breaker.

6.5.3 Experiment 3: Results/Outcomes.

This experiment found that the development of the prototype went well, neither experiencing any software driver related issue nor having to use manufacturer-specific SDK for using Bluetooth. The sample CDA file was successfully transferred from the mobile device to the paired laptop via Bluetooth with no performance issue. In addition, this experiment was successfully repeated on the Samsung Galaxy A3 phone (i.e. a device by different manufacturer) without any changes or reconfiguration. This proved that unlike the prior experiment, Experiment 2, use of Bluetooth as the alternative transfer mechanism will not suffer portability and interoperability issues.

Due the fact that the research context is highly proprietary, the detailed information on encryption mechanism used or security protocols employed in the current transfer mechanism using the Internet (i.e. security from data in transit perspective) is not public available. Therefore, this research was only focusing on the standards applied by and strict governance of the relevant authority bodies over the technology. Bluetooth's inbuilt security measures and standards are strictly governed by Bluetooth Special Interest Group (SIG) and IEEE standard 802.15.1-2005, and strict governance by these two reputable authority bodies can be considered having an adequate governance for an alternative electronic prescription transfer mechanism.

Therefore, this experiment concluded that the use of Bluetooth technology as the alternative transfer mechanism in the proposed mobile ETP solution is not only practical but also provides comparable assurance to the current approach (i.e. using the Internet) for the Australian healthcare industry. Although it was not the first choice of short-range wireless communication technology for this research, this experiment has proven that the Bluetooth technology provides adequate functionality and performance with sufficient security assurance for transferring electronic prescriptions between the EPS, EDS and client's/patient's mobile smartphone.

In general, use of Bluetooth technology made it possible to implement a prototype of a mobile electronic prescription transfer application that is both device manufacturer agnostic and EPS and EDS software vendor agnostic.

6.5.4 Experiment 3: Lessons Learnt.

Support for Bluetooth on mobile smartphones is no less than that of NFC and it comes with better support by the vendors from the software development perspective. As a mature technology, the use of Bluetooth in the development of this prototype required neither any vendor specific software development kit (SDK) nor software driver update. Another benefit of using this mature technology is an excellent portability and interoperability as this prototype works well on another Android smartphone by a different manufacturer without any issue and communicates seamlessly with the paired laptop exactly in the same way.

Bluetooth's requirement to pair the devices before data transfer operation was initially considered unintuitive and undesirable as it is the opposite of ubiquitous computing. However, since the pairing is not required for subsequent operations once the devices have been bonded, this experiment deemed the requirement for pairing as an added security feature for this application.

Although this experiment was conducted using a laptop with in-built Bluetooth capability, a USB Bluetooth adaptor/dongle can be used for this communication at the clinic or pharmacy instead of using a desktop PC or laptop with in-built Bluetooth capability. Bluetooth SIG's strict specifications and influence over the industry assures that it is vendor agnostic and the use of USB Bluetooth dongle will work just as well as the in-built Bluetooth feature.

6.5.5 Experiment 3: Modifications.

No further modification is required as this experiment succeeded in proving that the Bluetooth technology is suitable to be the transfer mechanism for exchanging electronic prescription data between devices such as a prescriber's EPS system, a patient's mobile device and a pharmacy's EDS system.

6.5.6 Conclusion

For this research, Bluetooth was not initially the preferred short-range wireless communication technology for transferring electronic prescription between the ETP participant devices (i.e. prescriber's EPS system, patient's mobile device and pharmacy's EDS system). However, this experiment proved that Bluetooth is suitable for such purpose in the proposed mobile ETP solution because it not only offers comparable security assurance to using the Internet but also provides a practical solution from the development, portability and interoperability perspectives (see Section 6.5.3 for details). It has a few inconveniences such as having to pair the devices for the first time use. However, use of other tool/technology such as NFC tags or QR codes can streamline this pairing process, and as an added benefit this pairing process can even be considered as an additional security measure.

6.6 Learning from the Research

Bluetooth is a mature technology with widespread support from almost all mobile smartphone manufacturers and has an excellent interoperability among supported devices with adequate support for security. Using Bluetooth, the process of establishing connection between supported devices is not as seamless as using NFC as it requires manual pairing for the first-time use. However, this pairing is not required for subsequent operations once the devices have been paired and bonded, and the extra step can in fact be considered an additional security feature in this application.

This experimentation's attempt to make the initial pairing process as seamless as in NFC by suppressing the pop-up dialog box (i.e. which lists all the devices to pair with) has failed due to the changes made in Android 4.1 and Bluetooth 4.1 for better security against harmful operations. Despite this minor hindrance, the development of the prototype went well and the sample CDA file was successfully transferred via Bluetooth to the paired laptop requiring neither vendor specific software development kit (SDK) nor software driver update. The prototype also executed well on another Android smartphone by a different manufacturer without issue and communicated well with the paired laptop in exactly the same way. From the compliance perspective, the strict compliance specifications and influence of the Bluetooth SIG and IEEE over the industry assures that it remains vendor agnostic with excellent portability and interoperability. Bluetooth's inbuilt security measures, widespread support by device manufacturers, excellent interoperability and portability and strict compliance governance make it a suitable candidate technology for securely transferring electronic prescriptions.

In addition, Experiment 3 succeeded in proving that Bluetooth technology is a suitable wireless communication technology for exchanging electronic prescription data for the proposed mobile ETP solution. Finally, this experimentation outcome proved Bluetooth to be a secure, vendor-agnostic and practical transfer mechanism for exchanging electronic prescription data between the prescriber's EPS system, patient's mobile device and pharmacy's EDS system in the Australian healthcare industry. Since no further revision or repetition was required, this iteration of the experimentation was successfully concluded, and this conclusion led to the next phase of the thesis; *Discussion of Results*.

The paper produced at the end of this stage (i.e. Research Paper 3 in Appendix A) briefly describes the outcomes of *Experiment 2* and *Experiment 3* for securing electronic prescription information in the proposed mobile ETP solution from the data in transit perspective. Subsequently, the paper proposed Bluetooth wireless communication technology to be the secured transfer mechanism alternative to using the Internet for transferring electronic prescriptions as part of the proposed mobile ETP solution. The research findings presented in *Research Paper 3* (in Appendix A) and produced at the end of this stage were verified by the "triple-blinded peer review" process.

Htat, K. K., Williams, P. A. H., & McCauley, V. (2017). Security of ePrescription: Data in Transit Comparison Using Existing and Mobile Device Services. In *Proceedings of the Australasian Computer Science Week Multiconference*. Geelong, Australia. ACM, doi: 10.1145/3014812.3014870

Contributions: Htat (75%), Williams (20%) and McCauley (5%)

CHAPTER 7. DISCUSSION OF RESULTS

7.1 Overview

This chapter begins with the collation of the experimentation outcomes from Chapters 5 and 6 into the Analysis Matrix partially populated in Chapter 4 (i.e. Table 4.2). It then provides further discussion built upon the literature review findings (Chapter 2), research results (Chapter 4) and the experimentation outcomes (Chapters 5 and 6) from a more holistic perspective. The purpose and use of handwritten signatures are then discussed, along with those of their electronic counterparts, digital certificates, and their potential role as more than a mere digital equivalence of handwritten signatures, actively preventing fraudulent activities in the first place. Subsequently, a framework to guide the development of an Android mobile ETP solution in compliance with the security requirements mandated by the Australian healthcare industry is constructed using the outcomes and knowledge obtained from the research activities conducted. Such knowledge is later extended further and another framework is derived for assessing Android mobile ETP solutions for their compliance with the security mandates. The last part of Section 7.3 mentions that despite this research's focus on Android OS both frameworks are mostly applicable to mobile ETP applications on any mobile operating system such as iOS. Finally, this section is concluded by a reflection on the Research Questions from a holistic point of view, based on the research outcomes.

The paper produced during this stage (*Research Paper 4*) compares the current ETP implementation with the proposed Android mobile ETP solution from a more holistic perspective and it was verified by the "triple-blinded peer review" process.

Htat, K. K., Williams, P. A. H., & McCauley, V. (2016). Future of Australia's eTP: Script Exchange, Script Vault or secure mobile alternative. In *Proceedings of the 14th Australian Information Security Management Conference,* Perth, Australia (pp. 52-59). doi: 10.4225/75/58a69d860a643

Contributions: Htat (80%), Williams (15%) and McCauley (5%)

7.2 Collation of Experimentation Results (Analysis Matrix collation)

To this point, analysis of the regulatory mandates and iterative experimentations of the candidate technologies has contributed to understanding of the security requirements and how well these candidate technologies comply with those requirements. The experiments focused on securing the electronic prescriptions from the data at rest and data in transit perspectives while they are being stored and transferred between the prescriber's electronic prescribing system (EPS), the client's/patient's Android smartphone and the pharmacy's electronic dispensing system (EDS). These experiments have provided sufficient materials and knowledge to construct a vendor agnostic experimental proof-of-concept prototype focusing on the security, interoperability, portability and practicality in the industry.

Using a rigorous analysis of the legislation, standards and regulatory mandates, Table 4.2 lists a set of security requirements for electronic prescription in the Australian healthcare industry. The experiments conducted in Chapter 5 and Chapter 6 provide data for further assessment and discussion on each candidate technology for their compliance with relevant security requirements and practicality in the industry. To enable such assessment, the following Table 7.1 collate the security requirements initially recorded in the Table 4.2 together with relevant experimentation outcomes. The right-most column of the Table 7.1 (i.e. "Technology conforming to the mandated requirement") briefly described the outcomes from the experiments conducted for each security requirements.

Table 7.1: Analysis matrix of Experiment outcomes for each security requirements of electronic prescription information

No.	Feature or usage	Jurisdiction	Governing regulations, standards & specifications	Security requirements mandated	Technology conforming to the mandated requirement
	Section (1): Security requirements for electronic prescription from data at rest perspective				
1	Encryption of the electronic prescription	Nationwide	***ATS 4888.2-2013*** section 5.3.6	The electronic prescription is to be encrypted using a symmetric key derived from DAK	The proposed solution also uses the same DAK and the prescription information is encrypted using a symmetric key derived from the DAK
2	Saving the DAK and any of its derived keys on any permanent storage	Nationwide	***ATS 4888.2-2013*** section 7.3.3	Minimum of 128-bit encryption for storing DAK or any of its derived keys on any stable storage	The experiment 1 proved that the Android platform supports the 128-bit symmetric encryption mandated by the specification. The experiment also found that the time taken for encrypting and decrypting the keys on the mobile devices is practical (i.e. acceptable). Please refer to the experiment 1, section 5.2.1, for further details.
3	HL7 message structure for electronic	Nationwide	***AS 4700.3-2014***	Mandated HL7 message structure	Theoretically, achieves better interoperability when comply

No.	Feature or usage	Jurisdiction	Governing regulations, standards & specifications	Security requirements mandated	Technology conforming to the mandated requirement
	prescription			for the electronic prescription	with this standard. But, only one of the current PES services, *Script Vault* from MediSecure, uses HL7 messaging protocol.
	Section (2): Security requirements for electronic prescription from data in transit perspective				
4	Security of electronic prescription	Nationwide	***ATS 4888.2-2013*** section 5.3.5	Security of data in transit between ETP service participants are specific to the implementation 'platform'	Bluetooth's inbuilt security measures and standards are specified by the Bluetooth Special Interest Group (SIG) and IEEE standard 802.15.1-2005. Strict governance by these two reputable authority bodies ensure an appropriately high level of security.

Table 7.1 together with Table 4.1 describes the essential security requirements for the electronic prescription and documents the research outcomes (i.e. analysis of the legislation, standards and regulatory mandates followed by a series of experiments) addressing each of those requirements for security compliance. It establishes the data from which the final conclusions were drawn after further deliberation in the next chapter, Chapter 8.

7.3 The Proposed Solution and Framework

The proof of concept prototype proved that by using the security compliance matrix, a mobile ETP application, compliant with security requirements, can be built using the Android OS and Bluetooth. This proof of concept prototype was presented merely to strengthen practicality of the research findings and was not intended to be a fully functional application demonstrating the end-to-end functionalities.

The Acts and Regulations governing the prescription of schedule drugs in all states and territories support the use of electronic prescription without requiring any amendments or changes. However, acceptance of an electronic/digital signature in place of a prescriber’s handwritten signature in prescribing is still unclear (i.e. neither explicitly accepted nor rejected) in the Australian Capital Territory, New South Wales, Victoria and the Northern Territory. Regulations of these jurisdictions require the prescriber’s signature to be present on the prescription but do not explicitly specify whether it has to be a handwritten signature of the prescriber or can be its digital equivalence. Another regulatory change required to support a fully electronic prescription system is found in sections 41(1) and 88(1) of the NSW Poisons and Therapeutic Goods Regulation 2008, which mandate that the supplying personnel/pharmacist’s endorsement of details, such as the prescription reference number, address and date the substance is supplied, be written on the prescription itself in ink. Such requirement cannot be met once the entire prescribing process is done electronically. However, these regulatory constraints and uncertainties do not concern the current ETP implementation because, along with the electronic copy of the prescription (i.e. the one uploaded to the PES server), it also produces a printed prescription which is signed by the prescriber, this signature satisfying these regulatory requirements. The printed prescription also accommodates the NSW prescription endorsement process. This is entirely due to the fact that the current ETP implementation was designed and built for the current legislation with change-averting as its highest priority, rather than designed for what was needed for the ETP process. This failure of process in the current ETP implementation imposed various obstructions in moving towards a fully electronic ETP solution from both regulatory and IT infrastructure perspectives. The ideal approach for ETP implementation would have been the simultaneous amendment of each jurisdiction's legislations and regulations in accordance with the outcomes from a proper, purpose-oriented problem identification and design process and the putting in place of the supporting eHealth infrastructures and facilities at Commonwealth and jurisdiction levels. In reality however, instead of a solution such as this, in which provisioning for future is put in place while the legislation is changed accordingly over time, the implemented solution was built solely for the current legislation, with change-averting as its highest priority. Therefore, transitioning to the fully electronic prescribing systems may require some regulatory changes in some jurisdictions as the fully electronic implementation eliminates the presence of prescriber's handwritten signature from the prescriptions.

Primarily, the purpose of a signature is to authenticate the content of the document to which it is applied to and one of the definitions provided by the ***Cambridge Dictionary*** for signature says "…to show that something has been written or agreed by you". Various mechanisms such as the use of wax seals from ancient Mesopotamia to the use of rubber stamps in fairly recent days have been employed to authenticate the content of the document to which it is applied. A handwritten signature accomplishes this authentication process passively and is not a useful mechanism in preventing fraudulent activities; however, the use of digital certificates has the potential to achieve much more. Whilst forging a signature makes the fraudulent activity a criminal offence when prosecuted, the use of digital certificates can prevent the fraudulent activity in the first place, or at least make the signature less vulnerable to forgery, since possession of the private key is vital to producing a digital certificate (Fillingham, 1997). In addition, since other highly regulated and critical sectors of government such as *Department of Immigration and Border Protection* and *Australian Taxation Office* have already widely adopted the use of digital certificates in their processes, the acceptance of digital certificates in place of handwritten signatures in the Australian healthcare industry is inevitable; it is merely a matter of how soon this change will take place. Moreover, the Electronic Transaction Act has recognised and approved alternatives to using handwritten signatures for the purpose of identifying a person and indicating the approval of the information contained/communicated ("The Electronic Transactions Act 1999", n.d.).

For that reason, despite some non-definitive results from investigating Subsidiary Research Question 1 (i.e. study from the legislative and regulatory perspectives) and the proposed mobile solution (i.e. any fully electronic prescribing process in this case) being not fully compliant with some jurisdictions' regulatory mandates due to the absence of the prescriber's hand written signature, this research proceeded further by conducting experimentations to answer Subsidiary Research Question 2 (i.e. iterative experimentations on the proposed solution's candidate technologies; the Android's encryption and the security of NFC and Bluetooth against each security requirements identified in prior stage). Except for the absence of the prescriber's handwritten signatures, the experimentation outcomes proved that the proposed Android mobile solution complies with all the security requirements mandated by the standards and specifications currently in place and implemented by the existing ETP implementation. Therefore, this research progressed further still by proposing a fully electronic mobile alternative to the current ETP implementation that not only has comparable security assurance but is also a cheaper – in fact, potentially cost-free – alternative, making use of the patient's Android smartphone as the substitute secured transfer medium. Hypothetically, the security of electronic prescriptions can even be potentially enhanced by using smartphone's unique ID in the proposed mobile ETP solution. Such feature not only provides audit trail but also can be used to prevent cloning of prescriptions.

The proposal of such mobile solution also aligns well with the Australian Digital Health Agency's (ADHA) recent work on a mobile enablement program which is designed to allow information to be extracted from the MyHR into third-party applications, and to create a way to upload data back into the MyHR system at a later time as this program progresses further.

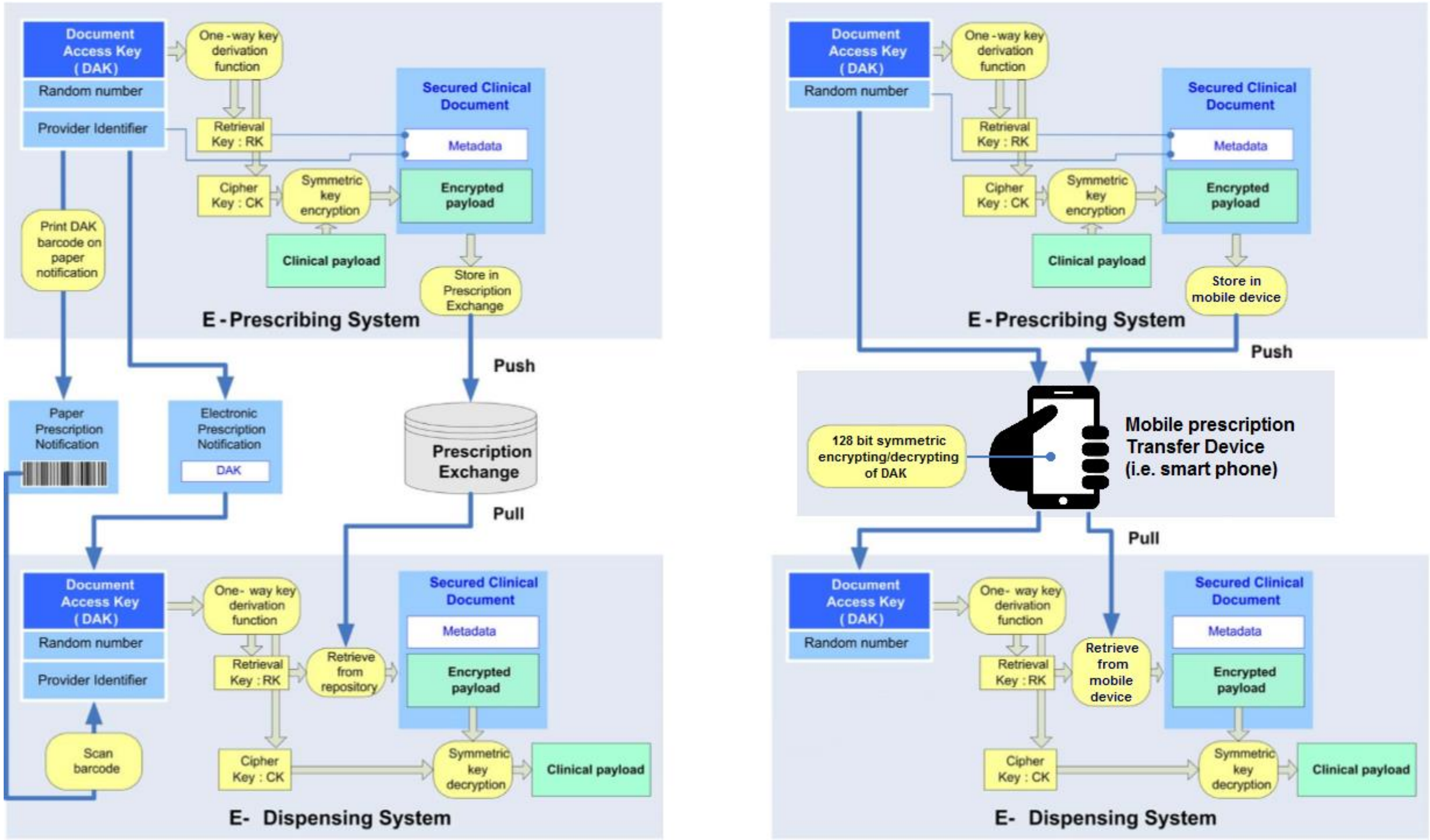


Figure 7.1: Comparison of two security models (PES vs Mobile implementation)

Figure 7.1 compares the security model of the current ETP implementation (using PES services) with that of the proposed mobile solution. Despite the controversial difference in the transfer mechanism employed for the electronic prescription, Figure 7.1 demonstrates that the changes introduced by the proposed solution have minimal impact on the ETP participants with whom it is interacting (i.e. minimal impact on the EPS and EDS). From Figure 7.1 it is also evident that the printing of the DAK barcode is no longer necessary in the proposed solution as it transfers the electronic prescription itself along with the DAK instead of just transferring the prescription notification carrying the DAK barcode which is later used in downloading the electronic copy of the prescription form PES server. This change eliminates the use of the printed DAK barcode, along with the use of the *Provider Identifier* component of the DAK itself. Since the prescription is directly transferred from the patient's mobile smartphone to the pharmacy's EDS system, this proposed solution can operate with limited or no internet connection for simple dispensing purposes (e.g. no script owing, PSB claiming or NPDR update operations etc.). However, the proposed solution currently is incapable of supporting certain features such as Script Request (e.g. in a script owing scenario) due to its disconnected nature. It would have to employ certain messaging service (e.g. SMS or email) to support such a feature, potentially introducing associated costs.

In current ETP specifications, the *Dispense Record* is primarily used for updating the *Dispensing State* of the prescription, issuing *Dispense Notification* to the prescriber and recording the dispense information to the National Prescription and Dispense Repository (NPDR). However, the automatic *Dispense Notification* service to the prescriber is currently disabled at the request of RACGP (McDonald, 2013a) and it is therefore irrelevant for the proposed solution to support this feature. In the proposed ETP model, the recording of the dispense information to the NPDR will be integrated into the pharmacy's EDS functionalities along with the other secondary use of the prescription information such as PBS online claiming. Hence, the proposed solution has minimal impact on the other ETP process participants. The security of the prescription information in the proposed mobile solution is governed by ATS 4888.2 in the same way as in the current implementation using PES services.

In the proposed solution, the potential issue for information sharing is reduced by strictly conforming to AS 4700.3-2014 and ATS 4888.3-2013 for electronic prescriptions. The implementation of the *Dispense Record* firmly adheres to ATS 4888.4-2013 for better information sharing. On the other hand, ATS 4888.5-2013 (Platform implementation specific prescription request HL7 CDA implementation guide) is not relevant for the proposed solution since it does not support *Script Request* functionality. Similarly, ATS 4888.6-2013 (Platform implementation specific web service) is also irrelevant for the proposed solution because at this point in time it does not make use of the web service for any of its functionalities. However, this technical specification is potentially applicable in future for implementing additional features and functionalities.

In addition, and as described in Figure 4.2 of Chapter 4, the proposed mobile electronic prescription transfer application also functions as a mobile repository of the patient's medication history. With the interface integrating the patient's mobile smartphone with the Hospital Information System in place, the patient's complete medication history can be transferred from their mobile smartphone directly to the Hospital Information System. This feature can be utilised to share the medication information with the other healthcare providers such as GPs and specialists. The ability to access such information enables the healthcare professionals to deliver better quality care, benefiting both patients as well as the healthcare providers.

The knowledge accumulated in and findings drawn from this intellectual investigation are subsequently utilised in constructing a framework to guide the development of a fully electronic Android mobile ETP application in accordance with security requirements mandated by the Australian healthcare industry. Figure 7.2 depicts this framework, which is the primary focus of this thesis.

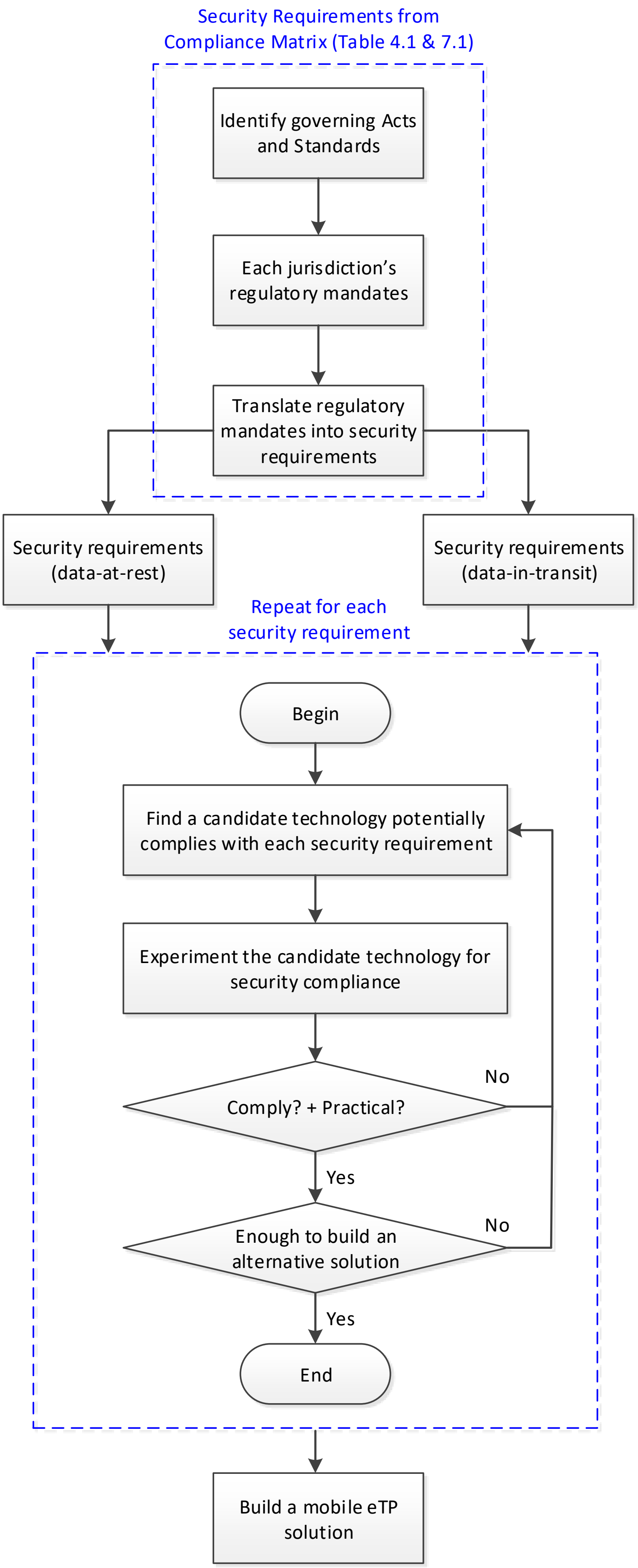

Security Requirements from
Compliance Matrix (Table 4.1 & 7.1)
Identify governing Acts and Standards
Each jurisdiction's regulatory mandates
Translate regulatory mandates into security requirements
Security requirements (data-at-rest)
Security requirements (data-in-transit)
Repeat for each security requirement
Begin
Find a candidate technology potentially complies with each security requirement
Experiment the candidate technology for security compliance
Comply? + Practical?
No
Yes
Enough to build an alternative solution
No
Yes
End
Build a mobile eTP solution

Figure 7.2: The proposed framework for developing a security compliant ETP solution

Moreover, such knowledge gained from this research is further utilised by deriving another framework (Figure 7.3) for assessing Android mobile ETP solutions for their compliance with the security requirements mandated by the Acts, regulations and standards in the Australian healthcare industry. Figure 7.3 explains how to undertake such compliance assessment for Android mobile ETP applications.

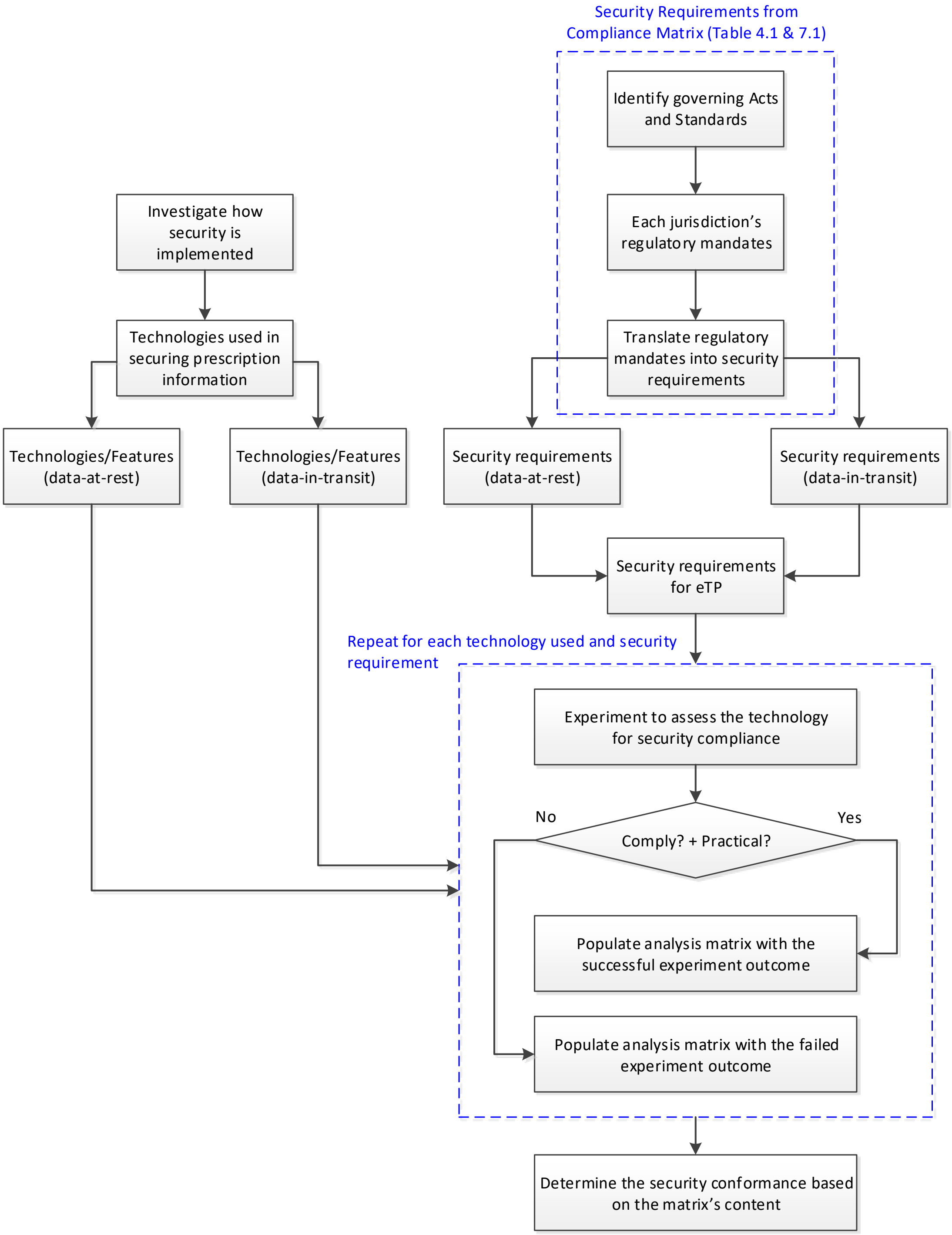

Security Requirements from
Compliance Matrix (Table 4.1 & 7.1)
Identify governing Acts and Standards
Each jurisdiction's regulatory mandates
Translate regulatory mandates into security requirements
Investigate how security is implemented
Technologies used in securing prescription information
Technologies/Features (data-at-rest)
Technologies/Features (data-in-transit)
Security requirements (data-at-rest)
Security requirements (data-in-transit)
Security requirements for eTP
Repeat for each technology used and security requirement
Experiment to assess the technology for security compliance
No
Comply? + Practical?
Yes
Populate analysis matrix with the successful experiment outcome
Populate analysis matrix with the failed experiment outcome
Determine the security conformance based on the matrix's content

Figure 7.3: The proposed framework for assessing Android mobile ETP application for security compliance

Although the framework in Figure 7.3 is an additional product of the research, it represents significant and particular usefulness within the health industry that is highly regulated but lacking in detailed guidelines for assessing the security compliance of ETP applications. Despite the fact that all the research activities conducted in this research are limited by the scope of this research (i.e. technologies and features available to the Android operating system), both frameworks are in fact mostly applicable to any fully electronic implementation of ETP application in the Australian healthcare industry. Certainly, some additional effort is required to generalise these frameworks so that they are fully applicable to other operating systems (e.g. iOS), technologies and features available on those operating systems. Whilst such line of inquiry is beyond the scope of this research, it introduces compelling future research potential within this ETP context.

7.4 Analysis Matrix

The derivation of the above two frameworks was made possible by the data analysis process, consisting of three integrated activities: data reduction, conclusion drawing and verification, all performed on the two analysis matrixes, Table 4.1 and Table 7.1. The investigations conducted and translation of the regulatory mandates into security requirements as part of answering the Subsidiary Research Question 1 populated the entire Table 4.1 (Analysis matrix of each jurisdiction's readiness for fully electronic ETP solution) and the first five columns of Table 4.2 (Analysis matrix of security requirements for electronic prescription information). Rows 1, 2, 6, 8, 9, 10, 11 and 12 of Table 4.1 indicate that the acts and regulations of Western Australia, Queensland, South Australia and Tasmania support not only the use of electronic prescriptions but also the absence of the prescriber's handwritten signature from the electronic prescriptions. While some states' regulations recognise the use of digital/electronic signatures, others' imply the same meaning by stating that a prescription that is not issued electronically shall be signed by the prescriber in his or her own handwriting. For instance, while sections 79 (7) and 190 (5) of Queensland's ***Health (Drugs and Poisons) Regulation 1996*** explicitly stated that as "The prescriber must sign a paper prescription or electronically sign an electronic prescription", sections 37 (1A) (1B) and 51 (1A) (1B) of Western Australia's ***Poisons Regulation 1965*** rather imply the same in a more deductive logic approach.

Nevertheless, despite their differing ways of wording, these jurisdictions are ready to progress towards fully electronic implementation of ETP from a regulatory perspective and therefore the proposed mobile ETP solution will work well without any regulatory change in these states. In the meantime, the rest of the jurisdictions' Acts and regulations (i.e. rows 13, 14, 15 and 16 of the Table 4.1) mandate the prescriber's signature on the prescription in various ways; some are more straightforward while others are in more confounded statements. Sections 35 (2) and 80 (2) of NSW's ***Poisons and Therapeutic Goods Regulation 2008*** clearly state that "…the prescription must be signed by the person by whom it is issued" while section 40 (a) and section 40's "***Note***" of the ACT's ***Medicines, Poisons and Therapeutic Goods Regulation 2008*** imply that electronic prescriptions also require prescriber's signature. However, none of these mandates explicitly state whether the prescriber's signature must be in handwritten form or its electronic/digital equivalence. These mandates, therefore, do not necessarily prohibit the use of a fully electronic ETP solution which makes use of electronic/digital signature of the prescribers, and hence the use of the proposed Android mobile ETP solution in these states may be possible without requiring regulatory changes.

In Table 7.1, *Analysis matrix of Experiment outcomes for each security requirement of electronic prescription information*, both rows 1 and 2 are about securing the prescription information while the data is at rest. Row 1 reveals that section 5.3.6 of the ***ATS 4888.2-2013*** mandates that the electronic prescription be encrypted using a symmetric key derived from DAK. Since the proposed mobile ETP solution is designed to use the same DAK and the prescription information is encrypted using a symmetric key derived from the DAK, it conforms to this security requirement. The right-most column of row 1 briefly recorded this for future use (i.e. analysis, discussion and framework derivation). Row 2 of the analysis matrix brings to light the fact that section 7.3.3 of the ***ATS 4888.2-2013*** requires a minimum of 128-bit encryption for storing DAK and any of its derived keys on any permanent storage medium/device. Experiment 1 (i.e. Encryption – Security of data at rest), conducted in response to Subsidiary Research Question 2, proved that the Android platform supports the 128-bit symmetric encryption thereby conforming to the security mandates imposed by ***ATS 4888.2-2013***. The experiment also found that the time taken for encrypting and decrypting the CDA document on the mobile devices is also practical (i.e. acceptable). Row 3 of the Table 7.1 reveals that HL7 message structure is recommended by the ***AS 4700.3-2014*** for the electronic prescriptions, although the more prominent PES operator, ***Script Exchange*** from ***eRx***, does not conform to this standard due to the fact that it was live nationwide seven months before the NEHTA published the first draft of the standard (“ETP Standards”, 2016). Since the proposed mobile ETP solution conforms to this recommendation, it will have better interoperability when interacting with other healthcare software components. The last row of Table 7.1, row 4, focuses on the security of the prescription information from the data in transit perspective. Section 5.3.5 of the ***ATS 4888.2-2013*** mentions that security of data in transit between ETP service participants is specific to the implementation “platform”. This research finds no further details on the recommended approach or how this should be implemented. Therefore, the Experiments 2 and 3 were conducted to establish whether the use of NFC or Bluetooth wireless technology provides security assurance comparable to the current transfer mechanism of using the Internet.

The preliminary study finds NFC to be a potentially suitable wireless communication technology for the proposed mobile ETP solution’s prescription transfer mechanism due to its widespread support by various smartphone manufacturers, its well-known interoperability and convenience of use and its close proximity communication range. However, Experiment 2 reveals that the use of NFC technology in the proposed mobile ETP solution will result in having a portability issue in practice. This research finds that, with the exception of Sony and NXP Semiconductors, the NFC device manufacturers do not make the proximity driver of their products available to the public. Therefore, only the Sony’s FeliCa card readers/writers can be programmed using the Windows Proximity API, and the rest of the NFC devices in the market require the SDK from the hardware manufacturer to interface with. Use of a specific SDK restricts the application to that particular hardware/device and this portability issue will severely impact the practicality of using the proposed mobile ETP solution in the industry. An ETP solution with such portability issue is impractical for the healthcare industry in Australia as the current electronic prescribing systems (i.e. a component of clinic management software) generally runs on existing hardware and system software platforms rather than on a vendor-provided hardware and software configuration. Therefore, the use of NFC technology is deemed not suitable for the proposed mobile ETP solution, and as a result, this research conducted another round of experimentation. The next experiment, Experiment 3, focuses on investigating whether the use of Bluetooth technology for transferring electronic prescriptions provides comparable security assurance to that of the current implementation. Bluetooth’s inbuilt security measures and standards are strictly governed by the Bluetooth Special Interest Group (SIG) and IEEE standard 802.15.1-2005. The strict governance by these two reputable authority bodies can be considered comparable to those of the current ETP implementation using the Internet. Unlike the outcome of Experiment 2, the development of the proof-of-concept went well without any portability issue, and the performance is also acceptable. This experiment effectively reveals that the use of Bluetooth technology in the proposed mobile ETP solution not only provides comparable assurance but is practical for the healthcare industry. However, the use of Bluetooth requires pairing of the devices (i.e. patient’s mobile smartphone with the prescriber’s and dispenser’s devices) for the first-time use (i.e. at the first visit to either the clinic or the pharmacy). As an added benefit, this extra step can be considered as an additional security measure rather than a mere nuisance. Moreover, this process can be streamlined by using other tools or technologies such as NFC or a QR code. Since every technology has its strength and vulnerabilities, however, this step should only be taken after a thorough investigation. Such line of inquiry is outside the scope of this research, but it suggests a compelling subject for further investigation with a view to extending this research.

7.5 Reflection on the research questions

This section reflects on the Research Questions by discussing how they came about, what actions were taken in response to them and how they have driven the progression of the research through the meticulous document analysis and vigorous iterative experiments and reflection.

7.5.1 Main Research Question

Can a technical framework be constructed to serve as a guide for the development of Android mobile electronic prescription transfer applications in compliance with the security requirements mandated by the Australian healthcare laws, regulations and standards?

The literature review and the preliminary study reveals that the current ETP implementation is tailored to suit the current regulatory requirements instead of being designed to facilitate the most beneficial healthcare outcome for patients and clinicians. While the current ETP implementation enabled the nation as whole to progress towards using electronic prescription with minimal legislative and regulatory changes, this change-averting solution has posed many obstructions in reaching the full potential benefits of eTP. Therefore, this research proposes an alternative solution with comparable security assurance which also tackles the shortcomings of the current ETP implementation, and creates a framework to guide the development of such solution in compliance with the security requirements.

Answering this Research Question involves devising two additional supporting questions. The first question endeavours to translate the regulatory mandates into security requirements for later integration into a framework. The second question takes on the investigation of how this framework can be used in assessing Android mobile ETP application for their security conformance, ultimately deriving a framework to guide the development of such mobile application in compliance with security requirements. Based on the research findings from these supporting questions, the Primary Research Question is answered by proving that it is possible to build a framework to guide the development of an Android mobile ETP application compliant with the Australian healthcare industry's security mandates.

This research not only draws the conclusion that it is possible to build the framework with which to guide the development an Android mobile ETP application in compliance with security mandates, but it also builds the framework that is derived from the proof-of-concept prototype developed as part of this research. Such framework, as well as the proof-of-concept prototype, is a significant contribution towards the national eHealth program's expansion into a mobile ETP context.

The preliminary study found little literature on existing proven theoretical frameworks and methodologies for use in this integrated field of medical informatics, public health and information security. Such lack of literature on the existing proven theoretical frameworks and methodologies drives the researcher to explore for a suitable theoretical framework and methodology to minimise (or prevent completely if possible) the unreliable research findings, and guide this research on track towards successful completion. The nature of this research (i.e. creating a technical framework based upon the decisions from law and opinions) drives its use of mixed methods, mixing exploratory qualitative research, iterative experimentation and reflection. The research employed to answer the first supporting question is of exploratory nature. Its endeavour to interpret legal text and explanations into a set of security requirements, providing a practical understanding for real-life application, fits well with the method selected for its earlier stage, this being the document analysis approach derived from Laverty's (2003) *Hermeneutical Circle*. Answering the second supporting question follows an iterative experimentation and reflection approach for examining how the security requirements constructed in the prior stage can be used in assessing Android mobile ETP solutions for their security conformance. For better and in-depth understanding of the findings, all the studies and experimentations performed for this research are conducted from two different perspectives; the security of the prescription information both in data at rest and data in transit.

The content of Table 4.1, populated by answering Supporting Question 1, indicates that although the Acts and regulations of various jurisdictions support the use of electronic prescription, the use of a digital/electronic signature in place of the prescriber's handwritten signature is not recognised by all the jurisdictions, as discussed earlier in section 7.3. However, since none of these mandates for the presence of prescriber's signature explicitly mention that it must be in handwritten format, they do not necessarily prohibit the use of a fully electronic ETP solution as long as it makes use of the electronic/digital signature of the prescribers. Since the proposed Android mobile ETP solution makes use of the prescriber's Medicare digital certificate, it may be possible to use the proposed Android mobile ETP solution in these states without any regulatory changes. Therefore, this research progresses further by proposing the Android mobile ETP solution and deriving the framework from it.

The proposed Android mobile ETP solution from which the framework is derived makes use of the patients' Android smartphone as the alternative transfer medium to using the PES services. Such a controversial solution requires proving that the proposed Android mobile ETP solution is as secure as – if not more secure than – the current ETP implementation using the PES services, thereby putting an end to the archaic belief that mobile applications are not secure enough for use in the healthcare industry (Barrett, 2011; Bromwich & Bromwich, 2016). Once the regulatory mandates have been translated into security requirements and recorded in the analysis matrices (i.e. row 1 and 2 of Table 4.2 and Table 7.1), it becomes evident that the electronic prescription is to be encrypted using a symmetric key derived from DAK, and the operating system running the mobile ETP application will need to support minimum of 128 bit symmetric encryption to store the electronic prescription, its associated DAK and other derived keys from DAK. Another crucial but vaguely defined security requirement recorded in the analysis matrices (i.e. row 4 of Table 4.2 and Table 7.1) effectively implies that the transfer mechanism used in the proposed solution is required to provide comparable security assurance to that of the Internet for transferring the electronic prescriptions. Further information on how the security is implemented from the data in transit aspect in the current ETP implementation is unavailable, as the research context turns out to be not only highly regulated but also highly proprietary. Therefore, prevented from comparing the implementation details such as the file transfer protocols (e.g. FTP, HTTP, HPPTS or other files sharing) used in current implementation versus the ones used in the proposed solution, this research endeavours to find an alternative transfer mechanism (i.e. a wireless communication technology) that is comparable in security measures to using the Internet from a more holistic perspective (i.e. using a more “black-box” approach).

7.5.2 Subsidiary Research Question 1

How can the security requirements imposed by the relevant laws regulations and standards in the Australian healthcare system be integrated into a framework for the assessment of mobile electronic prescription transfer applications?

As part of the bigger undertaking, this supporting question focuses on translating the regulatory mandates into a set of security requirements prior to integrating them into a framework. The objective is to interpret the legislative and regulatory requirements mandated by the relevant Acts, regulations and standards into a set of acceptance criteria (i.e. security requirements) to be complied with by the native security features, third-party tools and technologies available on the Android operating system platform for the development of a proof-of-concept prototype ETP mobile solution.

This is the part of the research governed by the document analysis approach, derived from Laverty’s (2003) *Hermeneutical Circle*, for deciphering the true meaning of what the legal texts imply and then interpreting them into a set of security requirements. This research is far more than a mere interpretation of text however, as it also endeavours to build a relationship between the legal explanation and their practical understanding for real-life applications. The research findings (i.e. translated security requirements) from answering this supporting question populate the analysis matrices (i.e. Table 4.1, column 1 to 4 of Table 4.2 and Table 7.1), leaving the last column of Table 4.2 to record the investigation and experimentation outcomes from the next stage of the research; iterative experimentations. Although not all the research finding are 100% in favour of the use of the proposed mobile ETP solution (i.e. any fully electronic ETP application in general in this case) due to the inherent absence of the prescriber’s handwritten signature, this research indicates that there is no obstacle from legislative or regulatory perspectives which explicitly opposes its use, since the proposed ETP solution uses the prescriber’s Medicare digital certificate in signing and encrypting the DAK associated with the electronic prescription.

Once the relevant regulatory mandates have been interpreted and recorded in the analysis matrices accordingly, the next stage of the thesis is commenced as a series of experimentations, followed by reflection based upon the experimentation outcomes against the identified security requirements.

7.5.3 Subsidiary Research Question 2

How can the assessment criteria framework from Subsidiary Research Question 1 be used in assessing the native security features and third-party tools on the ANDROID for the security compliance of mobile electronic prescription transfer applications?

The emphasis of this second supporting Research Question is to explore and verify which of the native security features, third-party tools and technologies available on the Android operating system comply with the security requirements for the development of mobile ETP solution. Such verification was performed through a series of experiments and reflection on whether the experimentation outcome conforms to the security requirements identified in the prior stage. These iterative experimentations and reflection are conducted from the perspectives of both data at rest and data in transit in order to provide better and in-depth understanding of the findings.

The exploration and verification activities conducted are governed by the iterative experimentation and reflection approach. In fact, every iteration of the experimentation is based on the Williamson's (2002) depiction of the typical action research cycle, with a few alterations specific to this research. Such adaption of the experimentation and reflection approach from action research is supported by Williamson (2002) and it fits well for the nature of this research. The experimentation outcomes are recorded in the last column of Table 7.1 and are used in determining whether the candidate technology of the proposed mobile ETP solution conforms to the security requirements.

Experiment 1 confirms that the Android operating system supports the 128-bit symmetric encryption and hence conforms to the security requirements recorded in rows 1 and 2 of Table 7.1 (i.e. security from data at rest perspective). In addition, the proposed Android mobile ETP solution also conforms to the requirement recorded in row 3 of Table 7.1, since it is designed to operate using CDA documents. This will also minimise any interoperability issues when interacting with other software components within the health sector. However, this does not seem to be a crucial requirement currently as only one of the current PES services (i.e. *Script Vault* from MediSecure) complies with this standard. Experiment 2 verifies whether the use of NFC for transferring electronic prescriptions between ETP participants provides comparable security assurance to that of the use of the Internet in the current ETP implementation. The research initially found the use of NFC technology to be a viable alternative transfer mechanism compliant with the security requirements for electronic prescription transfer, as well as a realistic solution in practice from end-user perspective. Regrettably, however, further experimentation reveals that the use of NFC technology imposes some unrealistic constraints for the development and deployment of the solution, and will have portability issues in practice. These subsequent findings render the use of NFC technology an impractical solution for the Australian healthcare industry. Therefore, another experiment (i.e. Experiment 3) is conducted to investigate whether the use of Bluetooth for transferring the electronic prescription offers security assurance comparable to that of using the Internet. This experiment shows that the use of Bluetooth not only offers comparable security assurance but also presents a practical solution for the Australian healthcare industry.

7.6 Summary

The proof-of-concept prototype developed as part of the iterative experimentation in this research is far from complete as it only focuses on the encryption and prescription transfer components critical for security conformance. However, the security requirements recorded in the analysis matrices are operating system and programming language agnostic, and in fact these matrices are applicable to any fully electronic ETP implementation whether a mobile or desktop application. During the iterative experimentations, Experiment 2 failed to prove that NFC technology is suitable for the proposed mobile ETP solution. That said, however, this technology should be kept under close observation as this situation could change drastically once the NFC device manufacturers make their devices' proximity drivers openly available to the public.

The goal of this research is the construction of a framework to guide the development of an Android mobile ETP solution in compliance with security requirements for the Australian healthcare industry. In addition to the achievement of this, this research derived another framework for assessing Android ETP applications for their security compliance. Although an unintentional additional product of the research, this second framework has no less value for the emerging eHealth industry than the first (i.e. the framework for the development of Android mobile ETP solution). As more eTP-related enhancements and innovations are developed for the mobile platform, the eHealth industry will be in critical need of a tool that can quickly and effectively assess the security compliance of mobile ETP applications, and the second framework devised in this research fills that need.

In summary, this research establishes the fundamental groundwork for future enhancements and innovations in a fully electronic ETP context for both mobile and desktop platforms in general. The proposed solution is perhaps somewhat limited, but the research effectively demolishes the archaic belief that mobile applications are not secure enough for use in the Australian healthcare industry, and this knowledge alone paves the way for countless opportunities and innovations in the mobile ETP context.

CHAPTER 8. CONCLUSION

8.1 Thesis Overview

In Chapter1, this thesis establishes the research journey with the statement of the problem in the use of electronic transfer of prescriptions in the Australian healthcare industry. The background and significance of the research are then discussed, followed by the establishment of the three Research Questions which dictate the research and are eventually answered through a series of steps. The literature review in Chapter 2 further elaborates on the issue mentioned in the problem statement and Chapter 3 discusses the selected theoretical framework and methodology that shapes the design of the research. Chapter 4 details the research results from answering the Research Questions, proposes the alternative mobile ETP solution and reviews the candidate technologies for use in the proposed mobile solution. Chapter 5 and Chapter 6 feature a series of experimentations conducted on the proposed solution's candidate technologies and their outcomes verify whether or not the proposed solution is viable from the perspectives of both practicality and security of data at rest and data in transit. These experimentations confirm that the proposed solution is both practical for use in the Australian healthcare industry and compliant to the security requirements detailed in the analysis matrices shown in Table 4.1 of Chapter 4 and Table 7.1 of Chapter 7.

Chapter 7 presents further discussion, from a more holistic perspective, of the research results, the proposed mobile solution and the experimentation outcomes. Also examined in Chapter 7 is the purpose and use of handwritten signatures and their electronic counterparts, digital certificates, the potential of these electronic signatures as more than a mere digital equivalence of handwritten signatures, and they could be put into practise. Also in this chapter a framework is derived from the analysis matrices with which to guide the development of an Android mobile ETP solution in compliance with the security requirements of the Australian healthcare industry. An additional framework is derived from the analysis matrices for the assessment of Android mobile ETP solutions for their security compliance. This chapter concludes with the reflection on the Research Questions based on the research outcomes. Chapter 8 summarises the research by highlighting the significance of the outcomes and its potential impact on the ETP in the Australian healthcare industry, stating its contribution to the body of knowledge. Future research to extend this study is also listed in Chapter 8. The last part of the thesis (i.e. Appendix A) documents the four publications arising from this thesis research in chronological order by the date submitted (i.e. not by publication dates). The first paper is the outcome from the literature review. The second paper compares the security of the prescription information, from the data at rest perspective, between the current ETP implementation and the proposed Android mobile ETP solution. Whilst also focusing on the comparison of security measures between the current ETP implementation and the proposed Android mobile ETP solution, the third paper considers the comparison from the data in transit perspective. The last paper briefly discusses the potential changes in the ETP context (e.g. Commonwealth subsidy criteria, the number of prescriptions per year etc.) and proposes the Android mobile solution, built upon the findings and technologies published in the second and third papers, as an alternative electronic prescription transfer mechanism.

8.2 Research Summary

The primary focus of this research was to devise a framework to guide the development of an Android mobile ETP application in compliance with the security requirements mandated by the Australian healthcare industry. In order to achieve this, the research began by studying the relevant Acts, regulations and standards governing electronic prescribing in the various jurisdictions of the Australian healthcare industry. These regulatory mandates were then transformed into a set of security requirements. This transformation made the regulatory mandates more easily understandable by non-regulatory experts and simplified the requirements that need to be fulfilled by the subsequent stages of the research. Next, mobile operating systems and wireless communication technologies were explored in search of an alternative solution which would be more cost-effective with comparable security measures. A series of experimentations were subsequently conducted to verify the candidate technologies for use in the proposed mobile solution, which proved that the proposed Android mobile ETP solution conforms to the security requirements mandated by the Acts, regulations and standards. Finally, a framework for the development of an Android mobile electronic prescription transfer application in compliance with security requirements was derived from the analysis matrices constructed and collated throughout this research.

Since this research was conducted in an emerging field which intersects the medical informatics, public health and information security, where there was very little literature about theoretical frameworks previously employed for a similar study within this context. The first part of the research was a study which embarked on interpreting and revising the knowledge of legal constraints and interpreting them into technical specifications, with the second part proposing a viable alternative mobile solution through a series of experimentations and finally deriving a framework. Therefore, this research employed a mixture of document analysis and iterative experimentation with reflection in exploring the potential solutions, verifying the candidate technologies and subsequently deriving a framework to answer the main Research Question. The process of deciphering the true meaning of the legal texts and interpreting them into a set of security requirements was governed by the document analysis approach, as it offers a theoretical framework for interpretive understanding or meaning with special attention to context and original purpose. The series of experimentations and framework derivation parts of the research were of applied research type with exploratory nature and the iterative experimentations and reflection approach was therefore employed when exploring and verifying the potential alternative solution and derivation of the framework.

The proposed solution from this research was a proof-of-concept prototype mobile ETP solution on the Android operating system platform which utilised Bluetooth wireless technology as a transfer mechanism for the electronic prescriptions. This proposed solution was devised from the first phase of the study which explored the potential candidate technologies (i.e. operating systems and wireless communication technologies) for this research. This study examined each candidate technology’s architecture, security model and governing standards in order to determine how well it suits the proposed solution. The first phase of the study found that both wireless communication technologies (i.e. NFC and Bluetooth) and the Android operating system potentially comply with the security requirements mandated for eTP. The experimentations conducted in the next stage of the research verified whether these candidate technologies truly conform to the ETP security requirements and their practicality for use in the industry.

The first experiment conducted was to verify whether the encryption capability of the Android operating system conforms to the security requirements from the data at rest perspective. Sections 5.3.6 and 7.3.3 of the ATS 4888.2-2013 mandates a minimum of 128-bit symmetric encryption for the electronic prescriptions and the storage of the DAK and any of its derived keys on any permanent storage. The prototype created for this experiment makes use of Android's "javax.crypto" libraries for encrypting/decrypting the sample CDA document with 128 bit AES encryption. This experiment successfully encrypted/decrypted the sample CDA document and proved that the Android operating system has sufficient encryption capability for this research's proposed mobile ETP solution. The subsequent experiment examined the NFC technology for its compliance with security requirements from the data in transit perspective. The prototype built for this experiment was written in C# .NET using the Windows Proximity APIs supported by the Windows Runtime (WinRT) and a USB ACR122U contactless RFID smartcard reader/writer from Advanced Card Systems (ACS). This experiment revealed that use of SDK from the NFC device manufacturer was required, imposing a significant limitation on the solution's portability. Due to the use of non-standardised hardware and software in primary care facilities and pharmacies, it is crucial that the proposed mobile ETP solution be hardware and software vendor agnostic. This experiment therefore established that the use of NFC technology in development of the proposed solution is impractical for the Australian healthcare industry. The next experiment investigated whether the use of Bluetooth for transferring electronic prescriptions in the proposed solution conforms to the security mandates from the data in transit perspective. Despite the inconvenience of having to pair the devices at the first-time use (i.e. either at the first visit to a clinic or a pharmacy), this experiment proved that transferring electronic prescriptions between the patient's mobile smartphone and the EPS and EDS via Bluetooth is as secure as using the Internet in the current implementation. Therefore, it was concluded that the use of Bluetooth in the proposed solution is secure enough and practical for the Australian healthcare industry.

Further in-depth discussion of both the rationale behind the proposed mobile ETP solution and the derivation of the framework was followed by the reflection of the Research Questions based upon the research findings. Although the outcomes from answering Subsidiary Research Question 1 revealed that not all the jurisdictions are ready for a fully electronic ETP implementation (i.e. some jurisdictions require the prescriber's signature in prescriptions), none of them explicitly mandated the prescriber's signature in handwritten form. Since the proposed mobile ETP solution uses the prescriber's Medicare digital certificate in signing and encrypting the DAK associated with the electronic prescription, it does not violate those jurisdictions' regulatory mandates. In addition to examining each jurisdiction's readiness for fully electronic ETP implementation, this investigation also interpreted the true meaning of legal texts into a set of security requirements and recorded them in row 1 to 4 of Table 4.2 and 7.1. This established the acceptance criteria for the next stage of the research; iterative experimentations for each candidate technology which potentially fulfil those security requirements. The first experimentation outcome proved that the Android operating system has sufficient encryption capabilities required to securely store the electronic prescription information. The next experiment revealed that the use of NFC as an alternative transfer mechanism for electronic prescription is not a practical solution for the Australian healthcare industry. Therefore, the experiment was repeated using Bluetooth. This experiment proved not only that the use of Bluetooth is a secure alternative to using the Internet for transferring electronic prescriptions, but that it is also a practical solution. Based upon these findings, a framework (Figure 7.2) was constructed in response to answering the Main Research Question for guiding the development of an Android mobile ETP application in accordance with the security requirements mandated by the Australian healthcare industry. Furthermore, the accumulated findings and knowledge from this intellectual investigation was utilised to derive another framework (Figure 7.3) for assessing Android mobile ETP solutions for their compliance with the security requirements mandated by the Australian healthcare industry.

The scope of this research and its experimentations focused exclusively on the Android operating system platform and NFC and Bluetooth wireless communication technologies in its exploration of potential candidate technologies for the proposed mobile ETP solution. This provides considerable opportunity for future research into various lines of inquiry and innovation within the ETP context.

8.3 Significance of Research

This research translated the relevant Acts, regulations and standards governing the transfer of electronic prescription in various jurisdictions into a set of security requirements and proposed a secured mobile alternative which has been verified through a series of experimentations. As a result, this research has produced significant outcomes from multiple perspectives: reduced healthcare expenditure, improved patient safety and the demonstration of obsolete regulatory requirements and processes in current ETP, the sole purpose of which is merely to conform to obsolete requirements, as described below.

The first significant outcome of this research is its potential to reduce the nation's healthcare expenditure. The proposed mobile ETP solution is a cheaper (if not completely cost-free in most cases) alternative to the current implementation with comparable security measures. If widely used, this proposed solution would substantially reduce the nation's spending on electronic prescription fees. These prescription fees currently cost the nation approximately AU$112,950 every day ("One billion eRx electronic scripts", 2016). The nation's increase in the aging population and chronic disease burden will only escalate this expenditure in the future and use of the proposed mobile ETP solution will make a significant contribution towards relieving this issue.

As depicted in Figure 2.3, Patient involvement in the current ETP implementation consists of little more than delivering the Document Access Key (DAK) from the prescriber to the dispenser for downloading the electronic version of the prescription from the PES servers. In reality, patients can contribute a lot more by managing their own healthcare and medication related information. Maintaining updated drug allergy information and keeping a consolidated medication history are contributions patients can make, and this information will enable healthcare providers to make better informed decisions resulting in significantly improved treatment outcomes. The proposed mobile ETP solution enables such patient involvement and encourages them to engage in managing their own healthcare information and subsequent care. This proposed mobile solution can also provide electronic Medication Management (eMM) systems with a consolidated medication history of the patient. Moreover, additional features such as alerts for script expiration and repeat-prescriptions can also be implemented as part of this mobile ETP solution on an individual basis (i.e. as plug-in modules) to enhance its benefits.

The translation of ETP regulatory mandates into a set of security requirements (see Table 4.2 for details) makes security compliance in this context more easily understandable by non-regulatory experts. This understanding removes the major obstacle for security experts and software developers in this context, and indeed paves the way for numerous opportunities and innovations in the future. Besides those future potentials, this translation of regulatory mandates also highlighted a number of regulatory mandates which have no constructive value to eTP. These mandates were put into effect merely to avert legislative change and its associated implications during the early stage of adopting eHealth in the Australian healthcare industry. Until these regulatory mandates are revised and repealed or amended to align with the Electronic Transaction Act, they will continue to create obstacles for any fully electronic implementation of processes (e.g. such as electronic prescribing and electronic referral) in the healthcare industry.

As part of synthesising the proposed mobile ETP solution, Section 1.2.2 and 2.4.2 of this research revealed some features of the current ETP implementation that could have supported for better healthcare outcomes and patient safety. These features, such as drug allergy alerts and harmful dosage alerts, which could significantly improve the patient’s safety, could be incorporated into the proposed mobile solution. Incorporating these features within a patient-controlled context, such as on their own smartphone, is more likely to ensure such alerts are not overlooked. Adverse drug event such as the death of Mr Jared Charles Olsen in 2015 could have been prevented if such critical warning is communicated effectively (“Inquest into the Death of Jared Charles OLSEN”, 2017).

Although it was beyond the scope of this research project, the two frameworks constructed (i.e. one for development of Android mobile ETP application in compliance with ETP security requirements for the Australian healthcare industry, and the other for assessing Android mobile ETP application for their security compliance) could be generalised for any fully electronic implementation of ETP in the Australian healthcare industry on various operating system platforms such as iOS and others.

In addition to realising those new potentials, the disconnected nature of the proposed mobile solution (i.e. not relying on Internet connectivity for transferring prescription) makes it suitable for use in locations such as remote regions of Australia, where the network availability is limited or unreliable. As briefly discussed in Section 1.2.3, This makes the proposed solution also viable for use in developing countries with poor or non-existent Internet connectivity, provided that there is no legislative barrier. In fact, the significant increase in smartphone usage in emerging and developing countries indicates the potential prospect of this proposed mobile ETP solution (Poushter, 2016).

Not only does the translation of the regulatory mandates into essential security requirements have broader uses than the scope of this research, the proposed mobile ETP solution also has potential to improve patient safety and healthcare outcomes in the Australian healthcare industry as well as in other countries and regions. Similarly, the frameworks constructed are not only applicable to the scope of this research (i.e. Android operating system platform) but can also be relevant for any fully electronic ETP implementation in the Australian healthcare industry.

8.4 Contribution to Knowledge

This research contributes to the current body of knowledge in the ETP context; first by building a bridge between the regulatory mandates in ETP and the security requirements for compliance verification; secondly by identifying the shortcomings in realising the full potential of the current implementation of eTP; thirdly by proposing a mobile alternative solution implemented on Android platform which can utilise the full potential of eTP; and finally by devising frameworks for developing and assessing such mobile solutions for security compliance as mandated by the acts, regulations and standards governing ETP in the Australian healthcare industry.

As a unique contribution of knowledge to the ETP context, this research transformed the Acts, regulations and standards governing the electronic transfer of prescriptions in various jurisdictions into a set of security requirements for implementation and compliance verification in the Australian healthcare industry (see Figure 2.9, Table 4.1 and 4.2 for details). Such interpretation is essential knowledge in bridging the gap between the high-level regulatory mandates and the implementation-level security requirements conforming to those mandates. Furthermore, the applicability of these security requirements for ETP is not limited to this research's proposed solution, implemented on the Android operating system platform only. They are applicable to any fully electronic implementation of ETP in the Australian healthcare industry developed on various operating system platforms such as iOS and Windows Phone.

This research also contributes to the body of knowledge by revealing the fact that, despite the current public impression of the advancement in electronic prescribing, many significant features of ETP have not been realised to their full potential (see Section 2.4.2 for details). Patients are therefore not getting the full benefit of the current ETP implementation despite its hefty ongoing cost on the nation. This research proposes an Android mobile solution as a way to further realise the potential of ETP and enable patients to gain greater benefits such as safer and better healthcare outcomes. Such a solution was created by conforming to the security requirements explored in the prior stage of this research (see Table 4.2 for details). Synthesising the proposed solution involved conducting a series of experimentations, and the experimentation outcomes proved that the prototype application developed on Android platform with Bluetooth wireless communication provided sufficient security assurance for transfer of electronic prescriptions (see Chapter 5 and 6 for details). This finding lays to rest the archaic belief that mobile solutions are not secure enough for the healthcare industry (Barrett, 2011; Bromwich & Bromwich, 2016). This knowledge itself potentially opens up other significant opportunities and innovations in the mobile healthcare industry.

The next contribution made by this research is the identification of regulatory requirements which have no actual value to the process of electronic prescription but which remain in effect as mere hindrances. It also highlights the components in the current implementation of ETP which are in place merely to satisfy the abovementioned historical regulatory requirements. These implementations pose limitations not only to the proposed mobile solution but to any fully electronic implementation in the Australian healthcare industry.

Finally, this research makes two unique, significant contributions by devising a framework which guides the development of an Android mobile ETP solution in compliance with mandated security requirements and a framework which assesses Android mobile ETP solutions for their security compliance (Figure 7.2 and 7.3). Although limited to the Android platform in the context of this research, both frameworks can be generalised with minimal effort for any fully electronic implementation of ETP in the Australian healthcare industry developed on various operating system platforms.

8.5 Future Research

This research can be extended in various ways. Generalising the framework to cover not only the Android operating system platform but any mobile operating system platform is one way to extend this research further. Since the outcomes from answering the supporting question 1 are applicable to any fully electronic ETP implementation, the need to translate the regulatory mandates into security requirements would be minimal for such continued study. In addition, such future line of inquiry could also make use of the theoretical framework and methodologies used in this research to repeat the process should regulatory change make it necessary to do so.

Another area in which this research can be continued is exploring the use of other forms of secured portable storage and transfer mediums, such as smartcards and self-encrypting storage devices. Whilst the assessment framework would require some adjustment to accommodate such expansion, this continued research would also be based upon the security requirements produced from this research unless there has been regulatory change in ETP context. As mentioned above, in the face of legislative or regulatory change such continued research would still benefit from following the theoretical framework and methodologies used in this research.

One future research area that would significantly improve the proposed mobile ETP solution is the facilitation of “script owing” and “script cancellation” features. The disconnected nature of the proposed solution made implementation of these two features difficult. At present, SMS (Short Message Service) and the SMD (Secured Message Delivery) facility of the eHealth infrastructure appear to be potential candidates for implementing these features. It calls for a thorough investigation, however, and a continued line of inquiry for this represents another future research area.

Since the proposed mobile ETP solution makes use of Bluetooth wireless communication for transferring electronic prescriptions between the EPS, EDS and the patient’s mobile smartphone, pairing of the devices is required for first-time use. The Bluetooth pairing process can be cumbersome at times, so streamlining this pairing process is in order. Such streamlining can be achieved by using technologies such as NFC tag or QR code to perform the pairing of the Bluetooth devices. However, every technology has vulnerabilities and introducing a combination of technologies may increase the risk. Such investigation opens another future line of inquiry extending this research.

Despite the fact that the proposed mobile solution chose Bluetooth over NFC for practicality and portability of the solution (i.e. availability of the proximity driver), the NFC also provided sufficient security assurance in securing electronic prescription information. Moreover, its very short communication range and simplicity in establishing communication certainly makes NFC a technology to be kept under careful observation for future use. Once the NFC device manufacturers make the proximity driver for their products publicly available in the same way Sony and XNP Semiconductors did for their FeliCa card readers/writers (Sharief, 2013), NFC may very well become a better suited wireless transfer mechanism than Bluetooth for electronic prescriptions exchange. Therefore, in addition to careful observation of changes/improvements in the NFC technology, further exploration on more portable use of NFC in software development would be another future research with significant impact on the mobile ETP context.

8.6 Summary

The proposed proof-of-concept mobile ETP solution and the frameworks built from this research may influence government departments, authority bodies and Health IT professionals to embrace modification of the current use of ETP in the Australian healthcare industry. In addition, this research has paved the way for future innovations and enhancements in ETP by making the regulatory mandates easily understandable for non-regulatory experts, and by establishing the fact that an alternative solution, in full compliance with these regulatory mandates, can be constructed using existing technologies.

Such knowledge effectively disproves the archaic belief that mobile solutions are not secure enough for the healthcare industry (Barrett, 2011; Bromwich & Bromwich, 2016), thereby creating other opportunities and innovations in the mobile healthcare industry. This also aligns well with the Australian Digital Health Agency's (ADHA) recent work on a mobile enablement program, designed to allow information to be extracted from MyHR into third-party applications, with a view to producing a mechanism to enable uploading data back into the MyHR system as the program progresses further. Together with a suite of other mobile healthcare applications such as the Healthi app by *Chamonix*, the MediTracker app by *Precedence Health Care*, the HealthNow app from *Telstra Health* and *Best Practice*'s patient app, the use of a mobile ETP application would make a significant contribution to building a more complete medication history and healthcare record of an individual. Availability of such information is a significant step towards more effective treatments and safer outcomes, benefiting both clinicians and patients, and with potentially less financial drain on the nation's healthcare expenditure.

In addition to their essential role in this research, the transformation of the ETP security requirements of the various regulatory mandates is applicable to any fully electronic ETP implementations in the Australian healthcare industry. Furthermore, since no previously established methodologies and frameworks have been verified and validated, particularly in this emerging eHealth context, the methodologies and framework used in this research may assist in future research in this sphere.

REFERENCES

Adopted specifications. (2016). Retrieved April 21, 2016, from Bluetooth SIG: https://www.bluetooth.com/specifications/adopted-specifications

Advanced NFC. (n.d.). Retrieved April 28, 2015, from Android Developers: https://developer.android.com/guide/topics/connectivity/nfc/advanced-nfc.html

All vulnerabilities. (n.d.). Retrieved June 7, 2016, from AndroidVulnerabilities.org: http://androidvulnerabilities.org/all

AMA Position Statement. (2009). Retrieved March 3, 2015, from Australian Medical Association: https://ama.com.au/sites/default/files/documents/Microsoft_Word_Position_Statement_on_Electronic_Prescription_Transfer_Sys%E2%80%A6_0.pdf

AMT PBS FAQs. (2016). Retrieved July 22, 2016, from Australian Digital Health Agency: https://www.digitalhealth.gov.au/about-the-agency/help-centre/frequently-asked-questions/amt-pbs-faqs

Android Bluetooth print stopped working on 4.1. (2012). Retrieved April 23, 2016, from Stack Overflow: http://stackoverflow.com/questions/12388503/android-bluetooth-print-stopped-working-on-4-1

Android Compatibility. (n.d.). Retrieved June 7, 2016, from Android: https://source.android.com/compatibility/index.html

Android Developers. (n.d.). Android Studio (Version 1.2.2) [Computer Software]. Retrieved April 28, 2015, from Android Developers: https://developer.android.com/studio/index.html

Android Interfaces and Architecture. (n.d.). Retrieved June 7, 2016, from Android: https://source.android.com/devices/

Android Security Bulletin. (2017). Retrieved November 19, 2017, from https://source.android.com/security/bulletin/2017-09-01

Android: Security Vulnerabilities. (n.d.). Retrieved June 7, 2016, from CVE Details: https://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-19997/Google-Android.html

Angers, J. & Machtmes, K. (2005). Anethnographic-case study of beliefs, context factors, and practices of teachers integrating technology. *The Qualitative Report,* 10(4), 771–794. Retrieved July 1, 2017, from http://www.nova.edu/ssss/QR/QR10-4/angers.pdf.

Answers to questions on notice. (2016). Retrieved July 22, 2016, from eRx Script Exchange: https://www.google.com.au/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwjhmYjPgPjNAhWOQpQKHXNdC1cQFggmMAI&url=http%3A%2F%2Fwww.aph.gov.au%2F~%2Fmedia%2FCommittees%2Fclac_ctte%2Festimates%2Fbud_1314%2FNEHTA%2FAnswers%2F031.pdf&usg=AFQjCNEQZleLbcdrLK69vmO9MxlfoOJkhA

Any Android phones that don't support Bluetooth. (2012). Retrieved April 20, 2016, from StackExchange: http://android.stackexchange.com/questions/24464/any-android-phones-that-dont-support-bluetooth

ANZ Mobile Pay. (2015). Retrieved April 20, 2016, from ANZ Bank: http://www.anz.com/personal/ways-bank/mobile-banking/mobile-pay/

Application Fundamentals. (n.d.). Retrieved November 22, 2017, from https://developer.android.com/guide/components/fundamentals.html

Apps that Connect to your My Health Record. (2017). Retrieved May 30, 2017 from My Health Record: https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/appconnect

Australian Medicine Terminology. (2016). Retrieved July 22, 2016, from Australian Digital Health Agency: https://www.digitalhealth.gov.au/get-started-with-digital-health/what-is-digital-health/clinical-terminology/australian-medicines-terminology

Avkash, K. (2014). Android Vulnerability to Privilege Escalation - Lollipop is the only Exception. Retrieved June 7, 2016, from Symantec: http://www.symantec.com/connect/blogs/android-vulnerability-privilege-escalation-lollipop-only-exception

Backgrounder. (2018). Retrieved June 4, 2018, from Canada Health Infoway: https://www.infoway-inforoute.ca/en/component/edocman/3139-prescribeit-backgrounder/view-document?Itemid=101

Barrett, C. (2011). Healthcare Providers May Violate HIPAA1 by Using Mobile Devices to Communicate with Patients. Retrieved February 12, 2018, from American Bar Association: https://www.americanbar.org/newsletter/publications/aba_health_esource_home/aba_health_law_esource_1110_barrett.html

Baseband Architecture. (2016). Retrieved April 21, 2016, from Bluetooth SIG: https://developer.bluetooth.org/TechnologyOverview/Pages/Baseband.aspx

Bennett, C.B. (2013). Are we there yet? A journey of health reform in Australia. M JA 2013; 199 (4): 251-255.

Blankenbeckler, D. (2010). An Introduction to Bluetooth. Retrieved April 19, 2016, from Wireless Developer Network: http://www.wirelessdevnet.com/channels/bluetooth/features/bluetooth.html

Bluetooth. (2016). Retrieved April 19, 2016, from Bluetooth SIG: https://www.bluetooth.com/what-is-bluetooth-technology/bluetooth

Bluetooth core specification. (2016). Retrieved April 21, 2016, from Bluetooth SIG: https://www.bluetooth.com/specifications/adopted-specifications

Bluetooth fact or fiction. (2016). Retrieved April 23, 2016, from Bluetooth SIG: https://www.bluetooth.com/bluetooth-technology/bluetooth-fact-or-fiction

Bluetooth SIG 2014 Annual Report. (2015). Retrieved April 21, 2016, from Bluetooth SIG: https://www.bluetooth.org/en-us/Documents/Annual_Report_2014.pdf

Bluetooth-Worm:SymbOS/Cabir. (2017). Retrieved from https://www.f-secure.com/v-descs/cabir.shtml

Boot, R. (2011). Why bother with eScripts? Retrieved April 17, 2017, from PULSE+IT: https://www.pulseitmagazine.com.au/news/australian-ehealth/783-why-bother-with-escripts?highlight=WyJ3aHkgYm90aGVyIHdpdGgiLCJ3aXRoIGVzY3JpcHRzIl0=

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, *9*(2): 27-40, doi: 10.3316/QRJ0902027

Brachmann, S. (2014). A Brief History of Google's Android Operating System. Retrieved June 7, 2016, from IPWatchdog: http://www.ipwatchdog.com/2014/11/26/a-brief-history-of-googles-android-operating-system/id=52285/

Bromwich, M. & Bromwich, R. (2016). Privacy risks when using mobile devices in health care. *Canadian Medical Association Journal, 188*(12): 855-856, doi: 10.1503/cmaj.160026

Callaham, J. (2017). The History of Android OS: tis name, origin and more. Retrieved November 19, 2017, from Android Authority: https://www.androidauthority.com/history-android-os-name-789433/

Cancellation of electronic prescriptions. (n.d.). Retrieved June 19, 2016, from Pharmaceutical Services Negotiating Committee (PSNC): http://psnc.org.uk/dispensing-supply/eps/cancellation-of-electronic-prescriptions/

Caused by: java.lang.SecurityException: Permission Denial. (2014). Retrieved April 23, 2016, from: http://www.cnblogs.com/xueqiang911226/p/3891852.html

Chan, A. T. (2000). WWW+smart card: Towards a mobile health care management system. *International Journal of Medical Informatics*, *57*(2-3), 127-37.

Clark, S. (2015). NFC Forum adds support for Type V tags. Retrieved April 19, 2016, from NFC World: http://www.nfcworld.com/2015/06/17/336050/nfc-forum-adds-support-for-type-v-tags/

Cole, M. & Avison, D. (2007). The potential of hermeneutics in information systems research. *European Journal of Information Systems*, 16(6), 820-833. doi: 10.1057/palgrave.ejis.3000725

CommBank Tap & Pay. (2016). Retrieved April 20, 2016, from CommBank: https://www.commbank.com.au/personal/online-banking/commbank-app/tap-and-pay.html

Communications Topology. (2016). Retrieved April 23, 2016, from Bluetooth SIG: https://developer.bluetooth.org/TechnologyOverview/Pages/Topology.aspx

Corbin, J. & Strauss, A. (2008). Basics of qualitative research: Techniques and procedures for developing grounded theory (3rd ed.). Thousand Oaks, CA: Sage.

Core System Architecture. (2016). Retrieved April 21, 2016, from Bluetooth SIG: https://developer.bluetooth.org/TechnologyOverview/Pages/Core.aspx

Coskun, V., Ok, K., & Ozdenizci, B. (2012). NEAR FIELD COMMUNICATION: FROM THEORY TO PRACTICE. Wiley.

Coskun, V., Ok, K., & Ozdenizci, B. (2013). Professional NFC Application Development for Android. Wrox.

Crotty, M. (1998). The foundations of social research: meaning and perspective in the research. SAGE.

Dashboards. (n.d.). Retrieved June 7, 2016, from Android: https://developer.android.com/about/dashboards/index.html#Platform

Difference between academic and professional doctorate degrees. (2017). Retrieved from http://opa.berkeley.edu/difference-between-academic-and-professional-doctorate-degrees

Document Analysis (n.d.). Retrieved July 2, 2017, from Ask Dr. Cath: http://www.drcath.net/toolkit/document-analysis

Does Android's Full Filesystem Encryption also encrypt the SD card? (2012). Retrieved June 7, 2016, from StackExchange: http://android.stackexchange.com/questions/26425/does-androids-full-filesystem-encryption-also-encrypt-the-sdcard

Doherty, J. (2015). Wireless and Mobile Device Security. Jones & Bartlett Learning.

eHealth. (2014). Retrieved October 11, 2016 from World Health Organisation: http://www.euro.who.int/__data/assets/pdf_file/0010/261694/6.-eHealth,-Factsheet-for-European-Parliament.pdf

Electronic Medication Management Systems - 2nd Edition. (2012). Retrieved July 22, 2016, from Australian Commission on Safety and Quality in Health Care: http://www.safetyandquality.gov.au/wp-content/uploads/2011/01/EMMS-A-Guide-to-Safe-Implementation-2nd-Edition-web-version.pdf

Electronic Transaction Act 1999 (Commonwealth)

Electronic Transfer of Prescriptions. (2016): https://www.guild.org.au/__data/assets/pdf_file/0025/5785/electronic-transfer-of-prescriptions-.pdf

Electronic Transfer of Prescriptions (ETP): Frequently asked questions. (2013). Retrieved July 22, 2016, from NPS Medicinewise: https://www.nps.org.au/__data/assets/pdf_file/0005/228974/NPS-MedicineWise-eTP-Information-sheet.pdf

Electronic Transfer of Prescriptions v1.1. (2010). Retrieved July 22, 2016, from Australian Digital Health Agency: https://www.digitalhealth.gov.au/implementation-resources/clinical-documents/electronic-transfer-of-prescription

Encryption. (n.d.). Retrieved November 24, 2017, from https://source.android.com/security/encryption

ePrescriptions. (2012). Retrieved March 3, 2015, from NEHTA: http://www.nehta.gov.au/component/docman/doc_download/1658-eprescriptions-factsheet?Itemid=

ETP Standards. (2016). Retrieved July 22, 2016, from eRx Script Exchange: http://www.erx.com.au/eprescribing/etp-standards/

Expenditure and Prescriptions Twelve Months to 30 June 2016. (2016). Retrieved April 18, 2017 from The Pharmaceutical Benefits Scheme: http://www.pbs.gov.au/statistics/expenditure-prescriptions/2015-2016/expenditure-prescriptions-report-2015-16.pdf

Express Scripts. (n.d.). Retrieved October 27, 2017, from eRx Script Exchange: http://www.erx.com.au/express/

Fereday, J. & Muir-Cochrane, E. (2006). Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods*, 5(1), 80–92. Retrieved 1 July 2017, from http://www.ualberta.ca/~iiqm/backissues/5_1/pdf/fereday.pdf.

Fillingham, D. (1997). A Comparison of Digital and Handwritten Signatures. Retrieved February 12, 2018, from http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall97-papers/fillingham-sig.html

Frequently Asked Questions. (2015). Retrieved July 22, 2016, from MediSecure: http://medisecure.com.au/faqs/

Gabriel, M. H., & Swain, M. (2014). E-Prescribing Trends in the United State. Retrieved June 4, 2018, from HealthIT: https://www.healthit.gov/sites/default/files/oncdatabriefe-prescribingincreases2014.pdf

Gregory, T. (2013). Electronic prescribing to reduce medication error. Retrieved March 3, 2015, from RACGP Conference 2013: http://racgpconference.com.au/gp13/PDF/presentations2013/BusinessPractice/1.pdf

Haataja, K., Hyppönen K., Pasanen, S., & Toivanen, P. (2013). Bluetooth Security Attacks: Comparative Analysis, Attacks, and Countermeasures. Springer

Hamblen, M. (2012). A short history of NFC. Retrieved April 20, 2016, from http://www.computerworld.com/article/2493888/mobile-payments/a-short-history-of-nfc.html

Henderson, J., Pollack, A., Gordon, J., & Miller, G. (2014). Technology in practice – GP computer use by age. Australian Family Physician, 43 (12),831-831

Herr, K. & Anderson, G. L. (2005). *The action research dissertation: A guide for students and faculty*. Thousand Oaks, CA: SAGE Publications.

Hildenbrand, J. (2017). What is the Android Open Source project? Retrieved November 22, 2017, from https://www.androidcentral.com/aosp

Hochmuth, P. (n.d.). Data velocity: Data in-motion vs. data at-rest. Retrieved from http://dellsecurity.dell.com/data-velocity-data-in-motion-vs-data-at-rest/

Holt, T. (2017). What Are Software Vulnerabilities, and Why Are There So Many of Them?. Retrieved June 23, 2017, from Scientific American: https://www.scientificamerican.com/article/what-are-software-vulnerabilities-and-why-are-there-so-many-of-them/

HTC. (2016). HTC Sync Manager [Computer Software]. Retrieved March 08, 2016, from HTC Support: http://www.htc.com/us/support/software/htc-sync-manager.aspx

IEEE. (2005). IEEE Std 802.15.1-2005. Retrieved April 19, 2016, from IEEE Standards Association: https://standards.ieee.org/findstds/standard/802.15.1-2005.html

Igoe, T., Coleman, D., & Jepson, B. (2014). Beginning NFC: Near Field Communication with Arduino, Android, and PhoneGap. O'Reilly

Inquest into the Death of Jared Charles OLSEN. (2017). Retrieved March 14, 2018 from Coroner's Court of Western Australia: http://www.coronerscourt.wa.gov.au/I/inquest_into_the_death_of_jared_charles_olsen_print.aspx

iOS: Supported Bluetooth profiles. (2015). Retrieved April 20, 2016, from Apple: https://support.apple.com/en-au/HT204387

James Reeve, J. & Sweidan, M. (2011). Setting a standard for electronic prescribing systems. Retrieved October 28, 2017, from NPS MedicineWise: https://www.nps.org.au/australian-prescriber/articles/setting-a-standard-for-electronic-prescribing-systems

Japan Association for Medical Informatics. (2014). Japan Association for Medical Informatics: explanation of the structure and guidelines for implementation. Retrieved August 19, 2016, from JAMI: https://www.jami.jp/jamistd/docs/SS-MIX2/descript-implemglonSS-MIX2_V1.2.pdf

Jolly, R. (2011). The e health revolution-easier said than done. Retrieved October 28, 2017, from NPS MedicineWise: https://www.aph.gov.au/about_parliament/parliamentary_departments/parliamentary_library/pubs/rp/rp1112/12rp03

Jürjens, J. & Rumm, R. (2008). Model-based security analysis of the German health card architecture. *Methods of Information in Medicine*, *47*(5), 409-16.

Kaye, J. (2014). Replace Cable Applications in Industrial Automation with Bluetooth Low Energy (BLE). Retrieved April 21, 2016, from Embedded Systems Engineering: http://eecatalog.com/lps/2014/02/07/replace-cable-applications-in-industrial-automation-with-bluetooth-low-energy-ble/

Kimura, M., Ohe, K., Yoshihara, H., Ando, Y., Kawamata, F., Tsuchiya, F., . . . Akiyama, M. (1998). MERIT-9: a patient information exchange guideline using MML, HL7 and DICOM. International Journal of Medical Informatics, 51, 59–68. doi: 10.1016/S1386-5056(98)00090-2

Leyden, J. (2003). Bluejacking ain't hijacking. Retrieved from https://www.theregister.co.uk/2003/11/21/bluejacking_aint_hijacking/

Liamputtong, P. (2009). *Qualitative Research Methods* (Third Edition). Oxford University Press.

M-HEALTH. (n.d.). Retrieved Oct 27, 2017, from RACGP: https://www.racgp.org.au/digital-business-kit/m-health/

Maddox, T. (2016). IoT hidden security risks: How businesses and telecommuters can protect themselves. Retrieved November 21, 2017 from TechRepublic: https://www.techrepublic.com/article/iot-hidden-security-risks-how-businesses-and-telecommuters-can-protect-themselves/

Mahmoud, Q. H. (2003). Wireless Application Programming with J2ME and Bluetooth. Retrieved April 20, 2016, from Oracle: http://www.oracle.com/technetwork/java/javase/downloads/index-156651.html

Market share held by smartphone operating systems in Australia from 2013 to 2017. (2018). Retrieved May 30, 2018, from Statista: https://www.statista.com/statistics/245191/market-share-of-mobile-operating-systems-for-smartphone-sales-in-australia/

Maxwell, J. A. (2005). *Qualitative Research Design: An Interactive Approach* (Second Edition). Sage Publications.

May, T. (2002). *Qualitative Research in Action*. Sage Publications.

McDonald, K. (2012). $10 million for prescription exchange interoperability. *PLUSE+IT*. Retrieved June 7, 2016, from PULSE+IT: http://www.pulseitmagazine.com.au/index.php?option=com_content&view=article&id=1223

McDonald, K. (2013a). RACGP prefers opt-in model for dispense notifications. *PLUSE+IT*. Retrieved June 9, 2016, from PULSE+IT: https://www.pulseitmagazine.com.au/news/australian-ehealth/1351-racgp-prefers-opt-in-model-for-dispense-notifications

McDonald, K. (2013b). Child health app released as PCEHR registrations grow. Retrieved June 9, 2016, from PULSE+IT: https://www.pulseitmagazine.com.au/news/australian-ehealth/1453-child-health-app-released-as-pcehr-registrations-grow

McDonald, K. (2014). PCEHR needs seamless medications curation: review panel. *PLUSE+IT*. Retrieved June 7, 2016, from PULSE+IT: http://www.pulseitmagazine.com.au/allied-health/1881-pcehr-needs-seamless-medications-curation-review-panel

McDonald, K. (2016a). Fred IT to release first phase of medicines workspace in NQ MyHR trial. Retrieved June 19, 2016, from PULSE+IT: https://www.pulseitmagazine.com.au/australian-ehealth/3000-fred-it-to-release-first-phase-of-medicines-workspace-in-nq-myhr-trial

McDonald, K. (2016b). MediTracker promises to do what MyHR hasn't and put GP record in patient's hand. *PLUSE+IT*. Retrieved April 9, 2017, from PULSE+IT: https://www.pulseitmagazine.com.au/australian-ehealth/3629-meditracker-promises-to-do-what-myhr-hasn-t-and-put-gp-record-in-patient-s-hand

Medical & Health. (2017). Retrieved from https://www.bluetooth.com/what-is-bluetooth-technology/where-to-find-it/medical-health

MedView and eRx a winning eHealth team. (2012). *eRx Script Exchange News*. Retrieved July 21, 2016, from http://erx.com.au/wp-content/uploads/2013/09/eRx_Newsletter_2012-2.pdf

MedView Medicines Workspace. (2016). Retrieved October 29, 2017, from FRED: https://www.fred.com.au/2016/07/medview-medicines-workspace-bridging-gap/

Member Directory. (2016). Retrieved January 14, 2018, from Bluetooth SIG: https://www.bluetooth.com/membership-working-groups/member-directory?page=1

Miles, M. B., & Huberman, A. M. (1994). *Qualitative Data Analysis* (Second Edition). Sage Publications.

Millard, E. (2004). Cabir: World's First Wireless Worm. Retrieved from https://www.technewsworld.com/story/34542.html

Mobile Phones & Smart Phones. (2017). Retrieved from https://www.bluetooth.com/what-is-bluetooth-technology/where-to-find-it/mobile-phones-smart-phones

Monegain B. (2013). E-prescribing in growth mode. Retrieved October 27, 2017, from Healthcare IT News: http://www.healthcareitnews.com/news/e-prescribing-growth-mode

Moukheiber, Z. (2014). How Surescripts Became The Dominant Electronic Prescribing Network. Retrieved June 4, 2018, from Forbes: https://www.forbes.com/sites/zinamoukheiber/2014/04/22/how-surescripts-became-the-dominant-electronic-prescribing-network/#33140d635aa0

MSIA Issues presented at the eHealth ICT meeting 13 March 2013. (2013). Retrieved July 22, 2016, from Medical Software Industry Association: http://www.msia.com.au/cicms/assets/files/pg35as3gr1so27.pdf

MVD: Mobile Vulnerability Database. (2013). Retrieved June 7, 2016, from VARUTRA: http://www.varutra.com/mobile-vulnerability-database-mvd.html

NEHTA Blueprint V2. (2011). Retrieved July 21, 2016, from Australian Digital Health Agency: https://www.digitalhealth.gov.au/implementation-resources/ehealth-foundations/EP-1048-2011/NEHTA-1026-2011

NFC phones: The definitive list. (2016). Retrieved April 20, 2016, from NFC World: http://www.nfcworld.com/nfc-phones-list/

NFC Troubleshooting Guide. (n.d.). Retrieved April 16, 2016, from Samsung: http://www.samsung.com/global/buildpc/data/Samsung_Slate_PC_Windows_Developer_Preview_NFC_Troubleshooting.pdf

NPS MedicineWise. (2012). Ehealth. Retrieved March 3, 2015, from NPS Medicinewise: http://www.nps.org.au/topics/e-health

NXP and Sony announce joint venture to build chips with FeliCa, Mifare, and NFC. (2006). Retrieved April 15, 2016, from SecureIDNews: http://www.secureidnews.com/news-item/nxp-and-sony-announce-joint-venture-to-build-chips-with-felica-mifare-and-nfc/

One billion eRx electronic scripts dispensed and counting. (2016). Retrieved July 22, 2016, from eRx Script Exchange: http://www.erx.com.au/one-billion-scripts/

Ostergaard, J. (2011). Lessons learned in Electronic Medication Management. *PLUSE+IT*. Retrieved June 7, 2016, from PULSE+IT:

http://www.pulseitmagazine.com.au/index.php?option=com_content&view=article&id=784:lessons-learned-in-electronic-medication-management&Itemid=226

Patrao, L., Deveza, R., & Martins, H. (2013). PEM-A new patient centred electronic prescription platform. *Procedia Technology, 9*, 1313-1319. doi:10.1016/j.protcy.2013.12.147

Patton, M. Q. (1990). *Qualitative evaluation and research methods* (2nd ed.). Newbury Park, CA: Sage.

Pickard, A. (2007). *Research Methods in Information*. London: Facet Publishing.

Poole, I. (n.d.). NFC Tags and Tag Types. Retrieved April 20, 2016, from Radio-Electronics: http://www.nfcworld.com/2015/06/17/336050/nfc-forum-adds-support-for-type-v-tags/

Poushter, J. (2016). Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies. Retrieved March 14, 2018, from Pew Research Center: http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/

PrescribeIT™. (2018). Retrieved June 4, 2018, from PrescribeIT™: https://www.prescribeit.ca/component/content/article?id=17&Itemid=149

Productivity Commission. (2015). Efficiency in Health, Commission Research Paper. Canberra, Australia.

Professional doctorates. (n.d.). Retrieved from http://www.unisa.edu.au/Research/Research-degrees/What-you-can-study/Professional-doctorates/

Publish Your App (n.d.). Retrieved November 21, 2017, from https://developer.android.com/studio/publish/index.html

Quinlan, F. (2000). Electronic prescribing in general practice: one small step. Australian Prescriber,(23):50-1.

Raphael, J. R. (2017). Android versions: A living history from 1.0 to today. Retrieved November 24, 2017, from Symantec: https://www.computerworld.com/article/3235946/android/android-versions-a-living-history-from-1-0-to-today.html

Reason, P., & Bradbury, H. (2001). *Handbook of action research : Participative inquiry and practice*. London: SAGE.

Ree, J., & Urmson, J. O. (1991). *The concise encyclopaedia of western philosophy and philosophers*. Routledge.

Reisenhofer, E., Bright, M., Mangione, J., Mosch, P., Jeff Neafsey, J., & Polak, P. (2016). Simplifying IoT: Connecting, Commissioning, and Controlling with Near Field Communication (NFC). Retrieved January 13, 2018, from NFC Forum: http://nfc-forum.org/wp-content/uploads/2016/06/NFC_Forum_IoT_White_Paper_-v05.pdf

Roughead, L., Semple, S., & Rosenfeld, E. (2013). Literature Review: Medication Safety in Australia. Retrieved October 28, 2017, from NPS MedicineWise: https://safetyandquality.gov.au/wp-content/uploads/2014/02/Literature-Review-Medication-Safety-in-Australia-2013.pdf

RxNorm. (2018). Retrieved June 4, 2018, from U.S. National Institutes of Health: https://www.nlm.nih.gov/research/umls/rxnorm/

Seale, C. (Ed.). (2007). *Qualitative research practice*. London: Sage.

Security. (n.d.). Retrieved June 7, 2016, from Android: https://source.android.com/security/

Set up Electronic Transfer of Prescriptions (ETP) in your Organisation. (2016). Retrieved July 22, 2016, from Australian Digital Health Agency: https://www.digitalhealth.gov.au/get-started-with-digital-health/set-up/set-up-etp-in-your-organisation

Sharief, K. (2013). Windows 8 and ACS ACR122u NFC reader compatibility issue. Retrieved April 15, 2016, from Microsoft: http://www.nfcworld.com/2015/06/17/336050/nfc-forum-adds-support-for-type-v-tags/

Standards Australia. (2013a). Part 2: Platform independent (logical) services model to support electronic transfer of prescriptions (ATS 4888.2-2013). Retrieved from http://www.standards.org.au/

Standards Australia. (2013b). Part 3: Platform implementation specific e-prescription HL7 Clinical Document Architecture implementation guide (ATS 4888.3-2013). Retrieved from http://www.standards.org.au/

Standards Australia. (2013c). Part 6: Platform implementation specific web service (ATS 4888.6-2013). Retrieved from http://www.standards.org.au/

SymbOS.Cabir. (2017). Retrieved from https://au.norton.com/online-threats/symbos.cabir-2004-061419-4412-99-writeup.html

Tan, L. (2007). Protect against Bluetooth threats. Retrieved from http://www.zdnet.com/article/protect-against-bluetooth-threats/

The Difference between RFID and NFC. (2011). Retrieved April 19, 2016, from http://cs.stanford.edu/people/eroberts/courses/cs181/projects/2010-11/NFCChips/difference.html

Townsend, K., Kufi, C., Davidson, A., & Davidson, R. (2014). Getting started with Bluetooth Low Energy. O’Reilly.

The Electronic Transactions Act 1999. (n.d.). Retrieved April 18, 2017, from Attorney-General's Department: https://www.ag.gov.au/RightsAndProtections/ECommerce/Documents/ElectronicTransactionsAct1999infosheet.pdf

Tutorial: Understanding Android's Security Framework (2010). Retrieved September 19, 2016, from http://siis.cse.psu.edu/android_sec_tutorial.html

Vulnerabilities. (2017). Retrieved June 23, 2017, from Norton Security: http://www.nortonsecurityonline.com/security-center/vulnerabilities.html

What can an attacker do with Bluetooth and how should it be mitigated. (2013). Retrieved April 20, 2016, from StackExchange: http://security.stackexchange.com/questions/26356/what-can-an-attacker-do-with-bluetooth-and-how-should-it-be-mitigated

Which Android runs which Linux kernel? (21 August 2013). Retrieved June 7, 2016, from StackExchange: http://android.stackexchange.com/questions/51651/which-android-runs-which-linux-kernel

Williamson, K. (2002). *Research methods for Students, Academics and Professionals* (Second Edition). Centre for Information Studies.

Winners the European Inventor Award 2015. (2015). Retrieved April 18, 2016, from European Paten Office (EPO): https://www.epo.org/learning-events/european-inventor/finalists/2015/amtmann.html

Wireless History Timeline. (2016). Retrieved April 22, 2016, from Wireless History Foundation: http://www.wirelesshistoryfoundation.org/wireless-history-project/wireless-history-timeline

Xavier, H. (2012). Using NFC (Near Field Communication) from Windows* 8 Applications. Retrieved April 15, 2016, from Intel Developer Zone: https://software.intel.com/en-us/articles/using-nfc-from-windows-8-applications

Appendix A. PEER REVIEWED PUBLICATIONS FROM THIS RESEARCH

Research Paper 1:

Htat, K. K., Williams, P. A. H. & McCauley, V. (2015).). The hare and the hortoise [*sic*]: The potential versus the reality of eTP implementation. In A. Georgiou, H. Grain, & L. K. Schaper (Eds). (2015). *Driving reform: Digital health is everyone's business*. *Studies in Health Technology and Informatics, 214*. IOS Press ebooks. The paper is available here.

Research Paper 2:

Htat, K. K., Williams, P. A. H., & McCauley, V. (2015). Security of ePrescription: Security of data at rest in Prescription Exchange Services vs on mobile devices. Paper presented at in the *Proceedings of the 4th Australian eHealth Informatics and Security Conference 2015*, Perth, Australia. (pp. 15-22). doi: 10.14221/aeis.2015.2. The paper is available here.

Research Paper 3:

Htat, K. K., Williams, P. A. H., & McCauley, V. (2017). Security of ePrescription: Data intransit comparison using existing and mobile device services. In *Proceedings of the Australasian Computer Science Week Multiconference*. Geelong, Australia. ACM, doi: 10.1145/3014812.3014870. A link to the paper is available here.

Research Paper 4:

Htat, K. K., Williams, P. A. H., & McCauley, V. (2016). Future of Australia’s ETP: Script exchange, script vault or secure mobile alternative. In Johnstone, M. (Ed.). (2016). *The Proceedings of 14th Australian Information Security Management Conference, 5-6 December, 2016, Edith Cowan University, Perth, Western Australia*. (pp.52-59). doi: 10.4225/75/58a69d860a643. The paper is available here.