THEMENBLATT **Public Key Infrastructure**

Erzeugung, Management und Prüfung elektronischer Zertifikate

- ✓ Starke Authentisierung für Intra-/Extra-/Internet-Ressourcen
- ✓ Sichere Kommunikation mit SSL/TLS
- ✓ Elektronischer Zeitstempel (qualifiziert - akkreditiert)
- ✓ Signatur und Verschlüsselung von E-Mail (S/MIME) und elektronischen Dokumenten
- ✓ Internet der Dinge (z.B. Smart Meter Datenaustausch)
- ✓ Mobile PKI und Mobile Device Management u.v.m.

Die Herausforderung

Vertrauen als oberstes Ziel

Der Nachweis von elektronischen Identitäten – egal ob Personen, Organisationen oder Geräten – lässt sich vertrauenswürdig nur durch den Einsatz elektronischer Zertifikate sicherstellen. Dies gilt abgeleitet ebenso für die Integrität elektronischer Dokumente und Nachrichten durch den Einsatz von elektronischen Signaturen. Auch beim sicher verschlüsselten Datentransport kommen zertifikatsbasierte Lösungen zum Einsatz. All diese Szenarien setzen eine Komponente zur Erzeugung, Management und Prüfung voraus – eine Public Key Infrastrucutre (PKI).

Ein Beispiel: vertrauenswürdige Kommunikation

Zum Aufbau einer abgesicherten elektronischen Kommunikation bietet sich der Einsatz kryptografischer Verschlüsselungslösungen an. Zur Überprüfung der elektronischen Identität von Absender bzw. Empfänger werden in der Praxis elektronische Signaturen an Dokumente und/oder Nachrichten angebracht.
Bei der asymmetrischen Verschlüsselung müssen für jeden Kommunikationspartner ein Schlüsselpaar (privat und öffentlich) erzeugt werden. Möchte nun ein Absender an den Empfänger eine verschlüsselte Nachricht übermitteln, benötigt er den öffentlichen Schlüssel des Empfängers.

Hauptbestandteile/Funktionen

- Registrierungsstelle
- Zertifikatsgeneration
- Zertifikatssperrlisten
- Verzeichnisdienst
- Validierungsdienst

Ausstellung elektronischer Zertifikate

Ähnlich wie in anderen Bereichen werden elektronische Zertifikate von der sog. Zertifizierungsstelle einer Organisation herausgegeben. Verwendet wird hier der Begriff Certification Authority oder CA. Die Gültigkeit von öffentlichen Schlüsseln wird hier durch digitale Signaturen der CA bestätigt.
Neben dem Schlüssel selbst enthält das digitale Zertifikat weitere Informationen, wie Gültigkeitsdauer etc. Als verantwortliche Instanz ist die CA die zentrale Zertifizierungskomponente in der Public-Key-Infrastructure.

Registrierung elektronischer Zertifikate

Zur Wahrung der Vertrauenswürdigkeit der CA ist vor Erteilung des elektronischen Zertifikates eine eindeutige Prüfung der Identität der beantragenden Person oder Organisation notwendig. Dies wird von der Registrierungsstelle oder Registration Authority (RA) geleistet.

Überprüfung elektronischer Zertifikate

Zur Überprüfung der Gültigkeit elektronischer Zertifikate wird ein Validierungsdienst oder Validation Authority (VA) benötigt. Generell unterscheidet man die Prüfung gegen eine veröffentlichte Zertifikatssperrliste (CRL) oder die Echtzeitprüfung durch einen Online Certificate Status Protocol (OCSP) Dienst. Die Wahl der Prüfungsvariante ergibt sich aus dem jeweiligen Einsatzszenario.

THEMENBLATT **Public Key Infrastructure**

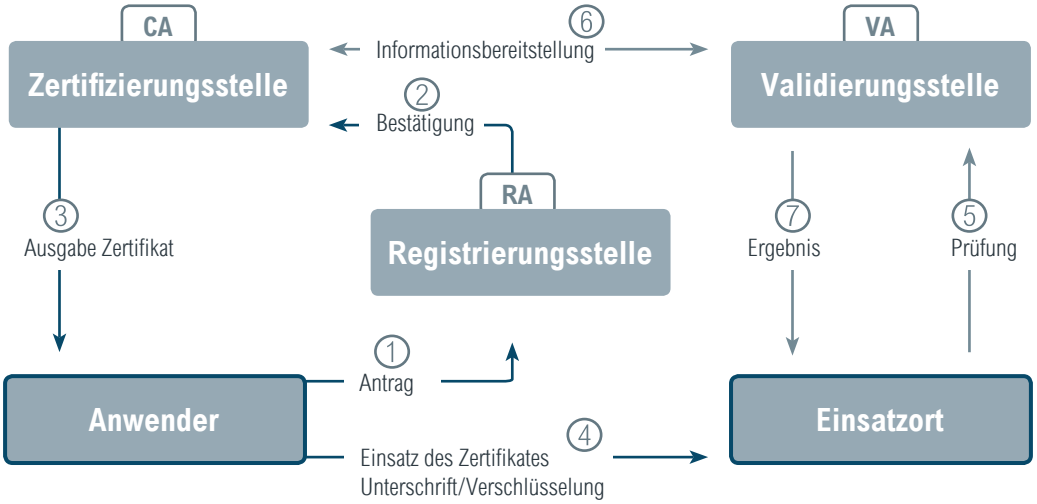
Erzeugung, Management und Prüfung elektronischer Zertifikate

Nachweis

In Abhängigkeit des juristischen Status der PKI wird in den meisten Einsatzfällen die rechtlich verwertbare Protokollierung aller Transaktionen in einer PKI sinnvoll oder gar notwendig sein. Grundlage dafür bietet die Archivierung dieser Transaktionen nach BSI TR-ESOR.

Empfohlene Systemkomponenten

- proNEXT Security Manager
- proNEXT Archive Manager
- proGOV Module



Die Lösung

Als komplexe Gesamtlösung verlangt eine PKI notwendigerweise optimal aufeinander abgestimmte Einzelkomponenten. Mit den Produkten der proNEXT Familie ist die procilon in der Lage, anspruchsvolle PKI zu realisieren.

Die Einsatzmöglichkeiten reichen dabei von Signatur und Verschlüsselung von E-Mails (S/MIME) über Authentisierungsprozesse bis zur schnellen Erzeugung von Zertifikaten im „Internet der Dinge“. Optimal sind alle Komponenten auch für mobile Anwendungen geeignet. Die Anbringung einer elektronischen Signatur an Dokumente ist ebenfalls abgedeckt. Je nach Status des Betreibers und des Sicherheitsstandard des zugehörigen Rechenzentrums können unterschiedlichste Lösungen aufgebaut werden. Dies reicht von einer Root-CA als sogenannter Vertrauensanker bis zu streng hierarchischen PKI mit mehreren Sub-CAs. Auch eine Cross-Zertifizierung mit anderen PKI ist realisierbar.

procilon realisiert PKI mit international nach CC EAL 4+ (Angriffsschutz hoch) evaluierten und nach dem Signaturgesetz bestätigten Standardkomponenten.

Die Anforderungen an Datensicherheit werden über eine Ende-zu-Ende Verschlüsselung unter Verwendung von AES 256 und RSA Verschlüsselung (2048 Bit Schlüssellänge) erfüllt.

Die Auswahl und Nutzung der kryptographischen Algorithmen und relevanter Parameter orientiert sich dabei an den vom BSI stetig aktuell gehaltenen Vorgaben und Empfehlungen.

Kontakt

procilon GROUP
Leipziger Straße 110
04425 Taucha

+49 342 98 48 78-31
anfrage@procilon.de
www.procilon.de