Next Generation Corporate PKI

Der Einsatz von zertifikatsbasierten Anwendungen für Personen und Systeme nimmt laufend zu. Die Gründe hierfür sind primär die einfache Verwaltung der Sicherheitsmerkmale und breite Unterstützung durch Applikationen.

Immer mehr Applikationen und Infrastrukturkomponenten unterstützen den Einsatz von Zertifikaten. Aufgrund der standardisierten Protokolle und Strukturen können die verschiedenen Komponenten reibungslos miteinander interagieren. Mit dem Einsatz moderner Public Key Infrastrukturen (PKI) können Zertifikate von Personen und Systemen effizient ausgegeben und verwaltet werden.

Warum Next Generation?

Das eigentlich Neue an der PKI sind die Komponenten im Zusammenhang mit der Ausgabe, Verwaltung und Validierung von Zertifikaten. Während bei bisherigen Public Key Infrastrukturen die Installation der Zertifikate und die damit verbundenen Ausgabeprozesse manuell und applikationsspezifisch durchgeführt wurden, werden bei der Next Generation PKI diese Prozesse einheitlich und standardisiert durchgeführt. Dies ermöglicht neben einer einfachen Ausgabe auch eine effiziente und sogar automatisierte Verwaltung und Überwachung der Zertifikate.

Architektur und Verantwortung

Die Ausgabe, Erneuerung, Sperrung und Verwaltung von Zertifikaten erfolgt über sogenannte Enrollment-Services. Eine PKI kann mehrere Enrollment-Services haben. Diese können beispielsweise nach Anwendungen oder Komponenten (z. B. Webserver, Netzwerkkomponenten, Laptop, iPhone, Smartcard usw.) oder auch nach unterschiedlichen organisatorischen Strukturen (z. B. Divisionen, Länderspezifisch usw.) aufgebaut werden.

Ein Enrollment-Service umfasst grundsätzlich die folgenden Punkte:

- Standardisierte organisatorische Prozesse im Zusammenhang mit der Registrierung oder Sperrung von Komponenten oder Personen
- Standardisierte technische Schnittstellen für die Ausgabe, Erneuerung, Verwaltung und Überwachung von Zertifikaten
- Standardisierte Metadaten für die organisatorische Verwaltung und Überwachung der Zertifikate (Benachrichtigungen von verantwortlichen Stellen usw.)
- Standardisierte Prüfpfade

Die zuvor genannten Punkte werden in enger Zusammenarbeit mit den Verantwortlichen der PKI und den Verantwortlichen des jeweiligen Enrollment-Services definiert.

Herausforderung Notfallprozesse

Bei personenbezogenen Zertifikaten, die auf Smartcards oder USB Tokens ausgegeben werden, müssen neben den zuvor genannten Punkten im Zusammenhang mit der Ausgabe und Verwaltung von Zertifikaten noch verschiedene Notfallprozesse etabliert werden.
Diese wären beispielsweise:

- Dezentrale Ausgabe eines neuen Tokens bei definitivem Verlust des bestehenden Tokens
- Dezentrale, rasche Ausgabe eines temporären Tokens bei temporärem Verlust des bestehenden Tokens (zu Hause vergessen)
- Sicheres Setzen eines neuen PINs bei Verlust des bisherigen PINs
- Sicheres Einloggen ohne Token bei Verlust des bisherigen Tokens auf Reisen

Bisher mussten die zuvor genannten Prozesse individuell spezifiziert und umgesetzt werden.
Next Generation PKI Komponenten wie beispielsweise die Microsoft 2008 CA in Verbindung mit Windows Vista oder Windows 7 unter Verwendung moderner Smartcards unterstützen standardisierte, organisatorische und technische Prozesse in diesem Zusammenhang. Die standardisierten und eng aufeinander abgestimmten Prozesse und Schnittstellen erlauben einen nachhaltigen Einsatz von Smartcards und USB Tokens.

Corporate PKI vs. Public PKI

Eine Corporate PKI sichert einem Unternehmen die Flexibilität, die es braucht, um die Enrollment-Services und die damit verbundenen technischen und organisatorischen Prozesse rasch und flexibel integrieren zu können. Ein Outsourcing einer Corporate PKI ist wenig sinnvoll, da die zentralen Prozesse wie die Registrierung von Benutzern und Systemen oder die Integration von PKI-basierten Applikationen nur durch das Unternehmen selbst durchgeführt werden können. Um eine Corporate PKI global bekanntzumachen, kann diese von einer öffentlichen CA subordiniert werden. Der Betrieb einer solchen «Public Corporate PKI» unterliegt den jeweiligen Richtlinien der öffentlichen CA und kann auch als Gütesiegel einer Corporate PKI betrachtet werden.

Wichtige Erkenntnisse

Immer mehr Unternehmen entscheiden sich für den Aufbau einer eigenen Public Key Infrastruktur. Primärer Treiber für einen solchen Entscheid sind die folgenden Gründe:

- Vereinfachen und standardisieren von administrativen und technischen Prozessen im Zusammenhang mit der Ausgabe und Verwaltung von applikatorischen oder personenbezogenen Sicherheitsmerkmalen
- Erhöhen und standardisieren der Sicherheit (Authentisierung, Verschlüsselung usw.)
- Nutzen von Off-the-shelf-Sicherheitstechnologien in modernen Applikationen ■

Keyon AG , 8645 Jona
Telefon 055 220 64 00, Telefax 055 220 64 01
info@keyon.ch, www.keyon.ch