TrustedIdentity Manager

Convenient creation and management of certificates and smart cards

Selectable inclusion of integrated PKI or external PKI

Flexible generation of certificates and personalization of smart cards

In an effort to improve security, companies and government agencies are increasingly switching from password-based authentication and encryption to certificate-based two-factor authentication. Consistent use of smart cards as the basis for electronic identities makes it possible to implement trustworthy authentication and encryption in a uniform and uncompromising manner. Examples include the Windows login, VPN access, hard disk encryption, S/MIME encryption and secure authentication for other applications and single sign-on. In this context, the ability to easily generate and manage user certificates is becoming increasingly important. Today's smart cards can store a number of certificates and allow them to be used by different techniques and applications. Until now, however, the setup and implementation of suitable public key infrastructures (PKI) and other tools needed to personalize and manage smart cards and certificates typically involved challenging processes that represented major technical and economic barriers for many organizations.

Fast implementation with TrustedIdentity Manager

The TrustedIdentity Manager makes it easy to introduce and manage secure certificate-based authentication and encryption. The solution offers an integrated, compact public key infrastructure (PKI) as well as all of the necessary components for activities ranging from personalization and management of smart cards to basic management of the certificates to enable fast implementation within the organization.

Since all of the work steps are integrated into a single system, the process moves forward very quickly. Diverse workflows, from decentralized personalization to user interaction and central procedures such as printing of PIN letters, can be deployed. TrustedIdentity Manager supports automated creation, modification, recertification and termination of identities during the entire use cycle.

Secure, flexible processes, from generation to storage

Using TrustedIdentity Manager, keys and certificates are consistently generated on smart cards so that private authentication keys never leave the user-specific smart cards. The certificates and personal unblocking keys (PUKs) are stored on a secure hardware appliance that only authorized persons can access via a web interface. The hardware component of TrustedIdentity Manager has a redundant design for maximum operating reliability.

This hardware component can be scaled for all sizes of organizations, from small to very large. The central recovery function allows users to use a personal unblocking key (PUK) or a challenge/response procedure to remotely reset a lost PIN.

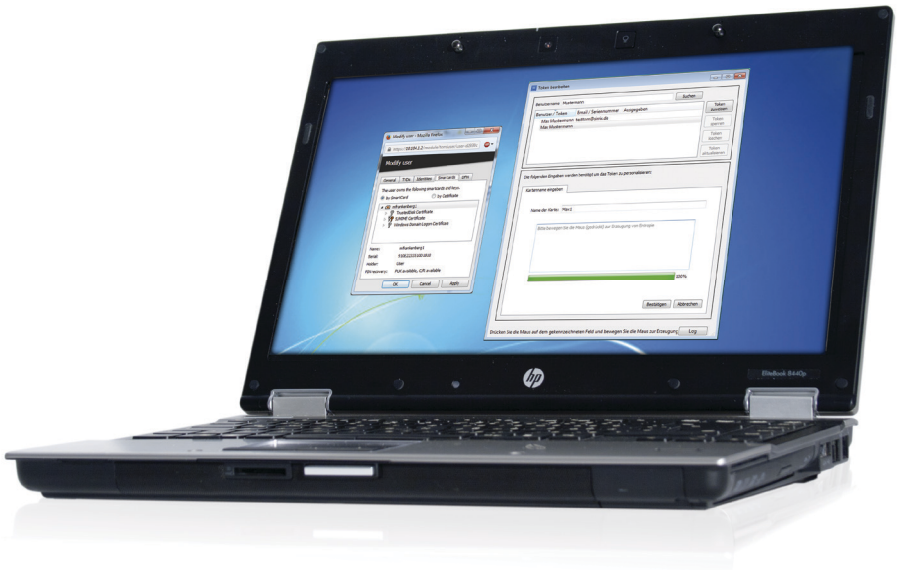
TrustedIdentity Manager

Convenient synchronization between TrustedIdentity Manager and directory services

Thanks to the ability to synchronize TrustedIdentity Manager with standardized LDAP directory services, an existing user and group organization can be used to save considerable effort during the implementation process.

The solution also allows existing public key infrastructures to be used.

The standalone TrustedIdentity Manager enables simple and cost-effective entry-level implementation in small organizations. This product is flexible and does not require a central server.



Features

Basic characteristics

- Available as extension to TrustedObjects Manager
- (TOM) or as standalone version
- Client tool usable in Windows 7 and Windows 8

Security

- Selectable inclusion of integrated PKI or external PKI
- Direct support for DFN-PKI and other corporate PKIs
- Key generation with secure random number generator on smart cards
- Optional storage of backup key material (e.g. S/MIME) on secure hardware components

Convenience

- Implementation of diverse workflows – from decentralized to fully centralized personalization
- Synchronization with standardized LDAP directory services
- Remote resetting of PINs using PUK or challenge/response procedure
- Verfügbar als Erweiterung des TrustedObjects Manager (TOM) oder als Stand-Alone Variante

Rohde&Schwarz Cybersecurity GmbH
Mühldorfstraße 15 | 81671 München
Info: +49 89 4129-206 000
cybersecurity@rohde-schwarz.com
www.cybersecurity.rohde-schwarz.com

3607573132

3607.5731.32 01.00 PDP 1 en July 2016