

The Directory-Enabled PKI Appliance: Digital Signatures Made Simple, Approach and Real World Experience

Uri Resnitzky
Chief Scientist
Algorithmic Research (ARX)
uri@arx.com
<http://www.arx.com>

Abstract

We present a novel approach for a PKI based digital signature system for documents in an enterprise setting. A centralized appliance securely stores users' private signing keys. The appliance interfaces with the existing enterprise directory to automatically provision users' keys and certificates. Users authenticate to the appliance using their existing directory credentials in order to access their signing keys. Client applications send document hash values to the appliance to be signed therefore the signing keys themselves never leave the appliance. Streamlined user interface methods enable easy acceptance by users, while streamlined management enables minimal ongoing investment by IT staff. Real world experience with the described system is presented and shows successful deployment in a variety of organizations and markets.

1. Motivation and Related Work

In recent years the market demand for electronic signature solutions in the enterprise market has increased substantially (Gartner estimated in July 2006 between 5 to 20 percent current market penetration and less than 2 years for mainstream adaptation of electronic signatures. In July 2005 the estimate was 2-5 years [Gartner], while the 2004 report did not even include electronic signatures). This is due to increasing

transitions from traditional pen and paper solutions to efficient paperless processing systems, as well as the advent of regulatory requirements in certain markets.

By and large traditional PKI has yet to deliver on its promise to fully answer these requirements in the mass market. Traditional PKI systems are based on distributing private keys to the end-users, which aside of security concerns [Marchesini], creates a high burden in logistics, cost, help-desk support and user acceptance [Whitten] and also introduces education obstacles [Nielsen]. Management of a large distributed system of any kind is extremely hard and PKI is no exception.

On the other hand, simplistic approaches for non-standard electronic signatures are increasingly being adopted [Gartner]. These solutions range from so-called click-wrap signatures and use of static signature images to proprietary keyed hash solutions. For many organizations expedited business processes, cost reduction and user-friendly systems – rather than the security concerns of signer authenticity, data integrity and non-repudiation – drive the decision to use electronic signatures [Gartner].

Unless low cost and easy to use and manage PKI-based systems are developed, the electronic signature market in general will leave PKI technology behind, or at best, PKI based systems will be deployed only by a relatively few enterprises that can afford the demanding costs.

Some related work aimed at making PKI systems easier to deploy and use has been presented in the past: A Plug and Play approach to PKI [Gutmann], Password Enabled PKI [Sandhu], Cryptographic Mobility Solutions [Gupta], Hardware secured Credential Repository [Lorch], Delegated Cryptography [Perrin] and putting CAs on the RA desk [Ellison].

Specifically for digital signatures, recent developments such as the OASIS Digital Signature Service (DSS) specification draft [OASIS] [Pope] - a specification for digital signature processing by web services - and the support in Adobe Acrobat 8.0 for so-called “Roaming Credential” servers [Landwehr] shows some promise.

We aim to make further advances in simplifying PKI deployments for digital signature purposes in enterprises of any size.

2. Design Criteria and Goals

Simplify the PKI problem domain by concentrating on digital signatures only and on deployments characterized by a well-known set of registered users defined in a directory (such as applications for internal enterprise employees as well as some business to consumer scenarios).

The system should be as transparent and invisible to the end-user as possible in order to increase user acceptance levels and reduce the need for training. There should be minimal or no direct end-user involvement in PKI-specific tasks (which may be difficult for end-users to perform) such as key generation, certificate enrollment or certificate renewal. The system should natively support file formats and applications users are already familiar with. Graphical User Interface (GUI) elements for signing and verification should be simplified. Graphical signature images should be used to enable the user to

associate the digital signature with the traditional pen-and-paper signature.

Minimize the overhead of PKI management by not assuming or requiring that the administrator has background or training in PKI. Such assumptions may be incorrect, especially in small and medium-sized businesses, and may lead to deployment frustrations or increased manpower and training related costs. The administrator should not be required to perform ongoing PKI-related per-user or per-certificate management tasks. The system installation should be as painless as possible with defaults that cover most deployment scenarios.

The provided system should contain all the required components. There should be no need for additional 3rd party components such as a CA service contract, private key tokens, signature capture pads or electronic signature software / plug-ins.

3. Our Approach

Secure appliance with Central Storage of Signing Keys – The system is based on a secure, centrally installed, network-attached appliance that provides all the required features and manages the private signing keys and certificates. The signing keys in this system are RSA [RSA] private keys with modulus size ranging from 1024 to 4096 bits. The appliance meets the security requirements for Host Security Modules (HSMs) [FIPS140] and smartcards including a hardened operating system and tamper resistance. Signing keys and user certificates are stored in a database within the appliance and are encrypted using a key which is erased upon physical tampering of the appliance. Users can securely (see “Application Integration” below) access their signing keys from whatever computer they are working on, but the signing keys themselves are never exposed outside the

appliance. In essence the secure repository can be regarded as a multi-user network-attached smartcard.

During a signature operation, once a user is authenticated (see the next section), the document's hash value (i.e., the result of applying the SHA-1 [SHA1] cryptographic hash function to the document's content) is sent to the appliance and is then signed within the appliance using the user's private key according to the PKCS#1 [PKCS1] specification. The resulting signature data is returned to the client and is used to build a Cryptographic Message Syntax [CMS] signature which is stored back into the document.

existing authentication system in use by the organization is used to enable users' access to their appliance stored signing keys. The user is prompted for their directory logon credentials which are then transmitted securely (see "Application Integration" below) to the appliance. The appliance verifies the credentials against the organization's existing directory servers using the LDAP [LDAP] protocol and grants access to the appropriate signing key accordingly. Secure LDAP authentication methods (such as LDAP over Transport Layer Security [TLS] and digest authentication) are used so as not to expose the user's credentials on the organization's

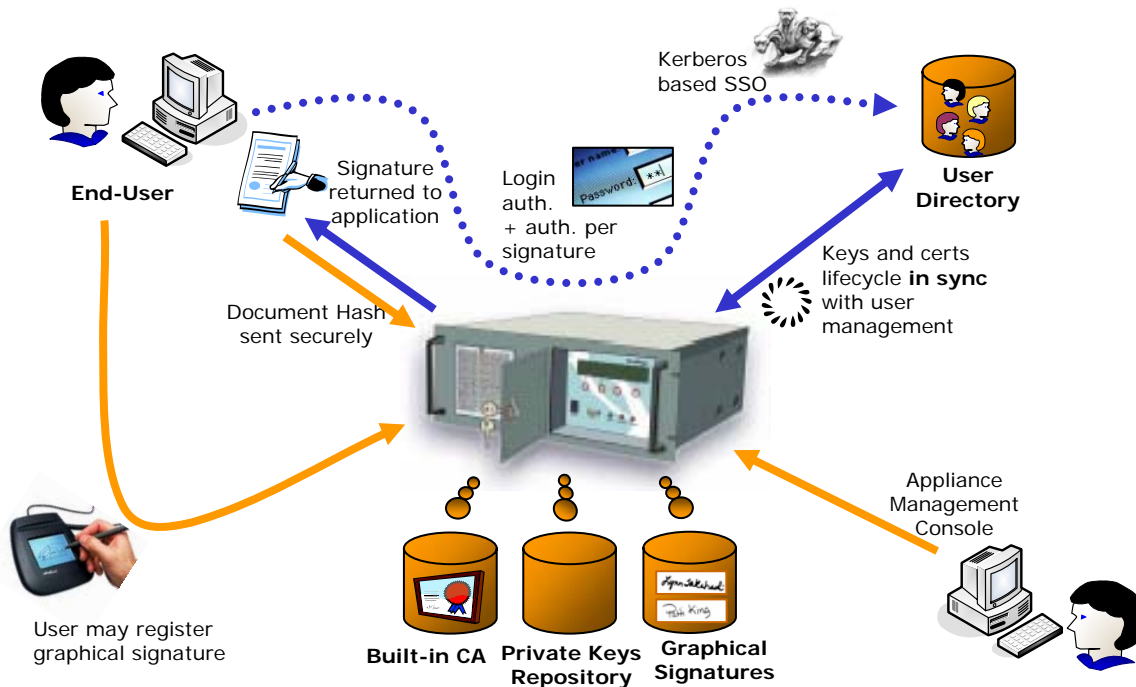


Figure 1: Architecture

The system provides a per-signature audit log. This enables an auditor to track each and every usage of any of the private signing keys contained within the appliance including the date and time of signature, the name of the signer and the hash value signed.

Leverage existing enterprise authentication infrastructure – The pre-

network. In essence this approach means that the signing key is viewed as a resource on the enterprise network to which only the authorized owner has access. In cases where single-sign-on to the directory is possible (specifically when the appliance is installed within an existing Microsoft Active Directory environment which uses the Kerberos protocol [Kerberos]), there is no

need to prompt the user for his credentials. Instead the Kerberos protocol is performed such that the user's identity is proven to the appliance using tickets granted by the directory server.

A policy setting, centrally enforced by the appliance, can be set to *require* users to manually re-enter their credentials each time they want to sign. These prompt-for-sign credentials are then securely transmitted to the appliance which validates them using secure LDAP authentication methods with the directory server. In addition, the appliance can be configured to use the Remote Authentication Dial in User Service [RADIUS] protocol in order to authenticate prompt-for-sign credentials with an additional external authentication server. This configuration is used to support a variety of authentication schemes such as two-factor authentication using one-time password devices.

Leverage existing enterprise directory and trust – User key generation, certificate enrollment, certificate renewal as well as revocation is automated based on data taken from and continuously synchronized with the organization's pre-existing user directory. The appliance includes a standalone built-in Certificate Authority which is initialized during appliance installation. The CA private RSA key is stored in the secure internal database. The CA root certificate is self-signed and includes subject name attributes which are defined during appliance installation. The appliance uses the LDAP protocol to periodically query the directory for users within a specific organizational unit (OU) which are members of a specific user group. These OU and group names are defined during appliance installation. Efficient query techniques are used to limit the load on the directory server. When a new user is detected the appliance retrieves the new user's information (common name and

email address), generates a new RSA private-public key pair and issues an X.509 certificate using the built-in CA. The certificate is constructed using a built-in template (which defines the value of extensions such as the key usage) and includes the subject's common name and email as retrieved from the directory. Note that the administrator is not required to configure the above mentioned template, rather it has default values which are designed to produce a certificate which can be used for as many purposes as possible with the currently known PKI-aware applications. The newly issued certificate is stored, along with the private key, in the internal database. The appliance automatically refreshes soon-to-be-expired user certificates for users who are still part of the directory. When a change is made to the attributes of the user's directory object (e.g. an employee changing her surname), the appliance retrieves the updated information, revokes the existing certificate and issues a new certificate for the user, based on the updated information and the existing private key. When an existing user is removed from the directory (in most cases upon leaving the organization), the appliance revokes the user's certificate from the CA and deletes the user's records including the private signing key from the internal database. This provides immediate revocation of the key material preventing any risk of forged signatures and greatly simplifying one of the major hurdles in traditional distributed PKI namely the risk that compromised signing keys will continue to be used. All the directory-enabled certificate management operations described above are performed transparently without end-user involvement.

In essence this approach means that the directory administrator (usually working with the HR department) serves as the system's RA. We rely on the fact that

organizations already have procedures and mechanisms in place to validate and control the trusted creation, modification and deletion of user objects and user attributes such as name and email in the directory.

Instead of the built-in CA, the appliance can be configured to communicate with an online CA service (using a proprietary web based protocol). In this case the same functionality is provided, with the difference being that the online CA enforces its certificate policy by validating the domain name used in the subject's email address as well as the organization name attribute in the certificate request. The online CA's policy delegates the verification of end-user identities and management of the credentials used to access the signing keys within the appliance to the customer organization's IT staff.

Publication into the directory of the CA root certificate, the CRL and users' certificates is also automatically and continuously performed. This enables smooth integration of PKI-aware directory enabled applications. This feature also enables automatic distribution of the CA root certificate into the trusted CA certificate stores of all clients in the Microsoft Active Directory domain, thus helping to automate trust in the CA root certificate within the organization.

Signing Documents in Native Format

– The approach for producing signed documents follows the most popular file formats users work with everyday: Microsoft Word and Excel, Adobe PDF, TIFF and XML forms. Native file signing produces signed files which preserve the original file format and can be viewed by the native associated applications. Where possible, verification of the signature will be done using built-in support within the native PKI-aware application (for example the ubiquitous Adobe Reader, and the built-in signature validation ability of Microsoft

Word XP and above). In order to enable legacy applications to produce digitally signed documents, a printer driver (i.e., a PDF distiller) is used that converts any data printed to it from any application into a signed-PDF document. Extensive use is made of the concept of Signature Fields which are visually distinct blocks added into the document which display the following data: signer's graphical signature image, signer's name (taken from the signer's certificate subject common name), signature date and time (in a variety of configurable display formats), signature reason (if entered) and the signature validation mark which indicates the validity status of the digital signature.



Figure 2: Signature Field Block

Streamlined GUI - Users may optionally register their graphical signature image (sometimes referred to as 'wet signature') using an electronic signature pad. The graphical signature image is securely stored within the appliance and is integrated into the signature block in native file signing. The combination of wet signature and digital signature provides a visual indication that the user is accustomed to enabling easy adaptation of the system by end-users. When using desktop applications to produce signed files, a streamlined user interface is presented to the user. In most scenarios it is sufficient to place the cursor in the desired location or drag and mark an area on the document and then click a single button to sign. After the appliance successfully generates the signature using

the user's signing key, a signature field block will be inserted into the document at the specified location.

A signing ceremony is not required. However it can be configured to include the optional elements of entering prompt-for-sign credentials, and specifying a reason for signing. Signing pre-existing empty signature fields (inserted at design time into the document template or form) is similarly easy.

Users should be aware that the act of signing a file does not prevent the file from actually being modified either from within the native application (such as Word or Excel) or from the outside (using a hex editor for example). However such modifications (and even 'benign' modification such as updating a date/time field within a Word document) will result in signature validation failure. Dealing with these issues of limiting modification access rights to signed documents is in the domain of document management and archiving systems.

Streamlined Management -

Management of the system requires minimal attention from administrators and is limited to system-wide tasks such as backup and restore of the appliance's encrypted database, secure loading of digitally signed firmware updates, modification of system-wide parameters and policy settings and download of audit logs. Management functions are only allowed for authenticated users that belong to a well-defined administrators group in the pre-existing organizational directory. Client software can be centrally deployed and configured by administrators. The client software detects and automatically connects to the appliance. This is achieved by searching the directory for an object created during appliance installation which contains the appliance's addressing information. Additional appliances can be added for load balancing

and high availability with data replication between appliances secured using Internet Protocol Security [IPSEC]. The appliance's clock can be synchronized with the directory or an external time server using the Network Time Protocol [NTP]. It is used to provide the signature-timestamp authenticated attribute when building CMS signatures.

Application Integration – The appliance integrates with the signing applications using either client-side software, or using a web services interface.

The client software contains plug-ins and applications to support native file signing. The client software communicates with the appliance over a TLS secured channel using a proprietary protocol. It provides support for the standard cryptographic APIs (Microsoft's Cryptography API [CAPI], RSA's PKCS#11 [PKCS11] and Sun's JCA [JCA]) for seamless integration with PKI-aware applications (such as Microsoft Outlook and Adobe Acrobat). The client software also includes Signature API [SAPI]. This easy to use, high-level API is a wrapper over the lower-level cryptographic APIs and is intended to be used by applications that are not PKI-aware and do not or cannot interface with the more complex cryptographic APIs. SAPI is a native file format signature API supporting the concept of signature fields as well as graphic signature image handling. As an example, SAPI can be used by a custom workflow application to enumerate and validate all the signature fields in a document, and route or process the document according to a business logic based on the number or identity of the persons which signed the document.

The appliance can be accessed directly by applications using a web-services (WS) protocol. This protocol is a profile of the latest draft of the OASIS DSS core protocol specification and implements the

full SAPI functionality direct from the appliance. When SAPI WS is used, no client component is needed, the entire document to be signed is sent to the appliance and the signed document is returned. In some cases (for example when signing PDF files) it is possible to save bandwidth by returning only the portions of the file which include the signature.

Signature Specific Features –The system provides a rich set of functionality specific to native digital-signature support for popular file formats. Within Microsoft Word and Excel it is possible to add *multiple* signature fields in order to support multiple levels of approvals. It is possible to require *dependence* of signature fields in order to make sure that clearing a signature field will ‘break’ the validity of dependent signatures. This supports hierarchical vs. side-by-side approvals. *Sectional* signing allows the user to specify that only the content of a specific cell-range or a document section is be signed. This has the advantage that other parts of the document can be updated or annotated within a workflow after the application of a signature without invalidation. The implementation uses these signature field attributes to decide which parts of the document content will be added to the hash value calculation.

4. Discussion

Note that due to the immediate revocation feature mentioned earlier, publication of a CRL by the built-in CA is not really needed. However a CRL is still published in order not to adversely affect existing functionality in PKI-aware client applications (for example the Adobe Reader enforces revocation checking by default). Because a CRL is published, and in order to limit its size, the built-in CA issues users certificates valid for one year only and then,

as long as the user is still defined in the directory, automatically refreshes them.

It may be reasonable under the described approach to issue a single very long lived CRL once at system installation, and then to issue very long lived certificates for each user instead of renewing them each year.

The limitations and tradeoffs of our approach include the need to be online when signing documents. This has to be weighed against the resulting benefit of the immediate revocation capability.

Our system provides true user mobility which is independent on the installation of smartcard readers and does not use software keys that need to be exported and imported to new machines. In addition, the most insecure point in the system, namely the end-user’s machine, does not contain any sensitive cryptographic keys, even in encrypted form, at any point during the use of the system. However the end-user’s machine is still vulnerable to abuse by attacks which allow a capable intruder to generate arbitrary signatures (but not to duplicate the private signing key for offline signatures). These same vulnerabilities exist in any smartcard based PKI system.

Our centralized approach may present to a potential attacker an attractive online target which, if successfully attacked, can yield access to many users’ keys. This means that the physical and logical security of the appliance and its computing environment must be sufficiently high to offset the risk. Further discussion on the subject of the security risks of centralization can be found in [Schneier] and [Perrin] which also covers some other relevant criticisms.

It should be noted that the system described here is most suitable for internal use within a single organization. This means that relying parties trust issues are limited to

securely distributing the built-in CA's root certificate following appliance installation to all machines within the organization. Existing IT management tools can easily support automating this task. In the case the online CA service is used, external trust is automatically achieved due to the fact that the online CA's root certificate is already built into most client platforms trusted certificate stores.

In cases where relying parties exist outside the organization and the built-in CA is used, the organization needs to publish its built-in root CA certificate and relying parties must manually import it into their trusted root stores. The system is delivered with a web site template to help IT staff setup a web page for easy download and installation of their root CA certificate by outside relying parties.

5. Real World Experience

In this section we provide details of four real-world deployments of the system presented above. For each of these deployments we describe the target market, types of documents signed, and usage statistics. The statistics were collected from the appliance audit logs, in each case covering a period of at least 4 months of usage. The statistics include the number of actual signing users, the average and peak number of total signatures per working day and the average and peak signature rate per user. We assume working weeks have 5 days of 8 hours each, and that each year has 52 working weeks. Peak values are measured over a full working week.

5.1 Radiology Center

This Missouri based center performs a full range of outpatient diagnostic radiology studies for approximately 300 referring physicians. The center's physicians

use the system to digitally sign (including a graphical signature) transcribed medical reports that are then electronically sent to patients' primary care physicians. This replaces the previously labor-intensive process of typing, printing, manually signing and faxing reports. Following an exam, a radiologist reviews a patient's films and other images, compares them with previous studies if available, and dictates a report. An on-site medical transcriptionist types the report (typically in Microsoft Word) and stores it in a secure internal database. The radiologist can then retrieve the report to review and digitally sign as required. Regulations such as HIPAA dictate that healthcare organizations must implement a system that ensures that electronic records and signatures are trustworthy, reliable and secure. Note that in this case the PKI signature is used to maintain integrity within the radiology center's own electronic record system. The electronically delivered reports are not verified by the receiving primary care physicians based on the digital signature, but rather by viewing the radiologist's graphical signature image. Transition to electronic signatures enabled the center to reduce report turn-around time from two or three hours to approximately ten or fifteen minutes from dictation to electronic delivery. Labor costs decreased significantly and accounts receivable billing and reporting also improved. This deployment illustrates that the PKI system has practical value, even within very small installations. The PKI system was installed by the customer with phone support only. Note that such small organizations do not have significant in-house IT expertise. The successful installations and use of the system indicates that the goals of making a simple to manage and use PKI system were met.

Industry	Healthcare
Signing users	9

Average signatures per working day	95
Peak signatures per working day	153
Average signature rate per user	once every 45 working minutes
Peak signature rate per user	once every 5 working minutes

5.2 Bus Manufacturer

This leading North American bus manufacturing company employs about 100 engineers which handle more than 200 electronic change orders per week. The company's business is characterized by intensive customizations which require just-in-time design, engineering and manufacturing with a short lead time. Design engineers use CAD applications which render drawings in PDF format. Each PDF file is then digitally signed together with the engineer's professional stamp and graphical signature. Drawings are then electronically stored and managed by a Product Lifecycle Management (PLM) system. Previously, each drawing was plotted on paper, signed by hand and then scanned (using a manual, expensive-to-maintain scanner) back into electronic form to be stored in the PLM system. In some cases physical transportation between facilities was required to achieve the manual signing process. The biggest benefit of the installed system to the company is the process streamlining from design to document control to production, saving a lot of time, eliminating manual phases and increasing the productivity of the engineering workforce. While the investment in the new system was justified by the savings related to the scanning of drawings alone, the company is now better suited to face its main challenge of high throughput design / build-to-order. The installation of the PKI system, performed by local IT staff with phone support, was

smooth and was followed by quick user acceptance reaching a usage level of over 100 signatures per day in under 2 weeks.

Industry	Engineering for Manufacturing
Signing users	98
Average signatures per working day	370
Peak signatures per working day	676
Average signature rate per user	once every 2.1 working hours
Peak signature rate per user	once every 6 working minutes

5.3 Clinical Trials Management

This company is a leading clinical technology services provider for the pharmaceutical industry, assisting drug manufacturers to setup systems to manage clinical trials. All 600 employees in three world-wide locations are using the system to sign large numbers of Word & PDF documents. These documents (such as Standard Operating Procedures and Audit Reports) are needed to demonstrate that the company's systems and operations are validated and quality controlled. The company is required to meet stringent industry standards such as GxP and the FDA Title 21 CFR Part 11 regulations for electronic records and electronic signatures. These regulations aim to ensure the accountability and data integrity of sensitive internal documents when moving from paper to electronic documents. The company undergoes between 40–50 customer audits annually to verify its adherence to those standards. The rapid deployment of the digital-signature system and its ease of use and tight integration with the existing user directory allowed it to be quickly adopted by company employees. Installation was achieved in a single day. Users were able to start signing documents right away and the signatures offered a look and feel that

emulated the traditional 'wet-signatures' people were comfortable with. To meet specific requirements in the FDA's Title 21 CFR Part 11, users are required to enter both user name and password each time they want to sign and in addition add their reason for signing. In some locations the system was implemented using a thin client approach – the end users remotely login into a Citrix server located at the HQ data center and sign documents directly on the HQ network. As a result of the deployment the approval process for new SOPs was expedited from 2 weeks to less than an hour. In the past, getting signatures from 3 people in 3 different offices around the world required the use of fax and courier services which are no longer needed. Electronically signing documents also reduced the need for every document to be printed, filed, microfilmed and archived. Lost or misfiled documents are no longer a problem, saving the company considerable time and money. The physical archive was replaced with an electronic document repository. Signed documents can be viewed and validated for long periods into the future as the validation uses the time when the signature was made (and not the current time) when computing the validity of the signer's certificates. However, we recognize that this does not address long term archival and cryptographic issues related to encryption algorithm aging, new analytical attacks being discovered, or evolution of storage technologies etc, which are outside the scope of our work.

Industry	Life-Sciences
Signing users	520
Average signatures per working day	72
Peak signatures per working day	133
Average signature rate per user	once every 3.5 working days
Peak signature	once every 56 working minutes

rate per user	
---------------	--

5.4 Analytical Laboratory

This company is one of the largest privately owned analytical laboratory network in North America. Their diverse range of high-quality analytical testing and consultation expertise support numerous industries including environmental sciences (water, air, soil, waste and toxicity testing), petroleum testing and field sampling services, food safety (food chemistry and nutritional labeling, veterinary drug residues and inspection), and forensics (human drug and alcohol testing, DNA, paternity and genetic identification). Approximately 100 project managers (located in 15 different labs) are using the system to electronically sign Laboratory Information Management System (LIMS) reports and Certificates of Authority in PDF, Word and Excel formats. The labs have over 1,500,000 samples tested every year in a wide spectrum of applications. With the digital signatures system implemented, signed reports can be submitted to clients as soon as the results are available in a compliant manner and as electronic evidence in a court of law. Previously the lab employees had to print, hand sign, fax, mail and archive hard copy documents associated with the paper-based processes. The labs increased their competitive advantage by decreasing the time it takes to submit reports to clients (from 1-3 business days with a paper process to immediately available using an electronic process). The lab is using dual appliances in high availability configuration. In addition, SAPI was used to directly integrate report file signing into their LIMS system. Since signed documents need to be validated outside the organization, the lab had set up their system so that the CRL is published to an externally accessible web address (instead to the default location on their internal directory). The lab's root CA

certificate was also published to an externally accessible web address along with instructions to clients on how to install this certificate in their local trusted root certificates store. It should be noted that since reports in this system are securely delivered to clients using a web portal, the lab's clients themselves are not necessarily concerned with validating the signatures. However the lab needs to protect itself from a scenario in which external parties may want to change a report to suit their needs. In this case the ability for stand-alone verification of a signed document outside of the lab's system is important for dispute resolution.

Industry	Sciences
Signing users	110
Average signatures per working day	1180
Peak signatures per working day	1400
Average signature rate per user	once every 45 working minutes
Peak signature rate per user	once every 5 working minutes

5.5 Environmental Impact

We calculate the weight of paper saved on a yearly basis in the above four deployments assuming each signature saves the printing of one standard letter-size sheet of paper. This results in an annual saving of 4480 lb (2030 kg) of paper.

Please note that the cost saving associated with the paper alone is very small compared with the other savings and benefits introduced with the digital signature system.

6. Conclusions and Further Work

In this paper we have presented a market-driven approach that enables the use of PKI technology for driving the adoption

of electronically-signed documents. We have shown how this approach is successfully deployed in the field by diverse organizations. We believe that wide spread use of PKI for electronic signatures is at hand using the approach outlined here and that every effort should be made to continue to bridge the gap between PKI technology and the mass market.

7. Acknowledgements

Thanks are due to David Chadwick and the anonymous referees for their thoughtful comments and the patient support received while drafting this paper.

8. References

[CAPI] R. Coleridge, "The Cryptography API, or How to Keep a Secret", <http://msdn2.microsoft.com/en-us/library/ms867086.aspx>, August 1996.

[CMS] R. Housley, "Cryptographic Message Syntax", IETF RFC 3852, <http://www.ietf.org/rfc/rfc3852.txt>, July 2004.

[Ellison] C. Ellison, "Improvements on Conventional PKI Wisdom", Proceedings of the 1st Annual PKI Research Workshop, pp. 165-176, August 2002.

[FIPS140] National Institute of Standards and Technology (NIST), "*FIPS Publication 140-2: Security Requirements for Cryptographic Modules*", <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>, May 2001.

[Gartner] V. Wheatman et al, "Hype Cycle for Information Security", Gartner RAS Core Research Note G00139428 http://www.gartner.com/DisplayDocument?doc_cd=139428, July 2006.

[Gupta] S. Gupta, "Security Characteristics of Cryptographic Mobility Solutions", Proceedings of the 1st Annual PKI Research Workshop, pp. 117-126, August 2002.

[Gutmann] P. Gutmann, "Plug-and-Play PKI: A PKI your Mother can Use", Proceedings of the 12th USENIX Security Symposium, pp. 45-58, August 2003.

[IPSEC] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol", IETF RFC 2401, <http://www.ietf.org/rfc/rfc2401.txt>, November 1998.

[JCA] Sun Microsystems, Inc., "Java Cryptography Architecture, API Specification & Reference", <http://java.sun.com/j2se/1.4.2/docs/guide/security/CryptoSpec.html>, August 2002.

[Kerberos] Microsoft Corp., "Windows 2000 Kerberos Authentication", <http://www.microsoft.com/technet/prodtechnol/windows2000serv/deploy/confeat/kerberos.msp>

[Landwehr] J. Landwehr, "Making digital signatures easier to use and deploy with roaming credentials", Adobe Security Matters Blog, http://blogs.adobe.com/security/2006/09/making_digital_signatures_easi.html, September 2006.

[LDAP] K. Zeilenga, "Lightweight Directory Access Protocol", IETF RFC 4510, <http://www.ietf.org/rfc/rfc4510.txt>, June 2006.

[Lorch] M. Lorch, J. Basney and D. Kafura, "A Hardware-secured Credential Repository for Grid PKIs", 4th IEEE/ACM

International Symposium on Cluster Computing and the Grid, pp. 640-647, April 2004.

[Marchesini] J. Marchesini, S.W. Smith, M. Zhao, "Keyjacking: Risks of the Current Client-side Infrastructure", Proceedings of the 2nd Annual PKI Research Workshop, pp. 128-144, April 2003.

[Nielsen] R. Nielsen, "Observations from the Deployment of a Large Scale PKI", Proceedings of the 4th Annual PKI Research Workshop, pp. 159-165, August 2005.

[NTP] D. L. Mills, "Network Time Protocol", IETF RFC 1305, <http://www.ietf.org/rfc/rfc1305.txt>, March 1992.

[OASIS] S. Drees et al, "Digital Signature Service Core Protocols, Elements, and Bindings", OASIS Digital Signature Services Technical Committee Draft, <http://docs.oasis-open.org/dss/v1.0/oasis-dss-1.0-core-spec-cd-r5.pdf>, August 2006.

[PKCS1] RSA Laboratories, "PKCS #1 v.21: RSA Cryptography Standard", <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf>, June 2002.

[PKCS11] RSA Laboratories, "PKCS #11 v2.20: Cryptographic Token Interface Standard", <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20.pdf>, June 2004.

[Perrin] T. Perrin, L. Bruns, J. Moreh and T. Olkin, "Delegated Cryptography, Online Trusted Third Parties, and PKI", Proceedings of the 1st Annual PKI Research Workshop, pp. 97-116, August 2002.

[Pope] N. Pope, J. C. Cruellas, "Oasis Digital Signature Services: Digital

Signing without the Headaches," IEEE Internet Computing, vol. 10, no. 5, pp. 81-84, September/October 2006.

Evaluation of PGP 5.0", Proceedings of the 8th USENIX Security Symposium, pp. 169-184, August 1999.

[RADIUS] C. Rigney et al, "Remote Authentication Dial In User Service", IETF RFC 2865, <http://www.ietf.org/rfc/rfc2865.txt>, June 2000.

[RSA] R.L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, vol. 21, no. 2, pp. 120-126, February 1978.

[SAPI] ARX, "SAPI Signature API Programmer's Guide Version 4.1", Pub. No. CSN.SAPI.V32.1206, Available on request from info@arx.com, December 2006.

[Sandhu] R. Sandhu, M Bellare and R. Ganesan, "Password-Enabled PKI: Virtual Smartcards versus Virtual Soft Tokens", Proceedings of the 1st Annual PKI Research Workshop, pp. 89-96, August 2002.

[Schneier] B. Schneier, "Security Risks of Centralization", Crypto-Gram, <http://www.schneier.com/crypto-gram-0403.html#11>, March 2004.

[SHA1] National Institute of Standards and Technology (NIST), "*FIPS Publication 180-1: Secure Hash Standard*", <http://www.itl.nist.gov/fipspubs/fip180-1.htm>, April 1995.

[TLS] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol", IETF RFC 4346, <http://www.ietf.org/rfc/rfc4346.txt>, April 2006.

[Whitten] A. Whitten and J.D. Tygar, "Why Johnny Can't Encrypt: A Usability