

Medieninformation zur sofortigen Veröffentlichung

Public Key Infrastructure PKI – Quo-Vadis ?

Zürich, 20. November 2001: Verschlüsselungen und elektronische Signaturen galten lange als Mittel, die Sicherheit, Integrität und Authentizität in offenen Netzwerken gewährleisten. Für viel Geld und unter grossem Standardisierungsaufwand wurden Zertifizierungs-Infrastrukturen aufgebaut und in der Folge kommerziell genutzt. Auf Grund mangelnder Anwendungen, technologischer Hemmnisse, unklarer bzw. unangemessener juristischer Situation sowie eines fehlenden allgemeinen Sicherheitsbewusstseins gerieten die entsprechenden Unternehmen in wirtschaftliche Schieflage. Die elektronischen Unterschriften laufen nun Gefahr, neben dem E-cash und anderen e-Anwendungen zu einer weiteren Internettechnologie zu werden, die sich auf dem Markt nicht durchsetzen kann.

Informationssicherheit ist heute eng mit dem Thema „digitale Signaturen“ verknüpft. Dabei wird zwar die Notwendigkeit der Verschlüsselung aufgegriffen, aber nicht klar genug verdeutlicht, dass e-Commerce ohne entsprechende Verschlüsselungsinfrastrukturen nicht florieren wird. Kommerzielle Zertifizierungsinstitutionen kämpfen dementsprechend mit grossen wirtschaftlichen Schwierigkeiten bzw. haben bereits aufgegeben.

In Public-Key Infrastrukturen (PKI) werden allgemein die öffentlichen Schlüssel der Teilnehmer verwaltet, die für die elektronischen Unterschriften benötigt werden, sowie die Zertifikate, welche die Echtheit dieser Schlüssel bestätigen. Zentrales Element jeder PKI ist die Zertifizierungsinstanz, auch "Trustcenter" genannt, welche die Identität der Teilnehmer prüft und Aussagen über Gültigkeit und Gültigkeitsdauer von Signaturen ermöglicht.

Benötigt das e-business eine funktionierende Infrastruktur für elektronische Signaturen ?

Über das Internet werden bereits heute erhebliche Summen für Einkäufe ausgegeben, ohne dass sich die Käuferschaft der möglichen Risiken bewusst ist. Namhafte Experten sind der Meinung, dass im Business to Consumer-Bereich (B2C) – also überall dort, wo Direktgeschäfte mit dem Endkunden stattfinden – elektronische Signaturen nicht notwendig seien. Dies mag erklären, warum Endkunden keinen Anreiz verspüren, sich für das Online-Shopping einen virtuellen Pass, sprich eine elektronische Unterschrift, zu besorgen.

Gibt es doch noch Hoffnung ?

Die Verfechter und Verkäufer von Technologie-Produkten setzen ihre Hoffnungen auf den wachsenden Markt von mobilen Netzzugangsgeräten wie Handies oder PDAs (Personal Digital Assistant). Beim Handy könnte die Authentifizierungssoftware und die dazu gehörende elektronische Unterschrift direkt in die Smart Card integriert werden, die für den Betrieb notwendig ist. Konsortien wie E-Sign oder M-Sign arbeiten bereits an entsprechenden Standards.

Auch die Architekten virtueller Rathäuser glauben, dass die surfenden Bürger elektronische Signaturen akzeptieren, wenn sich damit der Behördengang sparen lässt. Anwendungsgebiete wie Steuerwesen, elektronische Abstimmungen etc. bedürfen der einwandfreien und rechtsgenügenden Authentisierung der Partner – sowohl auf Bürger- als auch auf Behördenseite. Beide Gruppen haben ähnliche Interessen: der Bürger will wissen, wem er seine Informationen anvertraut, die Behörde muss wissen, wer die Informationen liefert.

Daher ist die Instanz eines vertrauensvollen, neutralen Dritten nötig, um die Signatur einer Person zuordnen zu können. Wer aber genießt das nötige Vertrauen, um die Aufgabe des Trustcenters zu erfüllen?

Die Erfolge einiger namhafter Schweizer Unternehmen, die Herausforderung PKI mit erheblichen Investitionen in den Griff zu bekommen, weisen auf die Notwendigkeit von PKI hin. Nach der Einstellung der Zertifikatsvergabestelle Swisskey drängen sich aber folgende Fragen auf:

- Ist eine übergeordnete Zertifizierungsstelle notwendig oder sollen die Unternehmen selbst - eventuell im Verbund mit anderen - Zertifikate ausstellen?
- Braucht die Schweiz eine eigene, nationale Zertifizierungsstelle oder könnten ausländische Institutionen die Anforderungen problemlos erfüllen?
- Wie lange wird es dauern, bis Zertifikate weltweit integriert und ausgetauscht werden können? Für welche Geschäftsprozesse ist das notwendig?
- Welche Konsequenzen ergeben sich für kleine und mittlere Unternehmen, die sich keine corporate PKI leisten können?
- Welchen Einfluss haben unsere heutigen Entscheidungen bezüglich PKI auf die langfristige und nachhaltige Entwicklung der Schweizer Wirtschaft?

Die vierte Berner Tagung für Informationssicherheit der Fachgruppe Security (FGSec), der Schweizer Informatiker Gesellschaft (SI) sowie des Informatikstrategieorgans Bund (ISB) informiert mit Referaten und einer Podiumsdiskussion. Schlüsselpersonen aus Wirtschaft, Verwaltung und Politik leisten einen Beitrag zur Klärung und Entwicklung dieser aktuellen Themenstellung mit Konsequenzen von grosser Tragweite. An der Tagung werden Beiträge zum Erarbeiten von Entscheidungsgrundlagen bezüglich PKI präsentiert. Anhand von Szenarien werden zudem mögliche zukünftige Entwicklungen kontrovers diskutiert.

Die Berner Tagung für Informationssicherheit findet am 20. November 2001, 13.30, im Hotel Schweizerhof in Bern statt.

Weitere Informationen

*Dr. Andrea Leu
C/o Senarclens, Leu + Partner AG
Freigutstrasse 8
8027 Zürich
01-201 73 00
andrea@senarclens.com*

*Anmeldung zur Tagung unter:
Fachgruppe Security, www.fgsec.ch*