2006

Review of the PKI status in New Zealand

Lech J. Janczewski
The University of Auckland, lech@auckland.ac.nz

Vladimir Petranovic
vpetranovic@gmail.com

Review of the PKI status in New Zealand

Lech J. Janczewski
Department of Information Systems and Operations Management
The University of Auckland
lech@auckland.ac.nz

Vladimir Petranovic
IT Security Consultant
Auckland
vpetranovic@gmail.com

Abstract

The research presented in this report was an attempt to answer the question: What is the situation with regard to the deployment of the PKI in New Zealand and are there attractive business models that can be successful in New Zealand? This work also provided an answer to the question of acceptance issues we face when deploying PKI in New Zealand. It attempted to find a workable model that could be appealing to New Zealand businesses and other organisations that need to use the Internet for conducting their affairs.

Keywords: PKI, Management of Information Security, Information Security case studies

1. Introduction

The research presented in this paper was an attempt to answer the question: What is the situation with regard to the deployment of the PKI in New Zealand and are there attractive business models that can be successful in New Zealand? This work will also try to give the answer to the question of acceptance issues we face when deploying PKI in New Zealand. It will attempt to find a workable model that could be appealing to New Zealand businesses and other organisations that need to use the Internet for conducting their affairs.

The report is divided into the following parts: in the first part we set up the PKI definition. Then we are presenting and commenting on the five New Zealand cases of an implementation system allowing for the secure transmission of information. It is then followed by formulating basic limitations of widespread PKI implementations in this country. After that we present a roadmap for building and implementing effective and efficient PKI systems in New Zealand. Conclusions close this report.

2. PKI definition

For the purpose of this project the following PKI definition was adopted: *Public Key Infrastructure is an enabler, underlying basis, or framework, of following public cryptography security services: authentication, integrity, confidentiality, time stamping, secure notary service, non – repudiation, privilege management, etc*.

3. New Zealand PKI developments

Contrary to many other countries, in New Zealand there is no general policy of PKI development and deployment. As a result we will present a number of fairly independent cases of PKI implementations which would demonstrate capabilities and issues related to PKI implementation in this country.

3.1. e-Government PKI Project

This case was selected because e-Government projects are on the forefront of PKI deployment in almost all countries. PKI technology seems to fit ideally into e-Government initiatives around the world.

At the beginning of the year 2000 the New Zealand government States Services Commission published the first documents about the New Zealand e-Government project (State Services Commission, 2000). Part of the e-Government project was the creation of the Secure Electronic Environment (S.E.E), i.e. a unit which would deal with security issues of internal Government operations (State Services Commission, 2003a). The key objective of the overall project was to develop and implement a secure electronic environment for the exchange of government e-mail (S.E.E. Mail) and access (S.E.E. Directory) to repositories of government information for authorised (S.E.E. PKI) public servants. Essentially, this would constitute a secure extranet for government agencies and building a base for development of a PKI to authenticate internal Government users (State Services Commission, 2003b). The S.E.E. PKI project scope stated that the project was strictly limited to the authentication of the users and encryption of the network traffic (State Services Commission, 2001).

This represented significant limitation of the scope and usefulness of the PKI itself. From the functionality perspective the project achieves only a small step forward compared to the worldwide-accepted encryption of network traffic and identification of the server side. This is most interesting due to the fact that SSL technology was developed, implemented and accepted by Internet users in order to verify unknown Internet merchants. So before an unprotected buyer sent the money order or credit card details to the merchant's server it could check the authenticity of the web site. The encryption of the network traffic itself was not so crucial, more an added functionality that was enabled by having certificates on the merchant's server.

The project seems to lack the leadership, courage, real scope and 'business case'. To support this conclusion it would be enough to evaluate the S.E.E. Mail project. Instead of using PKI as the basis for the development of the secure e-mail service that would provide confidentiality, integrity, non-repudiation, time stamp etc., State Services Commission (State Services Commission, 2003c) opted for the 'off the shelf' solution. That would allow to encrypt the traffic only between e-mail gateways. The traffic between the end-user and the e-mail remains unencrypted and hence exposed to eavesdropping. Secure e-mail represents an ideal application for PKI. However, such a PKI should exist in the first place before secure e-mail is rolled out. Unfortunately, Government agencies do not have any PKIs, so the easiest way to patch the security of

the e-mail messages when they travel across the Internet was to deploy 40 secure e-mail gateways. In essence this represents nothing more than simple a VPN between gateways.

3.2. Auckland District Health Board (ADHB)

ADHB was selected because Health Boards are Government funded institutions that deal with a level of information and privacy sensitivity that is hard to find anywhere else. In many research papers PKI technology was indicated to be the ideal one to protect the security and privacy of information in hospital environments.

The Auckland District Health Board is both a provider and founder of public hospital and health services. The Auckland District Health Board has almost two million patient contacts annually and provides regional services for 30 per cent of New Zealand's population. Auckland District Health Board's employs 7,500 staff (ADHB, 2004). Leakage of confidential patient information could have tremendous repercussions on any District Health Board operation and their public relation perception. Currently ADHB uses VPN cryptographic systems between hospitals in Auckland (Irving, 2004). This measure establishes the confidentiality of the network traffic when travelling between hospitals. Certificates are distributed to all ten wireless computers for the purpose of authentication. A temporary Certificate Authority server based on Microsoft implementation has been established to issue certificates based on auto-enrolment of the computers participating in the Windows domain.

Only encrypted information travels between hospitals in the Auckland region. There is no cryptographic solution in place to encrypt e-mail messages, stored confidential information and there are no facilities to protect authenticity or integrity of stored or relayed information, no mechanisms to time-stamp or to provide non-repudiation.

When those basic PKI services are not available to the users of the ADHB information system within their hospital it becomes irrelevant to discuss eventual need to protect the confidentiality, integrity and authenticity of the information travelling between hospitals, between hospitals and related institutions or simply between hospital and their business partners.

In a situation like this the best way to preserve the basic confidentiality and integrity of sensitive information is to use standard physical means of non-electronic data protection. Sensitive information could be stored in safe cabinets and relayed in envelopes with 'private and confidential' stamp. One could wonder if this is an adequate security setup.

3.3 Baycorp ID Services

This was an interesting case because it represented the first New Zealand public Certificate Authority i.e. the provider of one of the core services of PKI.

In the year 2000 Baycorp ID Services started to sell certificates to individuals and provided software to install their root certificate to the web browser i.e. machine local certificate store. Certificates were sold on an individual basis, by certifying individuals

within organisations. Together with lack of marketing, not knowing who to sell to was a major reason for the operation not taking off.

During December 2002, the CA operation ran by Baycorp ID Services was outsourced to the newly established company 'Digital Identity' which is still active today and operates by providing the infrastructure to the Baycorp ID Services. Digital Identity currently manages about 400 certificates. Baycorp ID Services managed to issue altogether 2000 certificates mainly to the individuals within health organisations (Webb, 2003).

The major issues identified by participants in this first New Zealand commercial Certificate Authority initiative are:

- The price of PKI: considering the high assurance criteria for governmental deployment of PKI technology set up by SEE, the price of compliance is about NZ$ 1,000,000 (around $600K USA).
- The price of individual credentialing is also considered to be very high, unless high certificate volume is achieved or credentialing conducted by individual organisation receiving PKI services (a hospital for example). Potential solution to this problem is to leave the credentialing process to the institutions that already have strong business around that area. Examples would be banks or major credit card companies.
- The presence of potential liability in the case of a security breach is very high and represents a major deterrent for anyone considering a commercial grade PKI services provision.
- Lack of critical mass for technology uptake is recognised to be the main problem in New Zealand. The health sector appears to be the only one that can has significant number of deployed certificates in order to demonstrate the viability of PKI technologies in New Zealand. However, at the present time it seems that the uptake of secure messaging within the health sector is slowing down.

Having all that in mind and perceiving PKI as a non-strategic technology with doubts in spread of PKI initiatives, it is not unusual that potential users of the PKI technology, such as the health sector, still run their exclusive, internal Certificate Authorities not recognised outside their onw domain. Such solutions are not SEE compliant and usually run on the systems unable to provide commercial grade security.

3.4. ASB Bank (ASB)

Protecting the integrity of data, privacy and security of their customers has to be one of the top priorities of leading New Zealand bank institutions. Because ASB deals with money, any security breaches could be costly. By default this makes ASB an interesting case.

ASB Bank is technologically one of the most advanced bank organisations in New Zealand. The recent launch of mobile banking that enables customers to access their accounts via mobile phone just emphasises ASB's technological advances (ASB, 2004b). This solution has some inheriting weakness: inadequate authentication method. Customers that want to access their accounts using the Internet or mobile phones need to

enter only their user name and password to authenticate. As a consequence manipulation of funds is not secure (ASB, 2004a).

Although user-name and passwords can be adequate authentication mechanism in a limited number of circumstances, it is absolutely inadequate for remote access over an open media such as the Internet. This is well known to ASB as it uses RSA token based user authentication for the remote access of internal systems. In other words, ASB has much higher protection mechanisms for much less exposed systems.

However, tokens have some disadvantages and probably the most significant one is their price. Some other disadvantages are administrative overhead, the need for the user to carry the token wherever they want to access the system. All these problems did not deter some other worldwide banking organisations using them to protect their customers and their business.

So where does the threat to ASB customers comes from and how could PKI help to alleviate it? The threat essentially comes from people that run scams with the purpose to extort (user-names and passwords) from inexperienced users of Internet banking. Last year New Zealand customers of various banks were targeted by phishing attacks. PKI and certificates could be the cheep alternative for the mass deployment of two factor authentication.

3.5. Tacit Group

Tacit Group (bought by Bravura Solutions in 2004) is a case of an average software development company that operates in the international environment. Therefore it is interested in security behind the borders of the company and the country.

As the insurance and financial sector systems providers, Tacit Group has developed particular sensitivity to it's own security, security of their products and their clients' security. Tacit Group represents a perfect organisation to review PKI implementation problems because of several attributes that can be contributed to the organisation (Petranovic, 2004). The organisation employs a highly sophisticated IT work force that represents potential threat to confidentiality and integrity of internal systems and information. Worldwide distribution of the work force requires careful security consideration per each case. Each group operates in a different socio-economic environment, different cultural, legal and political situation. Tacit Group has its employees operating in the clients' premises and vice versa, client developer and analysts operating in Tacit Group premises.

Tacit employs Lotus Notes/Domino and Microsoft PKI solutions. Tacit Group employees are members of the same Lotus Notes domain, which is also one PKI domain with single Certificate Authority on the top of the hierarchy. This enables easy authentication of all communication participants, people or Lotus Notes/Domino servers. All users are issued certificates that also contain private signing and decryption keys. Each certificate also contains a signed public key. All public keys are also stored in Domino Directory i.e. domain address book, that is LDAP compatible. Serious limitation of the Lotus

Notes/Domino PKI represents its relative closed architecture and when deployed as it is, from the box, it cannot expand and interoperate with incompatible systems. The answer to that problem was Microsoft's introduction of PKI into their Windows 2000 platform. That enabled Tacit Group to create another Certificate Authority and publish machine certificates for each computer installed. Those certificates are used for VPN and also encryption of internal sensitive traffic. Even with two PKI products deployed, Tacit Group has further security issues that could be solved with appropriate PKI. Regrettably, those issues are related to lack of proper PKI in New Zealand, Asia-Pacific and the World.

4. New Zealand PKI Issues

The presented above five cases clearly illustrate issues preventing wider implementation of the PKI solutions. Among them are:

4.1. Lack of vision and strategy

New Zealand is a small country with only about four million citizens. This causes huge problems as any sovereign country, regardless of its size, needs to have certain services, institutions and infrastructure to operate. If a country is small and unable to provide required infrastructure and services it is often advisable for it to form alliances with neighbours and countries in a similar position in order to solve some problems. Regrettably, on the PKI issues New Zealand does not co-operate (March, 2003) with the countries that form the core membership of the Asia PKI Forum, even though those countries are the ones leading the way in PKI deployment in the Asia/Pacific region (Tezuka, 2002).

When analysing the problems regarding lack of acceptance, regulation, leadership and interoperability it is not hard to understand why so many countries established their own country organisation that can congregate and represent diverse parties that have interest in PKI developments. Usually such an organisation is called a PKI Forum, but can be also disguised under some other, more generic name. Regardless of the name, the purpose of such organisation is to promote, educate, foster co-operation and standardisation, and generally to bring the individuals and organisations involved with PKI to a common place.

New Zealand does not have such an organisation. The consequences are that there is no common voice representing the PKI community and there is no one that has enough credentials to negotiate and co-operate with international PKI Forums.

4.2. Lack of regulations

Information technology security issues have been increasingly encompassing a legal component as a results of the fact that security professionals are more involved in legal aspects of their jobs. This is because governments around the globe have recognised that protecting computer systems is not enough and that law enforcement is needed to add weight to crimes committed by the use of computers.

Although PKI as a technology could be in centre of attention in a legal case, (especially when non-repudiation issues are involved) there are two other segments of law, which need to take into account when deploying PKIs.

The first segment deals with digital signatures and represents the basis of recognition of signatures that are in an electronic form. In order to recognise digital signatures as legitimate signatures, a country has to pass a Digital Signature Law. New Zealand had been waiting for a similar piece of legislation for five years longer than any other developed country. The New Zealand's Electronic Transaction Act (Electronic Transactions Bill, 2002) was passed by the parliament in 2002.

The major issue of the New Zealand Electronic Transaction Act is that it does not contain a useful digital signature law. The current one is too vague, which might have considerable consequences in legal practice where judges, who are technologically challenged, will have to formulate legal practice themselves on a case by case basis. New Zealand Electronic Transaction Act does not represent an adequate basis for the international co-operation on the legal interoperability projects.

4.3. Lack of funding

Although the authors (of this paper) do not have an insight into the funding issues, ultimately the reasons for lagging behind the developed countries in regard to PKI acceptance and penetration comes to the lack of funding. This is evident through the absence of any marketing efforts or media exposure. To be more precise, the only media exposure to PKI in New Zealand was a negative one. It coloured PKI as an unimportant, non-viable technology that will eventually take off in the distant future.

Because of the lack of funding, it may really happen that for New Zealand PKI becomes a technology of distant future instead of being a contemporary technology.

4.4 Price of PKI

The price of PKI technology has always been one of the usual culprits for the slow PKI uptake. In the past century PKI technology was very expensive and the price of initial setup of a secure Certification Authority was around one million US$. This left many interested parties out of the equation and forced to buy a small number of expensive certificates for important individuals or servers directly from the big commercial providers such as Verisign, Thawte and similar.

SSL, due to the low initial cost of a single certificate, developed to be the most successful PKI application. Relatively small number of commercial Certificate Authorities allowed web browser vendors to include the most important root certificates directly into web browsers or other certificate stores that made the authentication of web servers painless and easy from the perspective of the end user.

For some time it has been possible to acquire the whole PKI systems or components of the PKI i.e. PKT for free or almost free when they get included in products like operating systems or communication tools. This solution is an excellent chance for all the

organizations that feel a need to deploy or experiment with PKI to get hold of fully functional packages or at least some PKI components.

4.5. Feeling safe?

Traditionally, New Zealanders have not been too obsessed with security issues. The island geographical characteristic of New Zealand and thousands of kilometres from nearest neighbours have created a sense of security that is still so prevalent. Unfortunately, with the advent of the Internet the situation has rapidly changed, but the sense of insecurities related to the use of new communication tools did not propagate to most people. Therefore it explains why New Zealanders do not quite understand reasons for adopting the cryptographic methods of protection. The solution for this problem is education initiatives in the form of various security awareness programmes, development of acceptable computer use policies with appropriate enforcing measures, and designing of systems that users will not be able to avoid or sabotage.

4.6. Lack of expertise

Lack of expertise represents probably one of the largest problems for New Zealand. There are many reasons for that and some of them are circumstantial and cannot be changed, but the other ones will be addressed in this short analysis. Those issues are related to the previously mentioned lack of leadership, vision and strategy; lack of participating in the international interoperability projects, lack of legal support etc.

Lack of leadership and strategy results in disorientation and erosion of self-confidence when it comes to tackling the obstacles to further PKI deployment and catching up with the rest of the world in setting up a the framework for global PKI co-operation. Lack of leadership and strategy implicitly leads to the erosion of talented people who would otherwise jump on a train of PKI education, pilot projects and real projects. If the State Services Commission indicates that after a careful evaluation of PKI and a successful completion of the S.E.E. PKI project that there is going to be a ten years delay in implementation. This is because people are not ready to accept it and definitely will result in attrition of the resources to other more promising projects.

Lack of expertise is further showing its effect in the field of legal interoperability, where New Zealand made an effort in creating the Electronic Transaction Act based on models of organisations that do not represent the leading edge in legislative support for e-commerce. As a result of this, New Zealand now has an ambiguous piece of legislation that is effectively inadequate for defining the legal environment for PKI technology. With such a legislation New Zealand is further distancing itself from the rest of the leading e-commerce nations. This is because there is a lack of practical law that would support New Zealand participation in building an effective international legal interoperability framework. Without active involvement in building an international legal framework that would support the international use of the PKI technology, New Zealand will further drift in its irrelevance on the international stage and in its expertise.

5. Appropriate PKI Model

In the initial stages of this project there was an idea to develop a concept or appropriate model of PKI for New Zealand businesses. Thanks to the spiralling nature of the Kolb research model, during the repetitive analysis - synthesis stage, the literature review and especially the case studies (presented above) it became apparent that suggesting a PKI model for New Zealand businesses would not suffice. Not one single business is the same as the other and consequently not a single PKI implementation should be the same as another. The complexities related to PKI implementations guarantee a variety of possible approaches and diversity of PKI solutions that can be implemented. So instead of formulating a nation-wide PKI model we present rather the foundation tenets of a nation-wide PKI system.

6. PKI Foundation Tenets

6.1. Strong Business Case

It is often heard on PKI conferences that no one implements PKI for the PKI sake. What should be heard is that every PKI implementation requires a strong business case. The main reason for that lies again in the complexity of the technology and in the financial and personal commitment necessary to make PKI running properly. Many failed PKI projects in New Zealand point to the lack of strong business reasoning behind PKI deployment. The high profile failure of The Inland Revenue Department PKI implementation represents just good tip of the iceberg.

Only a strong business case can motivate implementers and sponsors of a PKI project to finalise it regardless of the obstacles encountered during the implementation.

6.2. Alternatives Explored

Besides having a strong business case, all viable alternative methods for achieving the same goal need to be explored. This is because sometimes there are acceptable methods for addressing the same security issue with some other technology that might be cheaper or less complex than PKI.

An example for remote authentication can be the very elegant RSA token solution that provides two-factor authentication mechanism by using time synchronisation without deploying digital certificates. Besides being simple to use, RSA tokens are impossible to copy to other media, which is sometimes the problem with digital certificates delivered on removable media.

RSA token works very well when authenticating remote users, but cannot be used for remote authentication of computers. Remote authentication of machines requires deployment of the digital certificates regardless of good authentication purpose (VPN or wireless client authentication for example). RSA tokens would authenticate a remote user when accessing a bank web site to perform a transaction, but not when utilising the VPN technology to connect to an internal bank network. The specific user could still be identified by RSA token, but her machine would require a digital certificate for the remote authentication.

6.3. Required Level of Implementers Expertise

Most of the failed New Zealand PKI implementation cases show that successful implementation of the PKI technology requires considerable theoretical and often practical implementation knowledge. This is regardless of the fact that a particular PKI implementation may be outsourced to an external company.

It is therefore necessary for a certain in-house implementation team to gain sufficient understanding and practical experience by running pilot projects so that possible surprises during a real PKI projects are minimised.

There are cases where even inexperienced users and often inexperienced administrators of a PKI system can successfully survive for some period of time without engaging into understanding PKI. Such cases are related to the off-shelf or plug-and-play PKI products that usually run in their own protected environment or shell. Outside their protected environment, such PKI implementations do not exist or function.

6.4. Scale of PKI Implementation

One of the most often heard complaints about PKI technology is related to the high support costs. Obviously, the larger the scale of implementation is, the larger the support costs are going to be.

300 to 500 PKI users implementations may not require specialised support staff dedicated to PKI only. For such a number of PKI users it is quite viable to train the existing network support staff to effectively execute and support the new PKI implementation over it's lifetime. General network support standards call for one support person per 60 users, but a more complex environment may require a larger support team to effectively deal with user population. Six to ten network administrators can efficiently support this current infrastructure and an additional PKI project during all phases of its lifespan.

It is prudent to involve as many as possible current network staff into a PKI project to serve as a back up for each other in case of any crisis. Many PKI implementations tend to extinguish because the principal driving force or PKI champion decided to leave the organisation.

The numbers of support staff mentioned here may increase with the complexity of the PKI implementation project. An 'off-shelf' or 'plug and play' implementation that operates harmoniously in the background without support may also be considered as an easy support/maintenance solution.

300 – 1000 PKI users implementations, unless extremely simplistic, may call for dedicated support staff. Simplistic implementations such as deployment of machine certificates only, that operate in harmony with Active Directory and the auto-enrolment mechanism, may not require dedicated staff to support them. However, the value of these implementations, which could be especially noticed in the case of PKI failure, may indicate whether additional dedicated staff are required.

For additional security, accreditation or if legal implications are involved, may also require implementation partners. Implementation partners are specifically required if an organisation of that size requires any tailor made solution that lies outside the usual, easy to deploy solutions.

1000 and above PKI users implementations almost by default require external implantation/integration partners. The value of implementations of that magnitude is usually such that specialised integration partners with specific product and technology expertise are necessary to prevent any project deviations and expensive mistakes.

The interaction between internal PKI support staff and integration partners frequently generates a productive environment that has its own controlled mechanisms preventing a project to go astray.

Large implementations are more likely to require more specific and tailored PKI solutions that 'off-shelf' PKI products are unable to deliver. In such situations an additional development and integration capability of implementation partner(s) is absolute necessity and almost always exceeds the capabilities of internal PKI support teams.

In conclusion of the PKI deployment scale discussion, one can notice that small-scale implementations will usually have simple installations or more complex but 'off-shelf' type products with no dedicated staff to support PKI. Large-scale PKI installations tend to have more complex PKI products installed, which are usually adapted to organisation specific needs. Sometimes such implementations require additional development and tailor made solutions that typically call for PKI integration partners. Mid scale implementations could swing both ways depending on the requirements of a business case. They can be simple or complex but the value of the installation calls for dedicated internal staff and sometimes, if the implementation is too complex, for an integration partner.

7. The Choice of Appropriate PKI Product(s)

Once a business organisation has necessary expertise and a strong business case it is required to make a choice of available PKI product(s) or external support. At the beginning of PKI deployment an organisation needs to carefully analyse their business environment and the case for the adoption of PKI technology. The choice of PKI product may depend on the following criteria:

7.1. What sort of PKI applications is the business case calling for?

The question PKI implementers should ask here is whether the business case is calling for a comprehensive PKI solution or a partial PKI - just one or two applications?

7.2. What kind of interoperability is required?

Interoperability is one of the key requirements for some PKI implementations, but there are also many PKI implementations which do not need interoperability at all. All PKI implementations that these authors have seen in the New Zealand environment were

usually partial PKI implementations with limited scope and no interoperability requirements.

7.3. What type of security is required?

When a business organisation is choosing its PKI technology, a considerable thought needs to be given to the security of the PKI operation. Not all PKI operations require the same levels of security as different PKIs are exposed to different levels of risk. Although today all PKIs should follow common guidelines for securing their operations there are ones that protect larger values or more sensitive data.

7.4. Are there any compliance issues?

Similar to the security of PKI operation issues, any business implementation may consider compliance issues with regulatory or accreditation bodies. This may be important for business organisations that plan to run commercial Certification Authority and sell their services to Government agencies and departments. In such cases, commercial Certification Authorities may seek Government (S.E.E.) accreditation. By achieving the accreditation commercial Certificate Authorities may start selling certificates or running Certificate Authorities for Government organisations. The problem here is the cost of the compliance.

7.5. Are there any legal implications?

If a certain organisation - business, educational or governmental - requires a PKI implementation that needs to support legal matters (for example lawyers may sign legal documents using digital signatures provided by PKI) then the PKI designers need to consider an implementation that is able to provide robust support in case a digital signature could be contested in court of law. If a PKI implementation has known bugs and issues that can render a digital signature useless if contested in a court of law then such an implementation must be avoided it is unable to support its primary function.

8. The Choice Integration Partner

If a business organisation does not have the necessary expertise, manpower or simply the PKI implementation is of large scale and external help and auditing is needed, an implementation or integration partner has to be selected.

It is common practice to have the integration partner chosen from the ranks outside the providers of PKI technology. One of the main reasons for separating the supply and integration roles lies in a less biased correlation to the deployed PKI technology of the integration partner.

It is advisable that the integration partner is chosen according to the common criteria from the pool of sufficient number of integrators.

9. Users Training and Acceptance

The user's acceptance of the PKI technology is deeply related to the success of the implementation. It also relates to the awareness of security risks in the environment where a particular business organisation operates.

Prior to any PKI implementation the structure of the user base has to be evaluated and also an appropriate PKI solution selected. For example, if there is expectancy that users may not understand PKI technology and may oppose it, a PKI solution that does not interfere with users needs to be considered. There are such PKI solutions, which operate in the background of the highly successful PKI-enabled applications, that users are not aware of. Usually such solutions are off-shelf or plug and play ones and may not be suitable for certain environments.

Whatever the case is, the user base needs to be respected and involved in the implementation during the initial phases; otherwise a steady opposition may be created which could then result in a complete denial of co-operation usually at the worst moment for implementers.

10. A roadmap to PKI deployment success

From the initial implementation considerations and the entire authors' experience with PKI implementations, and also from the various cases investigated in the analysis stage of this project, it is evident that not even general advice can be produced. Each individual business case not only has different PKI requirements and expectations, but also has very diverse starting points. This make the approach to a particular solution more feasible in comparison to other possible approaches. It is therefore necessary to consider a segmentation of the New Zealand business environment in order to produce a better fit of recommended solutions. Considerable time was spent on contemplating how to segment the business environment and it seems that most differences would emerge if the segmentation was done by size of organisations, comprehensiveness of the sought PKI solutions and interoperability requirements.

It is evident that larger organisations with stronger financial power are in the best position in regard to the technical decisions they need to make. Such organisations do not need to calculate between various inexpensive solutions. Instead, they can define precisely what they need and go for the best-fit solution that can be supported and additionally customised with the help from the integration partner. Large organisations face several concerns in the areas of proper definition of the business case, proper selection process for the integration partner and proper selection of the solution provider. The stakes in those areas are high simply because the bill presented at the end of the PKI implementation project could be within the range of several million New Zealand dollars.

The challenges that small business organisations face when they need to deploy PKI solutions are less in the financial area and area of selection of a competent integration partner and appropriate solution provider, but more in the technical area of selection of an appropriate product that will fit the description of their PKI business case most closely. The small organisations or PKI implementations designed to serve small number of users do not have the luxury of engaging with integration partners; they may not even be able to dedicate enough internal resources to the PKI project. And that is precisely where most New Zealand businesses find themselves and where the biggest PKI deployment risks

exist. The fate of a small PKI project may be best described as a deployment of cheep and inflexible PKI solutions with little or no real support.

Medium sized business organisations and medium size PKI projects find themselves in limbo between fully blown projects and small implementations, the position that is characterised with uncertainties related to both small and large projects. Depending on the actual size of the implementation and available funding, medium PKI projects are able navigate between various solutions, solution providers and integration partners. If a project budget or its size is on the lower end, a midsize project may just call for dedicated in-house PKI support staff but without technology extravaganza. Low-end midsize PKI projects may still be limited to relatively cheap and inflexible 'off-shelf' products, OS integrated solutions or even partial Open Source products.

One of the usual unfortunate situations that midsize companies and midsize PKI projects face are the ties with PKI solutions deployed in the past while these were small growing companies. Such situations may severely limit manoeuvring space of new designs and impose stringent limitations of choices for PKI designers, especially if some sort of backwards compatibility is sought after.

Another problem midsize projects may face is related to the situations where two smaller business organisations or two current PKI implementations are to be integrated. For any PKI Implementer such situations can represent a nightmare.

11. Conclusions

Majority of countries are going ahead with PKI deployment, solving interoperability and other obstacles on their way. Asia, the New Zealand's immediate business partner, is integrating their PKI efforts around the Asia PKI Forum, an organisation that deals with technical, operational and legal issues between countries. There is a clear plan, vision and leadership in the Asian PKI efforts. It appears that precisely that attributes lack in New Zealand.

It is now time to change this wrong attitude. This research presented analysis of the current situation in New Zealand and formulated a roadmap to these changes, including usage of a set of approaches geared towards the possible size of PKI projects. On the lowest end we recommend implementation of an off shelve systems, while at the top end customisation of a specialised PKI products using adequately trained groups of specialists.

References

ADHB. (2004). Auckland District Health Board Web Site. Retrieved 31/03/2004, 2004, http://www.adhb.govt.nz/

ASB. (2004a). ASB Bank Internet Banking Security. Retrieved 20/07/2004, http://www.asb.co.nz/story618.asp

ASB. (2004b). Mobile Banking - Fastnet Mobile. Retrieved 20/07/2004, http://www.asb.co.nz/section375.asp

Electronic Transactions Bill. (2002). Retrieved 07/05/2004, http://www.med.govt.nz/irdev/elcom/transactions/bill/bill.pdf

Irving, J. (2004). Network Manager: Auckland District Health Board, Internal document.

March, F. (2003). APEC TEL 26: New Zealand Delegation Report. Retrieved 04/05/2004, http://www.med.govt.nz/pbt/telecom/apectel/no-26.html

Petranovic, V. (2004). Network and Security Manager: Tacit Group Limited, Internal document.

State Services Commission. (2000). E-Government - A Vision for New Zealanders. Retrieved 03.04.2004, 2004, http://www.e-government.govt.nz/programme/vision.asp

State Services Commission. (2001). S.E.E. PKI Scope. Retrieved 03.04.2004, 2004, http://www.e-government.govt.nz/see/pki/scope.asp

State Services Commission. (2003a). S.E.E. - Secure Electronic Environment. Retrieved 03.04.2004, 2004, http://www.e-government.govt.nz/see/index.asp

State Services Commission. (2003b). S.E.E. PKI. Retrieved 03.04.2004, 2004, http://www.e-government.govt.nz/see/pki/index.asp

State Services Commission. (2003c). SEEMAIL. Retrieved 04/04/2004, 2004, from http://www.e-government.govt.nz/see/mail/index.asp

Tezuka, S. (2002). Achieving PKI Interoperability - An Experiment between Japan, Korea and Singapore and Future Plans. Paper presented at the Second Asia PKI Forum Symposium, Tokyo.

Webb, D. (2003). Technical Director: Digital Identity, Internal document.