TrustedIdentity Manager

Komfortable Erstellung und Verwaltung von Zertifikaten und Smartcards

Wahlweise Einbindung integrierter PKI oder externer PKI

Flexible Erzeugung von Zertifkaten und Personalisierung von Smartcards

Im Zuge der Erhöhung der Sicherheit wechseln zunehmend Unternehmen und Behörden von Passwort-basierter Authentisierung und Verschlüsslung zu Zertifikat-basierter, zwei-Faktorauthentisierung. Insbesondere die konsequente Nutzung von Smartcards als Basis von elektronischen Identitäten ermöglicht eine durchgängige, einheitliche und zuverlässige Absicherung von Authentisierung und Verschlüsselung. Hierzu zählen Windows-Logon, VPN-Zugang, Festplattenverschlüsselung, S/MIME-Verschlüsselung sowie sichere Authentisierungen für andere Anwendungen und Single-Sign-On. Damit gewinnt die leichte Erzeugung und Verwaltung von Benutzerzertifikaten eine immer höhere Bedeutung. Heutige Smartcards können viele Zertifikate speichern und bieten flexible Möglichkeiten der Nutzung durch verschiedene Verfahren und Applikationen. Bisher waren jedoch Aufbau und Implementierung entsprechender Public-Key Infrastrukturen (PKI) und weiterer Werkzeuge für Personalisierung und Verwaltung von Smartcards und Zertifikaten häufig mit einem hohen Aufwand verbunden und stellten daher für viele Organisationen eine technische und wirtschaftliche Hürde dar.

Schnelle Umsetzung mit TrustedIdentity Manager

Der TrustedIdentity Manager ermöglicht die einfache Einführung und das Management einer sicheren zertifikatbasierten Authentifizierung und Verschlüsselung. Die Lösung verfügt wahlweise über eine integrierte kompakte PKI sowie über alle erforderlichen Komponenten von der Personalisierung und Verwaltung von Smartcards bis zum einfachen Management der zugehörigen Zertifikate. Diese kann deswegen innerhalb kurzer Zeit innerhalb einer Organisation implementiert werden. Durch die vollständige Integration aller erforderlichen Arbeitsschritte in einem Gesamtsystem ist eine schnelle Umsetzung gewährleistet. Dabei können unterschiedliche Workflows von der dezentralen Personalisierung durch Benutzerinteraktion bis hin zu zentralen Verfahren mit dem Druck von PIN-Briefen eingesetzt werden. Der TrustedIdentity Manager automatisiert Erstellung, Änderung, erneute Zertifizierung und Beendigung von Identitäten während des gesamten Benutzungszyklus.

Sichere und flexible Verfahren von der Erzeugung bis zur Speicherung

Mit dem TrustedIdentity Manager erfolgt die Erzeugung der Schlüssel und Zertifikate konsequent auf Smartcards, so dass die privaten Autentisierungschlüssel nie die benutzergebundenen Smartcards verlassen. Die Zertifikate und PUK (Personal Unblocking Keys) werden hingegen auf einer sicheren Hardware-Appliance gespeichert, die über ein Webinterface ausschließlich durch berechtigte Personen im Zugriff ist. Die

TrustedIdentity Manager

Hardwarekomponente des Trusted Identity Managers ist redundant auslegbar und bietet damit eine hohe Betriebssicherheit.

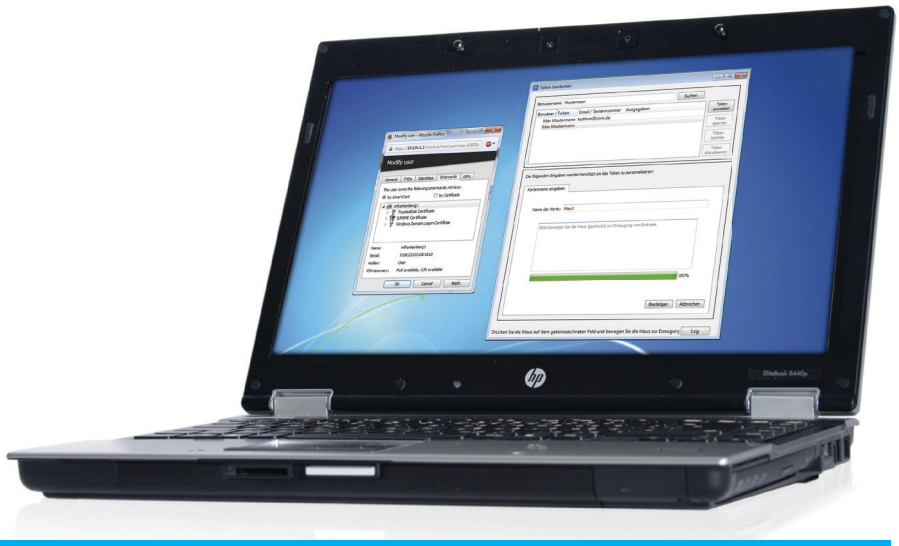
Weiterhin ist diese skalierbar für kleine bis hin zu sehr großen Organisationen. Die zentrale Recovery-Funktion ermöglicht einem Benutzer bei Verlust seiner PIN, mit Hilfe der PUK oder eines Challenge-Response-Verfahrens, die Remote-Rücksetzung der PIN.

Komfortable Synchronisation des TrustedIdentity Managers mit Verzeichnisdiensten

Die Möglichkeit der Synchronisation des TrustedIdentity Managers mit standardisierten LDAP-Verzeichnisdiensten, ermöglicht eine bestehende Benutzer- und Gruppenorganisation zu nutzen und dadurch erhebliche Mehraufwände bei der Realisierung zu vermeiden.

Gleichzeitig ermöglicht die Lösung die Nutzung vorhandener Public-Key-Infrastrukturen.

Für die leichte und kostengünstige Realisierung in kleinen Organisationen gibt es den TrustedIdentity Manager Stand-Alone. Dieser ist flexibel ohne zentralen Server nutzbar.



Features

Basiseigenschaften

- Verfügbar als Erweiterung des TrustedObjects Manager (TOM) oder als Stand-Alone Variante
- Client-Tool einsetzbar für Windows 7 und Windows 8

Sicherheit

- Wahlweise Einbindung integrierter PKI oder externer PKI.
- Direkte Unterstützung der DFN-PKI und weiterer Unternehmens-PKIs
- Erzeugung der Schlüssel erfolgt mithilfe sicherer Zufallsgeneratoren auf den Smartcards
- Optionale Speicherung von Backup-Schlüsselmaterial
- (z.B. S/MIME) in sicheren Hardwarekomponenten

Komfort

- Verschiedene Workflows von dezentraler bis hin zu komplett zentraler Personalisierung abbildbar
- Synchronisation mit standardisierten LDAP-Verzeichnisdiensten
- Remote-Rücksetzung von PINs mittels PUK oder Challenge-Response-Verfahren

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

3607573131

3607.5731.31 01.00 PDP 1 de July 2016