COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

Reference: Management and integrity of electronic information in the Commonwealth

THURSDAY, 19 JUNE 2003

CANBERRA

BY AUTHORITY OF THE PARLIAMENT

INTERNET

The Proof and Official Hansard transcripts of Senate committee hearings, some House of Representatives committee hearings and some joint committee hearings are available on the Internet. Some House of Representatives committees and some joint committees make available only Official Hansard transcripts.

The Internet address is: **http://www.aph.gov.au/hansard**

To search the parliamentary database, go to: **http://search.aph.gov.au**

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

Thursday, 19 June 2003

Members: Mr Charles *(Chairman)*, Ms Plibersek *(Vice-Chair)*, Senators Conroy, Humphries, Lundy, Murray, Scullion and Watson and Mr Ciobo, Mr Cobb, Mr Georgiou, Ms Grierson, Mr Griffin, Ms Catherine King, Mr Peter King and Mr Somlyay

Senators and members in attendance: Senator Lundy, Mr Charles, Mr Cobb and Ms Plibersek

Terms of reference for the inquiry:

To inquire into and report on:

The potential risks concerning the management and integrity of the Commonwealth's electronic information.

The Commonwealth collects, processes and stores a large amount of private and confidential data about Australians. This information is held by various Commonwealth agencies and private bodies acting on behalf of the Commonwealth. For example, the Australian Taxation Office keeps taxpayer records, the Australian Electoral Commission keeps electoral roll information and Centrelink keeps social security, family and health information. The Committee is concerned that the Commonwealth's electronic information is kept securely and in a manner that ensures its accuracy.

In conducting its inquiry the Committee will consider:

- the privacy, confidentiality and integrity of the Commonwealth's electronic data;
- the management and security of electronic information transmitted by Commonwealth agencies;
- the management and security of the Commonwealth's electronic information stored on centralised computer architecture and in distributed networks; and
- the adequacy of the current legislative and guidance framework.

WITNESSES

Committee met at 9.11 a.m.

BAMBURY, Mr Paul, Assistant Manager, Government Authentication, National Office for the Information Economy

BESGROVE, Mr Keith, Chief General Manager, Regulatory and Analysis Group, National Office for the Information Economy

ELSLEY, Ms Christine, Manager (Acting), Gatekeeper, National Office for the Information Economy

GRANT, Mr John, Chief General Manager, Government Services and Information Environment, National Office for the Information Economy

BLACK, Mr Allan Louis, Manager, Government IT Security, Defence Signals Directorate

MATTOCKS, Mr Glen, Manager, Whole of Government Projects, Defence Signals Directorate

CHAIRMAN—This is not a public hearing, it is a private hearing, but Hansard will record it for our secretariat's purposes.

Mr Besgrove—Yes, we understand that.

CHAIRMAN—We are here to learn from you what Gatekeeper is all about.

Mr Besgrove—Thank you very much, Chairman. The committee will recall that we appeared before the committee on 1 April. At that time I gave an explanation of NOIE's role and the sorts of things that we are responsible for. I do not propose to go through that again unless you particularly want me to.

CHAIRMAN—No, that is fine.

Mr Besgrove—We have also responded to a range of questions on notice from the committee on issues such as the cost of Gatekeeper accreditation; FedLink; decryption of messages encrypted with PKI; NOIE's views on the CSIRO's submission and questions related to other submissions, including Microsoft's; and the merits of PKI versus SSL, or secure socket layer, technology. So we have responded to a number of specific questions.

Our purpose in wanting to brief you in more detail about Gatekeeper I think comes from several areas. Firstly, it is clear from some of the submissions you have received that you are getting a particular view of Gatekeeper which we think may not be altogether accurate. Secondly, we think that it is clear from some of the questions that there is a degree of confusion in the marketplace about what Gatekeeper is and what it is not. So our purpose today is to try to put the facts in front of you as we see them.

The way that we would like to do that, if you are agreeable, is to go through a short presentation on Gatekeeper itself and then have a presentation which focuses specifically on the

technology and which should be able to pick up some of the questions that the committee has been asking in relation to the technology, and then we will throw it open to questions if you are comfortable with that approach.

CHAIRMAN—We are happy with that.

Mr Besgrove—I have overall responsibility for Gatekeeper accreditation and for private sector authentication issues. Mr Grant has a specific focus on government sector issues, including authentication within the government. Christine Elsley has direct responsibility for the accreditation process. Ms Elsley will begin by doing a presentation about Gatekeeper, what it is and what processes we go through, and then Mr Mattocks will give you a presentation in relation to the technology. So I will hand over to Ms Elsley.

A PowerPoint presentation was then given—

Ms Elsley—Gatekeeper evolved from the Investing for Growth statement in 1997. It was launched in May 1998 with the Gatekeeper strategy. Its full title was 'Gatekeeper: A Strategy for Public Key Technology Use in the Government'. This strategy is basically a whole-of-government framework for use of PKI in the Commonwealth. It was designed to provide a panel of service providers that were accredited to a certain level. Agencies needed to know they could trust that the services provided by certain organisations were at a level that they needed.

Why did this happen? The Internet came along. It is an open system. There was a perceived lack of trust in the Internet by users, so Gatekeeper was developed. In 1999 it was announced that any future online digital certificates issued by Commonwealth agencies would be compliant with the Gatekeeper framework. So that is where it came from. It came from the Internet developing and being implemented and starting to be used by Commonwealth agencies, and then a need was perceived by OGIT at the time that service providers had to provide services of a certain level.

Mr Besgrove—Sorry, you might explain what OGIT was.

Ms Elsley—OGIT was the Office of Government Information Technology.

Mr Besgrove—It was a predecessor organisation to one of the parts of NOIE.

Ms Elsley—So Gatekeeper is a standards based accreditation program which is totally technology neutral. It is not a product; it is a framework, and it is solely a framework. Service providers come to NOIE for accreditation under Gatekeeper. They have to go through certain hoops and processes to gain that accreditation. I have put in your pack a list of standards that Gatekeeper has as a base, and you will see that it is quite long and quite comprehensive.

Turning to the next slide, in the Gatekeeper framework a couple of types of organisations can come in for accreditation. One is a certification authority, which basically generates and issues the certificates. The other is a registration authority, which gets given application forms together with any evidence of identity documentation, basically checks that the documentation is eligible as per the Financial Transactions Reports Act and then passes that application to the CA for the certificates to be issued to applicants.

Mr Grant—Just to make that very clear, the registration authority is the proof of identity authority, so it provides that underlying level of trust that you are whom you say you are.

Ms Elsley—The registration authority is actually one of the most important parts of the whole process because it is based on trust and if you cannot trust the identity of the person who is applying for a digital certificate everything else falls down as a result. Within Gatekeeper there are a number of different digital certificate types, and within each type of certificate there are different grades. There are three grades within type 1 and type 2 certificates. They apply to basically a different point structure. There is a 50-point certificate, a 100-point certificate and a 150-point certificate, the identity requirements being much tighter as you go up the chain. The type 1 is issued to an individual. The type 2 is issued to an organisation but it will have an individual identified within the certificate. I will come back to the ABN-DSC, but the type 3 is issued to a device like a router, a web application or a browser. It is an inanimate object; it is not a human being.

The ABN-DSC is a variation of a type 2, grade 2 certificate. The business process sitting behind the ABN-DSC is different to a type 1, grade 2 certificate. The other difference is that the Australian Business Number, the ABN, is also within the certificate as well, so you get like a dual identity for an organisation. The name of the organisation is there and the ABN as well. That does not happen in an ordinary type 2 certificate.

Senator LUNDY—Why not?

Ms Elsley—It can. There is no reason why you cannot put an ABN in a normal type 2, grade 2 certificate, but it is not a requirement for the type 2.

Mr Grant—The ABN-DSC, which is your Australian Business Number-Digital Signature Certificate, was established as a certificate for dealing with government. The objective of the ABN-DSC was that with one certificate you could deal with federal, state and local government without having to have a different certificate for each. The ABN was simply used because it is a simple identity number for a company.

Senator LUNDY—To me, it makes perfect sense to remove that distinction, either to include the ABN-DSC in the type 2, grade 2 or—do you know what I mean?

Mr Grant—I understand what you are saying. There are instances where you might not use an ABN. A simple example— and I am not sure whether this is correct—might be in the health area. When doctors write prescriptions or claim, it is a provider number, not their company number, that actually comes into being. Consequently, the type 2 certificate allows for the relevant nature of the transaction to be taken into account, where within the Commonwealth with the ABN-DSC we have said any company dealing with the Commonwealth will use this particular format.

Senator LUNDY—We have had lots of discussions in the committee about unique identifiers and their role. Anyway, I will come back to it.

Ms Elsley—The other thing is that some organisations are not issued with ABNs—for example, charities—so there has to be some way of allowing those organisations to get a certificate as well. So they are the types of certificates.

Mr Besgrove—I think you should move on to GAC.

Ms Elsley—I think I should. The last dot point on that slide is the Gatekeeper accreditation certificate, which is a digital certificate. When service providers go through the entire accreditation process they are actually presented with an accreditation certificate. At the moment that is a paper certificate that they hang on their walls. We are putting in place a digital certificate that will assist with interoperability, in that different CAs will be able to identify those CAs that have been accredited by Gatekeeper.

Mr Grant—So it provides an electronic mechanism of testing that you have a CA dealing with a CA, both of whom are accredited.

Ms Elsley—Yes. When they come in for Gatekeeper accreditation it is not just the issuance of certificates that we look at; it is their whole business operations. We look at physical security—that is, the building that they house their certification authority or their registration authority in—and there are different standards for a registration authority and a certification authority. ASIO T4 do that on our behalf at present.

There is the logical security, which DSD do. That is quite an in-depth evaluation of their IT security. A component of the logical security is also the IT product evaluation, which is done under AISEP. I will not go into any details here other than to say that it can be a long process to obtain that.

The operational evaluation is NOIE's responsibility. It basically looks at their operations manuals and their disaster recovery and business continuity plans that are in place. The legal evaluation is a very important component, because there are some documents available to end entities such as subscribers or relying parties. The people who either get issued with the certificates or rely on those certificates have to decide whether or not to trust them. A certification practice statement is developed which covers the operations and the infrastructure of the CA and the certificates that are issued within it. Then certificate policies are developed for each certificate type that the certification authority issues and generates.

Within the CA, because there is a requirement that a CA be evaluated to the highly protected level, their staff have to be vetted to the highly protected level. The two organisations that do that at present are ASVS, the Australian Security Vetting Service, and APS, the Australian Protective Service. We sponsor the vetting for the organisations that require it.

There is also a requirement under Gatekeeper that all service providers be on the endorsed supplier list, so they have to apply to get onto that. Once they have done all those six points to the satisfaction of the competent authority, which happens to be the CEO of NOIE, they sign a contract with NOIE on behalf of the Commonwealth, which is a fairly comprehensive contract setting out the obligations that they have to fulfil or continue to fulfil. Every 12 months they have to undergo a compliance audit to ensure that they are still meeting the Gatekeeper criteria and policies.

CHAIRMAN—Who does that?

Ms Elsley—We have set up a panel of auditors. There are six on the panel. Examples of them are Ernst and Young, PricewaterhouseCoopers and KPMG. There are a couple of smaller ones as well: Stratsec.net and an organisation called MGI Wamstekers. So they all will be going through audit soon.

Mr Grant—You will see that it is actually a very comprehensive approach where we look at physical process and individual operations and approaches, and the objective here again is to retain the trust framework and the integrity of that framework because they provide services to a range of businesses and individuals.

Ms Elsley—Eight organisations are accredited under Gatekeeper. We accredit organisations, not the products that they sell. As I said, because of that comprehensive nature of the accreditation process, it is the entire organisation. So we have Baltimore Certificates Australia, whose business and operations have been taken over by SecureNet Ltd, who obtained accreditation as a CA, a certification authority, towards the end of last year; and Verisign Australia, which used to be eSign Australia—they changed their name to Verisign at the beginning of last year.

The Australian Taxation Office were the first CA and RA to be accredited under Gatekeeper. Australia Post are a registration authority only, and certification authorities are negotiating service contracts with Australia Post for them to undertake the registration process on their behalf. Telstra are a certification authority and registration authority, but they still use Australia Post as well. PricewaterhouseCoopers, through beTRUSTed, are also a CA. The Health eSignature Authority are a company 100 per cent owned by the Health Insurance Commission, and they are an extended services registration authority. An extended services registration authority is a registration authority which takes on some of the roles of a certification authority. In the case of HeSA, they actually generate and download certificates that are issued through their CA, which is SecureNet.

Mr Besgrove—I think it is fair to say that this slide is probably the heart of what we are trying to present to the committee. There is a great deal of confusion in the marketplace about what Gatekeeper is. People talk about Gatekeeper as if it were a product. It is not. It is an accreditation system—and that is not well understood—that enables these service providers to provide a range of products in an accredited framework. That is really the heart of it. While the committee may well understand that, I just wanted to reinforce that that is what Gatekeeper is, and when people compare Gatekeeper to particular products in the marketplace they are simply comparing apples and oranges. I just wanted to make sure that that was very well understood.

Ms Elsley—It is very easy for that confusion to occur when you have so many like terms out there in the marketplace—you have ‘Gateway’, you have ‘Gatekeeper’—and it is easy to mix them up, I think.

CHAIRMAN—Does each of the certified authorities have products?

Ms Elsley—They have specific hardware and software which they do not sell. They sell keys and certificates to—

CHAIRMAN—You have lost me.

Mr Mattocks—The accreditation process looks at accrediting the bodies to provide a service. The service is basically trust, but a token or a digital certificate is issued by them. So they do deliver a product in the sense of an electronic piece of information. Usually it is housed on a token of some sort like a smart card, but generally they are providing a service really.

Ms Elsley—It is more a service than a product.

Mr Grant—Senator, if I can put it in context—

CHAIRMAN—I am not a senator.

Mr Grant—I apologise, Chairman.

Ms PLIBERSEK—Now you will have to apologise to Senator Lundy for apologising to the Chairman for being a senator!

Mr Grant—I am used to Senate estimates; I was not thinking. Putting it into context, there is a series of products that in fact businesses or even agencies may use if they want to ensure the identity of the person or the organisation they are dealing with, but those products are used primarily for either communities of interest or one-to-one type operations. What we are talking about here with Gatekeeper is a public key. In essence, that means that if you go through the process of going to a registration authority and identifying yourself as Mr Childs—and we will assume you are working for the Commonwealth, which actually has an ABN-DSC for each agency—and you get an ABN-DSC then you should be able to deal within your delegation with any agency within the Commonwealth without fear that that transaction is illegal and without fear that the person performing that transaction is not in fact you.

So the difference that you have between what some of the companies have been presenting to you and what we have is this is a public key, so it is for multiple transactions between people who often do not know each in a much wider environment. The sorts of systems that have been put forward to you in some cases are community of interest transaction security or one-to-one transaction security. A simple example might be Ford many years ago had F1—I think it is up to about F4—which is their quality program. That is the community of interest because their suppliers are required to meet a certain quality standard. That quality standard meant nothing if their suppliers were providing parts to another car manufacturer because another car manufacturer might want a different quality standard.

Gatekeeper provides the standard for public key authentication or public authentication, and that is really the key difference here. Gatekeeper is not a product. Those accredited to Gatekeeper provide services which say, 'Here is my key. I am John Grant, and when you are dealing with me you know that you are dealing with John Grant.'

Senator LUNDY—We have been getting some feedback on Gatekeeper, and I think part of the problem has been that companies do not believe Gatekeeper is necessary because the market will determine what types of encryption products/security products to allow that sort of communication and they, as a market of products competing, do not want to be overly managed

by what they see as a high-level intervention by a government regulatory authority, which is what Gatekeeper is. Can you give us an insight into the public policy issues about the necessity for high-level regulatory intervention to manage the array of encryption products out there that subsequently sit within Gatekeeper?

Mr Grant—I might commence and then Keith Besgrove might come in after. First of all, Gatekeeper primarily focuses on PKI. The reason that it was established, as Christine Elsley said, is that there was a perceived market failure. There was no PKI standard—'public' being the key term here—so the Gatekeeper standard was created. The fact is that not only is authentication at PKI level. It can be, 'Can you identify yourself?' 'Show me a mirror,' through to PIN and password or perhaps biometrics. In the end with authentication you are trying to demonstrate confidence that you are dealing with whom you think and I am dealing with whom I think.

CHAIRMAN—I want to make sure I get this right. Private industry does not generally do it except in the defence field, but is it like obtaining a security clearance?

Mr Grant—It is not a security clearance per se.

Senator LUNDY—I think you are right.

Mr Besgrove—That is not a bad analogy. Having achieved that, you can then be trusted by others who do not know you.

Senator LUNDY—It is a digital version of your getting a bit of paper saying, 'I am Bob Charles,' and every time you communicate with a wide community, along with that communication, you send them part of that certificate so they can verify it is you by the information that you have.

CHAIRMAN—They will let you through the gate?

Mr Grant—That is it.

Mr Besgrove—Yes.

Mr Grant—The reason I baulked at 'security' is that this is about whom you are, not some of the other things that go with security.

Senator LUNDY—But there is a security layer, because it means that the communication and how that verification bit occurs is really locked up in some quite hefty technical security whizzbangery, which we will see in a minute, I hope.

Mr Besgrove—Yes, you will.

Mr Grant—Gatekeeper PKI provides that surety that in a transaction the transaction will be fulfilled. Non-repudiation liabilities are attached. At lower levels of authentication that may not be the case, but ultimately what you look at is the nature of the transaction and the nature of the

relationship, and the two transactors then have to determine what level of authentication they think is appropriate.

CHAIRMAN—Optus are highly critical of the time required and the expense involved in obtaining Gatekeeper accreditation. Of what advantage would it be to Optus?

Senator LUNDY—They could compete with Telstra.

Mr Grant—And with the others. The question is: what is their business driver for wanting to get accreditation at Gatekeeper level?

Senator LUNDY—The issue that Optus raise, and it is one that the committee is very interested in, is the competitive barriers that this high level of regulation presents. We had quite a lengthy discussion about the sort of more IT logistics accreditation process that affects them directly, but they and also others raised concerns about effectively the competitive barrier that the complexity of Gatekeeper accreditation presents.

Mr Besgrove—Perhaps I could respond to this in a slightly different fashion. When Gatekeeper was first developed by NOIE and by its predecessor organisation, OGO, there was no market in Australia. This was done in anticipation of public key infrastructure being a very important part of an authentication market in a growing market for e-commerce—public to public, private to private and public to private. So it was done in anticipation, and the public policy case was very much one of government wanting to put in place the building blocks for an effective market. Australia took this particular approach; other countries took somewhat different approaches. For example, in the United States they do not have an accreditation approach. However, they do believe that having a legitimacy to PKI for federal government transactions is important, so they have what they call their Federal Bridge system, which does a very searching audit of different private sector PKI systems and establishes how credible they are.

Senator LUNDY—It is a rating system.

Mr Besgrove—It is a rating system. That is a different approach—

Senator LUNDY—But it is less interventionist and allows all of those products to compete.

Mr Besgrove—Yes; I was going to come to that. The US took a particular model; Australia took another model. Rightly or wrongly you might say that one is superior to the other. Once you have invested a lot of time and energy in one particular route it is not easy to change streams, because they are very different. In a sense what we have with Gatekeeper is a decision four or five years ago to go down an accreditation route as opposed to a cross-recognition bridge type route. Both may be perfectly legitimate responses to the public policy need to have a level of surety at the highest levels.

The other compelling argument for government being involved in this area is that it recognised that levels of authentication would be required. PKI is concerned with only the highest levels, and there is no compulsion on anybody to use Gatekeeper. That is the other key message that we wanted to reinforce today: no Commonwealth agency is forced to use

Gatekeeper at all. Centrelink has chosen not to use it. As far as NOIE is concerned, that is fine because that is a business based decision they have made.

Mr Grant—I might just clarify that. You are not required to use PKI; if you use PKI you are required to use Gatekeeper.

Mr Besgrove—Sorry, I should have expressed it that way.

Ms PLIBERSEK—Sorry, I did not hear what you said.

Mr Grant—You are not required to use PKI level of authentication, but if you do use PKI level of authentication you are required to use Gatekeeper.

CHAIR—Remind me what Centrelink does.

Mr Grant—Centrelink is the human services—

CHAIRMAN—No, no—good grief!

Mr Besgrove—It provides welfare payments.

Mr Grant—It provides welfare payments—

CHAIRMAN—I know that.

Mr Grant—And obviously it has to identify the people to whom it is providing those payments.

CHAIRMAN—No, what—

Mr Grant—What level they are using?

Mr Besgrove—PIN and password and SSL, I think, but mostly PIN and password.

CHAIRMAN—I do not know what 'SSL' means.

Mr Besgrove—Secure socket layer. We will come to that in a moment.

CHAIRMAN—I know what Centrelink does!

Mr Besgrove—I apologise.

Senator LUNDY—Perhaps I could help by saying that the point is that some agencies and departments do not believe that PKI level authentication is necessary; hence what we have seen across the table is an argument develop that this is effectively an over-the-top system and unnecessary for widespread use in the Commonwealth. Many have said that.

Mr Grant—I might add the Federal Bridge is also for dealing within the federal American government, and that was the origin of Gatekeeper: for dealing with the federal government—and, by the way, state and territory governments.

CHAIRMAN—Maybe I am wrong, but haven't we moved further in a public sense—that is, the Commonwealth, and the states too, I think—in putting all government services online compared to other Western countries?

Mr Besgrove—I think we got there a lot earlier than many, but the rest are catching up very quickly.

Mr Grant—I think the answer is we do have a lot of services online. In fact, I have just been over to the US and Canada and had a look at what they have. We are in fact putting very similar services online, particularly in the business sense. So perhaps we have a minor lead; perhaps we are about the same. We focused on different areas. We are learning, though, that the nature of the requirement for PKI is much the same. It is where liability occurs if you get it wrong. For example, an engineer lodging a plan must sign but it does not matter whether it is an electronic or a written signature; it still has the same liability outcome.

CHAIRMAN—Just to be sure that my own trained mind in this area understands, Australia uses a certification system and the Americans certify products?

Mr Grant—No. In fact, the Federal Bridge recognises companies like these. It has a look at the same sorts of things that we do in terms of their physical, methodology and people security, and in essence the Federal Bridge provides a licence—it actually calls it a public key or a certificate—provides a certificate, to companies like this to issue certificates. So we have a very similar approach. The difference is, as I understand it, they do not perform the same level of scrutiny. That is in fact done more by accredited technical experts rather than by DSD, NOIE or whomever else.

CHAIRMAN—When you addressed this issue before I understood that there were completely different approaches. Now you are saying they are almost exactly the same.

Mr Besgrove—No; sorry.

CHAIRMAN—I am confused.

Mr Besgrove—They are different insofar as the Gatekeeper approach takes applicants who want Gatekeeper accreditation and puts them through a very rigorous and structured accreditation process in looking at all of those physical, people and so on security aspects mentioned in the previous slide. The Federal Bridge takes an existing PKI private sector provider and assesses it against a check list. If it does not match against the check list, it gets a fail or a pass and that is all. So it is up to that provider whether it then goes away and changes that, but the Federal Bridge does not care. It simply comes up with an assessment which says, 'We have looked at you, and against our four different levels of trust that we vet everybody against you are a 2'—or a 1 or a 3 or a 4—'and that is what we are going to tell everybody,' and it will be able to operate in a federal government market at level 2 but not at level 3. So it is putting the onus back on the private sector provider to do all the work and sort out everything it

needs if it wants to come up a level. So it is less directly interventionist, but in terms of pass/fail judgments it is not dissimilar. That is really what I think Mr Grant is trying to say.

CHAIRMAN—At the end of the day, both systems come up with a bit of paper or an electronic image that says you are okay?

Mr Grant—Yes.

Mr Besgrove—Yes, at different levels.

CHAIRMAN—Is that correct?

Mr Besgrove—Yes, that is correct, but they do it in different fashions.

CHAIRMAN—Who is more expensive?

Mr Besgrove—I am afraid I cannot answer that because we do not know the costs of the US system.

CHAIRMAN—We asked Microsoft that. They are coming back to us.

Mr Besgrove—Sorry, can I just qualify that?

CHAIRMAN—Who takes the longest?

Mr Besgrove—I do not know the answer to that either. However, if I could just add one qualification—

CHAIRMAN—We asked Microsoft that too.

Mr Besgrove—When you ask that question you need to actually ask the question: what is the cost of the totality of what they are doing to be a service provider in that market? It may well be that the US government part of it is maybe five per cent and we might be 20 per cent, I do not know, but if you look at the total cost of actually being able to operate in the market my suspicion is that they would not be wildly different.

Mr Grant—The issue is the cost of certification versus the business costs of being able to supply that service.

CHAIRMAN—Optus reckon that you are so expensive that they cannot apply.

Mr Besgrove—Sure. Can I focus on Christine's previous slide for a moment. Any private sector PKI provider will have to do that collection of things to be a private sector provider of PKI in the United States. They will have to do those things.

CHAIRMAN—Thank you.

Mr Besgrove—And we will have to do them here as well.

CHAIRMAN—It seems to me that, in relation to the differences between the two, what you are talking about more is annoyance rather than anything in substance.

Mr Besgrove—On Ms Elsley's last slide we are going to talk a bit about where we would like to take Gatekeeper. We think we can improve the system, and we wanted to share that with you as well, because we think it takes too long.

CHAIRMAN—I think some of your potential clients—

Mr Besgrove—They think so, too, yes.

CHAIRMAN—I know they think so.

Mr Besgrove—So let us move on to the next one.

CHAIRMAN—They told all of us.

Ms Elsley—I have spoken about accreditation, and that is the major part of the Gatekeeper framework. However, a little while ago—I cannot remember the date—NOIE also developed a cross-recognition policy, which is to cross-recognise other PKI domains rather than individual entities within that domain. So where accreditation accredits an organisation, like Verisign or Telstra, cross-recognition looks at a PKI domain like Identrus, the US, Europe, Singapore or Japan and assesses those domains on a kind of a system or using a process of policy harmonisation. It looks at the similarities between the two systems, between Gatekeeper and the system in the other PKI domain, maps the two and then looks at the differences. For those things that do not meet the level of Gatekeeper, it then asks the other domain to do a risk analysis and put in some mitigation strategies to alleviate the concerns under NOIE.

Mr Besgrove—Chairman, in the interests of time we might move through this.

CHAIRMAN—I was just going to say I do not know how long the others have.

Senator LUNDY—I have to go at 10 past.

CHAIRMAN—At 25 past I am a pumpkin!

Mr Besgrove—Okay. The key point here is a lot of work on cross-recognition is going on inside Australia, within APEC, with the Americans. A huge amount of work is going on to try to get PKI systems around the world to talk to each other. That is the bottom line.

Ms Elsley—This slide will be the last one. We are currently putting in place some policy changes within Gatekeeper. Basically, one is the liability regime of CAs. Liability was never evaluated under Gatekeeper for various reasons and now it will be. So we are finalising that. The other one is that we are changing or tightening the identity documents required in the registration process. Before there was the FTR regulation form 201, which is the document that is required to open an account. Any documents that go up to making either 100 or 150 points were allowed.

Now we are saying we want a primary document, which is a birth certificate, citizenship certificate or a passport, and then a secondary document or any number of secondary documents that go up to make the required points. However, if there is not a current photo on the primary documents, one of the secondary documents has to have a current photo. So that is basically how that is being tightened for the individual. There is also some tightening for organisation identification as well.

We are looking at transitioning Gatekeeper administration. Whereas some of the evaluation processes are carried out by organisations such as DSD, ASIO and AGS, the administration is managed by Gatekeeper and we are looking at transitioning that out to an organisation whose core business is more the accreditation business. So we are in the process of doing that as well.

Mr Besgrove—I think the key thing there is that we hope that that would enable us to streamline the process.

Ms Elsley—Yes, to streamline and speed it up.

Mr Besgrove—We might skip to the last dot point and move on to Mr Mattocks.

Ms Elsley—Yes, we will do that.

Mr Besgrove—The last dot point takes rather a long time.

Mr Mattocks—For my part of the presentation I would like to talk a little about PKI as the infrastructure, some certificates, digital signatures, the differences generally between gateways, FedLink, SSL, Gatekeeper and then PGP and the web of trust. Predominantly from a technology perspective they all implement the encryption in a similar way. The bottom line is really the difference in authentication—so whom or what you are authenticating at either end of the communication.

Just quickly on PKI, the important point from the PKI side of things is the 'I' for infrastructure. As we spoke about earlier, that includes the service providers, the people, the communications paths and security in a whole range of issues there. It is basically how you manage trust, where you get the trust from and how it happens. So in the Gatekeeper framework when an organisation goes through on a Gatekeeper accreditation, at the end of that, when they get the tick in the box, they are basically then trusted to operate that service on behalf of the government or for the government. At that point any certificate that is issued by a Gatekeeper vendor can be trusted. That is a critical point. That should do for that slide.

Under public key technology we then talk about the technology that is used as part of the infrastructure. Predominantly that is technology used by certificate authorities/registration authorities and includes things like the software and the hardware that are used; how their cryptography is implemented and how their certificates are generated, stored, saved and transmitted. In particular there I have identified the main different versions of certificates at the moment: just a piece of electronic data that is in what we call a soft certificate or a hard certificate, which is actually loaded onto a device such as a smart card, similar to a credit card. Again, that focuses largely on the encryption and products.

Turning to the next slide: to go back through public key cryptography, again it is really a binding between the authentication and authenticating the owner of the private key, so that a piece of cryptography is enabled and it generates a key pair, two cryptographic keys, one key being a private key, one key being a public key. They are linked in a very strong mathematical way.

Senator LUNDY—Can you just explain in a little more detail about that technology, the encryption and how it is done?

Mr Mattocks—Certainly I can. In fact, one of my slides towards the end goes into it in a little detail.

Senator LUNDY—I think it is important for the committee to understand the different levels of encryption and the sort of maths that is involved in creating the algorithms and why that is—I know you do not have long.

Mr Mattocks—That is all right.

Senator LUNDY—We have not yet had anyone sit on that side of the table and tell us how that happens.

Mr Besgrove—Do you want to go to that slide.

Mr Mattocks—We will jump to that slide towards the end. It is a very difficult and complex technology in some ways, but in other ways it ends up being relatively okay. Down the bottom is the private and public key pair. The private key is generally a very strong mathematical, encryption based number, I suppose, and these numbers are related to allow encryption and decryption. They are called an asymmetric key pair and they work in pairs. So you have one that will encrypt and its partner will decrypt. The one that encrypts is usually kept private and the one that decrypts is usually put out in the public domain.

Just to go back a little, in a symmetric key, which is the session key up here—in normal cryptography or historical classical cryptography you have a key that will encrypt data. Then that key can also decrypt data, the same data. If I have the encryption key and I send a message to you, you need that encryption key to decrypt it. Historically, the difficulty has been how you manage the delivery of that key from one person to another. If you put it in the public domain, then someone can copy it and then can decrypt the information.

Senator LUNDY—Mr Mattocks, can you go back another step. When you talk about a key, it is a string of numbers to which a mathematical equation applies and the amount of numbers relates to the size of the key?

Mr Mattocks—Correct.

Senator LUNDY—Can you just step the committee through that?

CHAIRMAN—Aren't you talking about the relationship between a number or a group of numbers or a sequence of letters or a group of letters versus the real letters?

Mr Mattocks—Yes. You will have some information and you, through a mathematical process, can apply—

CHAIRMAN—It is just like morse code?

Mr Mattocks—Yes, or similar in a way. It will convert information from one format into another.

CHAIRMAN—Why isn't it precisely like morse code? Morse code defines in a series of dots and dashes the letters of the alphabet, which can then be put together to form words, as I recall.

Senator LUNDY—What I was trying to achieve by asking Mr Mattocks those questions is that, for the purposes of the committee's inquiry, we need a little more technical information about how a key works, particularly as it relates to different levels of encryption, which I think relates to the system and all the rest of it.

Mr Besgrove—Perhaps we could take that on notice.

Senator LUNDY—I do not want to get sidetracked now.

Mr Mattocks—Next I was going to talk about the algorithms that are used.

Senator LUNDY—Sorry, I will leave you in peace.

Mr Mattocks—If that is what you are after.

Senator LUNDY—Yes. If you could step us through this slide and then go back to where we left off, that would be great.

Mr Mattocks—Certainly. In relation to the length of the keys for a symmetric encryption—so when you are encrypting data—for the government's purposes, we look at a minimum of 56 bits of data for the encryption of a symmetric key, or longer. There is the Data Encryption Standard and the Advanced Encryption Standard there with their key lengths on the slide. The length of the keys basically looks at the strength of the encryption that is applied to the information. So in a symmetric world where you have a shared key they are the algorithms that we use. In the private key, for the asymmetric public and private key pair we use longer key lengths and slightly different algorithms that are tailored to that implementation. The longer key lengths provide a stronger level of encryption.

Generally speaking in a PKI realm the reason behind that is that a session key is really used only once per message. Every time you send a bit of information you will use a new session key. When you are signing something using your private key you use it all the time, so it has a lot of reuse. That is one of the reasons why it has a longer key length.

Ms Elsley—You can be assured that there are no problems with that key being tampered with over a longer period.

Senator LUNDY—Just to make it really clear for the committee, the longer the encryption, the higher the number of bits in that sequence—

Mr Mattocks—Generally speaking, yes.

Senator LUNDY—The stronger—

Mr Mattocks—The stronger the encryption and the harder it is to break.

Senator LUNDY—Which means the harder it is to break, the longer it takes to break.

Mr Mattocks—Yes.

CHAIRMAN—Slide 6 in the pack shows an example of a digital signature.

Mr Mattocks—Yes. We can jump to that one.

CHAIRMAN—I just wondered on a practical level how in holy hell anybody would ever remember that.

Mr Besgrove—That is the whole idea.

Mr Mattocks—The good thing is you do not need to remember it.

CHAIRMAN—Therefore, how practical is it? I cannot remember my passwords.

Mr Besgrove—The whole idea is you never try to carry it around in your head.

CHAIRMAN—But that makes it not very secure. If I carry it around in my pocket and somebody steals my pants, we are in trouble.

Mr Besgrove—If you carry it around in a device which only you can use, then it is very secure.

Ms Elsley—You do not keep it on a piece of paper.

Mr Besgrove—Or if you do not carry it around at all but it is actually in a computer it may be more secure. There are different ways of making it secure using hardware.

Mr Grant—It also often has a second level, which is perhaps a password that you use with it and, if we look a few years out, potentially a biometric. So in fact you do not need to remember it, you can carry it around, and the level of surety that it cannot be reused is increasing.

Senator LUNDY—The thing about this system is that what you carry around is not the only way in which you can identify yourself, it has to meet up with other parts of the system, and that is what gives it strength. So on its own it does not really do anything; it has to be linked up with another part of the PKI system to have any purpose.

CHAIRMAN—I understand that. If you try to run your bank account online, you put in a series of numbers which defines your account number. You get your bank's web site first and then you put in a series of numbers. That then gets you up to the firewall and then they want some kind of code.

Mr Grant—Yes.

CHAIRMAN—With my bank, if I forget my code and fail to enter it correctly three times, I am offline permanently until I go back through a long authentication procedure to get back online again. That is really the two levels of protection, isn't it?

Mr Grant—It is. With the bank operation, which is a really good example, the data transferred is encrypted because they usually have SSL underpinning it, and then, as you said, you have your PIN and password. It is interesting because the National Bank began with a higher level authentication where in fact they put a public key—it might be a private key, actually—into your computer. But that meant you could deal online with the National Bank from only that computer. They changed that because the other banks were not doing it and it was too difficult for customers.

Senator LUNDY—Yes. The Commonwealth Bank had some downloads initially as well.

Mr Grant—Did they?

Senator LUNDY— But it did not last long.

Mr Mattocks—Just to go back to that slide, that is an example of a digital signature, which, yes, you do not normally need to carry around or remember. Normally it is something you carry with you, quite often on a smart card or some sort of plastic card, and generally you use a PIN or a password to unlock that. The computer system will then do the operations on your behalf. But I just put that up as an example of what it could look like. Sometimes you see it attached to messages on email.

I thought I would go through the next few slides and just show you the differences between the different authentication mechanisms that are used when you are dealing electronically. In almost all cases they implement encryption in the same way with the same algorithms. It is really the end points that you are authenticating that are different. As you have just pointed out, with SSL and similarly when you have to put a PIN in a second time you are authenticating yourself; the first time it is a device.

Mr Besgrove—Glen, I think we will need to move through this pretty quickly.

Mr Mattocks—Yes, I will breeze through. Flipping to the next slide, in a typical government environment or business we have a gateway. The little dotted box is pretty much what we define as a gateway. Quite often DSD conducts gateway certifications and we look at how that environment is managed from the security perspective. I have included in there a FedLink router. Routers direct traffic. I just want to explain exactly where the end points are when I talk about FedLink: typically at the firewall they are the brick walls up there; the web server, which will quite often house an SSL certificate; email; and then employees or people at the other end.

Turning to the next slide, for FedLink pretty much the authentication happens at that FedLink router and so does the encryption. So agency to agency what you are really authenticating is the agency's front door in a virtual sense.

CHAIRMAN—Not individuals; just the agency?

Mr Mattocks—Not the individuals, not the devices; just the agency. The next slide: for SSL encryption from the server—if you are, say, a bank and you are running a secure service—it is actually from the web server outwards. So the web server has the certificate and you are authenticating the web server out to the clients. Again, all you are really authenticating is the device that is owned by and sitting in the secure premises of the managers of that device.

Flipping to the next slide, from the other side of it, when you are visiting a secure web site as a client you can now see it goes all the way through to the client's desktop. So the browser you are at is actually authenticating back to the web server. That can be an issue when you are talking to citizens or people dealing online. For example, with Internet banking you could be sitting in an Internet café, so you are not authenticating the person; you are authenticating the machine they are sitting at, wherever they are. So that machine is identifying itself to the bank or to the web server.

Finally, for secure email, typically as an employee or a person you will have a private key which is yours and allows you to sign and authenticate yourself. Often it is on a token or a smart card of some sort. You then put in your PIN. It unlocks that and does the encryption, and then it goes all the way through to the person at the other end. In some instances the government—if they are joined up to FedLink, they can configure it to send secure email through FedLink as well; so you have two levels of security.

We have been through this slide. Finally, just the difference between Gatekeeper and the web of trust model.

Mr Besgrove—This is as ugly as the slide.

Senator LUNDY—It is like spaghetti—

Mr Mattocks—Yes, I left it to the end. As I spoke about before, when you go through a Gatekeeper accreditation, that is where the trust comes into play and from that point onwards any certificates issued by the Gatekeeper vendor can be trusted. In a web of trust model for PGP or similar technologies, it is inferred or implied webs of trust. So, if I trust you and you trust someone else, I by implication trust them. From the government's perspective, every person therefore has to manage that whole relationship and trust domain, every person has to go through that sort of process to identify whom they trust and whom they do not and whom by default or implication they trust.

Ms Elsley—If you put a PKI hierarchy against that, you would see that it is a much more simple hierarchy to manage.

Mr Besgrove—Mr Chairman, I think in the interests of time we might stop the presentation at that point. Are there any further questions you have?

Senator LUNDY—I have to go, but I think that has been really useful for the committee; so thank you very much.

CHAIRMAN—I am going, too. It certainly has been for me. Thank you.

Mr Besgrove—Thank you for the opportunity.

Resolved (on motion by **Senator Lundy**):

That the folder of documents presented by NOIE be taken as evidence and included in the committee's record as exhibit 18.

Resolved (on motion by **Senator Lundy**):

That the committee accept the transcript of the briefing given before it this day as exhibit No. 19 and authorise publication, including publication on the parliamentary database, of the proof.

Committee adjourned at 10.15 a.m.