PKI Adoption Case Study
(for the OASIS PKIA TC)

High Assurance Notary Authentication and US Electronic Notarization

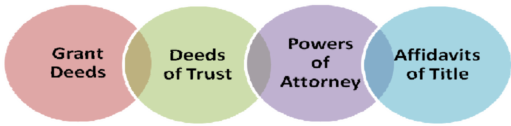
PKI Project Title	National eNotary Registry
Organisation concerned	National Notary Association
Timeframe of implementation	6 months to develop, test, and roll out
Date went live	January 2006
Case study author	Richard Hansberger
Contact details	rhansberger@nationalNotary.org

1. Business background

As the leading authority on the American Notary office, the National Notary Association (NNA) is committed to educating and supporting common law Notaries throughout the United States and to enhancing the value of the notarial act.

The Association's programs are designed to enhance Notaries' productivity and efficiency, promote professionalism, boost their careers and assist Notaries in serving society responsibly and ethically. In addition, the NNA seeks to strengthen the fraud-fighting role of the Notary and to address related industry risk management needs.

Thousands of times *every day*, a Notary assists corporations, government agencies, and private citizens by notarizing transactions that affect important legal rights and significant financial interests. Notaries serve as an impartial witness who safeguards these rights and interests from fraud and identity-theft related criminal conduct.



Through the National eNotary Registry (Registry), the NNA extends the notarial act into the realm of electronic transactions. The Registry provides legal and regulatory compliant electronic notarization services to individual and corporate members for commercial, private, and governmental electronic transactions. Where possible, some services are provided to the public free to promote the Notary's duty as a public official to serve the public at large by honoring all reasonable requests for notarial services.

2. Objectives for the PKI project

The Registry is premised on three fundamental objectives that address a variety of state and local laws, regulatory guidelines, and best practices that have traditionally governed Notaries.

- A Notary Public must use an electronic authentication credential when performing an electronic notarization. A credential identifies the Notary and serves as a reliable indicator of the Notary's authority.
- A Notary's electronic authentication credential must be trustworthy. The NNA sought and obtained accreditation from the Mortgage Bankers Association (MBA)'s Secure Identity Services Accreditation Corporation (SISAC) in its work as a Registration Authority to ensure that Registry credentials would meet stringent standards of trustworthiness in the mortgage industry (and, eventually, in every other industry Notaries serve).
- For electronically notarized documents to be reliable, interested third parties must be able to validate quickly and independently the Notary's electronic credential. Thus, the Registry maintains the free validation Web site (and related Web services), www.ensvalidate.org.

In addition to these three primary objectives, the Registry was created in response to several external business and government drivers identified by the NNA, the NNA's individual and corporate members, and state government officials who regulate Notaries.

- For commercial entities and private parties who rely on the value of notarized documents to authenticate transactions of great legal and financial significance, the Registry must provide a single source of

authentication and real-time verification of Notaries Public within a state and nationally.
- For government regulatory officials, the Registry must provide real-time access to Notary registrant data to authorized government parties (such as law enforcement or commissioning officials), as well as provide online revocation functions to protect the public from the acts of unauthorized or sanctioned Notaries.

Finally, for all who rely on the acts of Notaries (county recorders, courts, corporations, and individuals), the Registry's objectives are simple and clear. The Registry:

- Enables the simple, electronic management (i.e., issuance, revocation, renewal) of digital certificates used by Notaries;
- Allows relying parties to verify the revocation/expiration status of an ENS online;
- Facilitates the verification of the facts of an eNotarization more effectively than ever before;
- Enables the authentication or proof of electronic documents between states and nations; and
- Deters fraud by enabling faster, more accurate investigations, which ultimately protects citizens from identity crimes and document fraud related to the misappropriation of Notary credentials.

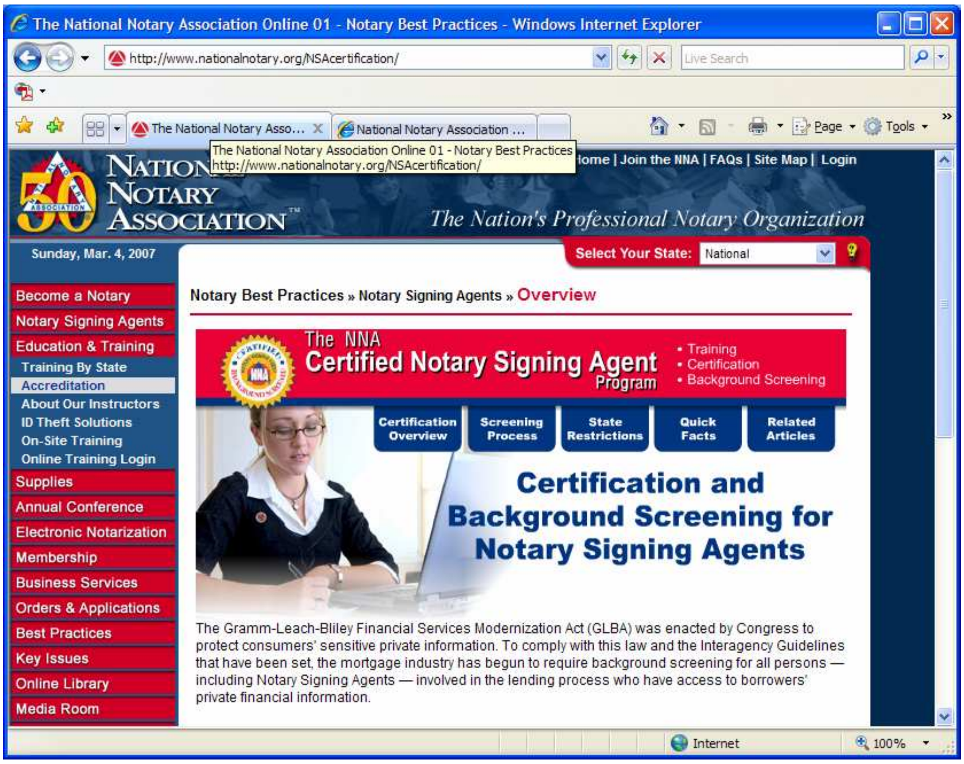
The number of users of the system is ultimately targeted at an active base of 1 million Notaries over the next ten years. The number of transactions these Notaries impact could reach well into the hundreds of millions annually.

3. System notes

- Externally, the NNA chose a relatively straightforward implementation of PKI, installing client digital certificates through an outsourced process managed by its selected Certificate Authority, ChosenSecurity.
- Installation occurs only on Windows-based operating systems (2000, XP, Vista) via Internet Explorer directly to the Windows certificate store.
- Through its CA, the NNA serves as a Registration Authority issuing SISAC Basic and Medium Assurance Level digital certificates to individual Notaries who use a variety of client Windows applications to digitally sign electronic documents, such as Adobe PDF or Microsoft Word documents. The NNA does not (and has no plans to) develop proprietary software to control the digital signature process, preferring instead to leave these processes in the hands of parties who have fiscal or legal responsibilities for the document being electronically notarized.
- The NNA requires its CA to maintain two Notary-specific certificate profiles:

- ENS Digital Certificate – valid for one year terms; issued in all states except Arizona, ENS digital certificates are valid for a period of one year.
- Arizona ENS Digital Certificate – valid for two years and whose attributes to Arizona statutory requirements.

- The subject attributes of each ENS identify the Notary uniquely to receiving parties and include, among other things, the Notary's full name as commissioned, the Notary's commission expiration date, and, in Arizona, a URL attribute that links directly to the Notary's commission status online.
- The Registry's unique AdminClient software, developed initially with Microsoft Consulting Services and managed by a Microsoft Certified Gold Partner, TAKE Solutions, Inc., handles all communications with the CA, including requests for certificate issuance, revocation, and renewal. All internal NNA staff are granted selective access to the records accessible by the software as required by their specific job functions. A handful of Registration Authority agents within the NNA manage access to and have direct responsibility for both the user accounts and Notary records maintained by the Registry.
- Finally, the Registry's vetting procedures are integrated into a larger NNA national background screening service originally developed to serve title insurers, settlement services providers, and national and regional mortgage lenders. This outsourced background screening service, outsourced to Sungard/Signix, satisfies certain regulatory requirements related to the Gramm-Leach-Bliley Act and FTC Safeguards Rule. This screening includes a county-level criminal records check, a SSN name check, and an OFAC check. An industry-developed matrix score results in a pass/fail result, and each applicant can avail themselves of an appeals and resolution process.



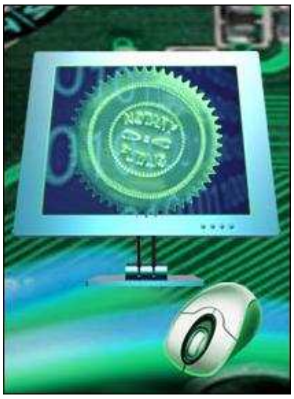
4. Business impacts

The impact of this project has been enormously beneficial to the NNA's mission, individual Notaries, and corporate members. Historically, Notaries have been governed and regulated in very different – sometimes very idiosyncratic – ways at a local level. Not so long ago, in some states a Notary's authority, for example, extended to the borders of a county line. This local management of Notaries resulted in enormous and largely unnecessary costs – both direct and indirect – to parties relying on Notaries. Imagine, for example, having a document notarized lawfully in one county and having that same document challenged in the neighboring county simply because it did not conform to the rules of the neighboring county.

The NNA has been committed to the development of practical standards and uniform laws for Notaries for 50 years. The Registry holds out the promise for the first time of a national infrastructure that could, one day, lead to an international and cooperative exchange mechanism for the cross-jurisdictional recognition of all notarial acts. This simple yet till now elusive goal would yield tremendous cost savings to both Notaries and the parties who rely on them, as well as greater legal consistency in the laws and customs that govern the recognition of notarial acts. Finally, the Registry enables greater security for notarized transactions, which translates into greater reliability and trust in the acts Notaries perform for private citizens, commercial entities, and government agencies.

Surprisingly, implementation of the project has not been terribly challenging, but as with many PKI-based systems, adoption is hard won.

5. Next steps and suggested improvements



Currently, the Registry manages client certificates installed locally on an end user's personal computer. This approach has disadvantages that are well documented, including the lack of portability of the user's private key, the risk of certificate corruption or loss in the event of a computer crash, and a myriad number of other issues that some suggest have hindered broader adoption of PKI-enabled applications.

To address these issues, the NNA will be adopting both hard token-enabled certificates for greater portability and "roaming" certificate technologies that enable server-side storage of the user's private key. In addition, the NNA has worked closely with standards groups to encourage and support the development of electronic document guidelines and specifications for industry applications that support the use of digital signatures (such as SAFE BioPharma, the mortgage industry's SMARTDOC and PDF initiatives, and others).

While the Registry support a national eNotarization infrastructure that has simply not been possible till this time, adoption of more portable and server-based systems will encourage and support greater development of practical, easy to use document processing applications that support use by PKI-enabled signers.

6. Your suggestions to the PKI industry

- Continued development of practical, consumer-based applications (such as Adobe's PDF extension technology or Microsoft Word 2007) to support the realistic affixation of digital signatures to electronic documents.
- Concerted and highly focused efforts (such as the work of the IETF's LTANS group or NARA) to address long-term storage and retrieval of digitally signed documents.
- Continued emphasis on the potent value of trustworthy and industry-neutral accreditations for Certificate Authorities and Registration Authorities in the United States.
- De-emphasizing the PKI panacea message (i.e., PKI will solve all our attribution and authentication challenges) and focusing messaging instead on actual applications providing tangible benefits to real people.