WHITE PAPER

PKI and Financial Return on Investment

August 2002

The objectives of this paper are to provide a reasonably fine-grained framework for the "Return" component of the PKI ROI equation, to advance the level of practical detail in discussions about the business case for PKI, and to generate specific ideas for PKI ROI analysis. It is not an objective – nor is it even possible, given the innumerable e-business processes that can potentially leverage PKI as their e-security foundation – to provide a single set of formulas or templates into which one can simply plug numbers and compute "the answer."

Introduction

This paper is not about technology; it's about time and money. That is, organizations often ask for help with not only the technology case, but also the business case, for their investments in Public-Key Infrastructure. In other words, what is the Return on Investment ("ROI") for PKI?

This is not always an easy question to answer – PKI is an e-security infrastructure, after all, and the ROI for an infrastructure of any kind can be difficult to quantify. Some don't try, and have implemented based more or less on a leap of faith. However, over time, the ROI for infrastructure often becomes unnecessary to quantify in dollars, because the capabilities it enables are both mission-critical and well understood. For example, when was the last time any large business required an ROI analysis to determine whether or not it should invest in enabling infrastructures like telephones, facsimile machines, or e-mail? The return on investment for any infrastructure is tied to the applications that use it; in commerce, government, financial and healthcare processes, the potential benefits are substantial. The return on investment from the applications it enables is the driver to use it.

Financial Returns: the "R" in ROI

As PKI becomes more widely deployed, and as more hands-on experience makes the total cost of ownership for PKI more accurately understood, we can turn our attention to the topic that generates the most enthusiasm in the corner offices: the *financial returns* made possible from PKI-enabled business processes.

What financial returns does public-key infrastructure really provide? Here, we provide a general framework for unlocking the financial returns that are made possible by implementing PKI-enabled applications. In considering this framework, the following simple step-by-step approach should be kept in mind:

> Focus on the Business Process. It's worth repeating that PKI is an e-security infrastructure, and infrastructure in the absence of a specific business process returns nothing. For example, if we invest in telephones, facsimile machines, and e-mail systems but never place a call, transmit a document, or send a message, what have we gained? Moreover, returns from e-security infrastructures are generally difficult (if not impossible) to separate from the returns from the business processes themselves. The primary focus – once it has been determined that authentication, data privacy, data integrity, digital signatures, or other e-security capabilities provided by PKI are important business requirements – should therefore be on the financial returns from the successful implementation of a particular (security-enabled) business process. This approach also accommodates the reality that financial returns are typically application-specific, company-specific, industry-specific, and so on.

Acknowledgements

White Paper is a deliverable from the PKI Forum's Business Working Group (BWG). Several member organizations and individuals have contributed by providing content, editorial assistance and editorial reviews.

Author:

Derek Brink
RSA Security

Editors:

Patricia Lareau
PKI Forum

Jeff Stapleton
KPMG, LLP

Contents

Establish Appropriate Metrics. With a proper focus on security-enabled business process, the next step is to establish the appropriate metrics for determining potential financial returns. The metrics chosen will logically be a function of not of not only the particular business process under analysis (e.g., is it an internal process? A customer-facing process? A partner-facing process?), but also the specific business objectives we have in mind (e.g., are we aiming to increase revenues? Lower costs? Improve efficiency?). A subsequent section (“Metrics”) discusses this topic in more detail.

Establish a Baseline for the Current State. Having established an appropriate set of metrics, the next step is to use them to establish a baseline for the business process under analysis, based on the way things are today. This is the “business as usual” scenario.

Compare to the Desired Future State. The same metrics can then be used to com pute the financial impact of implementing a new or improved business process that meets the specific business objectives we have in mind. This is the “business as a result of” scenario, i.e., the desired future state that will result from the successful implementation of a new or improved PKI-enabled business process.

The return on investment for any infrastructure is tied to the applications that use it; in commerce, government, financial and healthcare processes, the potential benefits are substantial. The return on investment from the applications it enables is the driver to use it.

If this straightforward approach sounds familiar, it should come as no surprise – it’s a time-honored method for establishing value, a process we’ve all gone through (consciously or otherwise) countless times before. We can step back and observe that PKI is not uniquely complex or difficult to analyze in this regard – on the contrary, this approach for computing financial returns for PKI-enabled applications is the same one used for virtually any other significant investment. All we need, given the relatively early stage of PKI market development, is a general framework to help organize the approach and jump-start a detailed discussion of potential financial returns.

The first, critical step is to frame the ROI discussion in the context of the key e-security enablers for a particular e-business process/application. The next step is to establish an appropriate set of metrics for determining potential financial returns.

This (straightforward) approach for computing financial returns for PKI-enabled applications is the same one used for virtually any other significant investment.

Metrics

The most appropriate metrics are a function of both the business process under analysis and one or more specific business objectives. Table 1 lists a number of potential metrics for certain example business objectives, and provides examples of “impact statements” in the form of questions that set up a comparison of the current state with the desired future state in terms of one or more specific metrics. Quantifying the answers to these questions is the key to unlocking the financial returns made possible by PKI-enabled applications.

Based on a number of case examples, we observe that quantifiable financial returns made possible by PKI-enabled applications tend to fall into one of the following four high-level categories: Revenues, Costs, Compliance, and Risks. The remaining sections of this paper explore these four categories in more detail, and include several examples of metrics that lead to quantifiable financial results.

Table 1: Example Metrics and Impact Statement

Business Process	Example Business Objectives	Potential Metrics	Example Impact Statements (The Key to Unlocking Financial Returns)
Customer-Facing	Maximize online revenues from existing customers	• % of revenue generated online • % of existing customers doing business online • % of customer wallet spent online • % drop-off rate • Repeat business rates • % of up-sell, cross-sell conversions • Lifetime revenue per customer	Two-thirds of our online customers don t complete transactions that require them to print, sign and mail paper documents. What would the financial impact be if we could reduce this drop-off rate to one-third by using digital signatures to complete the entire transaction online, as well as eliminate the cost of paper, printing, postage, and processing?
	Minimize costs of finding and acquiring new customers	• % of new customers acquired online • Cost of new customer acquisition • Brand perception, brand awareness	What would the financial impact be if we could leverage 50% of all established online account relationships with Line of Business #1 to create an online account relationship with Line of Business #2?
	Maximize customer satisfaction; reduce help desk and support costs	• # of incorrect order incidents • Service levels used • # of service / help desk requests • % of service / help desk requests resolved online	What would the financial impact be if authorized customers could resolve 80% of help desk calls directly, online, rather than by live agents over a toll-free number?
Internal	Increase responsiveness to changing market conditions	• Order cycle / delivery time • Product time-to-market • Product time-to-change	What would the financial impact be if we could reduce our process cycle time from X days to Y hours, while preserving the integrity and authenticity of documents and transactions?
	Reduce costs, improve productivity	• Cost of materials • Cost of services • Productivity per employee • # of service / help desk requests • % of service / help desk requests resolved online	What would the financial impact be if we could improve employee productivity and reduce help desk calls caused by password resets, by using PKI-based authentication with our Virtual Private Network or with our Reduced Sign-On initiative?
Partner-Facing	Tighten degree of system integration with strategic Partners	• % of production goods procured online • % of maintenance / repairs / operating supplies procured online	What would the financial impact be if we could shorten delivery times and reduce inventory, by enabling authorized users to procure 80% of all maintenance, repairs and operating supplies through a Web browser, mobile phone, or wireless personal digital assistant?
	Reduce Partnership costs, improve Partner reliability	• Comparative prices • Cost / Uptime of partner connections • Cost / Rate of partner repairs, replacements, returns • Cost, time commitment scorecard	What would the financial impact be if we could provide authorized strategic partners with increased access to sensitive information, without compromising security or giving up control?

Quantifiable financial returns made possible by PKI-enabled applications tend to fall into one of the following four high-level categories: Revenues, Costs, Compliance, and Risks.

Revenues

Business processes that generate new or increased revenue streams create perhaps the most compelling justifications for investments in enabling infrastructure such as PKI. Because revenue enhancements are generally more strategic than tactical in nature, however, they can also be somewhat more difficult to quantify.

Business processes that generate new or increased revenue streams create perhaps the most compelling justifications for investments in enabling infrastructure such as PKI.

Based on metrics such as those found in Table 1, we can reasonably quantify any number of incremental revenue streams for PKI-enabled applications. For example, suppose two-thirds of our online customers currently end up abandoning transactions that require them to print, sign and mail paper documents rather than allow them to complete the entire transaction online. What would it mean with respect to incremental revenue if we could substantially reduce this drop-off rate, say to only one-third, by using digital signatures to complete the transaction immediately while simultaneously minimizing the risk of subsequent repudiation? For many document-intensive industries (including financial services, insurance, healthcare, etc.) this would have an enormous impact on revenues – not to mention the potential for reducing the related costs associated with paper, printing, postage, and processing of traditional paper forms.

Other possibilities for quantifiable revenue-based financial returns include cross-selling or up-selling opportunities with established customers, an increased number of transactions per customer, higher rates of repeat business, etc. Important but less quantifiable examples in this category might include competitive advantage, strategic positioning, corporate brand/image, etc. A transactional Financial Services example is provided below.

Revenue Example: Online Brokerage Transactions

Organization: Online brokerage firm servicing self-directed individual investors

Application: Instant Account Opening – online, paperless process to open an online brokerage account and fund the account electronically using the ACH mechanism.

Business Benefits: Time to open a new account reduced from 3-10 days to less than 3 minutes, a critical factor in accelerating revenues from new account growth and from converting prospects more quickly to active traders – an impact of tens of millions of dollars. Cost avoidance compared to manual account processing and help desk calls related to new account openings; cost reductions from reduced mailing and storage costs – an impact of over $2M.

Benefits of PKI: Account activity acknowledged and authorized by electronic signatures; reduced risk through the use of stronger authentication; higher integrity of stored customer data.

Costs

Although cost reductions are generally more tactical than strategic in nature, they are generally the easiest returns to quantify.

Reductions in cost are perhaps the most reliable drivers of financial returns for PKI-enabled applications – that is, although cost reductions are generally more tactical than strategic in nature, they are also generally the easiest returns to quantify (hence their popularity). Cost-based financial returns are typically expressed as some combination of the following:

- Cost Savings: e.g., the new or improved business process is less expensive; we can spend fewer dollars than we did before.
- Cost Avoidance: e.g., the new or improved business process scales to higher levels; we can avoid spending as many additional dollars in support of new capabilities or expanded scale.
- Efficiency: e.g., the new or improved business process saves time; we can increase the velocity at which we conduct e-business.
- Effectiveness: e.g., the new or improved business process increases productivity; we can do more or different things with the resources we already have.

While it is impossible to generalize about the best sources for cost-based financial returns, at present there are three areas that seem to be particularly fruitful: help desk costs, telecommunications costs, and costs associated with the processing of electronic forms / electronic records.

The numbers in Table 2 illustrate why so many companies target the help desk as a rich and easy source of cost-based financial returns – end-users can usually experience faster, more convenient service at a reduction in cost of up to two orders of magnitude. Common PKI-enabled applications that can result in substantial reductions in help desk costs include corporate Intranets, Reduced Sign-On initiatives, Virtual Private Networks, and one-to-many Extranets. A Secure Extranet case study example is provided below.

Table 2: Example Cost Reduction Target - Help Desk

Type of Customer Service	Average Cost / Transaction
Agent (Phone-based)	$5.00
Agent (Web chat)	$2.50
Agent (E-mail)	$2.25
E-mail (Auto Reply)	$0.75
Web (Self-Service)	$0.05

Cost Example: Secure Extranet

Organization: Mutual funds, trust and investment services company

Application: Secure Extranet for 5,000 independent financial advisors. 7 x 24 self-service access to high-value financial and client information.

Business Benefits: Annual cost savings of approximately 40% compared to phone-based, agent-based system. Largest driver for cost savings is 3x reduction in toll calls and direct agent assistance.

Benefits of PKI: Privacy compared to previous process, and integrity of data; authentication of users; user accountability for data; customized content; reduced risk of data loss / theft; centralized control of trust properties.

Common PKI-enabled applications that can result in substantial reductions in help desk costs include corporate Intranets, Reduced Sign-On initiatives, Virtual Private Networks, and one-to-many Extranets.

Telecommunications costs also represent low-hanging fruit for cost-based financial returns, and are often used in particular to justify investments in Virtual Private Networks. Many organizations implementing VPN technology overlook authentication as a critical e-security requirement, however, on the mistaken assumption that an encrypted communications channel has fully addressed the problem of secure remote communications. Replacing a VPN's weak password-based authentication with stronger authentication technology such as PKI improves overall security by more strongly establishing who's on the other end of your VPN. This allows sensitive deal-making information to be available to remotely located individuals when it is critically needed without the fear of compromise while leveraging the cost advantages of extranet delivery.

Replacing a VPN's weak password-based authentication with stronger authentication technology such as PKI improves overall security by more strongly establishing who's on the other end of your VPN.

A third area ripe for harvesting cost-based financial returns has to do with the cost of processing paper forms, documents and business records. This is most relevant in document-intensive industries such as financial services, insurance, and healthcare, where enormous financial returns are possible from cost reductions in the "Four Ps" of paper, printing, postage, and processing.

The cost of manual document processing is very high: the average paper document is copied 9-11 times at a cost of approximately $18 and filed at a cost of approximately $20, plus the additional cost of storage, electronic media, physical plant, postage and other distribution. And mistakes are expensive: the cost of finding and retrieving misfiled paper documents is approximately $120. Of course there are other business benefits to electronic forms processing in addition to lower cost: wider, easier access; better quality; higher data integrity; lower growth in personnel requirements; etc.

As an illustration of the magnitude of financial returns of this type, Table 3 compares the average distribution cost through Internet-based channels with those through traditional channels for term life insurance, bill payment, and banking, respectively.

Table 3: Example Cost Reduction Target - The Four P's of Form/Document Processing

	Traditional Distribution	Internet-based Distribution
Term Life Insurance	$5.50	$2.75
Bill Payment	$2.75	$0.75
Banking	$1.08	$0.13

Cost Example: Electronic Mortgage Transaction

Organization: Home mortgage services

Application: Online mortgage transaction.

Business Benefits: 30-45 day cycle time reduced to 5 hours. Reduced risk of mishandled documents, errors and omissions. Reduction in administrative staff, training costs. Improved customer service. Savings of approximately 20% in total loan lifecycle costs compared to previous process.

Benefits of PKI: Provable chain of evidence as to the authenticity of documents; authorization to access documents based on user authentication.

Another area ripe for harvesting cost-based financial returns has to do with the cost of processing paper forms, documents and business records

Compliance

By compliance, we mean some business process that we are required to implement, or some e-security requirement that we are obligated to meet. Compliance generally refers to things about which we have very little choice, i.e., things we must do in order to stay in business as we know it. In some cases, compliance may be related to cost avoidance (e.g., avoid a fine); in others, it may be related to protecting an existing revenue stream. In any event, compliance-based business cases tend to be somewhat binary: above a certain threshold, we just do it. As it relates to e-security infrastructure, compliance-based arguments tend to come from one of the following four categories: *Regulatory, Partner, Customer, and Competitive.*

- Regulatory compliance: where failure to implement could mean fines, loss of revenues, jail terms, etc., e.g., HIPAA regulations for the U.S. healthcare industry, the Gramm-Leach-Bliley bill for the U.S. financial services industry, and Directive 95/46/EC for all enterprise in the EU.
- Partner compliance: where failure to implement could mean losing our ability to participate with a key partner or group of partners, e.g., a segment of the financial industry moving to the Identrus model for cross-certification.
- Customer compliance: where failure to implement could mean the loss of a business relationship with a key account, e.g., "all General Motors suppliers who wish to have their contracts renewed must implement technology X by a certain date".
- Competitive compliance: where failure to implement could mean the loss of competitive advantage and likely revenue loss, e.g., "our competitors are eating our lunch!"

Compliance-based business cases tend to be made not so much on the basis of precisely quantified financial returns, but on the basis of "the cost of doing business" or as a means to avoid "what will happen if we don't implement." In some cases — HIPAA and 22CFR Part 11 are good examples — compliance brings with it huge financial and efficiency benefits associated with paper reduction and the enablement of e-business strategies.

In some cases compliance brings with it huge financial and efficiency benefits.

Compliance Example: Clinical Data Exchange with Food and Drug Administration

Organization: Pharmaceutical Firm

Application: Electronic Management and Transmission of Clinical Test Results

Business Benefits: Compliance with the Health Insurance Portability and Accountability Act (HIPAA) and with Food and Drug Administration regulations at 21 CFR Part 11 (Electronic Records and Signatures); greater efficiency in approval cycle (over paper) to meet signatory requirements of the regulations; reduction in time-to-market for new drugs; faster revenue flow.

Benefits of PKI: Use of public key technology for electronic (digital) signatures, data integrity, user authentication and data confidentiality is recognized by 21 CFR Part 11 and by draft HIPAA implementing regulations as providing the strongest and most interoperable mechanism available for those purposes. Compliance with 21 CFR Part 11 is more straightforward since digital signatures are self-auditing, facilitating compliance with auditing and access management requirements. Interoperability is increased through the use of cross-certified certificates as opposed to complex userID/password management and harmonization. Months of time are saved in the signatory phase of document review for reporting clinical test results.

Risks

Until only recently, risk-based arguments were probably the most frequently used approach to justify investments in e-security infrastructure. Marketing campaigns and business cases alike were commonly based on arguments of fear, uncertainty and doubt (FUD). Selling security through fear can be reasonably effective, up to a point – for example, the Big Bad Wolf certainly sold fairy tales in volume for the Brothers Grimm – but it also tends to marginalize e-security as an operating expense, subject to being trimmed at the first round of budget cuts. Today, happily, there is beginning to be significantly less emphasis on FUD and more on the systematic management of risk.

Risk is an inescapable fact of e-business, and there are only four things we can do about it: accept it; ignore it (which is the same as accepting it); assign it to someone else; or mitigate it. Investments in e-security infrastructure that are made with prevention in mind are usually not highly visible (unless there's a problem), which tends to make risk-based justifications the least glamorous of the four categories in our model.

Selling security through fear tends to marginalize e-security as an operating expense, subject to being trimmed at the first round of budget cuts.

It seems obvious, but risk mitigation investments should be focused on things that are worth protecting, such as high-value information and high-value or high-volume transactions. For examples of "high-value" information, consider the following:

- Information that generates revenue, either directly or indirectly: information, programs, services, etc.
- Information essential to the smooth running of the company: operational information, administrative information, etc.
- Information pertaining to future revenue streams: research, new product plans, marketing plans, and customer databases
- Information that must be protected by law: personnel records, student records, patient records, etc.

Once high-value information has been identified, we can then make a reasonable attempt to quantify the impact of various security-related risk scenarios, using the familiar "impact statement" approach. For example:

- Productivity loss: e.g., what would the financial impact be if a security breach caused a sustained disruption of internal processes and communications? If we lost the ability to communicate with customers? (Keep in mind that 99.5% uptime still translates to 3.6 hours of downtime per month.)
- Monetary loss: e.g., what would the financial impact be if there were a security-related corruption of our accounting system, which led to delays in shipping and billing? If there were a diversion of funds? What would be the expense of recovery and emergency response?
- Indirect loss: e.g., what would the financial impact be if a security breach caused the loss of potential sales? The loss of competitive advantage? Negative publicity? The loss of goodwill and trust? Indirect losses are among the most difficult to quantify but also among the most compelling in the risk-mitigation category, especially for businesses built on the fundamental foundation of "trust."
- Legal exposure: e.g., what would be the financial impact of failure to meet contractual milestones? Failure to meet statutory regulations for the privacy of data? Illegal user or intruder activity on company systems? Your corporate counsel can potentially be an excellent source of justification for PKI-enabled business process.

Indirect losses are among the most difficult to quantify but also among the most compelling in the risk-mitigation category.

The answers to these risk-oriented impact statements can be difficult to quantify, but the financial implications can be extraordinary. And the risks themselves are very real – it seems that not a month goes by without a highly publicized security breach, and undoubtedly the vast majority of security breaches go unpublicized. The annual FBI/ Computer Security Institute survey on computer crime and security shows that over 80% of respondents now answer "yes" or "don't know" (which is probably the same as "yes") to the question "have you experienced some kind of unauthorized use of your computer systems in the previous year"; unauthorized access by insiders is twice as frequent as unauthorized access by outsiders, and growing; and the Internet has rapidly replaced internal systems and remote dial-up as the most frequent point of attack.

Risks *continued*

Risk Example: Identity And Access Card

Organization: Government Department

Application: Facility access; logical access to information and system services in a global information enterprise

Business Benefits: Reduced cost resulting from combined management of personnel identity, physical, and logical access for a geographically diverse population; the efficiency of converting paper processes to electronic processes while improving the information assurance posture for sensitive information

PKI Benefits: Common infrastructure to support geographically dispersed, mobile population in excess of 4 million; flexible but consistent registration processes; adaptable to multiple levels of assurance; full flexibility in providing confidentiality and authentication of communications and network transactions as well as verification of the data integrity and non-repudiation of these transactions

Financial Returns: Summary

The most important points for developing meaningful financial returns for PKI-enabled applications are to focus on the business process, establish appropriate metrics, and look for all relevant returns in the following high-level categories: Revenues, Costs, Compliance, and Risks.

As we have seen in the example metrics and impact statements provided in Table 1, by properly framing the ROI discussion in the context of the key e-security enablers for a particular e-business process, we can very quickly begin to quantify financial returns using a straightforward, widely accepted approach. In general, we believe that the benefits from PKI-enabled applications significantly outweigh the costs of PKI implementation. Yes, Virginia, there is a strong ROI for PKI.

As we said at the beginning, this is not about technology; it's about time and money. To put things in perspective, consider the parallels between current thinking about e-security infrastructure and the thoughts about various quality initiatives in manufacturing (Just-In-Time manufacturing, Total Quality Management programs, etc.) in the 1980s. A *com*mon business issue for pragmatic, non-technical executives at that time was the “Cost of Quality”, as in “Sure, these quality programs sound great, but how much will they really cost, and will there really be a return on my investment?” Then a provocatively titled little book – Quality is Free – helped business people to better understand and quantify the financial effects of poor quality: scrap, rework, longer cycle times, product returns, poor word of mouth, higher customer support costs, etc. So the phrase “Quality is Free” was really a concise, provocative summation of the concept that the cost of implementing quality programs was significantly less than the financial returns made possible by producing high quality products in the first place.

And so it is with e-security: the total cost of ownership for implementing an enabling e-security infrastructure such as PKI is significantly less than the financial returns made possible by PKI-enabled applications, when revenues, costs, compliance and risks are understood an quantified. In other words, “Security is Free”. Plus ça change, plus c'est la même chose.[1]

Copyright Statement

About PKI Forum

The PKI Forum is an international, not-for-profit, multi-vendor and end-user alliance whose purpose is to accelerate the adoption and use of Public-Key Infrastructure (PKI).

The PKI Forum advocates cooperation and market awareness to enable organizations to understand and exploit the value of PKI in applications relevant to their business.

Web: http://www.pkiforum.org
e-Mail: info@pkiforum.org
Phone: +1 781 876 8810

[1] The material in this paper is covered in more detail in PKI: Implementing and Managing E-Security, A. Nash, W. Duane, C. Joseph, and D. Brink, McGraw-Hill, ISBN: 0072131233, April 2001, chapter 11 (D. Brink).