**Edith Cowan University**
**Research Online**

Australian Information Warfare and Security Conference

Security Research Institute Conferences

2006

# Mediated Identification

D T. Shaw
*Edith Cowan University*

Originally published in the Proceedings of 7th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 4th - 5th December, 2006.
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/isw/18

# Mediated Identification

DT Shaw
School of Computer and Information Science
Edith Cowan University
Mount Lawley, Western Australia
dtshaw@student.ecu.edu.au

## Abstract

*Identity and identification are linked by variable meanings and applications and are essential in many remote transactions. Identification relying on mediation or third party intervention may be modified or withdrawn at will. Creating or re-establishing identity may require time and resources including artefacts such as the identity card usually sourced from a third party. The characteristics of the identification process and artefacts are discussed and the requirements of user-mediated identification artefacts are explored. The implicit link between user identity and artefact identity may be broken under certain circumstances.*

**Keywords**

Artefacts, authentication, identification, transactions

**Introduction**

Appropriate identification is fundamental to many transactions where participants may be allocated. Yet acceptance of cost and/or responsibility by one party may permit specific identification to be ignored. However, 'Identification' is more than 'naming of the parts', it establishes a group (peers) for transactions. Further, transactions rely on complex social phenomena and protocols that define the appropriate behaviour and criteria.

Protocols may have implicit (based on social practices) or explicit (based on written procedures) conditions and application. Many protocols require participation by a third party (arbitration and adjudication) (Schneier, 1996, pp. 23-27) whose identity is also important.

In part, identification gives group belonging (protection) to the individual while indicating unique existence within a group. Whatever identification is allocated to or assumed by any party, it may be repudiated after the fact for arbitrary reasons and durable records assist in resolving disputes. Additionally, such records need to be held by more than one party to minimise the opportunity for misconduct, collusion or, alternately, the records need to be unalterable.

While the process is explored further, the following terms are used: 'Artefacts' are objects, (which may be intangible) created to perform some task or function; '*Mediation' is the process of 'intervening between two parties in order to affect/effect a relationship between them;*' (O'Sullivan, Hartley, Saunders, Montgomery and Fiske, 1998, p. 176); 'Identification' is both the '*condition of being a specified person*' (TCOD, 1977, p533) and the '*process by which the individual merges at least some of another's identity with his or her own*' (O'Sullivan et al, 1998, p. 139); 'ID' is the artefact used to effect identification.

Regardless of the number of personal ID retained, generated and used by an individual, mediation is by relatively few primary artefacts such as the birth certificate, passport and driver licence. Artefact provenance affects their relative importance, and acceptance is linked to a belief that the 'false id' probability is acceptably small.

Given the centrality, necessity and utility of identification in daily activities, allocation of 'inappropriate' identification occurs. From informal activities such as individual misconduct to organisation or state-sponsored schemes, identification may be allocated to deny 'rights' or participation in social activities. (Baigent and Leigh, 2000, p. 32)

For example, 'excommunication' (ibid, p.33) denied the individual spiritual aid and encouraged social isolation by bystanders where civil rights and privileges were revoked. More formally, forcing individuals to wear symbols of inferior status to publicly indicate the denial of social participation.

Further, state sponsored action such as 'Nacht und Nebel' [online] decrees institutionalised the enforced disappearance of the individual with no information about the fate ever made available. Orwell mentions the category 'unperson' in his novel about totalitarian governments (Orwell, 1984).

While necessary identity may be allocated, arbitrated and adjudicated, there remains the possibility of identity denial, where existing artefacts are revoked or repudiated. While 'right' to issue ID, usually based on practical power, is not questioned here, is there a corresponding 'right' to withhold or withdraw identification? In general, international law and convention suggests no right (UNPRINC, 1989). Obtaining adequate identification or recreating lost identification may be complicated by political or social attitudes rather than just administrative proceedings. Yet, in practice, relatively few primary ID are used to create many more.

However, the paradox is that implicit or explicit identification may be ignored by any or all parties to a transaction regardless of validity or appropriateness. The simplest 'exchange of value' transaction requires only non-specific identification that need not apply to all participants. For example, the vendor desires payment and when paid may regard specific identification as of secondary importance. Further, credit card fraud may occur through the omission of simple checks such as signature verification.

The Bank-Customer-Vendor (BCV) transaction is an example of arbitrated, adjudicated or mediated processes. Ideally, as long as the bank ensures that the money comes from one account and goes to another correctly, neither customer nor vendor need to be identified to each other or other participants such as witnesses.

Commentators dealing with electronic and remote transactions (McKnight and Chervany, 2001) suggest that 'trust' is necessary to effect transactions, though this is not certain. The lack of trust may not be an insuperable problem. (Lamport, Shostack and Pease, 1982).

**Identity and Identification with Authentication**

Identity may precede identification and both rely on complex interrelated meaning. Dictionaries show some possible meanings and suggest that identity is more than the allocation of a name.

Identity is '*To consider or represent as precisely the same*' Broadway, (Broadway, 1931) or '*the state of having the same nature or character with*' (Collins, 1977, p. 496)

Identification is '*The act of establishing identity*' (Collins, 1977, p 496), or '*condition of being a specified person*' (TCOD, 1977, p533) or '*the ability to uniquely distinguish an entity*' (Pipkin, 2000, p. 15) or '*… the process of associating oneself closely with other individuals of reference groups to the extent that one comes to adopt their goals and values and to share vicariously in their experiences*' (Fontana, 1999) or '*process by which the individual merges at least some of another's identity with his or her own*' (O'Sullivan et al, 1998, p. 139).

Authentication is '*the act of proving as genuine*' (Collins, 1977, p. 68). Pfleeger suggests that '*Identification and Authentication: unique and certain association of an identity with a subject or object*' (Pfleeger, 1997, p. 316) or ' *… involves two steps: finding out who the access requestor is and verifying that the requestor is indeed who he/she/it claims to be*' (Pfleeger & Pfleeger, 2003, p. 256) or '*… identification is usually accomplished by the authentication of an asserted identity*' & authentication is the '*… act of verifying the identity of a potential user*'(OUP. 1983).

Pfleeger discusses identity mediation, developing trust and the cross-referencing of sources in case of doubt. (Pfleeger, 1997, p 135)

It can be seen that identity, identification, authentication and verification are intertwined. Further, identification requires a challenge (authentication).

**Source of Identification and Mediation**

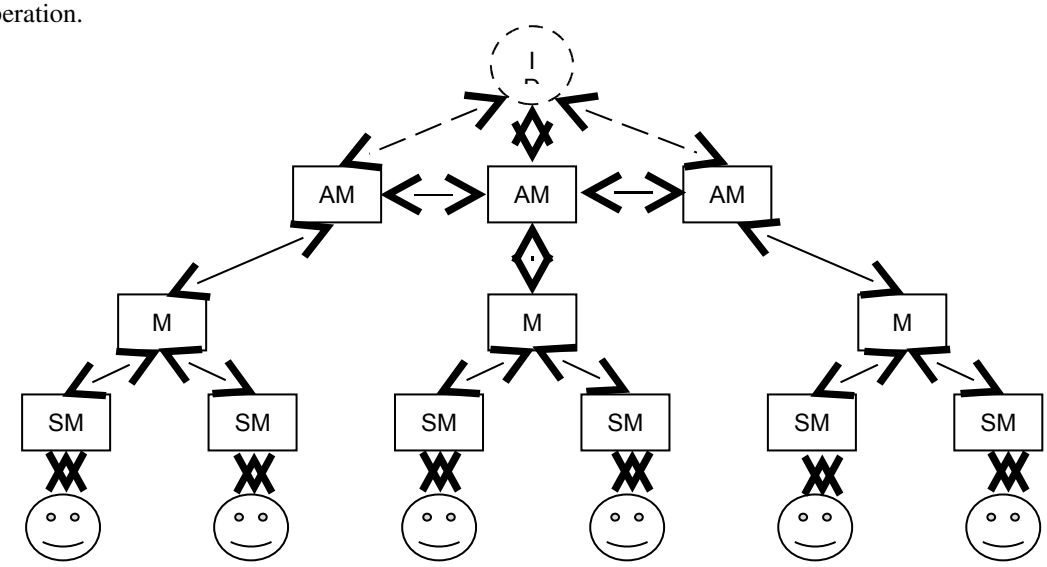
Mediation is essential in identification, where the recommendation of another influences a decision. Regardless of whatever 'identification' is tendered there must be a challenge, an event that requires 'proof' of identity. Surviving this challenge leads to trust based on experience.

In this structure, 'identification' originates from the arch mediator (AM) such as a national government that authenticates mediators (M) such as state governments who authenticate sub-mediators (SM) such as government agencies who 'identify' the individual. This hierarchy stems from an AM assuming identification responsibility (monopoly) and is maintained by belief that mediators will not issue false identification.

Research to date has not determined a central or original source of ID comparable to a primary standard for a physical unit such as length. Position, collegiality and cooperation legitimise AM activities, yet, with many governments, the practical power is founded on the consent/acquiescence of the population.

Many transactions rely on complex social phenomena (Boisot, 1987, p.91.) and also protocols that define the appropriate behaviour and criteria. These protocols may need arbitration and adjudication to function (Schneier, 1996, pp. 22-26).

In any transaction, uncritical acceptance of identification may facilitate misconduct or error, while demanding more than 'adequate' identification may be inefficient. Further, the amount and type of tendered identification is usually subject to participant choices. Consequently, identification relies on both parties for consent and cooperation.




In conclusion, identification/identity is the principal component of many transactions and is subject to constraints as well as human choices.

**Signatures as Identification**

One widely accepted artefact is the signature, yet an easily produced manual signature may not, for many natural reasons, be identical to a previous signature. Consequently, there exist mechanisms to support the challenge and verification of manual signatures. Disputes over manual signature validity may require the services of a handwriting specialist and depend on legal process. (Shaw & Maj, 2003)

Mitchell, Piper and Wild suggest that *'The crucial properties of a written signature are that it is easy to produce, easy to recognize but difficult to forge'* (IEEE92, 1992, p330).

As signatures may be used for a wide variety of activities, gradations of the signature process have evolved:

1. Initials of signatory (FB)
2. Full signature (Fred Bloggs)

3. Full signature & title block (Fred A. Bloggs, CEO, Atech Industries)
4. Full signature & title block with witness full signature & title block
5. Full signature & title blocks of all participants with authenticating artefacts

(Shaw and Maj, 2003)

Authenticating artefacts include the full ritual of the relevant signature process, eg the relevant protocol, costume and setting for a coronation. Additionally, there are aids to signatures such as the seal or signet. Other supporting information may include date, time, and context information not included in the transaction record.

Electronic signatures may also be legally used for assent and identity. Allen describes '*The Electronic Transactions Act*' that defines and regulates aspects of Australian law relating to electronic communications and commerce:

> *It was designed to enable, or facilitate, the development of electronic commerce in Australia (whether occurring over the internet or other media) by 'removing existing legal impediments that may prevent a person using electronic communications to satisfy obligations of the Commonwealth law'. (Allen, 2002, p.3)*

Menezes, Van Oorschot and Vanstone state*, 'Digital signatures must be easy to compute, easy to verify and have an appropriate lifespan'*. (Menezes et al., 1997, p30) It is clear that a digital signature must also meet the requirements of a written signature in contracts.

Consequently, electronic signatures should be easy to produce (compute), easy to recognise (verify), difficult to forge and have an appropriate life span. Electronic identification meeting these criteria may be used for local and remote transactions.

**Identification Processes**

Shaw and Maj identify three processes: 'Identification' permits 'Authentication' of activities and 'Verification' permits audit of same. Additionally, they describe two complementary identification forms: 'non-specific' that defines group membership and 'specific' which defines unique identity. (Shaw & Maj, 2002) Further, they define 'unilateral' and 'bilateral/multilateral' as categories. Unilateral identification occurs when an individual accepts non-specific or specific identification but is not identified in return. Bilateral or multilateral identification occurs when the identification process is shared.

For example, observing a person in uniform is a non-specific identification, and obtaining unique ID from them is specific identification. Self-identification may be made in return, giving bilateral identification. However, the nature of the artefacts used may be of interest.

Artefact provenance may be classified as follows: Applicability (local/wide), Source (centralised/decentralised) and Application (where usage protocols define constraints). Wide applicability describes artefact applicability where the range of operations exceeds the range of sources, for example, nationally sourced artefacts that are acceptable internationally. Local applicability describes applications where the range of operations is equal or less than the range of availability.

Central sourcing implies only one artefact source regardless of applicability and decentralised sourcing implies many sources, some of which may be competing.

Widely applicable, centrally sourced artefacts include the passport and other identification documents. Locally applicable, centrally sourced artefacts include professional registration, corporate identity cards. Wide, decentralised artefacts include credit cards and local, decentralised artefacts include bus tickets.

Flexibility and scalability assist in managing the identification process where choice of ID process and artefact permit cost effective, appropriate identification.

It is noted that artefact-based identification is hierarchical and the audit trail may be used to manage dispute. For example, a transit ticket (artefact) may link user identity (bank account number) with ticket number. By tracking

the ticket, the transit company may determine where/when a user boarded/exited a vehicle. Additionally, historical data may show normal and abnormal usage. While this may be used to optimise a business, there are concerns about the storage, handling and publication of the information. Improper use of this information may facilitate surveillance that may unfairly target sections of the public.

However, 'anonymous identification' (non-specific) may occur where the artefact not the bearer is important.

**Identification with artefacts**

Unilateral 'anonymous' identification occurs when an identification artefact is challenged. This 'challenge-response' process relies on the interrogator generating a challenge and storing the challenge and response. Re-identification occurs when the challenge-response pair is repeated. If necessary this process must evaluate all instances of the artefact to find a match.

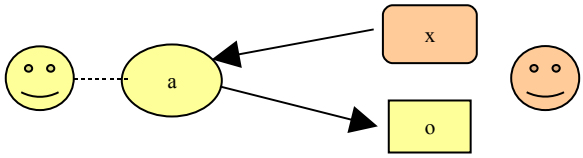



**Fig. 1.** Unilateral Non-specific Identification

In this figure, the interrogator stimulates the artefact, a with challenge, x and stores result, o. This identification may be repeated at any later time. However, to verify the identification (verification) the interrogator must check all artefact instances to ensure that the identification is unique and repeatable. This process may be used to bilaterally identify individuals.

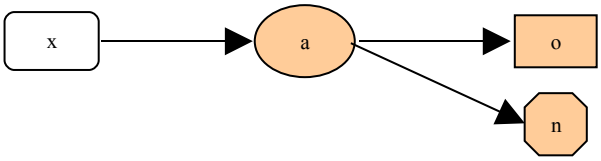



**Fig. 2.** Unilateral Specific Identification

Unilateral specific identification occurs when the unique artefact ID or Electronic Serial Number (ESN) is recorded as well as the input and output sequences. The artefact ID and by extension the person responsible for its use are identified. Re-identification occurs when the correct a is selected by using n (ESN) and the x and o are verified.

Both of these techniques may be combined or used bilaterally to provide information about other participants. Extensions of these simple techniques may be used to manage scalable and flexible identification in all categories.

**Smart Card Based Artefact**

Smart Cards have been used for Identification documents (ISO7816, 1995), Shaw and Maj discuss the requirements of an identification artefact to use in remote transactions. The artefact has been simulated in software after being modelled on a smart card, however, the following functions are desired:

- identify the bearer (external personalisation)
- perform data input and output
- identify the card (electronic serial number)
- control access to card services

- compute a secure hash value
- compute a signature value
- perform an encryption algorithm
- store a transaction record
- limit the number of new operations.

(Shaw and Maj, 2001)

These functions permit the user to control card services by personal identification number (PIN) to use the services provided in transaction protocols. The provision of hash, encryption and signature processes permit validation of transaction messages.

While a hash function may permit collisions, the signature generator function must be 'one-to-one' and 'one-way'. One-to-one indicates that each individual input is directly and uniquely associated to an individual output. One-way indicates that collated knowledge of output sequences will not assist in determining the signature generator function or input sequence.

The housekeeping functions include storing transaction records to prove that a particular artefact has been used in a particular operation. Limiting the number of new operations is necessary to minimise the amount of information that may be gathered to compromise the signature or encryption processes. The internal and external personalisation of the artefact is to provide identification. The external information does not require any electronic equipment.

Hardware design may make such a smart card resistant to attacks, (Kommerling & Kuhn, 1999), however, the security of this card design is in the uniqueness. While it may be cost effective to attack a major system such as 'Visa Card' through its protocols and simplistic artefacts, it may be very expensive to attack each unique card.

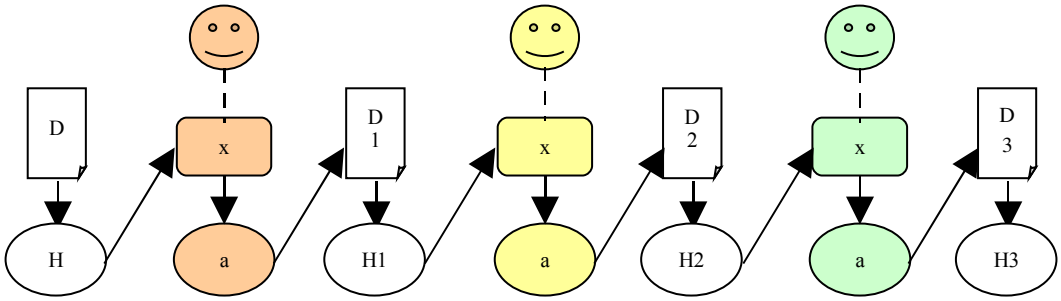



**Fig. 3.** Consecutive Signatures

It is noted that this artefact may be used in all categories of identification and permit authentication and verification (audit) of transactions after the fact. It is noted that this artefact may be unique or may have copies created for symmetrical transactions. The programming of the blank device may be similar to the programming of PLDs where fuses are blown, or through 'write once read many' (WORM) memory construction. It is proposed that an individual may create such an artefact from suitable, programmable blanks. Alternate implementations in hardware and/or software may also meet these requirements.

With associated protocols, this process can be scaled to include the outputs of associated signature processes creating consecutive or concurrent signatures that may provide scalability.

Multilateral consecutive signatures are used to indicate assent and responsibility for individual sections. If the signature generators are unique then the signatures will differ depending on sequence of operations. In the

figure above, each individual has a unique signature generator to produce a unique output for each individual input.

Consequently, this artefact may be used in all categories of identification.

**Recreating an Identification**

Where the primary source of identification fails, is no longer available or is repudiated there exist alternate mechanisms for recreating identification. These mechanisms are associated with 'group membership' of an individual and in part rely on the group identity.

The individual wishing to be identified by the group must first come into contact with at least part of it. By demonstrating various characteristics that are acceptable to the group (eg non-violent intent, cooperation etc) the basis of communication occurs. The accumulated experiences for both parties may lead to some permanent arrangements. For example, non-specific identification may permit the individual to continue transactions.

Specific identification may permit further transactions. As an example, an allocated 'nickname' may become the public (de facto) name of the person. Additionally, social role, physical characteristics, occupation, location or personal characteristics may assist a person to a personal name.

Acceptance of proffered identification is necessary for the continuance of transactions and an acceptor may choose how much identification is needed. For example, without speaking, an individual may contact a vendor, display suitable currency and point to an article. The unspoken request is to purchase the item. The non-specific identification as a 'customer' is mediated by the currency tokens underwritten by an AM. However, the vendor may require more identification.

With essential identification reliant on artificial/intangible entities, what options are available should a mediator err, lie or be duped and the artefact may be forged, stolen or inappropriate? Generally, there is a tacit acceptance of the error and effective sanctions against the mediator maybe few and impractical.

Peer pressure, if applicable, may not be heeded even if eventuated; ministerial complaint relies on a complex balance of power; Active sanctions need suitable support to be effective; Client pressure is difficult to organise. All of these methods rely on common cause made with others, that is, they have to identify with the protagonist.

Passive resistance (Satyagraha) may occur through the client opting out of formal identification processes. This may become a problem if enough people do not accept or receive the primary identification. Orwell (Orwell, 2000) describes the position of the Proles in '1984' and Huber suggests that with technological aid this may not be an impediment (Huber, 1994). Further, it may also affect the validity of the arch mediator, where public confidence supports the adopted role of ID purveyor. Assuming a loss of confidence in formal mediators, ID depends on peers, is local in scope, time-dependent and based on shared experience leading to mutual trust.

However, in 'Case 0', an individual has no peers with which to communicate and a name (identification) is, perhaps, superfluous. Laing suggests '… *the sense of identity requires another by whom one is known;* …'. (Laing, 1971, p. 139)

In 'Case 1', two equal individuals must learn by experience and example to communicate/compete/cooperate/coexist. Unequal individuals may not need specific identification, as non-specific identification is implicit in the master/slave, predator/prey relationship, though cooperation (symbiosis) may still be required.

In 'Case 2', three equal individuals must learn to compare, compete, cooperate/coexist, collude, conspire etc and these options may engender alliances that alter the balance of power. For example, secret agreement between two to disadvantage the third (Orwell, 2000).

In 'Case n', the sizeable group may resolve group identity and belonging issues by consensus. Concern for existing group relationships may affect an individual admission. For example, a member may be concerned that

personal status within the group is altered by an individual recommendation, hence anonymous voting protocols, such as a secret ballot (blackball/ostrakon) for inclusion or exclusion (exile).

In 'Case N-1', for N sufficiently large, the individual must negotiate admission where each group member may neither know nor interact with the individual. Identification is mediated by 'gatekeepers' who facilitate gaining adequate identification from and for the individual, yet formal identification criteria may be subject to interpretation which may include perceptions and prejudice among others. Regardless of the group's perception of its membership criteria, the interpretation by the gatekeeper is in effect.

The mediator/gatekeeper is empowered by the group and this links with the notion that a government is dependent on the population for its mandate. Building up trust in identification from the bottom has previously been augmented by the economies of centrally mediated id. The options provided by the electronic revolution for identification may encompass non-specific, partial, alternate as well as mediated ID.

**Withdrawing Identity**

The practice of inducing errors in databases is described as 'boggling' where the errors are deliberately designed to negate the data verification mechanisms in the information system (Shaw, Shaw and Maj, 2004) To deal with the implicit identification inherent in the linked account and artefact, the following scenario is proposed.

A social club, duly incorporated, negotiates a deal with a transit company for a discount on bulk ticket purchases. The members then contribute to a fund to buy the discounted tickets that are allocated to the members on a first come-first served basis. At the end of a time period the tickets are replaced with new ones and the remaining trips on the old tickets are redeemed for donation to a charity.

As the tickets are purchased by a legal entity using a legal bank account, the link between ticket number and non-specific group identification exists. Should the social club keep a record of who is allocated which ticket, then there is specific identification.

However, unused tickets are of equal value, and should two club members swap tickets, by accident or design, then the specific identification is no longer valid. This may not completely sever the link if there is collateral information in the records. The economies of not keeping specific records are worth considering. In the absence of legal requirements or the possibility of police serious crime investigation then keeping such records may be classed an unnecessary expense. It is noted that the concept of non-transferable tickets is apparently concerned with concessions and entitlements such as aged customer rather than specific identification.

Without repeated occurrences of 'mixed-up' tickets, collusion may be difficult to prove, though creating 'reasonable doubt' may be the intention. The group and individual responsibility for a notional offence may be difficult to elucidate, yet corroborative evidence from other sources may assist in resolving the inquiry.

Regardless of the implementation of a record system, the intent of the system is important. If the records are designed to track specific identity, the reason needs to be made plain. The increased opportunity for surveillance may lead to commercial exploitation of this information or political actions.

## CONCLUSION:

Identification is both socially and commercially desirable and is used to allocate cost and responsibility.

Construction/reconstruction of identity requires cooperation and acceptance from others and is based on shared experiences, common activities etc and this group identification underwrites the adopted user identification.

Identification must be scalable and flexible to permit the individual the maximum amount of freedom in effecting transactions. Artefacts used in the process must be able to identify the user, authenticate actions by the user and permit audit at any time to protect against claims of misconduct or error.

## REFERENCES:


Allen, M. (2002) E-business, the law and you - a guide for Australian business Prentice Hall Australia.

Baigent, M., and Leigh, R. (2000) The Inquisition Penguin books

Boisot, M. (1987) Information and Organizations Fontana Books ISBN 0-00-637126-4

Broadway (1931) The Broadway Concise English Dictionary, Grace Brothers Sydney

Collins (1977) Collins English Dictionary edited Irvine, A.H. William Collins and Sons

Fontana (1999) The New Fontana Dictionary of Modern Thought 3rd edition edited Bullock A & Trombley S Harper Collins

Huber, PW. (1994) Orwell's Revenge The 1984 Palimpsest Maxwell MacMillan Canada ISBN 0-02-915335-2 LoC 94-22921

IEEE92 (1992) Contemporary cryptology - The science of information integrity Edited Simmons, G.J. IEEE Press, Piscataway, NJ

ISO 7816-1 (1995) ISO 7816-1 : Identification Cards - Integrated Circuit Card with Contacts Part 1. Physical Characteristics International Standards Organisation.

Kommerling, O. and Kuhn, M.G. (1999) Design Principles for Tamper-Resistant Smartcard Processors Proceedings of the USENIX Workshop on Smartcard Technology (Smartcard '99), Chicago, Illinois, USA, May 10-11, 1999, USENIX Association, pp. 9-20, ISBN 1-880446-34-0.

Laing, R.D. (1971) The Divided Self Penguin Books, United Kingdom. ISBN 0 14 020734 1

Lamport, L., Shostak, R., and Pease, M. (1982) *The Byzantine Generals Problem*, ACM Transactions on Programming Languages and Systems, 4(3):382-401, July 1982.

McKnight and Chervany (2001) While Trust Is Cool And Collected, Distrust Is Fiery And Frenzied : A Model Of Distrust Concepts Proceedings of the Seventh American Conference on Information Systems Edited Strong, J. Straub, J. and De Gross, J.I. p. 883

Menezes, A.J., Van Oorschot, P., & Vanstone, S. (1997) Handbook of Applied Cryptography CRC Press ISBN0-8493-8523-7 LoC 96-27609

Orwell., G. (2000) Nineteen Eighty Four Penguin Books, United Kingdom

O'Sullivan, T., Hartley, J., Saunders, D., Montgomery, M., and Fiske, J. (1994) Key Concepts in Communication and Cultural Studies 2nd edition Routledge ISBN0-415-06173-3

OUP (1983) Dictionary of Computing edited Glaser E.L., Pyle, I.C. and Illingworth V. Oxford University Press UK ISBN 0-19-853905-3

Pfleeger, C.P. (1997) Security in Computing 2nd Edition Prentice Hall PTR

Pfleeger, C.P. and Pfleeger, S.L. (2003) Security in computing 3rd Edition Prentice Hall PTR

Pipkin, D. L. (2000) Information Security – protecting the global enterprise Prentice- Hall PTR

Schneier. B., (1996) Applied Cryptography 2nd Edition John Wiley and Sons ISBN0-471-11709-9 LoC 95-12398

Shaw, D.T. and Maj, S.P. (2001) A Single Protocol Smart Card for Multiple Applications. Proceedings of Information Systems Innovations 2001 American University of Dubai UAE Mar 19-21 2001

Shaw, D.T. & Maj, S.P. (2002) Multiple Applications With a Single Protocol Smart Card Proceedings of the Security Stream of the 17th IFIP World Congress, Montreal, Quebec, Canada, Edited Nardelli and Talamo

Shaw, D.T. & Maj SP (2003) Scalable and Flexible Electronic Identification proceedings of the 5th International Conference On Enterprise Information Systems - ICEIS2003, Ecole Superieure d'electronique de l' Ouest - Angers - France - 23-26 April, 2003

Shaw, D.T., Shaw, A. & Maj SP. (2004) '*Inducing Errors in Concatenated Databases'* Proceedings of the 5th Australian Warfare Information and Security Conference, Fremantle 25-26 November 2004

TCOD (1977) The Concise Oxford Dictionary

UNPRINC 1989 Principles on the Effective Prevention and Investigation of Extra-Legal, Arbitrary and Summary Executions, E.S.C. res. 1989/65, annex, 1989 U.N. ESCOR Supp. (No. 1) at 52, U.N. Doc. E/1989/89 (1989). *

Nacht Und Nebel http://en.wikipedia.org/wiki/Nacht_und_nebel Accessed June 2006

## COPYRIGHT

DT Shaw ©2006. The author/s assign SCISSEC & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SCISSEC & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors