6

Information Security

Introduction

6.1 In recent years Commonwealth agencies have rapidly expanded their use of the Internet as a contact point for their clients. In doing so, the agencies have changed the nature of the challenges to maintain the confidentiality and integrity of information in messages and data bases.

6.2 Despite the changing nature of the risks, however, there are numerous advantages to be gained by the use of electronic transactions: increased speed, increased customer participation and satisfaction, improved data keeping and analysis, increased productivity, improved product quality and better, more up-to-date, information for the public.[1]

6.3 In addition, NOIE considers that the risks can be minimised by a well designed and maintained security regime. Electronic records lend themselves more easily to robust security measures than do paper records. For the storage and transmission of very sensitive data, there are obvious benefits to be gained from an effective security protection regime, even though the initial cost may be considerably heavier than for less secure systems.[2]

6.4 Consideration of the increased risks and the increased ability of 'crackers' to break into seemingly secure computer systems has contributed to the decision by the Commonwealth to adopt a form of encryption known as Public Key Cryptography (PKC).

---

1 NOIE, *Online Authentication:: A Guide for Government Managers*, July 2002, pp 18-19.

2 NOIE, *Online Authentication:: A Guide for Government Managers*, July 2002, p. 19.

Public Key Cryptography[3]

6.5 The traditional form of message encryption, known as symmetrical encryption, uses a single secret key to both encrypt and decrypt messages. The weak point is the need for both parties to have the same key. If the key is intercepted and copied while being transmitted from one to the other, the whole system is compromised. Another problem is that a separate key will be needed for each different recipient. If the same key is used, all recipients will be able to read every message, not just the ones directed to them.[4]

6.6 In the PKC system, an asymmetric encryption technique is used. That is, the system uses two different but complementary (mathematically related) keys. One of these is known only to the holder – the private key. The other is a public key that can be known to anyone. A message encrypted with the public key can only be decrypted with the corresponding private key and vice versa. This means that anyone can use the public key to send a message and only the holder of the private key can decrypt it.[5]

6.7 PKC provides the following attributes for the communication of electronic information:

- **integrity**: the contents of the message received must be the same as that which was sent;
- **authentication**: the message can only have been sent by the purported sender; and
- **non-repudiation**: the sender cannot credibly deny that they sent it.[6]

6.8 To authenticate the identity of the sender or to ensure that a message has not been modified, the message can be sent with a digital signature appended. A digital signature is a special piece of data related to both the message being sent and to the sender's private key.

---

3 Public Key Cryptography is explained in more detail in Appendix F.

4 NOIE, *Online Authentication:: A Guide for Government Managers*, July 2002, p. 7; Mr Clarke, *Message Transmission Security (or 'Cryptography in Plain Text')*, 11 May 1998, http://www.anu.edu.au/people/Roger.Clarke/II/CryptoSecy.html , 28 October 2003, p. 3; and Computer Associates, *Submission No. 52*, p. 2.

5 Mr Clarke, *Message Transmission Security*, pp. 3, 10; NOIE, *Online Authentication:: A Guide for Government Managers*, July 2002, p. 8; Mr Engelman, *Transcript*, 2 April 2003, p. 153; Computer Associates, *Submission No. 52*, p. 2.

6 Mr Clarke, *Message Transmission Security*, p. 2.

Digital Certificates

6.9 Even when used correctly, PKC does not absolutely establish the identity of the sender – only that the sender had access to a particular private key. This problem can be resolved by using a trusted third party to verify the association between a public key and the identity of the owner of the associated private key.

6.10 Once that association has been verified and published in a digital certificate, other parties can trust that the person identified in the certificate holds the private key which matches the public key also referred to in that certificate. To achieve this, a significant number of infrastructure elements must be in place and functioning securely and effectively.[7]

Public Key Infrastructure

6.11 To implement the large-scale use of PKC requires the establishment of a Public Key Infrastructure (PKI), that is:

> … a set of procedures and technology that … enables users of a basically unsecured public network such as the Internet, to securely exchange information through the use of public and private cryptographic key pairs that are obtained and shared through a trusted evaluated infrastructure.[8]

6.12 Through the PKI, digital certificates are issued to properly identified applicants. The certificates are digitally signed, structured messages and achieve the aim of binding a public key to a verified identity. In doing so, they permit the accurate identification of an organisation or an individual.

6.13 The system consists of several components:

- Certification Authorities (CAs): trusted authorities which create and issue digital certificates. They may also create users' private keys (although, in practice, this is rarely done).
- Registration Authorities (RAs): check identities when new certificates are requested and process requests for renewal or revocation of existing certificates. In rare cases they also perform the CA functions of generating keys and certificates.

7 NOIE, *Online Authentication : A Guide for Government Managers*, July 2002, pp. 8-9.

8 NOIE, *Online Authentication:: A Guide for Government Managers*, July 2002, p. 8.

- Certificate or Key Holders: the end-user. They are issued with keys and certificates which enable them to digitally sign and encrypt electronic documents.
- Relying Parties: who receive, validate and accept digital signatures from key holders / subscribers.
- Repositories: which store and make available certificates and Certificate Revocation Lists (which are maintained by CAs).[9]

Gatekeeper

6.14 The Commonwealth PKI system is known as the Gatekeeper project. NOIE commented that Gatekeeper is not a product, as many people think, but a framework of standards used to measure the capability of applicants seeking accreditation as service providers.[10]

6.15 In late 1997 a number of agencies were investigating ways to enhance their service delivery by conducting business electronically. PKC was emerging as an accepted means of authenticating users, to ensure the security of electronic transactions. The Government decided to develop a national framework for the authentication of users of electronic online services. The then Office of Government Information Technology (OGIT) was charged with developing a strategy for the Commonwealth Government's use of PKC. OGIT formally established Project Gatekeeper in October 1997, and it was launched in May 1998.[11]

6.16 Application of the Gatekeeper standards is not compulsory for most Commonwealth agencies – each agency must make its own assessment of its need for security. However, if an agency decides that PKI is necessary, application of the Gatekeeper standards becomes compulsory for external use.[12]

6.17 On the other hand, firms or agencies wishing to become service providers must go through a long and comprehensive process to prove that they can meet all of the requirements of the Gatekeeper standards.[13]

---

9 NOIE, *Online Authentication:: A Guide for Government Managers*, July 2002, p. 29.

10 Ms Elsley, *Transcript*, 19 June 2003, p. 290; Mr Besgrove, *Transcript*, 19 June 2003, p. 293.

11 Gatekeeper Strategy, http://www.noie.gov.au/projects/confidence/Securing/Gatekeeperstrategy.htm, 28 October 2003.

12 NOIE, *Online Authentication:: A Guide for Government Managers*, July 2002, p. 4; Mr Besgrove, Mr Grant, *Transcript*, 19 June 2003, pp. 297.

13 Ms Elsley, *Transcript*, 19 June 2003, pp. 292-3.

Gatekeeper Accreditation

6.18 Firms or agencies seeking accreditation as Gatekeeper service providers – CAs or RAs – must meet stringent requirements which encompass all security enforcing aspects of their business and its operations. Accreditation is applied to the organisation, not their products. To use NOIE's words:

> The purpose of Gatekeeper accreditation is to provide an objective standard against which the competence of an organisation to deliver certification services can be assessed.[14]

6.19 Physical security of the premises is checked thoroughly by the Australian Security Intelligence Organisation (ASIO); the extent of these checks depending on what role is being requested under Gatekeeper. Different standards apply for CAs and RAs but in each case they would need to be assessed as Highly Protected by ASIO for their application to proceed.[15]

6.20 DSD carries out a detailed evaluation of the security of the applicant's IT system. This process includes an evaluation of the software involved.[16]

6.21 Operational evaluation of the applicant is handled by NOIE, which examines the applicant's operations manuals, their disaster recovery and business continuity plans and carries out a legal evaluation. The latter is necessary to establish the required level of trust for clients of the applicant.[17]

6.22 A Certification Practice Statement is developed by each CA/RA covering its operations, the infrastructure and the certificates to be issued. For each different type of certificate to be issued, a separate Certificate Policy is also developed.[18]

6.23 Security vetting of applicants is rigorous. The staff of each applicant must be vetted to the Highly Protected level. This is carried out by the Australian Security Vetting Service and the Australian Protective Service. Under the Gatekeeper arrangements, all service providers must also be on the endorsed supplier list administered by DoFA.[19]

6.24 When all of the requirements have been met to the satisfaction of the Chief Executive Officer of NOIE, a contract is signed on behalf of the

---

14 NOIE, *Submission No. 57,* p. 20.

15 NOIE, *Submission No. 57,* p. 22.

16 Ms Elsley, *Transcript,* 19 June 2003, p. 292; NOIE, S*ubmission No. 57,* p. 23.

17 Ms Elsley, *Transcript,* 19 June 2003, p. 292.

18 NOIE, *Submission No. 57,* p. 25.

19 NOIE, *Submission No. 57,* p. 24; Ms Elsley, *Transcript,* 19 June 2003, p. 292.

Commonwealth. The contract sets out in detail the obligations the service provider must fulfil. Every 12 months thereafter they must undergo a compliance audit to ensure that the Gatekeeper criteria are still being satisfied. The audits are carried out by one of a panel of auditors established and approved by NOIE.[20]

6.25 At the time of the inquiry, NOIE advised that eight organisations had achieved full Gatekeeper accreditation:

- Secure Net Limited as CA;
- Pricewaterhouse Coopers (beTRUSTed) as CA and RA;
- Australia Post as RA;
- Telstra Corporation Limited as CA and RA;
- eSign Australia Limited as CA and RA;
- Health eSignature Authority Pty Ltd as RA;
- Baltimore Certificates Australia Pty Ltd; as CA; and
- the ATO as CA and RA.[21]

6.26 In addition, the ANZ Bank was then undergoing the evaluation process for Gatekeeper accreditation.[22]

Commonwealth Agencies Using Gatekeeper

6.27 Government agencies participate voluntarily in Gatekeeper.[23] To date, very few agencies have chosen to participate. NOIE attributes this, in part, to the slow acceptance of PKC and the slow growth of the PKI market.[24]

6.28 The ATO was the first agency to attain full gatekeeper accreditation for their CA in May 2000. The HIC uses the authentication services of Health eSignature Authority Pty Ltd, which is a Gatekeeper certified RA.[25]

6.29 Some Government agencies have little or no need for certification. The type of business conducted by the ABS does not warrant the Bureau

20 Ms Elsley, *Transcript*, 19 June 2003, pp. 292-3.

21 NOIE, *Submission No. 57*, p. 5.

22 NOIE, *Submission No. 57*, p. 5.

23 Gatekeeper Strategy, http://www.noie.gov.au/projects/confidence/Securing/Gatekeeperstrategy.htm, 28 October 2003.

24 Mr Besgrove, Mr Dale, *Transcript*, 1 April 2003, p. 73.

25 Mr Farr, *Transcript*, 31 March 2003, p. 38; Gatekeeper Accreditation, http://www.noie.gov.au/projects/confidence/Securing/GatekeeperAccreditation.htm, 28 October 2003.

seeking certification. As it commented: 'People tend not to fraudulently lodge statistical returns on behalf of other people'.[26] Similarly, the Attorney-General's Department said that it has not yet found a business use for Gatekeeper.[27]

6.30 Other Government agencies have found that their authentication needs are met by less formal PKC, such as the Secure Socket Layer (SSL) protocol. DEWR said that it currently finds SSL to be sufficient:

> We believe that secure socket layer security is more than adequate for our interacting with the Job Network. … Certainly it is working well at the moment.[28]

Limitations of Gatekeeper

6.31 The Committee heard evidence on the limitations of Gatekeeper, in terms of cost and security.

Cost

6.32 A frequent comment by Government agencies and private companies was that Gatekeeper is too complex and / or expensive.[29] NOIE at first estimated that achieving Gatekeeper accreditation would cost around $300,000, but later commented that depending on circumstances and requirements, the cost has varied, in practice, between $200,000 and $2.2 million.[30] The use of Gatekeeper is not likely to expand until certification costs come down.

6.33 Some Government agencies are using authentication services that are not Gatekeeper accredited. A number of private companies offer their own authentication services in competition with Gatekeeper. These include Computer Associates and Check Point Software Technologies (Australia) Pty Ltd. Agencies outsourced to these companies use their services rather than the services of a Gatekeeper accredited provider.[31]

---

26 Mr Palmer, *Transcript*, 31 March 2003, p. 34.

27 Mr LeRoy, *Transcript*, 1 April 2003, p. 134.

28 Mr Burston, *Transcript*, 31 March 2003, pp. 63-64.

29 Ms Treadwell (Centerlink), *Transcript*, 31 March 2003, p. 30; Mr Besgrove (NOIE), *Transcript*, 1 April 2003, p. 73; Mr Wilson (Computer Associates), *Transcript*, 2 April 2003, p. 148; Ms Reich (SingTel Optus), *Transcript*, 2 April 2003, p. 194.

30 Mr Grant, *Transcript*, 1 April 2003, p. 80.

31 Mr Engelman, *Transcript*, 2 April 2003, p. 147; Mr Ferguson, *Transcript*, 2 April 2003, p. 185.

Security

6.34 PKIs such as Gatekeeper are '… not a foolproof solution to identity management'.[32] If a person's private keys are compromised, unauthorised people could impersonate them or read their messages. Thus private key security is of paramount importance to users of PKC. This has been highlighted as a crucial weakness of the PKC system as currently used, because few key holders can guarantee the absolute security of their keys. Private keys may be the target of crackers, viruses or worms. Hardware and software systems currently provide very little in the way of security features. [33]

6.35 The CA is expected to assure that the user of a certificate is who they claim to be. If such an assurance is incorrect and a party's reasonable dependence on that assurance resulted in economic cost, then the CA may be considered liable. In practice, few CAs are willing to take on this responsibility. Their policy statements are usually phrased to limit their exposure to liabilities. In these circumstances, CAs cannot reasonably expect their offers of assurance to be taken seriously, if they are not willing to stand by that assurance.[34]

6.36 Another key point in the security of any PKI system is the fast and effective revocation of compromised keys. However, the Committee was told that Gatekeeper does not make adequate arrangements for managing the revocation of compromised keys. This is seen by some as a critical weakness.[35]

Recommendation 9

6.37 **The Department of the Prime Minister and Cabinet should review and report to the Committee on the cost effectiveness of Gatekeeper versus other commercially available public key infrastructure products and systems.**

32 Computer Associates, *Submission No. 52*, p. 3.

33 Mr Clarke, *The Fundamental Inadequacies of Conventional Public Key Infrastructure*, 3 May 2001, http://www.anu.edu.au/people/Roger.Clarke/II/ECIS2001.html , 28 October 2003, p. 7.

34 Mr Clarke, *The Fundamental Inadequacies of Conventional Public Key Infrastructure*, pp. 8-9.

35 Mr Clarke, *Submission No. 51*, p. 4; AUUG, *Submission No. 58*, pp. 3-4.

6.38 Finally, users may be required to submit to intrusive authentication processes, which could, even then, still be circumvented by a determined impostor.[36]

Alternative Systems

6.39 There are several companies which claim that they could provide a system which would at least match the security and performance of Gatekeeper. Some systems, it is claimed, could also be supplied at lower cost.

6.40 In the end, the decision on the system to be used lies with the Chief Executive of each agency, provided that the chosen system meets the security standards suitable to its purpose. The Committee, however, considers that all agencies should weigh other options against Gatekeeper, when reviewing their security needs and to carefully assess the costs and benefits of each system before reaching a decision.

PKI Framework for the Authentication of Individuals

6.41 An extension of the use of PKIs, such as Gatekeeper, is that they can be used to authenticate the identity of members of the public, in cases when they deal with government agencies either in person or electronically. As such, PKI frameworks have the potential to make a range of transactions between agencies and members of the public easier and more secure.

6.42 Authentication processes established under a PKI would allow individuals to reliably present an identity to Commonwealth agencies. An individual user would register their identity with a RA and receive a certificate from a CA. The individual could then use this certificate with all Commonwealth agencies, since they will be able to verify the identity of the client with the CA.

Once Only Proof of Identify

6.43 Currently, however, there is no whole-of-government approach to the authentication of an individual.[37] An individual conducting business with several Commonwealth agencies must go through the process of

36 Mr Clarke, *Submission No. 51,* p. 4.

37 Management Advisory Committee, Report 2, *Australian Government Use of Information and Communication Technology: A New Governance and Investment Framework,* 2002, p. 35.

registering their identity with each one. If, for example, that client's address changes, each of the agencies that they deal with must be separately informed.

6.44 Time and effort could be saved if each individual only had to register their identity once and report any changes once. The Privacy Commissioner recognised that the collection of private information into centralised datasets would require high levels of transparency, explanation and consultation with the public if such a strategy was to stand a chance of being accepted by the public.[38]

Preventing Multiple Identities

6.45 Authentication is a useful tool for the prevention of identity abuse. In the past, there have been cases of Centrelink clients fraudulently claiming multiple benefits using multiple identities.[39] If a rigorous authentication process is put in place, it should be able to detect when a person applies to register a second identity. Biometrics may soon make this a practical possibility. The information available to the RA should then prevent anyone from fraudulently registering a second identity.

Preventing Identify Theft

6.46 Authentication can also help to prevent identity theft. This occurs when an impostor acquires enough information to impersonate another person. For example, an individual's certificate may be stolen and then used to impersonate them in dealings with Government agencies. Using PKI, the certificate issued to an individual could include identifying information, allowing Government agencies to check that the holder of the certificate is the person to whom the certificate was issued. PKI allows any certificate to be quickly revoked if it is compromised.

Authenticating Individuals

6.47 The problem remains of how an individual, as distinct from an agency or organisation, can be reliably authenticated. Current practices to establish identities call for an individual to provide a number of identifying documents ('100 points'). The problem is that some identifying documents

38 Mr Crompton, *Transcript*, 2 April 2003, p. 212.

39 Computer Associates, *Submission No. 38*, p. 5; Mr Engleman, *Transcript*, 2 April 2003, p. 144.

can be obtained without rigorous proof of identity and these could then be used to obtain the other necessary identifying documents.[40]

6.48 Furthermore, PKI assumes that the owners of private keys will be able to ensure their security. A PKI being used by an individual to transact business with agencies via their home computer will only work successfully if the private key is kept secure. Private keys stored on software will only be as secure as the computer systems which store them and there are ongoing concerns about the security of home computers.[41] Similar practical problems will arise when private keys are compromised and attempts are made to revoke certifications and warn other users not to accept bogus certificates.

6.49 The MAC of the Australian Public Service Commission has recently considered the issue of authenticating individuals. Its recommendations aim to achieve a consistent approach across Government departments. This may involve establishing primary identity documents for registering with Government agencies, supported by the establishment of a national online identity document validation framework.[42]

6.50 Gatekeeper appears to be an expensive, technically successful PKI for ensuring the privacy, integrity and security of electronic information transmitted by Commonwealth agencies, despite its low take-up by agencies generally. The take-up is likely to improve if its cost to users is reduced and as the use of the internet as a communication medium between agencies, and between agencies and their clients, expands.

6.51 Challenges will remain in reliably authenticating members of the public who use Commonwealth services.

---

40 Mr Clarke, *Human Identification in Information Systems: Management Challenges and Public Policy*, December 1994, http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html, 28 October 2003, pp. 14-17.

41 Mr Clarke, *The Fundamental Inadequacies of Conventional Public Key Infrastructure,* p. 7.

42 MAC, Report No. 2, p. 35.