

An OASIS PKI White Paper

Guidelines on how to determine Return on Investment in PKI

By Stephen Wilson (Lockstep Consulting)
for the Oasis PKI Education SC

Version 1.4, 28 June 2005



OASIS (Organization for the Advancement of Structured Information Standards) is a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards. Members themselves set the OASIS technical agenda, using a lightweight, open process expressly designed to promote industry consensus and unite disparate efforts. The consortium produces open standards for Web services, security, e-business, and standardization efforts in the public sector and for application-specific markets. OASIS was founded in 1993. <http://www.oasis-open.org>

The **OASIS PKI Member Section** fosters support for standards-based, interoperable public-key infrastructure (PKI) as a foundation for secure transactions in e-business applications. The OASIS PKI Member Section brings member organizations together in a neutral setting to increase knowledge about PKI and to initiate studies and demonstration projects to show the value of interoperable PKI and PKI-based solutions. The group collaborates and cooperates with appropriate standards and testing bodies to promote the adoption of open industry standards. <http://www.pkiforum.org>

Acknowledgements

This work was compiled with the valuable assistance of June Leung, Steve Hanna and the OASIS PKI Education Subcommittee. The input of Anders Rundgren towards the framework for understanding ROI is recognized in particular. This work is an evolution of the original ROI white paper from The PKI Forum, written by Derek Brink [1].

Executive summary

IT managers are under increasing pressure to deliver clear Return On Investment (ROI) figures. ROI is notoriously difficult to compute for IT infrastructure in general, and leading edge technologies like PKI in particular, where costs are easier to quantify than benefits. Yet in order to mount a robust business case for PKI, we must speak the language of all executive stakeholders, including financial managers. And this means we need ways to work out and talk about the ROI.

Here we provide a simple, practical framework for separately calculating the benefits and the costs of deploying PKI technologies and/or services in the enterprise. Costs are best understood in terms of a *digital certificate supply chain*, with a number of independent elements each able to be implemented in various ways, with differing associated expenses. The framework accommodates a wide range of contemporary PKI variations, including outsourced versus insourced CAs, thin client or fat client end user application environments, and the full range of private key media. The paper also provides a brief survey of some of the recent research done on e-business and infrastructure ROI.

An overview of recent ROI research in IT

In recent years, with demands for expenditure on the rise and technology cycles shrinking, IT managers have been increasingly called upon to deliver clear Return On Investment (ROI). Most organizations invested heavily in Internet and e-business systems throughout the 1990s. Towards the end of the decade, a litany of disappointing results had piled up around large IT projects. Applied Materials, Dell, Dow Chemical and Mobil were among many corporations whose managers were publicly critical of large scale enterprise technology investments [2].

After the technology bubble burst, even mainstream IT activities came under heavy scrutiny. And so, a simple reality of the current business climate is that leading edge technologies can be extremely difficult to cost-justify. And when they have had a chequered history as has PKI, the challenge of demonstrating a clear ROI is great. Yet it is a challenge that must be met *precisely because* of our tougher business environment.

ROI is a complicated matter in PKI and other types of e-business infrastructure because, as one researcher puts it, “e-business inter-organizational investments are deployed across multiple platforms, projects, vendors and partners” [3]. Conventional accounting methods are often blind to intangible benefits, and can be overly sensitive to old fashioned measures of productivity. For example, if a bank measures productivity according to the number of checks it processes, and if it has no metrics for customer convenience, then it might find paradoxically that automatic teller machines have a negative ROI because they displace checks [4][5].



In short, it is usually easier to measure cost than benefit. But instead of trying to tackle the measurement problem head-on, technologists often try to justify leading edge developments as “strategic”. There is of course some sense in this. New technologies often cannot be analyzed in conventional ways. Sometimes it is only the uncanny judgment of a visionary that brings the “Next Big Thing” to fruition, for the benefit of their organization. But can we rely on the hunches of visionaries? Do we know how often they are wrong? And should IT managers be immune to quantitative business analysis? Of course not. Some commentators have taken the strategic mode of argument to its logical conclusion, arguing that ROI itself is irrelevant [6]. This is a bold, politically charged strategy, which should not be tried out lightly on incredulous senior executives!

Advocates must take care not to get overly optimistic (or just plain lazy) in their arguments for PKI investments. Cynics have come to read the label “strategic” as code for ‘not measurable’ or ‘best guess’. And we must be willing to have our business proposals scrutinized by accountants and economists – so long as the analytical tools are fair. Indeed, if PKI really is important to many enterprises, then we should expect its benefits to move from strategic to truly quantitative at some point, and so become measurable.

The approach to determining ROI from PKI projects outlined in this paper is pragmatic and flexible. In Part 1 we outline the various ways in which PKI can deliver financial benefits, under three different headings, with specific suggestions for quantifying savings and/or new revenues. In Part 2, we describe a detailed framework for counting the cost of PKI.

PART 1: Quantifying the benefit of PKI deployment

There are three different types of financial return that can be quantified in order to estimate ROI in any given PKI deployment. Not all of these types of return will be applicable in each PKI project. The three types of return are described below, and illustrated using a number of “mini case studies”.

1. Savings (or new revenues) from PKI-enabled Business Process Re-engineering

The most powerful justifications for PKI tend to arise from risk analyses showing that a particular new e-business system requires the certainty of persistent digital signatures. The classic examples involve the paperless re-engineering of existing business processes, in complex environments with relatively high legal risks, and/or multiple relying parties. PKI is an enabler – because without the certainty of digital signatures, the organization could not bear the risk of these types of transactions – and in calculating ROI, most of the benefit can be attributed to the PKI investment, for the purposes of calculating ROI. In many re-engineered business processes, substantial savings are easily computed in respect of transmission, handling, copying and filing costs.

Mini case study: Electronic property conveyancing

The Australian state government of Victoria has developed an online system called Land Exchange for settling the buying and selling of real estate, the legal aspects of which are collectively termed conveyancing [7]. Land Exchange involves an electronic deed of title for the land, which is secured using digital certificates issued to various parties to the transaction. In its business case analysis, the government noted that “industry alone is estimated to absorb additional costs of around AU\$200 million p.a. that relate to such inefficiencies [from paper-based land transactions]” [8]. Electronic conveyancing is forecast to provide direct savings of AU\$70 per transaction for vendors and purchasers, and an overall saving to industry of AU\$33 million p.a. by 2010, assuming 66% of transactions are done electronically by that time.

The cost of conducting paper-based business can be analysed bottom-up through time-and-motion studies. However, this can be an exhausting exercise in itself. Sometimes the gross cost of paper processing can be more quickly figured from the top down:



Mini case study: Electronic company returns

The government of an Asian nation has modelled the cost savings of converting its paper based system of annual company returns to electronic filing, secured by digital certificates. Several million registered companies are currently required to lodge an annual return confirming details of their directors, office locations and so on. An agency comprising over 400 staff is dedicated to processing paper returns. The bulk of the salary cost and overheads represents the potential cost savings from moving to PKI-enabled electronic filing.

To calculate the benefits of PKI-enabled Business Process Re-engineering, consider the following questions:

- ❖ What costs are associated with processing paper based transactions?
- ❖ Which costs are likely to remain with online processing?
- ❖ Can all paper related costs be lumped together to ease the calculation?
- ❖ Does the business require long term secure storage for large volumes of paper?
- ❖ What proportion of paper-based transactions may go online, and when?
- ❖ What fixed cost will persist, even if a small proportion of transactions remain paper based?

2. Financial savings (loss reduction) from improved security

In applications where PKI is deployed to improve security, it should be possible to calculate the loss reduction. It may be rare for digital certificates to figure prominently in the prevention of hacking and overt cyber crime; these problems demand complex, multi-faceted responses, often without involving PKI at all. However, PKI is clearly valuable in fighting white collar crime and various types of fraud. Digitally signed e-mail is now an important tool for preventing impersonation and for maintaining a high quality audit trail around critical management processes. Of course, fraud will never be eliminated, yet in some cases an extra benefit may come from PKI lowering the cost of investigation, or making it easier to re-wind a wrongful transaction. High quality evidence of 'who did what to whom' is available directly from digital signatures, whereas traditional IT forensics can be expensive.

Mini case study: prosecuting a case of fraudulent e-mail

Within a major US corporation there was a long running, increasingly spiteful rivalry between two senior executives, one male, the other female. The woman tried to undermine the man by faking an e-mail, purportedly from him, making derogatory remarks about her. The other directors suspected foul play and hired IT forensics specialists from a Big Four firm to retrieve evidence from mail servers and PCs to establish what really happened. Eventually, the woman's plot was exposed and she resigned before the matter got to court. The investigation took six weeks and cost over US\$200,000 in consulting fees alone.

If senior executives were required to use digitally signed e-mail, this type of fraud would be easier to trace, cheaper and quicker to investigate, and more difficult to perpetrate in the first place.

Mini case study: stock exchange announcements

Publicly traded companies are required by law to announce certain types of matters to their stock exchange in a timely manner. Fraudulent bad news created by a company's rivals can be used to manipulate share prices. In some places, company announcements are transmitted to the stock exchange by faxes bearing unique bar codes issued by the exchange to each listed company. The bar codes often come in the form of a roll of self-adhesive labels. If the labels are stolen or duplicated, then the company is vulnerable to fraud. One stock exchange in SE Asia is understood to experience this type of fraud on average once every 18 months. The direct cost of each event runs into hundreds of thousands of dollars, with forensic investigations, public relations, legal costs, and down time. The indirect damage to the company and its share holders can be immeasurably greater.

Several stock exchanges plan to move to digitally signed company announcements, and will issue special digital certificates to listed companies for the purpose (directly analogous to the roll of bad code labels).

Mini case study: investigating a major insurance scam

In 2000, the insurance arm of a major Australasian bank was defrauded through an organized series of bogus claims made over a lengthy period of time. Much of the evidence involved in the following lawsuit was in electronic form on the bank's mainframes and client-server systems, but could not be directly authenticated because of its age and complexity. The history and origins of the fraudulent claims had to be reconstructed from audit logs and backup tapes, documented, and attested to in court by expert witnesses. A large team of security consultants from a Big Four firm spent over four months on the case, at a cost well in excess of US\$1,000,000 in fees alone.



Mini case study: misdirecting a bank's confidential communications

In a widely publicized case in 2004, the Canadian Imperial Bank of Commerce (CIBC) temporarily stopped using fax machines to transmit confidential client data between branches, after it was found that for several years, funds transfer forms had been mistakenly transmitted, not to the bank's processing centre, but to a scrap-yard. The direct and indirect costs to CIBC of this mishap included reimbursement of losses due to lost transfers, marketing campaigns to restore customer confidence, the lawsuit launched by the scrap-yard owner, the investigation launched by the Canadian Privacy Commissioner, and the switch to couriers from fax. Such disasters can be avoided by encrypted e-mail and PKI, which provides strong controls over the origin and destination of sensitive communications, and ensures in the event of misdirected transmissions, privacy is not compromised.

To calculate the benefits of improved security, consider the following questions:

- ❖ Does your organization have internal data on the cost of fraud events, including expenditure on investigation and prosecution?
- ❖ If a transaction had to be rewound, what would be involved in retrieving the necessary data?
- ❖ Does your ability to rewind become more difficult over time as audit logs get archived to tape or lost altogether?
- ❖ Are sensitive legal issues – such as human resources, mergers & acquisitions or lawsuits – communicated by e-mail amongst senior executives?
- ❖ Are you vulnerable to fraudulent e-mail?
- ❖ In the event of an IT forensic investigation, what would be the cost implications of diverting your internal IT resources?

3. Financial savings (overhead reduction) from improved identity administration

Single Sign On (SSO) type applications utilizing PKI can deliver substantial reductions in administrative overheads, as measured for instance by more efficient user provisioning, or by reduced help desk load for password resets. The benefit is even greater when PKI is implemented in smartcards or USB keys, delivering two factor authentication.

To calculate the benefits of improved Id Management administration, consider the following questions:

- ❖ What is the typical rate of password resets experienced by your help desk?
- ❖ Can reduced help desk load be quantified?
- ❖ How much user downtime is saved in provisioning new users through SSO?
- ❖ Can that time be converted into quantifiable value? For example, if provisioning online customers or road warriors, do they start generating revenue sooner?

- ❖ Can convergent smartcard solutions for Id Management be leveraged for the benefit of other parts of the organization, such as id badges and facilities access?

Special cases of mandated PKI

There are other special cases of cost-benefit realization in certain regulated sectors where PKI has been mandated. For instance, the Singapore Monetary Authority mandates that PKI be used to secure online transactions over a certain dollar limit; if an institution wishes to play in that market, then the investment necessitated by its PKI obligations can be treated simply as a cost of doing business. In Australia, organizations that deal online with the federal government are generally required to use digital certificates, available from a restricted set of accredited service providers, or else set up their own compliant PKI and have it accredited.

An interesting grey area is emerging in several sectors where PKI is not mandated as such and yet it is emerging as the de facto standard. For instance, nothing in the HIPAA regime explicitly requires the use of digital signatures and PKI; neither does the FDA's well known "Part 11" electronic signatures rule.¹ These initiatives are philosophically consistent with the technology neutral approach of the US federal government, including the ESIGN legislation, and leave room for organizations to interpret their electronic signature requirements in the context of their own businesses. However, with the majority of compliant systems turning out to be PKI-based, we are approaching the point where non-PKI systems for HIPAA and FDA purposes will be unusual. For organizations using non-PKI solutions to convince regulators that their systems are workable will start to involve extra compliance costs.

Note that in cases where PKI is an accepted cost of doing business, and not subject to a go/no-go investment decision, the focus on ROI should switch from making the business case for PKI, to ensuring that the money is spent as wisely as possible. The cost framework described in this white paper should be useful for managing expenditure as well as for building business cases.

¹ For example, Part 11 states "While requiring electronic signatures to be linked to their respective electronic records, the final rule affords flexibility in *achieving that link through use of any appropriate means*, including use of digital signatures and secure relational database references. *The final rule accepts a wide variety of electronic record technologies*, including those based on optical storage devices. In addition, as discussed in comment 40 of this document, the *final rule does not establish numerical standards for levels of security or validation*, thus offering firms flexibility in determining what levels are appropriate for their situations." (emphasis added) Final Rule, FDA 21 CFR Part 11 *Electronic Records; Electronic Signatures* Para III.C.3 page 13432; www.fda.gov/ora/compliance_ref/part11/FRs/background/pt11finr.pdf.

PART 2: Estimating the cost of deploying PKI

PKI can be implemented in an increasingly wide range of ways. No single best model has yet emerged; perhaps one never will. However, at this stage of its evolution, PKI generally entails a number of standard elements. We can consider these elements as making up a digital certificate “supply chain”, each of which can be sourced more or less independently. Good advice is widely available on the various options; see for example the Burton Group Technical Position on PKI [9].

Our cost framework looks at each element of the digital certificate supply chain, and breaks down the fixed and variable cost components of each, as follows.

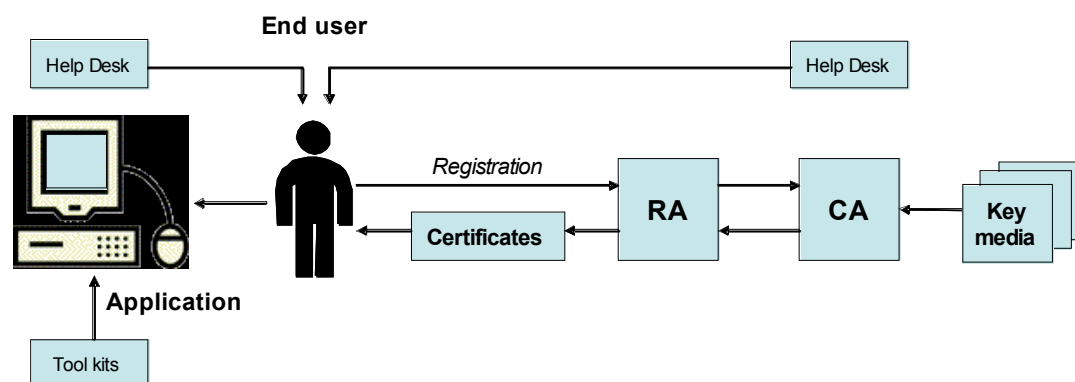


Figure 1: Digital Certificate Supply Chain (showing flows of goods and services)

Application related

All costs associated with PKI enablement of the Application, including planning and designing, ‘shopping around’ for a CA solution, acquiring any necessary PKI toolkits and ‘glueware’, and integrating PKI components with the application. In supply chain parlance, the Application is the eventual ‘consumer’ of certificates, and sits at the end of the supply chain.

End user related

All costs associated with supporting end users, including help desk, education, and the marketing efforts frequently undertaken to promote the benefits of PKI. Note that some costs are borne directly by the user; for example, the user may need to spend time and money presenting in person to a Registration Authority (RA).

Certificates	The cost of certificates themselves. Outsourced CA service providers and CA software vendors usually charge a fee per certificate, which can be paid by application scheme operators on behalf of the users (and possibly passed on) or paid directly by the users themselves.
RA	Costs associated with front-end registration. Internal enterprise RAs operated for example by an organization's HR or customer service department might utilise regular office staff and accommodation, with little or no incremental cost. A bureau style third party RA on the other hand, providing general purpose identity certificates may have significant set-up, infrastructure and staffing costs. Third party RAs may have to make provision (or purchase insurance) to cover potential liability for errors and omissions.
CA	Costs associated with the backend Certification Authority operation. Investment in security, cryptographic systems, infrastructure, personnel, facilities and compliance related activities will be required in line with the risk profile of the PKI's business application, and the scale of the user population. Enterprise CAs supporting internal applications might be implemented using commodity software products and operated within the organization's IT shop. On the other hand, a commercial third party CA could require purpose built facilities, site redundancy, and major independent audits, as well as provision or insurance to cover potential liabilities incurred by the CA operation.
Key media	Costs of the media in which end user private keys are conveyed. Can be close to zero for simple soft certificates, or can entail licence fees for roaming soft certificate solutions. Additional hardware expenses might be associated with certain media like smartcards where readers may be required.

Four types of cost can be identified and need to be estimated to determine the Total Cost of Ownership for a PKI system:

A. Fixed Establishment Costs

B. Variable Establishment Costs

(Note that the initial certificate distribution is counted here as the first instance of an annual certificate cost, because initial registration and renewal are traditionally priced the same).

C. Fixed Annual Costs

D. Variable Annual Costs

The table below outlines the types of costs under each of these four categories, associated with alternate ways of implementing the major supply chain elements.

<i>Element</i>	<i>Deployment</i>	<i>Fixed Setup Costs</i>	<i>Variable Setup Costs</i>	<i>Fixed Annual Costs</i>	<i>Variable Annual Costs</i>
Application As described by the Burton Group, applications may basically be either Fat Client or Thin Client, depending on their required level of functionality [9].	Fat Client	Shopping around for CA solution If applicable, negotiations with external CA Developer training PKI related design (digital signatures, certificate validation, lifecycle management, audit logs etc.) PKI systems integration PKI toolkit licences	Nil	PKI toolkit support fees	PKI toolkit support if licensed according to number of users
	Thin Client	Shopping around for CA If applicable, negotiations with external CA	Nil	Trivial ²	Nil
User related Users' experience of certificates depends on whether they are general purpose certificates from an external CA, or application specific certificates from the enterprise.	<i>General Purpose Id Certificates</i>	Marketing campaign ³	User training Marketing materials	Help Desk (fixed cost component)	Help Desk (variable component) In person presentation to RA Processing revocations due to staff/member turnover Processing revocations due to compromised keys
	App. specific certificates	Trivial ⁴	Nil	Trivial ⁵	Help Desk (variable cost PKI related component) Processing revocations due to compromised keys ⁶

² It is assumed that PKI related operating system patches will be installed as a matter of course during routine maintenance.

³ Typical e-business schemes which use external PKI require a marketing campaign to promote the benefits and encourage users to take up certificates.

⁴ If certificates are well embedded in an application, they should require no promotion as such, and no more training than does the application itself.

⁵ With embedded certificates, no separate PKI help desk is required; the one application related Help Desk will do.

⁶ Revocations due to staff or member turnover represent no incremental cost over and above the enterprise's exit procedures.

<i>Element</i>	<i>Deployment</i>	<i>Fixed Setup Costs</i>	<i>Variable Setup Costs</i>	<i>Fixed Annual Costs</i>	<i>Variable Annual Costs</i>
RA The RA will either be a third party bureau for externally issued identity certificates, or an enterprise RA.	<i>General Purpose Certificates</i>	Nil as such ⁷	Nil	Nil as such ⁸	Liability cover / provision
	OR <i>Enterprise Certificates</i>	RA software licence fee RA hardware Operator training	Nil ⁹	RA software support RA hardware support RA staff cost RA audit	Limited ¹⁰ liability cover / provision
CA The backend CA can be operated by the enterprise or else outsourced; see e.g. [9].	<i>Outsource</i>	Nil as such ¹¹	Nil	Nil as such ¹²	Liability cover / provision
	OR <i>Insource</i>	CA software licence fee CA hardware including cryptographic modules CA facility build / fit-out CP/CPS development User Agreements Operations documentation Legal review & signoff		CA software support CA hardware support Operations staff cost Facility security Facility upkeep Power & services CA audit	Limited ¹³ liability cover / provision

⁷ An external identity certificate service is likely to pass on a proportion of its fixed RA costs (including software licence, annual software support fees, RA hardware purchase, annual hardware support, RA staff cost and audit) in its annual certificate fees, the proportion depending on the total certificate population.

⁸ See note against *Fixed Setup Costs* at left in the table.

⁹ For really big deployments, there may be scale-dependent element of the RA setup cost, if multiple personnel and workstations are needed to service the users.

¹⁰ With enterprise certificates, liability for potential damages caused by the certificates should be subsumed into application related liability arrangements, assuming that the enterprise certificates can be constrained from re-use outside the application.

¹¹ An external identity certificate service is likely to pass on a proportion of its fixed CA costs (including software licence, annual software support fees, hardware, annual hardware support, staff cost, facilities upkeep, and audit) in its annual fees, the proportion depending on the total certificate population.

¹² See note against *Fixed Setup Costs* at left in the table.

¹³ See note against *Variable Annual Costs* above.

Element	Deployment	Fixed Setup Costs	Variable Setup Costs	Fixed Annual Costs	Variable Annual Costs
Certificates		Nil	Nil	Nil	Issuance/Renewal fee
Key media	<i>Soft Certs</i>	Nil	Nil	Nil	Nil
Private key media will be selected according to the risk profile of the application, the exposure to identity theft, and degree of sophistication of the user environment	OR <i>Roaming Soft Certs</i>	Up front license fee	Nil	Nil	Roaming solution licence Incremental help desk load ¹⁴
	OR <i>USB keys</i>	Nil	Per USB key cost	Nil	Replacement of a proportion of lost & damaged keys
	OR <i>Smartcards</i>	Nil	Per smartcard cost Per reader cost ¹⁵	Nil	Replacement of a proportion of lost & damaged smartcards Support fees for readers

¹⁴ The roaming soft certificate solution remains somewhat novel and can be expected to bring some incremental help desk load.

¹⁵ Smartcard readers are increasingly built into standard PC equipment; the need for extra readers will decline over time.

Other resources

Finally, several very good resources are also available to help work out ROI in other ways, or to make the business case in general for PKI.

The General Services Administration released its *Approach for Business Case Analysis of Using PKI on Smart Cards for Government-wide Applications* in 2001 [11]. This report provides a detailed and multi-faceted framework for analyzing the financial cost-benefit of PKI implemented on smartcards. It also presents two detailed case studies, on the Federal Deposit Insurance Corporation (FDIC) and another major (unidentified) government agency.

Verisign in collaboration with consultants Blue Bridge has produced a quantitative treatment of ROI for PKI [12]. Rather than create a generic framework, this document examines five killer applications (messaging, access control, VPN, online account activation and forms). Its advice on ROI modeling methodology is especially clear and pertinent.

For those interested in ROI more broadly, across information security and other arms of IT infrastructure, some useful further reading is indicated below.

References

- [1] PKI and Financial Return on Investment PKI Forum August 2003
- [2] Putting the Enterprise into the Enterprise System Thomas H. Davenport, Harvard Business Review, Volume 76 , Issue 4 1998
<http://portal.acm.org/citation.cfm?id=280995> (to purchase the article)
- [3] An Approach to Evaluating E-Business Information Systems Projects Virginia Franke Kleist, Information Systems Frontiers 5:3, 249–263, 2003
www.kluweronline.com/article.asp?PIPS=5141885&PDF=1 (to purchase the article)
- [4] Return on Investment Analysis for E-business Projects Mark Jeffery, Kellogg School of Management, Northwestern University, 2004
www.kellogg.northwestern.edu/faculty/jeffery/htm/publication/ROIforITProjects.pdf
- [5] Beyond the productivity paradox Brynjolfsson, E., & Hitt, L, Communications of the ACM, 41(8), 49–55, 1998 <http://ebusiness.mit.edu/erik/bpp.pdf>
- [6] **CEO Perspectives: Calculating Return on IT Investment - A Pointless Effort?** David A.J. Axson, DM Review Magazine, February 2001
www.dmreview.com/article_sub.cfm?articleId=3015
- [7] Is a dongle your key to Electronic Conveyancing? Land Title Office, Victorian Government, March 2004
www.landexchange.vic.gov.au/ec/newsroom/download/ECNewsMar2004.pdf
- [8] Land Exchange (LX) Case Study, Government of Victoria, July 2004,
<http://www.egov.vic.gov.au/pdfs/Land%20Exchange-shh-30April-v1.0-CIO.pdf>



- [9] Technical Position on PKI Burton Group, November 2003
<http://www.burtongroup.com/guests/content/dss/testdrive/techpositions.asp>
- [10] The United States Patent and Trademark Office Entrust “Customer Success” story www.entrust.com/success/index_uspto.htm
- [11] Approach for Business Case Analysis of Using PKI on Smart Cards for Government-wide Applications by Booz Allen Hamilton, for the General Services Administration CIO PKI/SMART Card Project, 18 April 2001; see <http://www.smartcard.gov/information/bahfinal18apr01.doc>
- [12] Return on Investment – Public Key Infrastructure Verisign and BlueBridge, 2002
www.verisign.com/stellent/groups/public/documents/white_paper/005320.pdf

Further reading

Return on Investment for Information Security Department of Commerce, Government of New South Wales, 2004 <http://www.oict.nsw.gov.au/content/7.1.15.ROSI.asp>

Return on Investment Methodology for Evaluating EBusiness Infrastructure Chip Gliedman, Giga Research, 2001 www-8.ibm.com/e-business/au/pdf/roi/16_Giga.pdf

Executives Need to Know: The Arguments to Include in a Benefits Justification for Increased Cyber Security Spending Timothy Braithwaite in Information Systems Security, Auerbach Publications, September/October 2001; see also http://egov.alentejodigital.pt/Page10549/Seguranca/execs_need_to_knw.pdf

Finally, a Real Return on Security Spending CIO Magazine, 15 February 2002; see www.cio.com/archive/021502/security.html