

Z1 Backbone of Trust

Kostendruck und Globalisierung sind zwei Trends, die die Nachfrage nach eBusiness-Lösungen ankurbeln. Viele Unternehmen haben aber zu Recht Vorbehalte ihre Geschäftsprozesse über öffentliche Datenleitungen (z.B. Internet-Verbindungen) abzuwickeln. Zu hoch ist das Risiko, Opfer von Industrie- und Wirtschaftsspionage zu werden. Public Key Infrastructure-Technologie (PKI) bietet alle notwendigen Sicherheitsfunktionen, die für eine sichere eBusiness-Infrastruktur notwendig sind: eindeutige Identifizierung der Benutzer, Datenverschlüsselung sowie elektronische Signatur. Die Trennung von privaten und öffentlichen Schlüsseln (public keys) hat sich seit über zwei Jahrzehnten bewährt. Die Verfahren sind weltweit standardisiert und anerkannt. Obwohl PKI-Technologie inzwischen auch Bestandteil moderner Betriebssysteme ist, setzen nur wenige Organisationen diese wirklich ein.

Die Mitarbeiter der Zertificon Solutions GmbH haben in den verschiedensten PKI-Projekten mit Unternehmen und öffentlichen Institutionen ähnliche Erfahrungen gemacht: Der Verwendung der privaten Schlüssel (private keys) z.B. per SmartCards wurde in PKI-Projekten viel Aufmerksamkeit gewidmet und die Verteilung an die Mitarbeiter ist in vielen Organisationen geglückt. Allerdings übernehmen die *private keys* nur einen Teil der Sicherheitsfunktionen. Mit *private keys* können z.B. verschlüsselte E-Mail-Nachrichten lesbar gemacht werden. Andererseits sind für die essentiellen Sicherheitsfunktionen wie die Überprüfung der Absender-Echtheit einer E-Mail oder die Verschlüsselung einer E-Mail der öffentliche Schlüssel (public key) einer Person oder Organisation notwendig.

Meistens erfolgt die Bereitstellung eines *public keys* über ein Zertifikat. Mittels eines Zertifikats bestätigt eine dritte Instanz (ein Anwender, besser aber ein TrustCenter oder eine Certification Authority (CA)) die Echtheit und die Zugehörigkeit des öffentlichen Schlüssels zu einer Person oder Organisation.

Anwender, die verschlüsselte E-Mail versenden wollen, benötigen daher nicht nur die stets aktuellen und authentischen Zertifikate **aller** Kommunikationspartner, mit denen sie vertraulich kommunizieren wollen, sie müssen vor **jedem** E-Mail-Versand **alle** Zertifikate bis hoch zur ausstellenden Instanz auf Gültigkeit prüfen.

Dies erfordert nicht nur das erforderliche Verständnis, sondern auch vertieftes IT-Know-how und eine ganze Reihe von Arbeitsschritten. Die Praxis zeigt, dass Anwender mit diesem sog. externen Zertifikatsmanagement völlig überfordert sind, Organisationen die Kosten für die Schulung der Anwender und den Aufwand für das Zertifikatsmanagement scheuen und PKI-Projekte an dieser Stelle oft abgebrochen wurden. Dabei spielt es keine Rolle, auf welchem der beiden weltweit gleichermaßen verbreiteten Standards (X.509-Standard oder OpenPGP) die PKI-Lösung basiert: Für einen „normalen“ PC-Anwender ist die Beschaffung und die Überprüfung der Gültigkeit von Zertifikaten zu komplex und unverständlich.

Mit **Z1 Backbone of Trust** stellt Zertificon Solutions eine server- und XML-basierte Lösung vor, die eine PKI anwenderfreundlich macht und die getätigten Investitionen rettet.

Z1 Backbone of Trust trennt das Management der externer Zertifikate von den Client-Anwendungen z.B. für firmenweite eMail-Sicherheit und konzentriert die Beschaffung, Verwaltung und Validierung von externen Zertifikaten und PGP-Keys auf dem zentralen Z1 BOT Server.

Das externe Zertifikatsmanagement mit Hilfe eines zentralen Zertifikatsservers bietet folgende Vorteile:

- Komplexität und Kosten der PKI-Handhabung sinken
- Anwender-Akzeptanz und Nutzung steigen
- outsourcing-fähig (= kann von externen Dienstleistern z.B. in Berlin durch PSI Net als MSS (Managed Security Service) betrieben werden)
- Ermöglicht eMail Security als Dienstleistung
- Ende-zu-Ende Sicherheit bleibt gewährleistet (Client-Anwendungen führen die Sicherheitsfunktionen weiterhin lokal aus)
- Anwendungen, die öffentliche Zertifikate verwenden (PKA), werden durch die Zentralisierung deutlich „schlanker“ und einfacher im Roll-out
- Durch die Synchronisierung mehrere Systeme (Z1 BOT Server) kann beim Einsatz in ausfallsensiblen eBusiness-Systemen Hochverfügbarkeit gewährleistet werden
- Das Sicherheitsniveau ist durch automatisierte Prozesse immer auf dem aktuellsten Stand
- Das Sicherheitsniveau ist durch den gemeinsamen Zertifikatspool einheitlich (ausscheidende Mitarbeiter werden Rechte entzogen, neu hinzukommende Mitarbeiter werden automatisch in die geschützte Kommunikation zu externen Geschäftspartnern einbezogen)

Kontakt

Michael Zeyen
Zertificon Solutions GmbH
Landsberger Allee 117
D-10407 Berlin
phone: +49-(0)30-5900 300-33 (fax -99)
mail: m.zeyen@zertificon.com
<http://www.zertificon.com>