Mr Bob Charles MP
Chairman
Joint Committee of Public
Accounts and Audit
Parliament House
Canberra ACT 2600

Dear Mr Charles

PUBLIC KEY INFRASTRUCTURE

The public hearings of your Committee's Inquiry into the Management and Integrity of Electronic Information in the Commonwealth on 1 April 2003 addressed a range of issues associated with the implementation of Public Key Infrastructure (PKI) in the Commonwealth. In particular, the following questions were taken on notice by NOIE officials:

1. Provision of NOIE's views on the CSIRO submission to the Inquiry
2. What level of encryption is provided by PKI and SSL respectively?
3. What scope do Government administrators or technical support providers have to decrypt messages encrypted with PKI at its current level of encryption?
4. Provision of a technical briefing on the operation of PKI including the level of encryption, the process of decrypting messages sent via that system and the authorities associated with that
5. Provision of NOIE's comments on statements in the CSIRO submission relating to FedLink
6. How much does it cost an agency to achieve Gatekeeper® accreditation?

Please find attached a series of papers prepared by this Agency, in consultation with other agencies as appropriate that address the above questions. In relation to Q4 we consider that the PKI/SSL paper and the additional information on Gatekeeper® attached to our response to Q6 provide sufficient information on the technical aspects of PKI and Gatekeeper®. I understand that, in addition to this, arrangements are in hand for the Committee to be briefed in more detail on the operation of Gatekeeper® and that members will provide an indication of the specific aspects of the program on which they require additional information.

As a general comment with respect to the wording of Q6 above, government agencies do not generally seek Gatekeeper® accreditation, rather it is the private sector certification service providers that undergo the accreditation process. As such the cost of Gatekeeper® accreditation is not met by the agency but by the service provider. The objective of NOIE's strategy in this regard is to stimulate the development of a service provider market that not only provides certification services to agencies but also to the wider business community.

You may also be interested to note that we are responding directly to CSIRO on the matters raised in their submission and at your Committee's hearings concerning Gatekeeper® and FedLink.

NOIE officials are available to meet with your Committee to discuss any of the matters raised in the attached papers should you require.

Yours sincerely

Keith Besgrove
Chief General Manager
Regulatory & Analysis
2 June 2003

Joint Committee of Public Accounts and Audit Inquiry into the Management and Integrity of Electronic Information Held by the Commonwealth

QUESTION ON NOTICE:

The Committee asked if NOIE would examine the CSIRO submission and provide its views on its comments (see Attachment 1).

ANSWER:

In 1998 when *Gatekeeper: a strategy for public key technology use in the government* was developed it was determined that the Commonwealth did not want to monopolise the digital certificate market. As a result it decided to create an open environment which supported businesses (and government agencies where necessary) could gain accreditation as either CAs or RAs to meet business and market needs.

In 2000 NOIE decided to implement a single trust point in Gatekeeper by establishing the Gatekeeper Accreditation Certificate Certification Authority (GAC CA). When established, it is intended that this authority will sign the public certificate of each CA accredited by NOIE. NOIE chose not to implement a Policy And Root Registration Authority (PARRA) as defined in the Gatekeeper strategy because of the potentially significant liability implications should it accept the traditional responsibilities of policy and registration inherent in such authorities.

The GAC acts to facilitate technical interoperability and asserts that CAs that have been issued with a GAC operate and continue to operate under Gatekeeper criteria and policies. Accredited CAs continue to self-sign their root certificate and to be responsible for approval of policies relating to their own operations.

The establishment of the GAC will have the effect of addressing the liability issues inherent in a single trust point.

It is intended that the GAC will be issued to CAs that have satisfied the requirements for full Gatekeeper accreditation. Issue of the GAC represents electronic confirmation that a CA is Gatekeeper accredited.

The GAC is nearing completion and is due for formal release in the second half of 2003. As the highest point in the Gatekeeper framework it will provide the 'trust' point for interoperability purposes both nationally and internationally.

CSIRO SUBMISSION TO JCPAA (5/03/03)

Public Key Infrastructure and Encryption

15. The present Gatekeeper guidelines for the Commonwealth government seem to suggest that the gatekeeper Public Key Infrastructure is a large mesh of trusts, instead of a more logical Commonwealth tree of trust. The gatekeeper guidelines ensure that organisations that wish to join this mesh conform to a useful and consistent standard, but it is also a prohibitively expensive exercise, with only the largest organisations able to compete. This seems to be a costly duplication exercise for the Commonwealth Government and not consistent with a whole of government approach which would facilitate the uptake of PKI services.

16. It could be more useful to see a Commonwealth Root Certificate Authority created (where the setup costs would only be incurred once), and all Commonwealth agencies become their own Registration Authorities. This would see agencies vet each person or computer system, and then, through clearly defined channels, request the certificate from the Commonwealth Root Certificate Authority. One significant outcome of this approach would be that Commonwealth employees and devices, would be clearly identifiable as such, where the present guideline does little to 'brand' Commonwealth resources.

17. National and international communications between the Commonwealth, other organisations and CSIRO’s research collaborators are complicated by the mesh of trust model. International partners will not be able to verify gatekeeper certificates without importing all of the Root certificates in the mesh first. It may be better to import one Commonwealth Root Certificate for all Australian Commonwealth resources. There are also issues with cross certification and encrypted communication with research partners where there needs to be cross certification of certificates where different standards are applied.

18. Current inter-agency encryption links are supported by the FedLink initiative. Unfortunately, because of the wide-area bandwidth requirements (currently up to 10Gb), CSIRO is not able to use these services. CSIRO has a greater need for encryption with its national and international collaborators and it can be restrictive and difficult for CSIRO’s customers to understand the need to use products endorsed on the Defence Signals Directorate Evaluated Product List.

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT
Reference: Management and integrity of electronic information in the Commonwealth
TUESDAY, 1 APRIL 2003 CANBERRA

Page 74)
CHAIRMAN—Would you mind having a look at submission No. 39 in this inquiry, on our web site, and coming back to us in writing with your view of its comments?

(Page 80)
CHAIRMAN—CSIRO were not just unhappy with Gatekeeper. They commented that they were unable to subscribe to FedLink, because of the wide area bandwidth requirements. They found it too restrictive and their customers had difficulty understanding the need to use products endorsed on the DSD evaluated products list. Do you want to comment on that?
Mr Grant—I would have to follow that up with CSIRO. I find that an interesting statement in so far as FedLink provides encryption across a public network.
CHAIRMAN—I know.
Mr Grant—It provides a very cheap level of encryption for agencies and receivers. It is not actually meant for agencies dealing with the private sector.
CHAIRMAN—That is what I thought.
Mr Grant—It is for agency-to-agency dealings across jurisdictions. So that is an interesting comment by CSIRO.
CHAIRMAN—I would appreciate your comments, because I admit I was a bit surprised. I have one last brief thing on Gatekeeper. Do you have any idea of the costs to install it?
Mr Grant—You do not install Gatekeeper per se. It is a standard, and it allows for the accreditation of registration and certification authorities. Registration authorities look at evidence of identity checks and certification authorities allow the certificates to be checked for validity. In that context, businesses and, obviously, some government agencies have sought that accreditation. My understanding is that it is in the $300,000 range, but it may be more.
Mr Besgrove—I would not like to quote a bald figure of that sort. It depends upon the scale of the implementation and on whether you are seeking accreditation as both a registration and a certification agency or as just one or the other.
CHAIRMAN—Who would have a better idea than NOIE?
Mr Besgrove—We could get that information for you—
CHAIRMAN—Thank you.

Joint Committee of Public Accounts and Audit Inquiry into the Management and Integrity of Electronic Information Held by the Commonwealth

QUESTION ON NOTICE:

What level of encryption is provided by PKI and SSL respectively?

ANSWER:

Background

This brief was requested by Senator Lundy at the Committee's public hearings held on 1 April 2003 and has been prepared in consultation with the Defence Signals Directorate (DSD).

NOIE's approach

NOIE promotes and facilitates the use of Information and Communications Technology (ICT) in government-to-business, government-to-government and business-to-business e-commerce communications. It aims to ensure technology is appropriately applied in respect to business needs. Public Key Technology (PKT) and Public Key Infrastructure (PKI) are powerful technologies which can be effectively deployed to meet a number of business needs around the confidentiality, integrity, authentication and non-repudiation of electronic communications.

Public Key Technology

PKT is based on a form of cryptography and relies on two keys - a public key and a private key. The subscriber must keep the private key secret. The public key can be made known to others and made publicly available. PKT can provide four services, these are;

- **Confidentiality**. This is achieved by encrypting a message with a subscriber's public key. The message can only be decrypted with the subscriber's private key;
- **Authentication**. The identity of a subscriber can be assured in online transactions by the subscriber 'signing' an electronic communication with their private key. This authentication is performed by the application of the public key to the digital signature;
- **Integrity**. Where a subscriber signs an electronic document a message digest or hash of the message is produced, this is essentially a number (hash value) derived from the text of the message, any other message will produce a different number. If the hash value remains the same after the message has been received then the message integrity is assured. That is, the message hasn't been altered in transit;
- **Non-repudiation**. Where an electronic message is signed with a digital signature, the fact that it was signed with a particular key cannot be repudiated or denied. In practice, this means that there will be irrefutable evidence of this, unless it can be shown that the private key was applied by other than its unique and rightful holder.

Depending on the design and application of the system, PKT can deliver some or all of these. Secure Sockets Layer (SSL) is an example of the deployment of PKT to provide web server authentication and confidentiality of communications.

Public Key Infrastructure

PKI is a system of cryptographic technologies and standards, management entities, management processes, policies and controls, to enable the widespread and open use of public key certificates.

The main components of a PKI are:

- CAs - issue and revoke digital certificates;

- Registration Authorities (RAs) – conduct the initial verification of a potential subscriber's identity and/or attributes;
- subscribers – digital certificate holders;
- relying parties –entities when relying on the contents of a digital certificate in communicating with subscribers; and
- directories – may store public keys, digital certificates or Certificate Revocation Lists (CRLs).

The main operations and processes of PKI are:

- registration – the process whereby a potential subscriber makes themselves and/or their relevant attributes known to RA;
- key generation – the generation of one or more key pairs by the CA or by the subscriber;
- certification – the issue by a CA of a digital certificate to a subscriber;
- certificate expiry – the allocation of a period for which a digital certificate will remain valid;
- certificate revocation – the revocation of a digital certificate prior to its expiry (eg where the private key has been compromised); and
- CRLs – lists of revoked digital certificates.

A digital certificate is an electronic document signed by a Certification Authority (CA) that associates a subscriber with a key pair. The certificate contains the subscriber's public key and other information including the cryptographic algorithm supported a serial number, and the distinguished name[1] of the subscriber. The certificate is issued to the subscriber.

Signing and Encryption Key Pairs

Two key pairs are used, a signing key pair and an encryption (or confidentiality) key pair. The signing key pair is used to authenticate, verify the integrity of and prevent repudiation of a message. The encryption key pair is used to provide the confidentiality function of PKI.

The keys operate as inverses:

- Only the holder of a private key can decrypt a message someone else has encrypted with the corresponding public key. The sender of a message who wants the contents to be kept confidential during transit uses the public key (which is freely available) of the recipient's encryption key pair to encrypt the message – only the recipient holds the private key so only they can decrypt and read the message; and
- Conversely, a message, which can only be decrypted using a public key, must have been encrypted using the corresponding private key. The sender of a message who wants to prove to the recipient that they are the sender and verify the integrity of the message uses the private key of their signing key pair to encode the message (or a hash of the message) – the recipient uses the sender's public key to decrypt the message and knows that it could only have been sent by the sender.

Subscribers of public-key based systems must be confident that when they use a public key (whether to decrypt a 'signed' message they receive or to encrypt a confidential message they are sending) the person they are communicating with owns and controls the associated private key.

[1] Distinguished Name is a unique identifier assigned to each Key Holder, having the structure required by the Certificate Profile and as specified in the relevant CP

Secure Sockets Layer (SSL)

The SSL protocol is a set of rules governing encrypted communication between two machines over a network which could include the Internet.

SSL was developed to secure the transmission of data over the Internet and in particular for web-based transmissions. Authentication can be verified by the use of PKI certificates which may or may not be generated by a trusted CA. The user should verify that the certificate being presented to them is correct for that machine, and a user can in some instances deny or allow the SSL connection.

The authentication process under SSL uses public key encryption and digital signatures to confirm that a server is in fact the server it claims to be. Generally it does not authenticate the user however in some circumstances it may be possible to set it up to do so. Once the server has been authenticated, the client and server use techniques of symmetric key encryption to encrypt the information they exchange. A different session key is used for each transaction. This impedes a hacker's ability to decrypt messages.

It should be noted that SSL only provides confidentiality and limited server authentication. It does not provide non-repudiation unless supported by a combination of appropriate private key protection, user willingness and ability to validate digital certificates. In addition it does not protect data before or after it has been transmitted.

SSL is a widely used technology and versions of the protocol may be suitable for use by Commonwealth agencies. SSL is a protocol, not a product, but products using SSL may be submitted for evaluation by the AISEP[2]. Agencies can contact the Information Security Group at DSD for further advice on the use of SSL in any application.

DSD recommends the following configuration for maximising SSL cryptographic security

- Only allow SSL version 3.0 sessions
- Disable reversion to SSL version 2.0
- The key exchange algorithm should be RSA with a key length of at least 1024 bits.
- The cryptographic algorithms selected for the sessions should be one or more of the following:
    - Triple-DES in CBC mode, 168-bit session key, SHA MAC
    - Triple-DES in CBC mode, 168-bit session key, MD5 MAC
    - RC4, 128-bit Key, SHA MAC
    - RC4, 128-bit Key, MD5 MAC

Additional information and guidance on use of SSL by agencies is available from the DSD website:

http://www.dsd.gov.au/infosec/publications/SSL_policy.html

Matching Technology to Applications - Authentication

As an example of NOIE's approach to the use of technology, the case of authentication is considered.

In its Online Authentication Guide for Commonwealth Managers several different technologies which can be used for authentication and how these may operate in conjunction with one another are discussed. There is no single right answer for this important question "Which authentication solution is required?" The approach adopted should be determined by the outcome of a risk assessment and subject to the preparation of an associated business case. Agencies should also consider the needs and expectations of their customers. Generally, more effective solutions are more expensive. Public key cryptography solutions have typically been adopted by agencies where strong authentication is necessary.

In assessing the level of authentication required agencies need to consider the following:

[2] AISEP stands for Australasian Information Security Evaluation Program

- Different applications will demand different levels of authentication.
- Agencies should carry out a risk assessment to determine which authentication solution will be used.
- Risk management should be part of the overall business planning process.
- Agencies should consider using the ANAO *Better Practice Guide* when choosing their authentication solution.

The table in Appendix 1 provides authentication options for online transactions. It provides examples of Information and Transaction types, Identification requirements, Authentication and Confidentiality requirements and Non-Repudiation expectations against four stages approach to delivering government services online as outlined in the Australian National Audit Office (ANAO) better practice guide, Internet Delivery Decisions (www.anao.gov.au).

Whether PKI, SSL or password based systems are deployed is a business decision for the relevant agency or organisation which should be based on an analysis of business needs and a risk assessment. Agencies should treat their authentication requirements for each transaction on a case by case basis.

The relative merits of SSL and PKI

As can be seen from the table in Appendix 1, the use of PKI for authentication is recommended for transactions involving PROTECTED or HIGHLY PROTECTED classified information while SSL is recommended for transactions involving IN-CONFIDENCE classified information. An important consideration is whether the identity of the transacting parties needs to be authenticated by an offline process. As discussed above, SSL only authenticates servers so where an application requires high assurance of the identity of parties, then the use of PKI is appropriate.

If a confidentiality application is being considered, SSL and PKI can both be used but there are advantages and disadvantages with each approach. SSL is deployed between servers and browsers. It is essentially a point to point application. SSL is ideal where a secure channel from a public facing website to the host server is required. An advantage of SSL is that it is very user friendly.

PKI, on the other hand, can be deployed to protect communications between any two parties with digital certificates. It is more flexible than SSL but also less user friendly as the users are required to manage their keys.

Algorithms and Key lengths

While the strength of cryptographic algorithms is critical for protecting against brute force attacks, there are other risks associated with the implementation of cryptographic applications. It should also be understood that both PKI and SSL may employ a number of algorithms for cryptographic functions such as key exchange, hashing and encryption. It may not be appropriate to compare the key lengths associated with different algorithms.

Cryptography is a highly technical field. DSD is responsible for the testing and approval of cryptography for Commonwealth government use. Please see Appendix 2 for details of the cryptographic algorithms and key lengths approved by DSD.

DSD is in a better position than NOIE to advise the Committee on technical matters relating to cryptography.

Appendix 1

Stage	Information Type	Transaction Types	Identification Requirements	Authentication & Confidentiality
1 This is the equivalent of a website that publishes information about the agency and its services.	**Public** This includes information that does not have any security implications and can be made freely available to the public.	Any member of the public can view agency services and publications.	Generally speaking, none required, but is dependent upon agency requirements.	Generally speaking, none required, but is dependent upon agency requirements.
2 This stage allows Internet users to browse and interact with the agency's database(s).	**Agency Official** Agency specific information whose compromise may or may not cause embarrassment to the agency.	Customers may be provided with browse or update of limited personal information privileges based upon their relationship with the agency.	Whether identification is required, or achieved online, or requires the physical presence of the customer at an agency shopfront is a decision for agencies to make.	Password and PIN/User ID (and cookies) or challenge and response or one-time password.
3 This includes stages 1 & 2 and permits users to enter information on the website, exchange or transact secure information with the agency.	**In-Confidence** Information whose compromise could cause damage to the Commonwealth, the Government, commercial entities or members of the public.	Customers may be given privileges to declare personal circumstances based upon their relationship with the agency.	Agencies may decide that the physical presence of the customer is required to confirm their identity. Evidence Of Identity (EOI) documents should be provided by the customer and verified by the agency.	Password and PIN/User ID with SSL or PKI.
4 This is the same as stage 3 but in addition the agency, with the user's prior approval, shares that user's information with other government agencies.	**In-Confidence** Same as above.	Normally associated with the repayment of debts or payment for services.	Physical presence of the customer is required to confirm their identity.	• Password and PIN/User ID with SSL or PKI; • PKI business requirements are 100 points of EOI for an ABN-DSC.
	Protected or Highly Protected Information whose compromise could cause serious damage to the Commonwealth, the Government, commercial entities or members of the public.	Passage of Protected or Highly Protected information across the Internet.	Physical presence of the customer is required to confirm their identity.	PKI (Digital Certificate) requirements are determined by the agency.

Appendix 2

Key Lengths approved by DSD for Government use for data classified as UNCLASSIFIED, IN CONFIDENCE and PROTECTED.

Agencies are required to contact DSD for advice on keylengths for data classified as CABINET-IN-CONFIDENCE, RESTRICTED and HIGHLY PROTECTED.

Symmetric Algorithms

DES with a key length of at least 56 bits using Cipher Block Chaining or Cipher Feedback mode. DSD does not approve the use of the Electronic Code Book mode.

AES with the valid key lengths of 128, 196 and 256 bits are approved.
AES is approved for securing material at HIGHLY PROTECTED and RESTRICTED.

Asymmetric Algorithms

Digital Signing Algorithm (DSA) with key length of at least 1024 bits
Rivest Shamir Adleman (RSA) with key length of at least 1024 bits.

Hashing Algorithms

Secure Hash Algorithm (SHA-1) is generally used in conjunction with DSA.
Message Digest 5 (MD5) is generally used in conjunction with RSA.

Key exchange

Diffie Helman, and RSA are approved. For SSL implementations, RSA is recommended with a key length of at least 1024 bits.

SSL

For SSL the following combinations are recommended;
Triple DES in CBC mode, 168 bit session key, SHA-1 MAC
Triple DES in CBC mode, 168 bit session key, MD5 MAC
RC4, 128 bit key, SHA-1 MAC
RC4, 128 bit key, MD5 MAC

References

Online Authentication Guide for Commonwealth Managers

http://www.noie.gov.au/publications/NOIE/online_authentication/index.htm

Gatekeeper Strategy

http://www.noie.gov.au/projects/confidence/Securing/Gatekeeperstrategy.htm

Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals

http://www.privacy.gov.au/government/guidelines/index.html#a

Joint Committee of Public Accounts and Audit Inquiry into the Management and Integrity of Electronic Information Held by the Commonwealth

QUESTION ON NOTICE:

What scope do the Government administrators or technical support providers, have to decrypt messages encrypted with PKI at its current level of encryption?

ANSWER:

It is NOIE's position that Government administrators or technical support providers should be unable to decrypt messages encrypted using Gatekeeper accredited products.

However, agencies do need to consider some important business continuity issues when deciding to implement PKI within their organisation, particularly where that information has been encrypted. An agency's ability to continue business might be severely hampered if the information cannot be accessed for some reason.

To ensure business continuity, agencies may consider the use of a key recovery service from the agency's Certification Authority, or key escrow by a third party.

Any such implementation to manage business continuity however will need to ensure that agency personnel are fully aware of the process and that a complete and reliable audit trail is maintained. The Certification Authority's key recovery service will need to be appropriately evaluated and accredited under the Gatekeeper strategy.

It should be emphasised that only the encryption key is allowed to be held in escrow so as to enable business continuity. The signing key is not allowed to be held in escrow under any circumstances.

The PSM states that if an Agency uses an encryption system that provides a 'key recovery' facility, that facility is to be set up in such a way that the keys are always available to restore the original clear text of an encrypted document.

The DSD ACSI 33 notes that with respect to Key Recovery, encryption products listed on DSD's EPL, where practical, must provide a means of key or data recovery. In particular, Handbook 9 lists criteria for Key Recovery that encryption products must meet in order to be approved for use by Commonwealth agencies.

Please refer to the NOIE's *Online Authentication Guide for Government Managers* for further information.

Joint Committee of Public Accounts and Audit Inquiry into the Management and Integrity of Electronic Information Held by the Commonwealth

QUESTION ON NOTICE:

The submission from CSIRO comments on FedLink. Would NOIE comment on this aspect of the CSIRO submission?

ANSWER:

The Committee showed interest in the uptake by agencies of FedLink. It was concerned that the uptake is low and seems to be in favour of wider implementation. Each agency was asked if they were using FedLink, if not, why not and if they are what they think of it.

In its submission CSIRO was critical of FedLink as indicated by the following extract:

18. *Current inter-agency encryption links are supported by the FedLink initiative. Unfortunately, because of the wide-area bandwidth requirements (currently up to 10Gb), CSIRO is not able to use these services. CSIRO has a greater need for encryption with its national and international collaborators and it can be restrictive and difficult for CSIRO's customers to understand the need to use products endorsed on the Defence Signals Directorate Evaluated Product List.*

The Committee asked NOIE, on notice, to respond to CSIRO's criticism.

What is FedLink?

FedLink is a Virtual Private Network (VPN) that provides secure and trusted communications across the Internet allowing secure communications between Australian Commonwealth government agencies. At this stage it is not available to organisations outside the Commonwealth, although consideration may be given to this in the future.

Agencies using FedLink can designate hosts (servers) in their environment. E-mail is the most commonly nominated server for FedLink although FedLink is not type sensitive as far as data goes. Any data sent from the nominated host to a FedLink connected recipient is automatically routed to the FedLink service and encrypted. FedLink has no restrictions in relation to the size of the data. However, agency-specific firewalls may have limitations that are not overridden by FedLink and that restrict the size of incoming information.

FedLink and Gatekeeper

FedLink is not a Gatekeeper accredited process however NOIE does mandate that the FedLink VPN makes use of the Type 3 Infrastructure Certificate issued by a Gatekeeper accredited CA.

Agencies that have signed up to FedLink

Agency	Status
Aboriginal and Torres Strait Islander Commission	In Progress
Agriculture, Forestry and Fisheries Australia	Connected
Attorney-General's Department	Connected
AUSTRAC	Connected
Australian Antarctic Division	In Progress
Australian Bureau of Statistics	Connected
Australian Competition and Consumer Commission	Connected
Australian Customs	In Progress
Australian Government Solicitor	Connected
Australian National Audit Office	Connected
Australian Nuclear Science and Technology Organisation	In Progress
Australian Prudential Regulatory Authority	Connected
Australian Public Service Commission	Connected
Australian Taxation Office	Connected
Bureau of Meteorology	In Progress
Commonwealth Director of Public Prosecutions	In Progress
ComSuper	Connected
Defence Signals Directorate	In Progress
Education Science and Training	Connected
Employment and Workplace Relations	Connected
Environment Australia	Connected
Family and Community Services	Connected
Health and Ageing	Connected
Immigration and Indigenous Affairs	In Progress
Industry, Tourism and Resources	In Progress
Office of National Assessments	Connected
Office of Parliamentary Counsel	Connected
Prime Minister and Cabinet	Connected
Social Security Review Tribunal	In Progress
Transport and Regional Services	In Progress
Treasury	In Progress
Total	**31**

FedLink and CSIRO

CSIRO staff have attended FedLink technical and business application briefings facilitated by NOIE, however, there may still be a degree of misunderstanding of the operation of the FedLink system as evidenced in the CSIRO submission.

Bandwidth issues

CSIRO's 10Gb bandwidth requirement (a connection to the Internet at the bandwidth) does not inhibit the organisation from using FedLink for secure communication to and from other Commonwealth agencies.

It is not necessary for all communication flows to enter through the FedLink router. It is possible for agencies to set up their infrastructure so that unencrypted communications do not flow through the FedLink router but are directed to another communications router.

Defence Signals Directorate Evaluated Product List

The PSM mandates that where Commonwealth information is secured by cryptography, the cryptographic measures must be approved by DSD and the cryptographic products are to be selected from the Evaluated Products List (EPL).

Joint Committee of Public Accounts and Audit Enquiry into the Management and Integrity of Electronic Information Held by the Commonwealth

QUESTION ON NOTICE:

How much does it cost an agency to achieve Gatekeeper® accreditation?

ANSWER:

It is not possible to provide the cost to an agency of achieving Gatekeeper® accreditation. There is a range of factors that affect the cost. The following explains those factors.

Gatekeeper® brings together the set of standards that underpin the level of trust expected and required in a PKI environment. The NOIE website contains all relevant information on Gatekeeper® accreditation criteria.

Agencies may use evidence of identity processes and digital certificates (or other tokens approved for the purpose of authentication) provided by Gatekeeper®-accredited enterprises, but few will seek Gatekeeper® accreditation themselves. At present, the Australian Taxation Office is a Gatekeeper®-accredited Certifying Authority that is able to issue digital certificates and the Health Insurance Commission (HIC) has a Gatekeeper®-accredited Extended Services Registration Authority.

Primary factors that affect the cost of Gatekeeper® accreditation are:

- whether an organisation is applying for accreditation as a Registration Authority (RA) or a Certification Authority (CA); and
- the extent to which costs are attributed to the specific process of obtaining Gatekeeper®, or to the infrastructure required to operate a Gatekeeper®-accredited enterprise. These latter costs can include special purpose building needs or operational methodologies, which may more appropriately be regarded as normal costs of their "business" model.

The respective accreditation requirements for CAs and RAs generally mean that the accreditation of an RA will take less time and cost less money than would be the case for a CA applicant. An RA is primarily responsible for the validation of the identity of persons or organisations applying for a digital certificate. It does not require the sophisticated computer systems or the same level of security infrastructure as a CA.

The accreditation process is, in many respects, an iterative process. It involves the applicant working with the relevant evaluators to ensure that their model complies with all relevant standards or requirements. In this context, poor quality documentation requires greater input from evaluators and more document iterations, which can result in extended time and costs to applicants. Applicants that have a good understanding of PKI generally, and Gatekeeper® requirements in particular, may be able to produce documentation that more adequately meets the requirements of the evaluators. In such cases, fewer document iterations will be required, reducing the cost to applicants.

The complexity of the applicant's proposed operations is also a factor that will impact on the time (and thus cost) of the accreditation process. While a number of normative documents that are used in the accreditation process are standards, others such as RFC2527, are more accurately regarded as guidelines; thus they allow for interpretation. As a result the time taken for the evaluation process can vary between applicants.

Finally, the number of applicants seeking accreditation at any one time also can impact on the timing of the accreditation process, with consequent effects on the cost of accreditation. This reflects the resources available to evaluating organisations.

Setting aside business costs, direct costs associated with achieving Gatekeeper® accreditation include:

- fees levied by evaluating agencies (all evaluating agencies except NOIE operate on a cost recovery basis);
- professional costs including engagement of consultants and lawyers;
- direct outlays on production of Gatekeeper® documentation required for accreditation, including operating manuals and methodologies; and

As stated above, these costs can be significantly affected by factors such as the quality of initial documentation or the extent to which an applicant understands the requirements and the process of Gatekeeper® accreditation.

NOIE has sought information from Gatekeeper® accredited service providers on the costs of obtaining accreditation and, as expected, the information provided varies significantly, depending on the factors outlined above. At the lower end of the figures provided is an estimate of around $200,000 for an RA accreditation. At the upper end of the scale is an amount of $2.2 million for full CA accreditation, although this estimate includes an amount for items that may be considered "business costs", as discussed above.

There has been commentary alleging high costs for Gatekeeper® accreditation. NOIE has no evidence that substantiates such claims. Further, NOIE considers that such estimates are likely to costs directly associated with the establishment and, or operation of the business, rather than the direct costs of accreditation.

Attached, for the Committee's information, is additional information about the Gatekeeper® strategy, its origins, purpose and operation.

ADDITIONAL INFORMATION ON THE GATEKEEPER® STRATEGY

The following information is provided about Gatekeeper® with a view to explaining its origins, purpose and position in the 'trust hierarchy'. For example it provides information about the position held by Gatekeeper® among a range of other technologies such as Secure Socket Layer (SSL) and Commonwealth programs such as the FedLink Virtual Private Network (VPN) and the Gateway certification program (managed by DSD).

ORIGINS

The Gatekeeper strategy was launched in May 1998 by the National Office for the Information Economy (Office for Government Online) with the release of *Gatekeeper - a strategy for public key technology use in the government.* The strategy was developed in response to the identified needs of agencies to introduce public key technology to support authentication and identification in Government online transactions.

The strategy ensures that this is done under a whole-of-government framework that ensures integrity, interoperability, authenticity and trust for both agencies and their customers. This is an important step in enabling the government to embrace electronic commerce.

In July 1999 it was announced that any future online digital certificates issued by Commonwealth agencies to business and individuals are to be compliant with the Gatekeeper framework.

In November 2000, all State and Territory Governments agreed to adopt the Commonwealth Government's Gatekeeper strategy, where appropriate, to support electronic transactions within their respective jurisdictions.

WHAT IS GATEKEEPER® ACCREDITATION?

Gatekeeper® accreditation is a formal recognition of the competence of an organisation to deliver certification services to Government agencies. As a result of obtaining Gatekeeper® accreditation service providers are able to demonstrate their trustworthiness. Certification services comprise both registration functions (ie conduct of evidence of identity checks) and certification functions (ie generation, issuing and ongoing support to an agency's management of digital certificates). The former is referred to as Registration Authorities (RAs) and the latter as Certifying Authorities (CAs).

The Gatekeeper® accreditation process for CAs and RAs is rigorous, addressing all aspects of the organisation's operations. This process ensures that applicants maintain compliance with appropriate Commonwealth policies and practices, including privacy and security, and also ensures interoperability between accredited organisations.

Accreditation criteria for CA's include:

- compliance with Commonwealth Government procurement policy;

- security policy and planning;
- physical security;
- technology evaluation;
- CA policy and administration;
- personnel vetting;
- legal issues; and
- privacy considerations.

The CEO, NOIE grants accreditation to organisations that successfully meet all of the Gatekeeper® accreditation requirements. Accreditation can be granted at either Entry or Full levels. Entry level involves the accreditation of the infrastructure (operational, security and legal) supporting PKI products. Full accreditation also involves certification of products and technologies (including cryptography) to the appropriate standard under the Australian Information Systems Evaluation Program (AISEP) managed by DSD. This process is in accordance with the Government requirement that where necessary Commonwealth information is protected by DSD approved products.

WHAT IS THE PURPOSE FOR HAVING AN ACCREDITATION SCHEME?

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.

Gatekeeper® is a standards based accreditation program. It is technology neutral and also provides a foundation for cross recognition of other PKI domains and certificates issued by certification service providers operating within those domains. This cross-recognition applies not only nationally (for example, the recognition of Identrus banks) but also internationally (for example, as part of broader mutual recognition or free trade agreements).

LINKAGES BETWEEN GATEKEEPER®, FEDLINK, SECURE SOCKETS LAYER (SSL) AND OTHER TYPE 3 (MACHINE TO MACHINE) IMPLEMENTATIONS

FEDLINK

FedLink is a Virtual Private Network (VPN) that provides secure and trusted communications across the Internet for Commonwealth agencies. FedLink is not a Gatekeeper® accredited process. However, NOIE requires that the FedLink VPN makes use of Type 3 Infrastructure Certificates issued by a Gatekeeper® accredited CA.

SECURE SOCKETS LAYER (SSL)

SSL is a protocol not a product. It is a set of rules governing encrypted communication between two machines over a network that could include the Internet.

Service Providers may propose to use SSL as part of their business model for Gatekeeper® accreditation as a CA. This is assessed by DSD on a case-by-case basis.

GATEWAY CERTIFICATION

While Gatekeeper® accredits service providers to deliver digital certificates at an appropriate level for government agencies, the Gateway Certification process assists Commonwealth agencies to minimise the risks incurred by connecting their systems to public networks such as the Internet. The Gateway Certification process review is conducted by DSD review and provides independent verification that appropriate risk management strategies have been employed in the gateway environment, and that identified countermeasures are in place and operating effectively.

Certification entails an independent reviewer validating that system security safeguards are operating in compliance with an organisation's security policy. This requires the certifier to examine the security objectives and risk assessment to verify the residual risk. The information provided to the certifier should be sufficient for them to report the residual risk and there should be documentary evidence that the system is implementing the identified policy objectives and countermeasures.

GATEKEEPER®

Gatekeeper® is a standards-based accreditation program that assesses an organisation's competence to deliver registration or certification services to Government agencies. An organisation may be both Gatekeeper® accredited and Gateway certified, but both processes are conducted independently of one another. In a similar manner a Government agency may have established a FedLink system for secure communications but not be Gatekeeper® accredited – the two are mutually exclusive.

HOW MANY ORGANISATIONS ARE GATEKEEPER® ACCREDITED?

To date, eight organisations have achieved full Gatekeeper® accreditation:

- SecureNet Limited - 9 October 2002 as a CA
- PricewaterhouseCoopers (beTRUSTed) - 7 March 2002 as a CA and RA (beTRUSTed is accredited to issue ABN-DSCs)
- Australia Post - 20 December 2001 as a RA
- Telstra Corporation Limited - 9 October 2001 as a CA and RA (Telstra is also accredited to issue ABN-DSCs)

- eSign Australia Limited - 5 April 2001as a CA and RA (eSign is also accredited to issue ABN-DSCs)
- Health eSignature Authority Pty Ltd - 19 January 2001 as a RA - Extended Services
- Baltimore Certificates Australia Pty Ltd (CAPL) - 20 November 2000 as a CA
- Australian Taxation Office - 16 June 2000 as a CA and RA

The following organisation is currently undergoing evaluation for Gatekeeper® accreditation as a core RA:

- ANZ Bank (applied 31 October 2001).

COMPONENTS OF GATEKEEPER® ACCREDITATION

The essence of the Gatekeeper® accreditation process is the production by the applicant of a series of documents that describe in detail the nature of the proposed Gatekeeper® operations. Some of these documents are publicly available and provide critical information for end users of the certificates (Certificate Policy (CP) and Certification Practice Statement (CPS)). Others are protected documents that detail the organisation's security practices (eg the Disaster Recovery and Business Continuity Plan (DRBCP) and the Key Management Plan (KMP)). These documents, as well as their practical implementation (eg implementation of the Protective Security Plan (PSP)) are evaluated by a number of authorised government agencies against a range of national and international standards.

PHYSICAL SECURITY

The T4 Protective Security Group within the Australian Security Intelligence Organisation (ASIO) undertakes evaluation of the physical security of an applicant's facilities. Three security classifications for Gatekeeper® operations are possible: IN-CONFIDENCE, PROTECTED and HIGHLY-PROTECTED.

For RA sites operating at the In-Confidence/Protected level, this will involve an assessment by T4 of the organisation's operations against the physical and administrative security requirements specified in Section C and D of the Government Protective Security Manual 2000, (PSM), and the physical security requirements of Chapter 6 of the Australian Communications Security Instruction No. 33 (ACSI 33), "Security Guidelines for Australian Information Technology Systems." For CA sites operating at the Highly Protected level, the assessment is also against the physical security requirements of Chapter 6 of the Australian Communications Security Instruction No. 37 (ACSI 37), "Australian Government Standards for the Protection of information Technology Systems Processing Non-National Security Information at the HIGHLY-PROTECTED Classification".

Additionally the T4 evaluation also involves an assessment of the compliance of the organisation's facilities with a range of Australian Standards and Australia Building Codes that deal with issues such as physical construction, fire egress, security hardware and alarms, and so on.

The T4 evaluation may be an iterative process depending on whether the applicant has an established facility or is proposing to construct a greenfields operation.

LOGICAL SECURITY

DSD conducts an evaluation of all the broad logical or IT security elements of the applicant's proposed operations for compliance with relevant ACSI standards and also references Australian Standards such as AS7799 "Code of Practice for Information Security Management" as part of the evaluation process. Key documents evaluated by DSD include the Protective Security Plan (PSP), Key Management Plan (KMP), and Security Policy. Internal consistency across each of these documents and a clear linkage to the Threat and Risk Analysis (TRA) is a key element of the DSD evaluation.

IT PRODUCT EVALUATION

The Australasian Information Security Evaluation Program (AISEP) was established to facilitate the evaluation of products against the internationally recognised standards, the Common Criteria (CC) and the Information Technology Security Evaluation Criteria (ITSEC). Under the program, evaluations are carried out by Australasian Information Security Evaluation Facilities (AISEFs), which are commercial companies. Only companies licensed by DSD can perform this function, and DSD certifies the results of these evaluations.

Once products have been certified they are listed on DSD's Evaluated Products List (EPL) as having undergone the process of detailed examination of their security to ensure they work correctly and effectively to provide the stated level of assurance to meet an agreed security target. The Evaluated Products List (EPL) was established to assist in the selection of products that will provide an appropriate level of information security and is updated as products are evaluated.

COMMON CRITERIA

Australia is a signatory to the Common Criteria Recognition Arrangement (CCRA) and has a Memorandum of Understanding with the United Kingdom (U.K.) that allows mutual recognition of products evaluated under the CC and ITSEC. Under current program rules, Mutual Recognition does not incur a cost if there is a sponsorship letter from an Australian government agency. If there is no sponsorship letter, then there is a fee charged in accordance with the level of assurance sought. The cost of having products evaluated through the AISEP is significant and varies depending on the level of assurance sought. However, this is comparable with costs incurred overseas and represents a one-off cost. That is, a product only has to undergo evaluation once in order to be placed on the DSD Evaluated Products List (EPL).

ENDORSED SUPPLIER ARRANGEMENT (ESA)

The ESA application process is based on information supplied by businesses accompanied by a signed Declaration certifying to its accuracy. The process undertaken by the Department of Finance and Administration assesses the information included in the application and to be granted Endorsed Supplier status businesses must satisfy all criteria.

An Endorsed Supplier maintains currency of information about its business directly on the ESA Searchable web site. Information that is able to be edited is limited and when changes are made, accepted in good faith. All Endorsed Suppliers are subject to periodic review to ensure validity of information and their continued compliance against the criteria.

Criteria that are considered at the time of assessment include:

- Financial viability;
- Favourable referee reports (a successful track record to deliver);
- Product and service compliance with the agreed industry standards;
- Compliance with certain Commonwealth Government policies;
- Agreement and adherence to the Endorsement rules;
- An appropriately signed Head Agreement (for suppliers of IT and Major Office Machines only); and
- Industry development (for suppliers of IT and Major Office Machines only).

PERSONNEL VETTING

All CA staff are required to be cleared to the HIGHLY-PROTECTED classification before accreditation can be granted. This includes all staff with access to CA secure areas and back-up personnel. These positions are determined as Positions of Trust, and should be kept to a minimum.

The Australian Security Vetting Service (ASVS) and the Australian Protective Services (APS) are tasked to undertake vetting of non-Commonwealth people employed in the private sector, who, either as individual contractors or employees of a company which has secured a contract with a Commonwealth agency, require access to sensitive national security or non-national security matter as a result of those contractual obligations.

Currently, the ASVS/APS cannot undertake vetting of private sector personnel without Commonwealth sponsorship. CAs wishing to clear their personnel should provide names and contact details of personnel to NOIE for sponsorship and processing of their application.

Applicants seeking accreditation as a Core RA are only required to have personnel cleared to the IN-CONFIDENCE classification. This can be undertaken by the organisation itself without the need ASVS/APS involvement but must include the following:

- Police background check
- Awareness session with each employee

- Signed non-disclosure between the organisation and each employee
- Development and implementation of appropriate training courses for each employee

LEGAL EVALUATION

The Australian Government Solicitor (AGS) evaluates the following documents submitted by Organisations:

Certificate Policy (CP)

A CP is "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements". A CP is also the place where the position on a range of legal issues is set out including in relation to obligations/responsibilities of the participants in the trust hierarchy, liability as between the participants, financial arrangements, confidentiality, intellectual property and privacy

Certification Practice Statement (CPS)

A CPS is a statement of the practices, which a CA employs in issuing certificates and includes both legal and technical issues. A CA with a single CPS may support multiple certificate policies (used for different application purposes and/or different certificate user communities). It is possible that different CA's with non-identical CPS's may support the same certificate policy.

Subscriber/Relying Party Agreements

Subscriber and Relying Party Agreements basically contain a summarised version of the terms and conditions set out in the CPS and relevant CP.

The fundamental reason for evaluating these documents is to ensure that they adequately describe an effective chain of trust, and can be read and understood by those who need to read and understand them. In the evaluation of these documents the following issues are addressed:

(a) the CPs and the CPS addresses all the issues that, pursuant to RFC 2527, should be addressed;

(b) the operational practices described in the documents are workable and can be understood by those who need to understand them. In particular, the Authorised Legal Evaluator should address issues which will be of specific concern to Agencies and Subscribers (eg CA termination);

(c) the documents make adequate provision for the protection of Personal Information - to the standard required of agencies under the *Privacy Act 1988* (Cth);

(d) other specific Commonwealth legal requirements are clearly reflected in the documents (eg retention of records under the *Archives Act 1983* (Cth));

(e) the documents are free from other legal defects (eg ensuring that they do not state presumptions about the legal effect of using Keys and Certificates which are inconsistent with the *Electronic Transactions Act 1988* (Cth)); and

(f) the documents, which need to be read and understood by the entities in a PKI, but in particular the Subscriber, are;
- consistent within and between themselves;
- sufficiently informative, clear, coherent, and unambiguous.

OPERATIONAL EVALUATION

There are two key documents that establish the operational or business model for a Gatekeeper® service provider:

- The Concept of Operations (ConOps); and
- The Operations Manual.

NOIE is the primary evaluator of these two documents although both DSD and AGS will consider elements of the documents that impact on or relate to their evaluation of other aspects of the applicant's operations. This is to ensure that the suite of documents that define the organisations Gatekeeper® operations are internally consistent.

A central document in the Gatekeeper® accreditation process is the ConOps. It is the first document lodged by any Applicant and is effectively an overarching document that encompasses all aspects of the Applicant's operations as a CA and/or RA. It not only provides guidance for the development of other key documents by the CA/RA required by Gatekeeper® but is also regarded as a "living document" insofar as it can change over the course of the accreditation process as amendments are made to other documents. The CONOPS is not finalised until immediately prior to the execution of the Head Agreement.

As the Applicant moves through the evaluation process the interaction with Evaluators may identify issues with respect to the implementation of their business model. As a result it may become apparent that changes need to be made to the business model and hence the ConOps will require amendment to ensure that it continues to be a viable and workable proposition and that consistency between the documents is maintained.

The security documents provide essential input into the development of the CA/RA Operations Manual. This document describes how the organisation will be operated and managed on a day to day basis including a description of the functions and responsibilities of personnel within the organisation.

SIGNING OF HEAD AGREEMENT WITH THE COMMONWEALTH

The Head Agreement is based on a template agreement developed by the Australian Government Solicitor (AGS) and NOIE and links the Gatekeeper® criteria to a legal framework. The Head Agreement is not an evaluated document but is negotiated between NOIE and the Applicant. The Head Agreement is a critical document in that it provides a legal framework within which the CA/RA can operate its business and also provides the

Commonwealth with mechanisms to ensure the on-going compliance of the Service Provider with the Gatekeeper® accreditation criteria.

CROSS RECOGNITION

Cross-recognition amounts to a formal and reciprocal recognition by the competent PKI authorities (top trust point) in one *recognising* PKI domain of the authority and capacity of the competent PKI authorities in another *recognised* PKI domain, to impose, manage and enforce PKI standards and trust processes appropriate for confident acceptance of those certificates in the recognising domain.

In practice, cross-recognition means that certificates issued in a *recognised* domain may be relied upon with some confidence by relying parties in the *recognising* domain.

A community of interest is thereby able to rely upon certificates issued from an external PKI for use in certain applications, within the limits of the accredited certificate policy for those certificates. As stated, however, the recognising domain would not be *guaranteeing* the status and reliability of foreign certificates.

Cross-recognition (as distinct from cross-certification) does not entail technical interoperability or serve as a guarantee by recognising authorities that a foreign certificate will have the same status and reliability as a non-foreign certificate. Relying parties (RPs) should be provided with information sufficient for them to make an informed assessment about the certificate's reliability and fitness for purpose; in particular, whether the certificate:

- has been issued from a recognised, trusted PKI domain, and is still valid; and
- is of a type and purpose (apparent from the Certificate Policy for the certificate issued by the CA) appropriate for the application facing the RP.

Cross-recognition will not become an alternative to Gatekeeper® accreditation, and therefore will not provide a short-cut for providing PKI services to government.