IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Hershey PA 17033-1117, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITP4137

Strategic Issues In Implementing Electronic-ID Services: Prescriptions For Managers

Bishwajit Choudhary
Advisor (Business Development & Strategy), Norwegian Banks' Payments Central, Norway
Bishwajit@hotmail.com or bc@bbs.no

ABSTRACT

During the past few years, e-security solutions (e.g., digital certificates, e-signatures, e-IDs) gained tremendous attention as they promised to plug the existing security loopholes and create global trusted e-markets. Implementation of such critical, complex and costly security solutions demands their thorough assessment at technical as well as business levels. Based on the author's experience at one of Scandinavia's leading vendors of e-banking solutions, the paper develops basic concepts, discusses strategic (product, market and technical) concerns and finally summarizes the contemporary challenges facing the implementation of e-ID schemes.

INTRODUCTION

The diffusion of e-services over open networks (Internet and Wireless) has accentuated concerns on privacy infringement, data corruption and false denial of services. This poses not merely business and legal questions, but challenges the very 'trustworthiness' of such networks as the motor of future e-commerce. Not surprisingly, the need for a robust e-security infrastructure has become essential to critical online support services (e.g., authentication, verification, authorization), value added e-solutions (for banking, commerce, stock trading) and securing the legacy systems (like customer databases, transaction histories, archives etc.).

In this backdrop, the paper introduces basic concepts, discusses strategic issues in implementing an electronic ID scheme and is organized as follows: In the first section we describe e-IDs, digital certificates and a certificate issuer (main player in operating an e-ID scheme). The needs of two other actors (namely, end-users and merchants) have been discussed in the following section. Later, the implementation of e-ID schemes is explained using a business model and selected technical considerations. Finally, we summarize key recommendations and contemporary challenges.

The expected audiences of this paper are the product and project managers implementing digital security solutions in general and e-ID schemes, in particular.

UNDERSTANDING THE BASICS

A Digital Certificate (or simply a 'certificate') is analogous to an electronic 'passport' and comprises a set of policies (or customers' rights) bound to a number of key-pairs, user's Distinguished Name (DN), name of the certificate issuer (Certificate Authority or CA) and sometimes the user-profiles. An e-ID contains a digitally signed statement from the CA and provides an independent confirmation of the certificate. A certificate (usually) also contains 3 key pairs, one each for signing, encryption and authentication. Each key pair, in turn, comprises a Public Key (publicly available) and a Private Key (known only to the authorized user). This e-security technology is popularly known as 'Public Key Infrastructure' (or PKI). *PKI is a collection of hardware, software, policy and human roles that successfully binds a subscriber's identity to a key pair (public and private) through the issuance and administration of digital certificates all through their 'life-cycle' (creation, maintenance, archival records and destruction).*

A certificate can be stored in a smart card or PC hard drive or diskette or server. It has a 'lifetime', after which it can be either suspended temporarily or terminated permanently (by the CA), if not renewed by the user. Depending on a CA's security policy, there can be different types of certificates:

Identification Certificates: CA checks that the user-name corresponds to something in the non-digital world and binds this name to the certificate issued. CA identifies the client and confirms that the client is as s/he purports to be.

Authorizing Certificates: In the medium term, a CA is likely to begin certifying both, the user-attributes and user-identity. Value-added online services such as one-to-one marketing, loyalty programs, etc. can then be provided based on user-attributes. Such a certificate states subject's address, age, relations to an organization, etc.

Transactional Certificates: They attest that an observer witnessed some form of formality (for e.g., lawyers confirming and authenticating their client's e-signatures in 'real time' from a remote location).

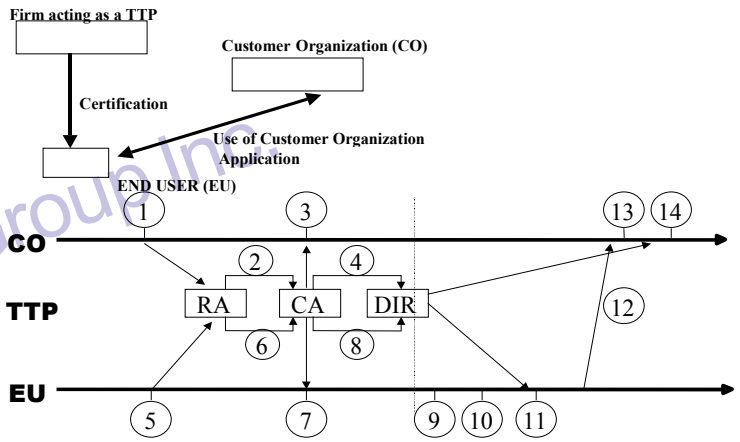
A certificate usually ensures:

- User Privacy, ensuring confidentiality
- User-Identity and rights authentication, through verification services
- Data integrity, assuring the originality of message
- Non-Repudiation (or non-denial) of the parties actually involved

Given the centrality of a CA's role in running an e-ID scheme, it is also referred to as a Trusted Third Party (TTP). *A TTP is an unbiased firm that contributes to and (often) takes liability for the lapses in security of electronic services.* In figure 1, we have presented a simple business model needed to roll out an e-ID scheme. This would also help managers identify specific roles for their businesses and points of external partnerships. We now describe the activities illustrated in the Figure 1:

1. Customer Organization (CO) or End User (EU) applies for a certificate to an RA (Registration Authority), an office authorized (by a CA) to accept & verify certificate requests.
2. If RA approves the application, it sends a request to CA.

Figure 1: Certificate value-chain[1]



This paper appears in *Issues and Trends of Information Technology Management in Contemporary Organizations,* the proceedings of the Information Resources Management Association International Conference.

3. CA returns an acknowledgement to CO, together with the CO's private keys (if generated by CA).
4. CA then publishes the CO's certificate(s), certified public keys in the TTP's directory.
5. EU will follow the same sequence of events (5 to 8 above). All the events from 1 to 8 are 'once-only' events. After event step 8, both the CO and the EU have certificates and are ready to do business. Events from 9 onwards (right side of the dotted line) through the time line show how a transaction is sent from an EU to the CO. These events maybe repeated as many times as the end-user wishes.
9. EU then runs a suitable application on his/ her system, perhaps a standard Browser, a special application supplied by CO. This generates a message which is to be sent to the CO
10. The message is digitally signed using the private signing key of the EU.
11. EU fetches the public encryption key of the CO from the directory – or, if s/he already has it, s/he checks that s/he has the correct key and that it is still valid (i.e., has not been revoked). The message is then encrypted using the CO's public key.
12. Transaction message is sent to the customer organization.
13. The CO decrypts the message, using its own private decryption key. It discovers the identity of the end-user, which claims to have sent the message.
14. The CO fetches or checks the end-user's public signing key from the directory and then checks the signature on the message to ensure its origin from EU and integrity during transmission.

STRATEGIC MARKET ISSUES

The needs of merchants and end-users define the value-propositions that a CA needs to deliver. In most cases, a CA itself provides e-services, besides the PKI support.

Merchant's Desires

- Authentication: Confirming a buyer's identity before making the sale. A merchant may also wish to build a database of customers and their buying profiles.
- Certification: The merchant may need proof that the buyer possesses an attribute required to authorize a sale. For e.g., some goods may only be sold to people over 18 years.
- Confirmation: The merchant needs to be able to prove to a third party involved in the transaction (such as a credit card company) that the customer did indeed authorize the payment.
- Non-Repudiation: The merchant wants protection against the customer's unjustified denial on order placement or non-delivery of goods.
- Anonymity: The merchant may want to control the transaction information disclosed.

User's/ Buyer's Desires

- Authentication: As stated above
- Integrity: As stated above
- Recourse: Comfort that there is an option if the seller fails to perform or deliver.
- Confirmation of order/ payments through a receipt.
- Privacy/ Anonymity: Control over the amount of information disclosed to merchant

A TTP needs to align the sales arguments for its e-security services with the specific needs of merchants and users. Such needs can be summarized in one word: 'PAIN' ('Privacy Authentication, Integrity & Non-repudiation'). Leading banks, post offices and telecom operators usually compete for the prized position of a TTP. TTPs strategically position themselves based on one or more of the following criteria:

1. Geographical reach (national or regional or global)
2. Industry specialty (banking or telecom or government etc.)
3. Specificity of certificate use with respect to
   - 3.1 Segments: B2B or P2P or P2B/ B2P or Government
   - 3.2 Solutions: Banking or Entertainment or Gambling etc.

In Norway, the banks (acting as the TTPs) have decided to first issue the 'Identity' certificates for the private markets and 'PKI-enable' their respective 'Net-bank' applications, as it immediately provides the banks with a huge volume of (already) authenticated user base.

STRATEGIC TECHNICAL ISSUES

To complement the discussions above, we now tabulate the specific technical factors necessary to establish a PKI. Their classification and discussions have been narrowed down to include only the most critical ones.[2]

Table 1: Mandatory factors necessary to establish a PKI

MANDATORY FACTORS	
1.	Subscriber initialization
2.	Registration & Certification
3.	Certificate Publication (in directory)
4.	Revocation request processing (update, suspension, revocation/ termination)
5.	CRL (Certificate Revocation List) Publication

Subscriber initialization- PKI must provide a capability to initialize new subscribers through user- friendly interfaces. Usually banks do this through their Net-banks (for existing 'authenticated' users), branch networks (for new subscribers), backed by a robust certificate life cycle management system (for request processing, certificate production, archiving and distribution).

Registration and Certification: It is the capability to issue and certify (sign) certificates and includes:

- **Initial request:** The capability for subscribers to initiate and submit a certificate request securely to the Registration Authority (RA) and/or CA in such a way that subscribers can generate key pairs. This helps RA/CA to validate subscriber's 'proof of possession'.
- **Certificate Issuance:** A capability for the RA/ CA to issue a certificate containing information and provide a capability for the certificates to be signed by the CA(s) as determined by the certificate policy.

Certificate publication: A capability to publish certificates in a repository such that recipients (or 'relying entities') can verify their certificates and entities that require a subscriber's public key to encrypt a message/session can retrieve it from this repository.

Revocation request processing: A capability to process requests from subscribers and administrators that particular certificates be revoked.

CRL publication: PKI must provide capabilities to publish/ distribute the CRLs, such that certificate recipients can be informed of certificates that have been revoked.

Network communications: Intercommunication between subscribers, managers and various PKI components must use the existing communications channels- TCP/IP, WANs, telephone networks, etc.

Table 2: Interoperability factors necessary to establish a PKI

INTEROPERABILITY FACTORS	
1.	Network Communications
2.	Pre-Existing Software
3.	Pre-Existing Standards
4.	Integration with legacy systems

Pre-existing software: PKI must be capable of managing certificates according to the formats and standards that exist in the current versions of the software already in use.

Pre-existing standards: A capability to publish certificates to a directory structure using commonly used basis as Lightweight Directory Access Protocol (LDAP).

Interoperability with legacy systems: PKI should offer integration tool-kits necessary to make complete security infrastructure, typically, firewalls, Virtual Private Network and Authorization systems.

Table 3: Scalability factors necessary to establish a PKI

SCALABILITY FACTORS	
1.	Distributed Human Administration
2.	Policy flexibility
3.	Auditability

Distributed human administration: PKI solution support for distributed administration to multiple people operating at geographically distinct locations.

Policy flexibility: PKI solution must be able to support a variety of certificates, corresponding to different certificate policies (which can differ due to type of e-service, segment or place of use).

Auditability: PKI must provide a capability to audit its main functions, include a running log of PKI activity, capability to reconstruct the state of specific certificates at some time in the past and log the activities of the PKI administrators. The logs must be tamper-proof and accessible only to authorized administrators.

In Norway, under a common 'BankID' initiative, over 150 banks & bank-groups, acting as the CAs have decided to provide the branded trusted solutions and outsource several components of their PKI (Root CA server, Bank specific CA server, Directory services and Certificate Management System) to a central operator. This operator is hosting the PKI for different e-ID schemes:

1. BankID scheme (for Norwegian banks inside Norway).
2. Operator's proprietary ID scheme for large businesses (in the Nordic region).
3. Global Online ID scheme (e.g., Identrus solution) for large international players.

CONCLUDING REMARKS

To summarize the discussions, the value of e-ID multiplies manifold in following conditions:

1. A flexible certificate policy (with respect to security levels, certificate carriers, etc.).
2. Use of open standards (for effective PKI integration with legacy systems, modifications etc.).
3. Presence of channel independent 'trusted' solutions (wrt. PCs, mobile devices etc.).
4. Presence of a large user-base.
5. Continued demand for PKI-enabled services.

However, fierce standards wars and brand rivalries between content providers and security vendors, complex revenue and liability sharing models (among partners), coupled with multiple legal interpretations of e-signature directives are some barriers to a large-scale implementation of e-ID schemes. Addressing such challenges demands tremendous business and technical skills, besides legal expertise. While the need for secure e-markets is well understood, the road ahead seems less obvious.

ACKNOWLEDGEMENT

I thank my team leader, Mr. Øyvind Apelland, Senior Vice President (Trusted Services), Norwegian Banks' Payments Central for his support and encouragement.

ENDNOTES

1 Based on 'PKI Report', Norwegian Banks' Payments Central, Oslo, 1999

2 A detailed version of this (classification) methodology has been used at the Norwegian Banks' Payments Central in specific e-ID & PKI sub-activities (Business cases, Projects, Planning, and Quality System).