IRM PRESS
701 E. Chocolate Avenue, Hershey PA 17033-1117, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.irm-press.com
ITB9075

Chapter V

Strategic Issues in Implementing Electronic-ID Services: Prescriptions for Managers

Bishwajit Choudhary
Norwegian Banks' Payments Central, Norway

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 security loopholes and create trusted electronic markets. Implementation of such critical, complex and costly security solutions demands thorough assessment at technical, as well as business levels. Based on the author's experience at one of Scandinavia's leading vendors of banking solutions and infrastructure, 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 electronic services over 'open' (Internet and wireless) networks has accentuated concerns about privacy infringement, data corruption and false denial of services. This poses not merely business and legal questions, but also challenges the basic 'trustworthiness' of open networks as the potential 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 brief, these issues summarize the backdrop for this paper.

In the first section, we introduce some basic concepts. The needs and roles of players (vendors of e-ID scheme, merchants and users) are discussed in the following section. Later, the implementation of e-ID schemes is explained using a so-called 'certificate value chain' and selected business and technical considerations. Finally, we summarize the contemporary challenges in implementing e-ID. Throughout the paper, we have tried to present simple methodologies that will help managers develop business and technology strategies. Our 'target' readers are the (product/project) managers in different stages of implementing e-ID schemes (planning-strategy, infrastructure establishment and e-ID 'enabling' of new services).

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 besides 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 three 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' (PKI). Stated formally, *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, 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 who s/he purports to be.