

Digital Signatures and the Hidden Costs of PKI White Paper

July 2008



Digital Signatures **Made Simple**

Secure
Simple

Introduction

The implementation of a digital signature (standard electronic signature) solution can expedite and secure business operations, reduce costs, advance business processes, and improve an organization's competitive advantage. However, if an organization implements an incompatible digital signature solution, it could end up costing thousands, if not hundreds of thousands of dollars more than necessary. Previous to delving into the various financial distinctions of the digital signature options, it would be relevant to address the differences of electronic signatures in general.

Electronic signatures can be broken down into two broad categories: Those that use Public Key Infrastructure (PKI)-based technology and those that do not. Non-PKI-based electronic signatures are considered insecure and non-compliant with regards to legal standards, as they aren't unique to the user, they do not identify the signer, they cannot detect changes in the documentation after signing, and there is no guarantee of sole control for the signer.

PKI technology is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA), allowing individuals to encrypt messages to each other, and enabling the various parties to a document to establish message integrity, confidentiality and user authentication, even if the parties have never had prior contact.

This paper will focus explicitly on the category of electronic signatures that use PKI technology (digital signatures), the different methods that can be employed to implement them, as well as their benefits, drawbacks, and costs.

Elements of PKI Technology

PKI technology consists of three basic parts:

- ▶ **A Registration Authority (RA)** - The RA is the authentication process in the network that verifies user requests for a digital certificate. The RA tells the certificate authority (CA) to issue the digital certificate.
- ▶ **A Certificate Authority (CA)** - The CA issues the digital certificate, which contains a public key and the identity of the owner. This certificate validates that this public key actually belongs to the certificate.
- ▶ **A Database** - The repository, or database, stores the digital certificates.

Evaluating Solution Options

Companies that have decided to implement digital signatures have several different approaches to consider, each offering different value propositions. The following provides a brief overview of these options, which will be discussed in greater detail later in the paper.

- ▶ **Managed PKI - Outsourcing the Solution** - Outsourced PKI refers to a PKI solution that is owned and operated by a trusted third-party entity known as a Certificate Authority (CA). The CA assumes responsibility for setting policy, managing the technology and infrastructure, and owns the legal liability

Table of Contents

Introduction	2
Elements of PKI Technology	2
Evaluating Solution Options	2
Comparing Digital Signature Solution Costs	3
Managed PKI	5
Traditional PKI	6
Server Side Signing	7

on behalf of the client. This approach does not require purchasing hardware or software. However, when factoring set-up fees per user license, annual renewal fees, and in-house IT support, the costs can be considerable.

- ▶ **Traditional PKI - Developing an In-House Solution** - In-house implementation involves the acquisition of PKI software and hardware in order to deploy digital certificates. Full-time, dedicated staff is required to create, manage, and support the systems and users. Utilizing this approach allows the organization to control and customize their digital signature solution according to their needs and infrastructure. Implementing an in-house option, even if using free software, can be the most costly approach to PKI technology.
- ▶ **Server Side Signing - An Off-the-Shelf Solution** - A new concept in PKI technology, also known as Server Side Signing, leverages the existing infrastructure that is currently in place at a company. This approach involves deploying a centralized appliance installed on the company's network that immediately works in sync with the company's user directory. Rather than reinventing the wheel, this solution compliments the company's existing infrastructure. As far as costs are concerned, Server Side Signing involves the minimal purchase of hardware and per user license fees (roughly \$63,000 for 1,000 users over a three-year period).

Comparing Digital Signature Solution Costs

The decision of which PKI solution to utilize is often based on a comparison of only the most obvious costs. These costs may include charges for client software, licenses, hardware, server software, and installation. These are important factors to consider, but they are only a small part of the total cost of ownership (TCO) of digital signatures solutions. It is equally important to compare not only the obvious one time costs, but the recurring annual charges as well.

Table 1 shows the basic cost analysis per solution that must be taken into consideration when computing the TCO for each PKI approach.

		Outsourced (Managed) PKI			In-House PKI System			Server Side Signing		
One-time costs	Number of users	100	250	1000	100	250	1000	100	250	1000
	License cost per user	-			-			Less than \$100		
	Setup fee	\$10,000	\$15,000	\$20,000	-			-		
	Setup costs (IT)				\$35,750 (1/4 Full Time Equivalent)					
	Hardware	None if using risky software tokens; \$20-\$60 per user for hardware tokens (not inc. reader if required!)			\$3,000	\$5,000	\$10,000	\$10,000 - \$25,000		
	Software licenses	-			Varies			-		
	PKI consulting fee	-			\$12,000-\$75,000 (5-30 days X \$2,500/day)			-		
	Dev. For app. support	Varies (support for non-PKI-aware apps, compliance req. etc.)			Varies (support for non-PKI-aware apps, compliance req. etc.)			None. Extensive 3 rd party app. Support		
Annual costs	Physical security	-			\$5,000 (Hardened room/building)			None (Hardened enclosure included)		
	License cost per user	\$50	\$43	\$33	-			-		
	IT staff time	\$71,000 (1/2 Full time equivalent)			\$35,750	\$71,000	\$143,000	Zero-management		
	Service fee	\$25,000	\$35,000	\$45,000	-			-		
Total costs	Maintenance	-			Varies			Less than \$10,000		
	Year 1 cost	\$111,000	\$131,000	\$116,000	\$91,500	\$128,750	\$205,750	Less than \$80,000		
	Year 2+ cost	\$101,000	\$117,000	\$149,000	\$35,750	\$71,000	\$143,000	Less than \$10,000		
	3 Year TCO	\$313,000 Min.	\$365,000 Min.	\$414,000 Min.	\$163,000 Min.	\$270,750 Min.	\$491,750 Min.	Less than \$100,000		

Figure 1: Cost Comparison Chart for Implementing a PKI Solution

Digital Signatures Made Simple

Managed PKI – Outsourcing the Solution

In the world of high tech, outsourcing is a popular solution. It is often considered an easy way to allow your company to focus on its core business. There is no need to invest in hardware, software, or personnel; therefore, the TCO seems to be relatively low.

The Certificate Authority (CA), the outsourcing company, owns the digital signature solution and is responsible for the physical facility, the processing facility, operations and maintenance, as well as the legal framework. The CA is also responsible for all legal and security issues, as well as for changes in technology. In addition, the outsourcing entity assumes the responsibility for setting policy, and managing the information technology. Even though the client company can maintain control of certificate issuance, co-branding and management, the major responsibility for maintenance, scalability, and policy management is left to the outsourcing company.

Outsourcing is faster to deploy than in-house PKI efforts as the infrastructure is already in place. Also, this option is a way to avoid initial money and manpower shortages, since it does not require heavy up-front investments in infrastructure or additional staffing. Outsourcing is therefore attractive to companies that lack expertise and ongoing IT support, as PKI technology is fairly complex, as well as companies with smaller financial resources.

While a managed solution certainly has benefits, it can be very costly in the long run. Even though the initial costs are low, as seen in Table 1, the TCO can become prohibitive. Outsourcing companies charge annual renewal fees and service fees for ongoing support. After a few years, these annual fees can add up to more than the initial cost of implementing a traditional in-house system.

In addition, there are fees for customization and upgrades, and a company that employs a managed PKI solution needs to rely on a second party, with its own schedule of priorities, to implement every change necessary, no matter how simple it may be.

Costs and Issues of Provisioning and Managing Personal Signature Tokens

Depending on the outsourcing company, a managed solution may provide a company's employees with either hardware or software tokens for signature purposes (e.g., tokens are required for deploying and managing signature keys and certificates). It should be assumed from the onset that some of these devices will be misplaced or destroyed as time passes. The logistics issues, costs and helpdesk support of replacing these devices and/or the loss of production time due to lack of a device is a major factor to consider when deciding on an implementation method.

Organizations also need to be aware of managed solution scenarios where they may find themselves locked into an agreement with a managed solution provider that has become so expensive (due to the initial investment in set-up fees, user licenses, etc.) that it becomes cost prohibitive to change the managed solution provider.

In conclusion, while delegating all of the digital signature technology to an outsourcing company may seem enticing, as there is no significant upfront cost, the truth is that the total cost of ownership has no limit. Table 1 shows that costs can run up to \$313,000 for just 100 employees and close to half a million dollars for 1000 employees.

Traditional PKI – Developing an In-House Solution

Most of the companies that choose to develop a traditional in-house PKI implementation, base their decision on the perceived merits of greater control and flexibility and lower costs over the long term. With Traditional PKI, the expectation is that the solution can be implemented using the existing IT personnel without any additional expenses.

An in-house solution gives a company the flexibility to issue and revoke certificates quickly and implement policies that can be tailored to meet business needs. However, with an in-house solution, all of the infrastructure and services, including legal liabilities, project management, and manpower resources become the responsibility of the company utilizing them. This means that the company must assume total responsibility in several different areas: setting policies, managing the root keys, digital certificates and the private keys, as well as maintaining the necessary audit logs to comply with government regulations. When determining the expenses associated with developing an in-house solution, the costs of creating a Certificate Revocation List (CRL) or an Online Certificate Status Protocol (OCSP) request (both are used to revoke a user's privileges for digitally signing), must also be acknowledged. These costs are not inconsequential.

The company must also determine, implement, and document policies and practices that ensure that PKI-standards are being enforced according to government regulations. In addition, it must also assume responsibility and risk for certificate issuance and authentication.

Furthermore, if a company chooses to invest in an in-house model, it must be prepared to continually make new investments in hardware upgrades to accommodate additional users. The company should also be prepared to repeatedly invest in software upgrades, as new versions of software are released.

Choosing a traditional PKI implementation involves a major investment with several up-front costs. The first step is to choose the desired software. Many companies are enticed by the offer of "free" software, such as the Microsoft Certificate Server in Windows 2003. Even though the software is "free", as the cost comparison table shows, this option is not so "free" if you take into account the TCO, which includes the total amount of resources the undertaking will require. According to Microsoft's own assessments for Managing a Windows Server 2003 Public Key Infrastructure (<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/mngpki.mspx#EBF>), the initial set up effort alone demands 13 days (105.5 hours) of work. That's a tremendous amount of resources that need to be committed up-front for the solution, without even acknowledging the additional 90 days per year (720 hours) of ongoing operational tasks this type of solution necessitates. In addition to the cost equivalents such a commitment of resources requires, a company that chooses a software package will often have to pay licensing fees as well. Moreover, hardware (dedicated servers) must also be purchased, in order to deploy digital certificates.

Once the hardware and software are purchased, it is essential to have experts in PKI technology, who are able to take responsibility for defining the company's certificate practices and policies for the creation and distribution of digital certificates. Additionally, dedicated IT staff will also be required. Building a PKI-based solution is a very complex process and implementing it requires a major investment in technical know-how. If the company does not have the required experts already on staff, then PKI consultants will need to be hired at the rate of approximately \$2,500 per day.

Once the solution is up and running, there are generally additional expenses. The company is responsible for the physical plant, which includes security for the encryption keys, back-up and disaster plans, as well as all the other incidentals that create a secure software environment. This is a critical issue. If the keys

are not protected properly, it opens the door to forgery, and individuals from within or outside of the company may access the keys and use them to sign with the digital signatures of unsuspecting employees.

For companies that aren't experienced with handling the necessary commitments involved with traditional PKI implementation, the process can be extremely daunting, if not impractical. However, there is an upside to all of this investment - An in-house implementation, if done properly, may actually prove to be an excellent solution customized perfectly for a company's business. It can offer support for proprietary applications and services that an outsourced solution may not be willing to provide. This solution reduces the cost per user because it keeps the cost of issuing certificates low, since there is neither an original nor an annual license fee per user. An in-house solution offers a company total control, flexibility, and scalability of their solution.

Creating an in-house system is neither easy nor inexpensive. According to the cost comparisons in Table 1, minimum costs for 100 employees can be \$1,630 per person. For a larger company with 1000 employees, these costs could run in excess of \$491,750.00.

Server Side Signing – An Off-the-Shelf Solution

The off-the-shelf or server side signing solution is a secure, PKI-based, efficient and cost effective digital signature solution. This approach eases the complications associated with deploying a digital signature solution and eliminates the necessity of investing in a traditional and expensive PKI implementation, while enabling your company to maintain control that is lost with an outsourced solution.

Server side signing involves installing a designated server on a company's network to serve as a central repository for the user's private signing key that works with the existing company directory (for example Microsoft Active Directory). The server stores the keys in a secure environment allowing users to access their signing keys from any computer while making sure that the keys never actually leave the original server. In effect, server side signing can be thought of as a multi-user, network-attached smart card.

The advantages of server side signing are:

- ▶▶ **Cost** - Investment is much lower, (it could be only 10% of traditional/managed PKI solutions) because there is no need to create a new infrastructure; the only hardware needed is a server. Expensive PKI consultants are not necessary because this is a user-friendly, plug and play type installation.
- ▶▶ **Time** - Deployment can be accomplished in a matter of hours. The system can be up and running quickly, allowing users to begin digitally signing documents within hours of initial deployment.
- ▶▶ **Management** - Since server side signing leverages your company's existing user network directory, there is practically no management needed for the system. In effect, it is a **zero** management solution.

The server side technology also comes with a built-in CA that generates keys and certificates for users. Users are authenticated and authorized every time they sign into their computer using the existing company directory authorization or a standard authentication protocol such as Radius, OTP, Biometric, etc. Server side signing works with many different applications, such as Microsoft® Word, Excel®, Outlook®, Adobe® PDF, TIFF, AutoCAD®, InfoPath®, Lotus Forms, and many more. It can even provide for a graphical signature - users can create a visual signature that can be stored in the server and added to documentation using a signature capture device.

Server side signing works with an existing CA or an external CA. The existing CA can use the server to generate private keys and issue certificates. When working with the external CA, the server is used for key and certificate secure storage as well as signature operations. Other mechanisms, based on the external CA's enrollment process, should be used for generating end-user private keys and certificate. The server not

only stores the user's private key, it also signs the document meaning that the private key never leaves the server. Application integration can be done using either client software or via a web service protocol.

The assets of server side signing are clear and there really is no downside. It is a basic, easy-to-install and easy-to-use solution, enabling any company to have total e-security with an exceptionally cost-effective and affordable price tag.

Conclusion

Research indicates that for most companies a major obstacle to deploying a digital signature solution is the prohibitive cost of implementing this type of complex solution. Whether a company chooses to outsource a solution to a trusted third party or to develop a tradition solution in-house, the decision can cost close to half-a-million dollars over a three-year period for only 1,000 users. This is a major investment per user for a company of any size.

The simple fact is that server side signing can provide all the benefits that your business needs, without having to invest tremendous amounts of money in third party expertise or reoccurring fees. Server side signing is as effective of an option as the other implementations, and it's easily arguable that it is a superior option. Server side signing employs user-friendly systems that do not involve the hidden costs or frustrations of an in-house or an outsourced implementation. Moreover, server side signing generally costs 10% of the total cost of an in-house or outsourced solution.

As it becomes increasingly more essential for companies to implement a digital signature solution to comply with government regulations being enacted in North America and the European Union, a server-side signing solution, like ARX's CoSign® digital signature solution, is an extremely attractive, efficient, and cost effective solution. CoSign meets all of the criteria for security and complies with all of the legal standards of PKI technology. CoSign is easy-to-deploy and easy-to-use. CoSign doesn't require a significant up-front investment, nor does it pass control of your digital signature solution to an outsourcing company. On the contrary, the server side signing solution offered by ARX's CoSign allows your company to retain control, flexibility and scalability.

ARX CoSign – A Server Side Signing Solution

ARX's CoSign® is a non-forgable, simple-to-use, turn-key solution to provide digital signatures for your company. It is based on standard PKI technology that gives your company the control and flexibility it needs without the high cost. It enables your company to implement an affordable PKI solution but eliminates the hidden costs and headaches of both the traditional and the outsourced solutions.

CoSign digital signatures allow companies to expedite business processes, reduce costs, comply with industry regulations, increase document security, and help organizations go green.

CoSign features include:

- ▶ **Seal documents** - Investment is much lower, (it could be only 10% of traditional/managed PKI solutions) because there is no need to create a new infrastructure; the only hardware needed is a server. Expensive PKI consultants are not necessary because this is a user-friendly, plug and play type installation.

- ▶ **Multiple signatures** - Deployment can be accomplished in a matter of hours. The system can be up and running quickly, allowing users to begin digitally signing documents within hours of initial deployment.
- ▶ **Third party application support** - Since server-side signing leverages your company's existing user network directory, there is practically no management needed for the system. In effect, it is a zero management solution.
- ▶ **Audit trail** - Maintains a chronological sequence of audit records.
- ▶ **Web trusted** - Provides a trusted CA service for worldwide verifiable signatures.

About ARX

ARX has over 20 years of experience assisting life sciences, healthcare, governmental, engineering, banking, financial services organizations and commercial sectors to secure and streamline their business processes and transactions. ARX offers a wide range of highly scalable products designed to simplify, secure, and accelerate electronic business. For more information, please visit www.arx.com.

Digital Signatures Made Simple