E-SIGNATURE FOR CORPORATE ENVIRONMENTS

TrustedX

Virtual SmartCard

Description

TrustedX module for centrally managing keys and certificates:

- User keys are stored in a centralized repository that acts as a virtual smartcard.
- Users need only a standard plug-in that integrates in their applications (Explorer, Chrome, Acrobat, Office, etc.).
- Certificates can be used for both signing and encrypting (secure email with Outlook).
- Keys can be shared among several corporate users (i.e., corporation certificates).
- Centralized reporting and auditing system. All key usage is logged.

Benefits

Centralized management and control

- No need for local repositories. Keys and certificates are stored centrally in a secure and audited repository.
- Policy and role based access control. All key usage is logged.
- Multiple users can share the one certificate. Each user's usage of the key is always logged.

User oriented

- Signature/PKI complexity is masked and users only need to know one password.
- Users can have one or more certificates and also use shared certificates.
- Uniform user experience. Seamless desktop integration that is independent of the work station.

Easy to deploy

- No need for user re-provisioning as using corporate repositories (LDAP/AD, etc.) is supported.
- No deployment of cards or readers. Users can use their corporate credentials to enable their virtual cards.
- Standard desktop integration. Users can use their certificates in their applications.

Cost savings

- The advantages of a PKI without the cost of deploying and managing physical cards or local repositories.
- Elimination of the costs of administering key and certificate repositories distributed/duplicated in different user stations.• Costs arising from card loss and undetected fraudulent use are avoided.

TrustedX

Virtual SmartCard

Functions

Virtual SmartCard includes a Microsoft CAPI and/or PKCS#11 plug-in for users to remotely use the PKI keys and certificates stored in TrustedX from their desktop and office applications.

Virtual SmartCard supports key and certificate enrollment and renewal processes being performed by the users or integrated with Microsoft Autoenrollment.

Policy/role based usage

- With the one credential, users can access one or more virtual cards according to their “authorized” policy/role.
- A virtual smartcard under a policy/role can have multiple authorized users. For example, multiple authorized users can use a corporation’s certificate.

Mobility and access control

- As it is centralized, Virtual SmartCard can be used from any work station. It is enabled with a static password or a one-time password (OTP), depending on the policy/role.
- Authorization policy based system, including additional access controls: IP address, use time-period, authentication strength, etc.

Standard integration

- As it uses standard Microsoft CAPI and PKCS #11 plug-ins, it is compatible with popular browsers, Microsoft Office and common Java/.NET development tools.

Provisioning

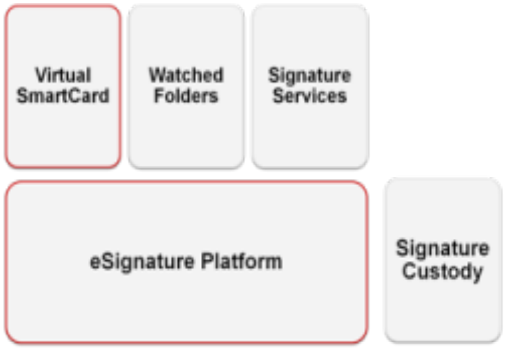
- Virtual SmartCard users can be provisioned from corporate LDAP/AD repositories or independently.
- Users can register virtual smartcards via the CA’s Web page.
- Compatible with Microsoft Autoenrollment (SCEP) services in Windows corporate environments.
- Integrated with Safelayer’s KeyOne LRA for face-to-face registration.
- Adaptable to other types of key registration and renewal procedures through integration with TrustedX.

Security and trust

- Policies/roles increases the security for virtual smartcard access: password different to the system password, use of strong and/or one-time passwords (OTP) required.
- The centralized system with an HSM FIPS 140-2 Level 3 provides a higher level of security and key protection.

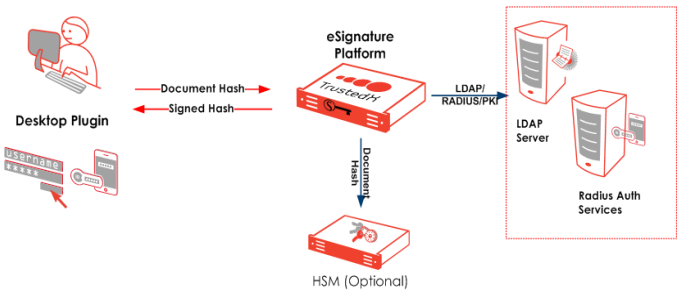
Solution scalability

- The Virtual SmartCard module is part of the TrustedX solution. This module is shown highlighted in the following diagram in relation to the other TrustedX modules.



Architecture

The following figure illustrates the Virtual SmartCard extension in the complete TrustedX solution. The HSM shown in the figure is optional.



Technical specifications

- **Format:** Software appliance. Contact for more information about supported hardware or virtual machines.
- **Integration in desktop applications:** Compatible with Microsoft CAPI and/or PKCS#11 for Windows environments .
- **Access to authentication services:** Authentication based on LDAP/AD and TMS compatible with RADIUS protocol.
- **Event monitoring:** Simple Network Management Protocol (SNMP).
- **Database and directory access:** Oracle, Microsoft SQL Server and MySQL. LDAP directory access protocol.
- **HSM support:** PKCS #11 devices approved by Safelayer.

Safelayer Secure Communications S.A.
Basauri, 17 Edif. Valrealty Edif. B Pl. Baja Izquierda Ofi. B
28023 Madrid (Spain)
Tel. +34 917 080 480 Fax +34 913 076 652

www.safelayer.com
World Trade Center (Edif. Sud- 4ª Planta). Moll de Barcelona s/n
08039 Barcelona (Spain)
Tel. +34 935 088 090 Fax +34 935 088 091

SAFELAYER