Proposed Model for Outsourcing PKI

PKI could make a comeback as an outsourced service with the right method and roadmap.

BY CHRISTOPHER McLAUGHLIN AND DR. GERAINT PRICE

Royal Holloway University of London

Produced by the Information Security Group at Royal Holloway, University of London in conjunction with TechTarget.

ABSTRACT

Public Key Infrastructure (PKI) is often referred to as a pervasive substrate - the technological layer that permeates the entirety of the organisation on which PKI services are established. From the mid 1970s when Whitfield Diffie and Martin Hellman published their paper New Directions in Cryptography [1] the concept of public key cryptography - for the first time - allowed two entities with no previous relationship to communicate information securely over unsecured channels. PKI provides the infrastructure that allows public key cryptography to function within a hierarchical structure, providing an acceptable level of trust between two entities. Outsourcing is the process of acquiring sources or services from an external source. Our model brings together the concepts of both PKI and the outsourcing model, allowing any organisation to outsource a PKI system within the scope of the businesses strategic goals and objectives. Our proposed model takes into account the need to use existing models, procedures and practices in support of an outsourced PKI model. These include processes to ensure that any outsourced solution adds value to the organisation, and that there is a business plan that allows the alignment of the outsourced PKI to support the overall strategic plan.

Christopher McLaughlin
Security Consultant, Accenture

Dr. Geraint Price
Information Security Group
Royal Holloway, University of London

Proposed Model for Outsourcing PKI

1 INTRODUCTION

PKI and outsourcing are phenomena that gained widespread industry exposure in the 1990s. Both were regarded as ways to allow organisations to cut cost and use new technologies to gain business advantage. Whilst outsourcing took off, PKI failed to make an impact due to the cost of setting up the system and the requirement for skilled staff, which at the time were few and far between. The failure of PKI can be shown by the problems encountered by Baltimore Technologies which was a company valued at £7 billion at the height of the dotcom

This article was prepared by students and staff involved with the award-winning M.Sc. in Information Security offered by the Information Security Group at Royal Holloway, University of London. The student was judged to have produced an outstanding M.Sc. thesis on a business-related topic. The full thesis is available as a technical report on the Royal Holloway website http://www.ma.rhul.ac.uk/tech.

For more information about the Information Security Group at Royal Holloway or on the M.Sc. in Information Security, please visit http://www.isg.rhul.ac.uk.

boom, to a company with only £25 million in cash in 2003[2]. At a share meeting in Dublin, Baltimore's PKI technology was sold to beTRUSTed, a PWC subsidiary, with its core software security business sold to UniCert. The downfall of Baltimore Technologies was not entirely of its own making but the failure of PKI to take off. This was due to the difficulty and cost of implementing PKI, and the lack of requirement from businesses of such an expensive overhead.

It now seems that outsourcing in many industries is falling out of favour amid complaints about poor service. Many UK banks, building societies, and service providers have brought some of their outsourced activities back into the business. PKI on the other hand has been proven to have solid business applications and cost benefits. According to the European Association for E-identity and Security (EEMA) at their EEMA UK Regional Interest Group meeting titled Management and Application of PKI in Corporate Environments, a consensus was reached by the 26 delegates that:

"The fact that the benefits of strong PKI across many business applications outweigh the cost of the PKI infrastructure management; and that PKI is not just about securing things, it is also an enabler for new, cost-effective, efficient, business processes which were hitherto not feasible because of security risks, legislation etc"[3]

This view is supported by Stijn Bijnens, Senior VP Identity Management, CEO Ubizen. In a presentation to the Leuven Security Excellence Consortium, IT Security Congress [4], Bijnens discussed the general implementation problems of PKI in organisations during the dotcom boom. He also discussed the resurgence of PKI due to the renewal of interest by Governments keen to pursue ID card schemes, whilst at the same time, applying pressure to commercial organisations to meet compliance requirements. PKI still has its opponents and one of the most outspoken is Bruce Schneier. In a paper co-written with Carl Ellison, entitled, "Ten Risks of PKI: What you're not being told about Public Key Infrastructure."[5] Schneier and Ellison discuss organisations' failure to understand the risks associated with PKI, and accuse the computer security industry of "the year of the…" syndrome. It says that every year a new technology or product emerges that is hailed as the new fix for an organisation's woes and argues

It now seems that outsourcing in many industries is falling out of favour amid complaints about poor service.

that PKI is one such technology. The paper refutes the argument that PKI is essential in order for e-commerce to flourish. In reality the e-commerce market without PKI has flourished with the value its value in 2005 estimated at $8.5 trillion[6]. But with greater public awareness of the dangers of identity theft and credit card fraud, businesses have to provide a solution and PKI is a tool that can help to combat these threats. In our opinion this will only occur when the benefits of a PKI outweigh the cost, which is a view supported by Stijn Bijnens and the EEMA.

2 PROPOSED AB-5C MODEL

Our proposed model is designed as a new process for anyone carrying out PKI outsourcing activities and has a set of baseline standards that have to be met. It is a method of analyzing aspects of the selection and definition of and outsourced PKI solution. The main sections of the AB-5C Model are:

- (A) – Adding value to the organisation.
- (B) – Business strategy.
- (5C) – Competencies, Conditions, Culture, Continuity and Change.

The model we propose defines the importance of adding value to the organisation, details the strategy that the organisation uses when planning an outsourced PKI and defines a set of variables that have to be met by any outsource provider.

2.1 Adding value to the organisation

The key success factor of an outsourced solution has to be that it adds value to the organisation by meeting, or exceeding, the business goals laid out by senior management.

By deciding to outsource, senior management have to understand that the commitment involved is not necessarily limited to a cost-cutting exercise; the CEO and board have to ensure that the solution is backed by senior management with the correct level of funding. Being realistic about the benefits of an outsourced PKI solution is important when meeting the expectations of stakeholders. PKI is a technology solution in support of the business goals and objectives and not a quick fix - it should not be implemented just because the technology is available.

2.2 Business Strategy

Strategic planning is not a solitary discipline

Being realistic about the benefits of an outsourced PKI solution is important when meeting the expectations of stakeholders.

and has to be looked at from different views in order to understand the processes and consequences of long-term decision-making for the organisation. There are four common views to look at when determining strategy - the futurity of current decisions; processes; philosophy; structure.[7]

The futurity of current decisions looks at the cause and effect of decisions over a pre-agreed period of time, allowing management to adjust the planning considerations accordingly and to factor in any alternatives that need to be considered.

The process view starts with the setting of the organisation's aims and objectives and defines the processes, policies, guidelines and strategies to support the achievement of those aims and objectives.

The philosophical view is not a strict process-driven view but a thought-driven process that guides decision-making.

Finally, the structural view determines the various models that strategic planning can follow, such as centralized, de-centralized and devolved structures with each of the organisation's strategic planning streams coming together to form the organisation's overall strategic plan.

2.3 Competencies – Defining the Enterprise Security Architecture

In our model, the method used for measuring competencies is based on the Sherwood Applied Business Security Architecture (SABSA), which itself is based on the Zachman Framework.[8] There is no direct correlation between SABSA and PKI, but as an Enterprise Security Architecture its principles can be adapted to a PKI deployment. SABSA is characterized by the fact that all decisions are derived by analyzing the business requirements for security of an organisation. This methodology makes the SABSA model very desirable when defining an enterprise security architecture for outsourcing PKI both for the organisation, its outsource partner and the alignment of the organisation's competencies. The SABSA operational security architecture is based on a six-layer model which is the basis of a process-led methodology for creating security architectures.[9] The operational security architecture spans five layers which are the:

Contextual layer – Describes business policy making, business risk assessment processes, business. Requirements collection and specification, organisational and

There are four common views to look at when determining strategy - the futurity of current decisions; processes; philosophy; structure.

cultural development,

Conceptual Layer – Major programmes for training and awareness, business continuity management, audit and review, process development for registration, authorization, administration, incident handling, development of standards and procedures,

Logical Layer – The logical layer encompasses the security policy making, information, systems classification and management of security services. It also defines the security of service management, negotiation and interoperability standards for security services. An important aspect of the logical layer is that it defines how to provide an audit trail and monitoring and innovation of actions.

Physical Layer – Development and execution of security rules, practices and procedures – including: cryptographic key management; communication of security parameters between parties; synchronization between parties; Access Control List (ACL) maintenance and distributed Access Control Entry (ACE), backup management (storing, labelling, indexing), virus pattern search maintenance, event log management and archiving.

Component Layer – Products, technology, evaluation and selection of standards and tools, project management, implementation management, operation and administration of individual components.

2.4 Conditions – Modelling Outsourcing based on PKI Requirements

This part of our model looks at the modelling of organisational outsourcing based on the requirements of PKI within the organisation. It takes a qualitative approach and forms the basis of the model by being an integral part of the common operating environment between the organisation and the outsource partner. The requirements are developed by a composite project team made up of people from the organisation and the outsource partner with a strict governance hierarchy in place to ensure that the outsource partner can provide the PKI requirements and also to ensure that the implementation meets the organisation's business goals and objectives.

The method for qualitative analysis of conditions will encompass the following:

- PKI Enabled Services

- PKI Application Enablers
- PKI Business Drivers
- PKI Supplier Provisions
- PKI Deployment Considerations
- PKI Operational Considerations
- PKI Information Dissemination
- PKI Trust Models

We propose a theoretical model that will provide organisations with criteria to qualitatively assess each of the above conditions. This model will allow the composite project team from the organisation and outsource provider to determine the ability of the business to meet their goals and objectives with regard to PKI. Each condition is graded Low, Medium or High with a base score attached to each:

- Low (Base Score 0.0-3.9) – The condition is not required to meet the business goals and objectives.
- Medium (Base Score 4.0-6.9) – The condition is not required but may assist in meeting the business goals and objectives.
- High (Base Score 7.0-10) – The condition is a mandatory requirement in meeting the business goals and objectives.

The composite project team assigns the qualitative value for each of the conditions depending on the extent to which:

- it adds value to the organisation
- it is aligned with the organisation's business strategy.
- it meets the competencies required by the organisation.
- it meets other requirements laid out by the organisation.
- it is in cultural alignment with the organisation and the outsource provider.
- it provides for continuity of operations
- it allows for the organisation to retain management control during periods of change.

After the initial Low, Medium or High grade has been assigned, the capability for each condition is then assigned a base score for a weighted factor analysis and plotted on a graph to illustrate the importance of the condition to the organisation. For instance, having multi-factor authentication has a high base score of 9.6 as it is a mandatory requirement for meeting the business goals and objectives of the organisation.

This process gives the composite project further detail in which to support the analysis of the most suitable condition in meeting the organisation's goals and objectives. A full example of this process can be found in the thesis, Section 4.7.

1.1 CULTURE – ALIGNING ORGANISATIONS FOR STRATEGIC PARTNERSHIP

Any organisation selecting an outsource partner needs to ensure that the culture of both organisations is properly aligned. For our model we have used the Seven-S Model [10] developed by McKinsey & Company in the 1970s. This model was originally developed for analyzing the culture and behaviour of organisations but can be adapted to organize a company in a holistic and effective manner.

The model is split into two parts. The first contains the hard S's - strategy, structure and systems - which are the core business functions of the organisation and are "hardwired" into the organisation. The second part – the soft S's, the skills, shared values, style and staff - deal with people in the organisation, how they interact with one another, the skills they possess and the style in which they carry out their tasks. Each of the seven S's are briefly described below:

Structure – One of three models: centralized, decentralized or devolved.

Strategy – The direction and scope of an organisation over the long term, which achieves advantage for the organisation through configuration of resources to meet the needs of the markets and meet shareholder expectations.

System – The organisation's system defines the formal and informal procedures by which an organisation operates and gathers information. A system is used to create a culture of innovation from existing innovation within the organisation.

Shared Values – The organisation's shared values are the guiding concepts that are not normally part of the organisation's goals and objectives. Shared values are the core ideas on which the organisation was founded and form the fundamental principles that will allow everyone in the organisation to feel as if they are working towards the greater good.

Skills – The skills that are present in the organisation's staff are crucial to the

Any organisation selecting an outsource partner needs to ensure that the culture of both organisations is properly aligned.

success in meeting the goals and objectives of the organisation. Having the right people, with the right skills on the right projects will provide a platform for success.

Style – The organisation's style is the leadership approach of top management and the organisation's overall operating approach. It is also the way in which the organisation's employees present themselves to clients, suppliers and the outside world.

Staff – Staff in this context also deal with all human resources issues such as recruitment, integration, training and the provision of continual career development.

1.2 Continuity – Ensuring Effective Continuity of Operations

Continuity management is the process by which plans are put in place and managed to ensure that services can recover quickly and effectively from any incident. This is paramount to the organisation's success, as customers want an uninterrupted service – for every minute systems are down money is lost and reputation damaged. [11]

For our model we propose the use of ITIL Service Continuity, their mission statement:

"Support business continuity management functions by ensuring that IT services can be recovered in the event of a major business disruption within required timescales." [12]

The most critical aspect of the mission statement is that the IT services affected are recovered within agreed timescales. This will have been defined in any contract between the organisation and the outsource provider. ITIL aims to achieve this by covering all of the major business functions of the organisation with IT services continuity plans and ensuring that these plans are thoroughly audited and tested – from this it is possible to determine realistic timescales for recovery.

1.2.1 Incident Management

For our model, we have designed two flowcharts for incident management processes. The first is the initial incident management flow process. A full example of this process can be found in the thesis, Section 4.9.2. This deals with the response of the organisation for the initial incident to the resumption of the system back to its normal state.

Continuity management is the process by which plans are put in place and managed to ensure that services can recover quickly and effectively from any incident.

The second process we have developed is the post-incident review procedure. This deals with the review of the procedures taken during the incident and analyses the processes to ensure that they were carried out effectively and that any lessons learnt from the incident can be incorporated into the initial incident flow process.

1.3 Change Management – Strategy for Technological Change in Outsourcing

Change management is a key area where the organisation has to ensure that their selection of strategic outsource partner allows for change to take place seamlessly in order to continually meet the organisation's goals and objectives. Change management activities are an important aspect of outsourcing. Too often outsource partnerships are entered into and the organisation finds that it has lost management control. This often hinders, if not completely prevents the organisation's ability to adapt to technological change and allow them to meet their strategic objectives. Having change management specialists as part of the project team is essential in

"Recognizing the risks associated with studying and implementing a transformation tool such as outsourcing and assisting in creating an environment in which such an initiative can be successful." [13]

For change management we use the framework proposed in a PA Consulting Sourcing Interest Groups New York Regional Meeting when a framework for outsourcing and outsourced-enabled change was introduced. In the presentation one of the topics discussed was how often change occurs within an organisation and the statistics are as follows:

"89% of organizations make changes to their organizations with 65% changing their business processes, 78% implementing new IT Systems and 14% carrying out other change initiatives, if an organization outsource key systems and then are unable to manage these systems then the core business of the organization will suffer, affecting not only profitability but also the organization's reputation." [14]

The components of the PA framework are:

- Building a compelling case for change – building a business case within the strategy of the business.
- Engaging change leaders at every level – building commitment amongst leaders

Change management activities are an important aspect of outsourcing.

- Winning the commitment of critical stakeholders – identify and engage stakeholders
- Designing the business to deliver what is important – agreement of future business architecture
- Driving the programme – designing a high level programme for governance

All of which provide the following benefits:

- Tangible benefits to the business
- Reduction in risk and complexity
- Sustainability – building a compelling case for change which is supported at all levels
- Delivery based on sound information which is relevant to the business

2 CONCLUSION

Our model brings together existing models, processes and methodologies as well as our own thoughts on some of the areas that businesses have to understand in order to successfully outsource its PKI. In fact this model can be adapted for any technological outsourcing activity. The thesis introduces some of our own concepts into the model such as the common operating environment. This is the area in which both the business and outsource partner interact and is built by aligning the organisation's strategic goals with the competencies of the outsource partner based on a shared culture and strategic objectives. The value of having a common operating environment in our model is explained in Section 4.11 of the thesis.

Section 2.17 details how an instrumental component for the success of an outsourced PKI is the necessity to treat the outsource partner like a TTP (trusted third party) in order to maintain some the protection of the company's sensitive information. The trust that is formed between the entities during this process is the basis for the common operating environment. Gauging the competencies of the outsource partner is an important aspect of ensuring that the model is utilized effectively. For this we have incorporated the SABSA model for the analysis of the business requirements to provide the security architecture is paramount. The operational security architecture provides a process-led methodology for the creation of the security architecture. Our model allows the organisation to map competencies against a recognized and widely used model to ensure the outsource provider has the correct competencies to allow the organisation to meet its strategic business goals and objectives.

The conditions that are laid down for successful strategic partnership between the organisation and the outsource partner come from the decisions made by the composite project team. These decisions are based on a qualitative approach with the experience of both parties with the following taken into consideration:

- Feasibility
- Cost effectiveness
- Meeting client requirements
- Capabilities of the outsource partner
- Meeting the goals and the objectives of the organisation

It is imperative that any outsource arrangement has effective continuity management which ensures that plans are put in place to recover services should an incident occur. It would be wise to use an existing, standardized method for doing this as it has been thoroughly tried and tested. ITIL provides a good system to enable organisations to recover within an acceptable timescale either by countering the incident or using a standby partner to run the services.

Our model aims to add value to the organisation whilst maintaining the integrity of the business strategy. It also takes careful consideration not only of the technical or process aspect of outsourcing PKI but also the culture of the organisations involved in the outsource partnership. This model is only the beginning in the road to develop a robust set of processes for outsourcing PKI which is effective, affordable and relevant to the needs of the business community.*

Ron Condon

UK bureau chief
searchsecurity.co.UK

Ron Condon has been writing about developments in the IT industry for more than 30 years. In that time, he has charted the evolution from big mainframes, to minicomputers and PCs in the 1980s, and the rise of the Internet over the last decade or so. In recent years he has specialized in information security. He has edited daily, weekly and monthly publications, and has written for national and regional newspapers, in Europe and the U.S.

3 REFERENCES

[1] Whittfield Diffie & Martie E. Hellman, 1976: New Directions in Cryptography. Found at http://crypto.csail.mit.edu/classes/6.857/papers/diffiehellman.pdf

[2] M. Loney. Baltimore's death spells gloom for PKI. ZDNet UK. 2003. Found at. http://news.zdnet.co.uk/security/0,1000000189,39118180,00.htm

[3] EEMA UK Regional Interest Group meeting 2007: The management and application of PKI in corporate environments. Found at http://www.eema.org/index.cfm?fuseaction=events.content&cmid=337

[4] S. Bijnens. Why PKI is getting a second chance. Leuven Security Excellence Consortium. IT Security Congress. Found at. http://www.l-sec.be/calit.htm

[5] B. Schneir & C. Ellison. Computer Security Journal, v 16, n 1, 2000, pp. 1-7 Ten Risks of PKI: What you're not being told about Public Key Infrastructure.
Found at. http://www.schneier.com/paper-pki.html

[6] OUT-LAW News. B2B e-commerce to reach $8.5 trillion in 2005.
Found at. http://www.out-law.com/page-1470

[7] G. A. Steiner. Strategic Planning – What Every Manager Must Know. Free Press Paperbacks. Simon & Schuster. 1997. (p. 13-15)

[8] The Zachman Framework. Found at www.zifa.com

[9] SABSA Overview.
Found at www.sabsa-institute.org/the-sabsa-method/sabsa-overview.aspx

[10] The Seven S's: Framework for Analyzing and Improving Organisations.
Found at: http://www.1000ventures.com/business_guide/mgmt_inex_7s.html

[11] The Seven S Model: A Managerial Tool for Analyzing and Improving Organisations.
Found at. http://www.1000ventures.com/business_guide/mgmt_inex_7s.html

[12] Continuity Management. ITIL & ITSM World.
Found at http://www.itil-itsm-world.com/itil-8.htm

[13] Open Guide. IT Service Continuity Management: Continuity Management / Disaster Recovery / Business Continuity. Found at http://www.itlibrary.org/index.php?page=IT_Service_Continuity Management

[14] PA Consulting. Sourcing Interest Groups New York Regional Meeting. 2005.
Found at
http://www.sourcinginterests.org/Regional%20Presentations/2005NewYork/Delivering%20Change%20Through%20Sourcing%20by%20PA%20Consulting%20-%20NY%20v2.pdf