



Authentication platform

This white paper describes a platform for authenticating users and managing different types of credentials in a web based environment. It also discusses the associated benefits, as well as general considerations before implementation of different authentication mechanisms.

Why is this important?

Organizations today offer any number of financial services through their web sites, such as stock trading, online banking, and insurance management. Username and password (single factor authentication) is still the most common way of authenticating end users – a method that in most cases is not safe enough. An effective two-factor authentication system (2FA) is necessary for compliance with requirements (WHICH?), reducing fraud and protecting an organization from information theft. Safety must be considered a vital part of all online services involving the handling of sensitive information and monetary transactions.

Solution overview

The Authentication Platform allows organizations to manage a wide array of different authentication methods, including PKI (Public Key Infrastructure) certificates, OTP (One Time Password) tokens, and SMS OTPs. Different user groups can be equipped with different credentials depending on the level of risk. Furthermore, users can order, revoke and renew credentials through a web based portal without having to contact help desk. The solution also features a monitoring functionality, which allows administrators to keep track of users.

Considerations

The implementation of appropriate authentication methodologies should start with an assessment of the risk posed by the institution's Internet banking systems. The risk should be evaluated in light of the type of customer (e.g., retail or commercial), the customer transactional capabilities (e.g., bill payment,

wire transfer, loan origination), the sensitivity of customer information being communicated, the ease of using the communication method and the volume of transactions.

An effective authentication program should be implemented to ensure that controls and authentication tools are appropriate. Authentication processes should be designed to maximize interoperability and should be consistent with the overall strategy for Internet based customer services. The level of authentication used in a particular application should be appropriate to the level of risk in that application.

The method of authentication used in a specific Internet application should be appropriate and reasonable from a business perspective in light of the reasonably foreseeable risks in that application.¹⁾

The risk assessment process should:

- ✓ Identify all transactions and levels of access associated with Internet-based customer products and services;
- ✓ Identify and assess the risk mitigation techniques, including authentication methodologies, employed for each transaction type and level of access; and
- ✓ Include the ability to gauge the effectiveness of risk mitigation techniques for current and changing risk factors for each transaction type and level of access.²⁾

¹⁾ "FFIEC GUIDANCE Authentication in an Internet Banking Environment", Financial Institution Letter FIL-103-2005.

²⁾ Ibid by the organization itself as well as a number of national eIDs and OTPs generated by all common OTP tokens.





WHITE PAPER

Solution Description

The heart of the solution is a platform for issuing soft tokens or smart cards with certificates. It also comprises a web portal for end user self-service issuing, revoking or renewing certificates, and other credentials.

Included is also a server that sends OTPs to end users mobile phones on request. The OTP is then used for logging on to an application or a web service together with a username and password.

A validation server is used for verifying the authenticity of user credentials. The server is pre-configured to verify issued certificates.

A PKI client is distributed to end users to enable certificate log on, PIN management etc.

Use case examples

Enrolment:

A customer fills out a registration form at the website and submits it. A letter is sent to the customer containing first time log on information. A PIN is sent in another letter. Upon receiving the letters the customer again browses to the website and logs on using the provided information. The user can then download a PKI client as well as a certificate. This certificate is used for future log on. An alternative to sending mail is to let the system send an SMS containing the PIN and log on information to a pre-registered cell phone number.

Renewal/revocation:

The user browses to the web portal, logs on using the appropriate credential, and selects the desired action from an easy-to-understand menu.

Installation/integration

The system needs virtually no configuration. It ships with well defined interfaces for smooth integration with any existing environment. The system integrates well with common Identity Access Management systems.

Management

The system is managed through a central management console. It allows administrators to add or remove users, issue and revoke certificates, as well as perform general monitoring of the system.

Main Solution Components

Nexus Certificate Manager provides a trustworthy, open, standards-based system for the production and administration of electronic credentials. By offering increased functionality and security to its users, Certificate Manager remains the industry's most effective tool for PKI deployment. Certificate Manager is able to scale from the internal electronic ID deployment of small corporations, up to hundreds of hosted CAs, and manage millions of certificates with a proven ability to issue certificates at very high rates.

Nexus MultiID Server is a validation platform that handles a number of different client types, certificate issuers and certificate status services. It is module-based, making it easy to add support for additional PKI clients, protocols, catalogues and online certificate status verification services when the need arises. Furthermore it is stateless, which allows for extreme scalability.

Nexus Personal is a small footprint PKI client that enables secure authentication and digital signatures with both smart cards and soft tokens. It supports all major smart cards and is available for Windows, Mac OS and Linux platforms. Nexus Personal is the leading PKI client in Sweden. It is used by Swedish BankID (the largest Swedish national eID) – during 2010 the install base will reach ? million.

Benefits

In addition to the advantages mentioned above, a secure authentication platform brings added business benefits, by increasing the dialog between a brand and the customers.

This enables an organization to:

- ✓ Maintain customer trust and loyalty.
- ✓ Protect and strengthen the brand by minimizing the risk of identity fraud.
- ✓ Capture customer data, and send marketing information to registered customers.

Attract new customers with a secure and easy-to-use solution.

