

Secure Electronic Environment Project



A project jointly undertaken by the State Services Commission, Treasury and Department of Prime Minister and Cabinet

29 March 2000

Introduction

The purpose of this paper is to discuss the experience gained by the secure electronic environment (SEE) project through developing a proof of concept prototype, for securing e-mail and shared content between the State Services Commission, the Treasury and the Department of the Prime Minister and Cabinet.

Background of the SEE Project

The SEE project is a joint initiative by the State Services Commission, the Treasury and the Department of the Prime Minister and Cabinet, known collectively as the central agencies.

Project Objectives

The objectives of the overall project from the SEE project scope document are:

'to develop and implement a secure electronic environment (SEE) that will:

- a) enable data and information classified up to 'SENSITIVE' or 'RESTRICTED' level to be shared between member agencies;
- b) be scalable to meet the needs of a wider-Public Service user base, and in the longer term to a wider state sector user base, if this is feasible;
- c) reduce duplication of data holdings by facilitating sharing and reuse of common data sets;
- d) improve security for member agencies;
- e) be adaptable to changing business requirements; and
- f) provide a foundation for eventual extension to meet the security and management requirements of 'CONFIDENTIAL' level data and information without unnecessarily constraining system or business functionality, or unduly limiting appropriate external connections or communications.

Project Deliverables

The deliverables from the SEE Project Scope Document can be summarised as will be:

- D1 - Policies and guidelines for secure email and content for member agencies
- D2 - Appropriate governance, management, monitoring, funding and liability structures.
- D3 - Selected examples of appropriate static, dynamic and collaborative content applications to provide applications for evaluation of the pilot and to provide an initial base of value in the environment.
- D4 - Secure email between the State Services Commission, the Treasury and the Department of the Prime Minister and Cabinet,

- D5 - Necessary technical and management infrastructure i.e. shared IT hardware, software and management facilities

Relationship to Other Projects in the State Sector

The SEE project will develop a secure environment that can be scaled up to electronically connect government agencies so that sensitive or restricted data and information can be shared via e-mail or secure remote access to data repositories.

The Government will not be able to pursue many e-government initiatives without appropriate security. The SEE project will develop an appropriate security infrastructure, that can be scaled to provide the necessary level of security for a particular set of requirements. The SEE project is seen as a high priority within the proposed e-government programme. The project is being coordinated within the overall e-government programme.

Approach

Several drivers for the SEE project are different to overseas examples of secure-exchange environments already in use. These can be summarised as follows.

Respecting autonomy of agencies

SEE should not require strong centralisation and investment in government-owned private networks. The aim is better coordination of existing investment in firewalls, servers, routers, Internet connections and IT skills rather than outsourcing or creation of a new infrastructure. Maintaining autonomy of NZ public sector agencies is an integral part of the approach to SEE.

Small-scale prototype

The SEE prototype is both staffed and funded largely by the central agencies to establish a proof-of-concept. Keeping the project at this scale has allowed experimentation, involvement and development of key staff, and learning-by-doing, without compromising security, daily business, or requiring extra seed-funding.

Central agency co-operation

The project team and sponsors consider that the central agencies have a strong business need for security. However while the central agencies can be thought of as a sectoral cluster they maintain relationships with every department and state agency. They have strong incentives to design a way to work securely with everyone in government, not only each other.

Secure exchange at the level of the individual

Overseas thinking is that entire *agencies* sign up to secure information exchange. The consequent impact on business flexibility for the prototype stage, led to consideration of PKI. The prototype SEE architecture focused on the individual proving their identity and role and being granted access to information accordingly. Because of this approach, individuals in seven agencies have been able to use secure e-mail and the secure web site, while agencies as a whole avoided large up-front costs.

Extending overseas models

The SEE prototype architecture gave us information about what it would be like for our businesses to work with PKI. Because it is a recent market development no one could advise us on this. The prototype achieved appropriate levels of security by using the user-to-user model of secure exchange as did the overseas models that connected agency-to-agency via private networks and proved that PKI was a feasible alternative. Some secure environments have contracted for a private network first. We considered that Internet was reliable enough for ordinary business e-mail and web use, so would be adequate for the SEE prototype.

Summary of principles

The following design principles are apparent in the SEE prototype:

- agency autonomy,
- preserve business flexibility,
- a virtual not physical network,
- eventual scalability to whole of public and state sector,
- small-scale learning exercise,
- ensure security is adequate by testing with our own businesses,
- use the Internet as the carrier if possible.

Summary 'Sensitive' or 'Restricted'

For the purposes of the SEE project 'Sensitive' or 'Restricted' has been defined as:

'Information where compromise would have one or more of the following impacts:

- be likely to cause substantial distress to individuals;
- affect diplomatic relations adversely;
- make it more difficult to maintain operational effectiveness or security of New Zealand or allied forces;
- cause financial loss or loss of earning potential to individuals or companies;
- prejudice the investigation of crime;
- breach proper undertakings to maintain the confidence of information provided by third parties;
- impede effective operation of the government, development of policies, and the budget process;
- breach statutory restrictions on the disclosure of information;
- disadvantage government in negotiations with others.'

THE SEE PROTOTYPE

Objectives of the SEE Prototype

The pilot was implemented for 37 users spread more or less equally across the three central agencies:

- ⇒ using public key technology to authenticate users (via 1024 bit private key pairs), individual certificates, smart cards and readers
- ⇒ using 168 bit secret key encryption (MS US domestic encryption add-on)
- ⇒ using the Internet as the transportation mechanism.

The following objectives were set for the prototype:

OBJECTIVE 1: Prove it is possible to send secure email authenticated by individual, between all 3 agencies, with full functionality.

OBJECTIVE 2: Create prototypes of 3 types of content tools for users to access static, dynamic and collaborative applications.

OBJECTIVE 3. Test 1 and 2 for usefulness, quality of service and security by giving users hands on experience and recording their feedback.

OBJECTIVE 4. Test if 1 and 2 met security requirements.

OBJECTIVE 5 Test connecting to legacy applications using PKT.

OBJECTIVE 6 Test access granularity.

Method for developing the Prototype

In August 1999 the Content team began a search for business processes to design a prototype around. We asked our Steering Group and several senior people in Treasury, DPMC, and SSC to identify

- ⇒ processes that did not work well and might benefit from being done electronically,
- ⇒ that involved sensitive level material
- ⇒ timeliness - real business processes happening at that time, and
- ⇒ only involved the central agencies.

Out of this survey came the decisions to include in the prototype

- ⇒ secure e-mail to Restricted/Sensitive level,
- ⇒ a shared workspace for the SEE project team discussion and documents on a secure web site (static and collaborative content),
- ⇒ a contact list of all the staff in the central agencies on the web site (dynamic content),
- ⇒ support for two business processes.

The goal of the prototype was to show key people the potential to support real business requirements, based on a low-cost proof of concept approach.

A Public Key Infrastructure was approved as the technical architecture for the prototype on the basis that it provided the level of security needed for Sensitive/Restricted information exchange but did not lock out adding a further layer for protection of Confidential-level exchange at a future date.

What was Achieved

Between November 1999 and February 2000, 37 people received digital certificates and smart cards with their private keys stored on them. Smart card readers and software was installed and personal certificates and keys were registered in their browsers and email clients.

These people then had to e-mail their digital certificates to colleagues on the pilot so they could exchange encrypted email on a one-to-one basis.

The person's certificate information was also registered onto a secure web-server. For valid user requests an SSL session was opened. For all other attempts at access the browser's request for data was rejected

Dynamic content was available – users were using Active Server Pages to query and view results from a database containing contact details and reports-to data. They could search by partial name, or browse by hierarchy.

A collaborative area was set up using e-forum software. Four forums were created and valid-user lists created so that group-access granularity could be demonstrated.

Static information was to be made available using a commercial-off-the-shelf (COTS) product. Work was discontinued when we realised that budget and time available did not match the complexity of building the proxy server routines to add security to this COTS product.

The proposed business processes could not be supported, one was cancelled and the other proved to be not feasible. In the end the business process that was of most value for testing purposes was the SEE Project itself.

Workarounds

A number of work-arounds were introduced into the prototype environment, to simplify the exercise, and to reduce risk and cost. These workarounds are not suitable for an operational business system and will need to be addressed before an operational environment is developed and implemented.

- ⇒ Directory
- ⇒ E-mail clients
- ⇒ Firewall configuration
- ⇒ Active Content

PROJECT MANAGEMENT

Processes for participation by non-central agency members

The SEE Project Advisory Group (PAG) was the main way that other agencies were actively helping to define what the SEE would deliver. One or two provided extra advice on several occasions and most took the opportunity to talk to the Project Coordinator directly about their concerns.

Two web/Intranet experts – one from Te Puni Kokiri and another from the National Library, a technical expert from the Ministry of Fisheries, and a security expert from the Government Communications Security Bureau (GCSB) joined the SEE Project.

Working group management

The groups doing the work (Technical and Content) met separately during scoping but met as a combined team while the prototype was going live. The very high number of boundary issues made it far more effective to combine the teams at this point. The two streams of work interlock to a far greater extent than has been seen to date with overseas models using a private network or a virtual private network as the carrier.

MAJOR LEARNINGS

The impact of setting up and running the prototype stage of SEE has been wide-ranging even though the user group was below forty and spread over seven agencies.

Governance

1. The governance structure of future SEE is now viewed as crucial to its success.
2. Explicit rather than tacit understandings of firewall policies and security practices will be required between IT personnel in SEE-using agencies.
3. SEE-connected agencies will have to audit their internal practices around classifying and handling information/data.
4. The prototype content server demonstrated the potential for improved information sharing between agencies. Exploiting this potential will require careful championing.
5. From talking to the technology architect on the SEE equivalent in UK Government, the implementation of SEE will be challenging. High level sponsorship will help to ensure uptake, and there is a clear need to put considerable effort into publicity.
6. Policies for handling of encrypted email need to be established, to maintain confidence that information is available for OIA purposes, legal cases, and the department's own record-keeping requirements.

Security

7. Many of the policies governing IT security in government agencies should be redeveloped because the business environment has changed so radically. They need to be oriented towards a majority of agencies doing business via the Internet, and relative risk management rather than risk avoidance.
8. E-mail and web-based systems place more emphasis on the individual's role in departmental security and their potential to be a weak link in the chain. Previous security policies have placed more emphasis on deliberate external breaches, rather than internal or "socially engineered" breaches that are seen more often in an electronic business environment.
9. Active content (e.g. scripting using Java, JavaScript or ActiveX) was used for a couple of functions on the prototype web-site. This highlighted the need for a

security policy on allowing Internet active content (a significant security risk), into agencies. There will need to be management controls on use of active content.

Technology

10. Interoperability based on open standards is still maturing. Some products do not yet support S/MIME and other PKT/PKI standards. If only a few products inter-operate well then lack of choice sets up a proprietary secure environment, which raises concerns. Implementation of SEE email at DPMC, a GroupWise site, highlighted where non-Microsoft sites may have to invest a large amount of effort to implement SEE, with no guarantees of success.
11. Current PKT is not seamless from the user perspective. Implementation of PKT within applications can be awkward and may not always work. Seamless operation at the desktop and elsewhere is crucial to success of SEE (as overseas projects also found).
12. The use of secure e-mail depends on sensitivity of the task at hand as well as the role of the person. So a decision to encrypt and sign e-mail is made each time. Our organisations also frequently use e-mail distribution lists (one to many) which does not easily function within the one-one communication model currently available. New versions of client software may resolve these issues, but they are not available yet.
13. PKT suited secure web-based content better than e-mail, if you require the content to be secured to the level of the individual user. The dynamic and collaborative web-based content therefore worked well with PKI.
14. Conversion of legacy applications is achievable. The estimated cost range is dependent on the application.
15. The role of a directory containing authentication information for government employees becomes essential with a distributed architecture. Providing secure content without this core set of valid certificate information and access rights, even to three agencies, is unmanageable.
16. The prototype highlighted the need for good co-ordination of rollout, policies, and user training across agencies, with high-level support from management.
17. With third party issuing of digital certificates, staff are going to be asked to share private information about themselves. The purpose, and benefits, of having digital certificates have to be very clear.
18. It is very important that those who handle documents of identity (e.g. passports or birth certificates) in the agencies managing the certificate-application process are respectful of the information and the providers.
19. It is very important that the department dealing with the certificate issuer is clear on what the issuer is checking for when they agree to grant a digital certificate.
20. There will be HR issues for agencies. The most explicit example of this is the need to ensure that employment contracts reflect the security requirements of working in a distributed electronic environment

Did SEE as prototyped fit with our businesses?

21. SEE did not fit in these areas. The central agencies need to communicate securely across all of government. The ability to securely communicate only between the central agencies, was of limited benefit. For secure e-mail to be effective (use distribution lists, run inter-agency committees and projects), many other government employees would also need to have digital certificates issued.

22. SEE had some fit in these areas. Business practices around security classification have become differentiated over time. Greater consistency of handling restricted/sensitive level material is needed and awareness of what the different markings mean. This is important for establishing trust between our agencies.

23. SEE had a good fit in these areas.

- It is closely aligned with our increasing use of the Internet and the overall approach to security being taken in our agencies. The prototype users confirmed this in the evaluation survey.
- Prototype users said secure e-mail was not a step change from what they were used to doing, unless they normally *faxed or couriered* sensitive material to people in the other agencies.
- Support for collaboration and common business processes was provided. A secure electronic environment would help to break down information 'silos' in the public sector and encourage agencies to move from paper to electronic distribution of information. However just introducing the technology would not accomplish this and other kinds of incentives would also be needed for this to happen.

Prototype successes

- Secure e-mail and content actually ran and was used (the concept was doable)
- Strong individual authentication and encryption was implemented to an acceptable standard
- A real business process (the SEE Project itself) was enhanced and supported
- Five of six objectives for the prototype were achieved. The sixth objective could have been achieved with a greater budget and familiarity with the application software

Prototype limitations

The following issues will need to be resolved before implementing an operational environment:

- Interoperability between PKT and desktop applications is not yet mature
- Seamlessness for users is an issue, particularly with e-mail
- A central agency system is of limited benefit because the businesses work with mostly with other agencies and Ministers offices
- Users and agencies have to be well informed about the process of applying for 3rd party supplied digital certificates
- Capacity (expertise and resources) within agencies
- Technology fit with 'the way we do business around here' has to be better

- Business processes will need to be re-engineered to address security needs and to leverage the advantages of the technology
- Issues around directories, quality of service, denial of service attacks, intrusion detection and firewalls will need to be explored (prototype was too limited to learn much about these).
- Content will not be ready for a while, the 'killer apps' are currently not out there

Did the prototype support the overall SEE Project?

Did we go the right way – yes, because no one could tell us what PKI would be like for our businesses and a small prototype was the best way to learn that.

Did we gain value from the prototype - yes, the prototype was a high value exercise. It has provided a great deal of necessary information for an eventual roll-out.

CONCLUSIONS

The prototype has been a catalyst to find out where systems and practices need improvement to do secure business over the Internet. We have developed a realistic understanding of the risk-management costs and benefits for security in our organisations.

What will fit with government organisations is a secure environment, delivering encrypted e-mail to begin with, that will work across a majority of agencies. This only needs to ensure security of transmission over the Internet. As collaboration and content become more significant and valuable, strong authentication of individuals will become much more useful and necessary. In future agencies have to be able to control access to information yet make it available to qualified users of that information.

Agency authentication of email and web servers increases the trust in the information content. It would enable access to on-line material that is currently hard to access. Agency level encryption is desirable, for all official communications, to retain privacy.

User level authentication/encryption would be useful for a limited number of people. It would be cost feasible to roll out technology to this group. User level authentication would be useful, for participating in web forums and other cross-agency applications.

Security policies and current technical architecture will need to be audited to ensure that they can support secure communications – the work to implement the audit recommendations is likely to be significant.

Directory services based on X500/LDAP could support a resource discovery for government information and information services within New Zealand, including resources.

While the project has demonstrated highly effective communication privacy and authentication controls there is still a reasonable amount of work to do before the SEE can be truly considered a “secure environment”. This will include investigation into intrusion and misuse detection and management, firewall and boundary controls, and system and information management agreements and controls.

More work is required to explore the changes in behaviour and attitudes that are required when working in a more collaborative and open way – essentially, exploring what trust actually means in an e-government environment. Although the current trust mechanisms are well established for existing process and paper based exchanges of information, these need to be reviewed.

In today's Internet-centric and fast-paced world the SEE Project is an important and timely introduction into fast and secure electronic interaction. A number of other projects have arisen concerning secure networks between and within various agencies, but none have looked so seriously at the possibility of a 'whole-of-government solution'. The interoperability problems we have encountered, within this very limited pilot, indicate that any such project that ignores this wider scope will lead the Government into building islands of secure communications with multiple solutions and/or manual intervention required to communicate between any of these islands.

The various options we looked into all had, and still have, advantages and disadvantages. Until we as Government have used the technologies and gained an understanding of their strengths and limitations we are unlikely to be capable of making such informed predictions as this would require – a "chicken or the egg" situation. Even then there may not be one clear "correct" solution, but instead solutions that suit a particular application more than another based on its specific user, information and security requirements. A "one size fits all solution", while possible over an homogenous community, will result in uneconomical and inappropriate solutions in the wider, and more varied, community of all-of-Government.

The way forward then, is not to develop "a network" or even a single 'environment', but to develop a toolbox of standards, guidelines and mechanisms that can be mixed-and-matched to fit a particular solution. PKT will be a key component of the toolbox, but rather than providing keys and certificates for everyone in Government, provide them to the relevant point in the communications path for the access control and level of granularity required.