

PKI (Public Key Infrastrukturen) und Digitale Signaturen

Heilbronn, 11. März 2002

Eberhard Holler
Consulting & Networks

PKI - Die Anforderungen kommen vom E-Business

E-Business umfasst alle geschäftlich relevanten Vorgänge, die Unternehmen und staatliche Stellen über offene elektronische Netze abwickeln.

- **Voraussetzung: leistungsfähige Sicherheitsverfahren**
 - Sicherstellung der **Vertraulichkeit** und **Integrität** (Nichtveränderung) der übertragenen Informationen,
 - Nachweis der **Identität** von Personen (Authentisierung)
 - **Nicht-Abstreitbarkeit** von Willenserklärungen (Signieren).
- Um verbindlich miteinander zu kommunizieren, muss sichergestellt werden, dass derjenige auch wirklich derjenige ist, für den er sich ausgibt.

PKI - Asymmetrische Kryptographie

PKI verbindet Schlüsselpaar (privater und öffentlicher Schlüssel) mit einer Person, aber auch mit IT- Objekten.

- Entscheidend für die Sicherheit des Verfahrens ist, dass der private Schlüssel einmalig und die Geheimhaltung gewährleistet ist.
- **Historie**
 - Entwickelt Mitte der 70er Jahre durch W. Diffie und M. Hellman

PKI - Asymmetrische Kryptographie

Zertifikate werden von einer vertrauenswürdigen Instanz ausgestellt.

- **Vertrauenswürdige Instanz.**
 - ZDA: Zertifizierungsdiensteanbieter, Trust Center, CA: Certification Authority)
- **Angaben**
 - Name, Gültigkeitsdauer, ZDA, öffentlicher Schlüssel
- Um das Zertifikat vor Manipulationen zu schützen, wird es vom Aussteller (ZDA) elektronisch signiert..
- Die Vertrauenswürdigkeit einer ZDA wird in einem Zertifikat von der Regulierungsbehörde für Telekommunikation und Post (RegTP) verbrieft.

PKI - Asymmetrische Kryptographie

Signieren und Verschlüsseln sind unterschiedliche Vorgänge.

- **Signieren**
 - Sicherstellung der Nichtabstreitbarkeit und Integrität
 - Signieren mit privatem Schlüssel des Absenders
 - Prüfung der Signatur mit öffentlichem Schlüssel des Absenders
- **Verschlüsseln**
 - Sicherstellung der Vertraulichkeit
 - Verschlüsseln durch öffentlichen Schlüssel des Empfängers
 - Entschlüsseln durch privaten Schlüssel des Empfängers

PKI - Asymmetrische Kryptographie

Die digitale Signatur ist in Deutschland und Europa gesetzlich geregelt.

- **Historie**
 - Erstes Signaturgesetz (SigG) vom 22. Juli 1997
 - Erste Signaturverordnung vom 22. Oktober 1997
- **Heute**
 - Signaturgesetz vom 22. Mai 2001
 - Signaturverordnung vom 22. November 2001
- **Im Gesetz wird unterschieden zwischen**
 - Elektronischen Signaturen
 - Fortgeschrittene elektronische Signaturen
 - Qualifizierte elektronische Signaturen
 - Qualifizierte elektronische Signaturen mit zusätzl. Anforderungen

PKI - Infrastrukturkomponenten

Die Infrastruktur einer PKI besteht aus IT-, Netzwerk- und Sicherheitskomponenten für Funktionen, wie:

- Registrierung
- Schlüsselerzeugung
- Zertifikatserstellung
- Schlüsselspeicherung
- Zertifikats- und Schlüsselverteilung
- Verzeichnisdienst
- Zertifikatsüberprüfungs- und Sperrdienst
- Anwendungsintegration

PKI - Authentifizierung von Personen und Objekten I

In der virtuellen Welt der offenen Netze ist Authentifikation eine zentrale Anforderung.

- **Personen**
 - Der Nachweis der Identität ist Voraussetzung für die Verbindlichkeit digitaler Willenserklärungen.
- **Personen-bezogene Merkmale (Attribute)**
 - Nachweis, dass eine Person, bestimmte Merkmale aufweist, wie Beruf, Funktion im Unternehmen,...
- **Webserver**
 - Nachweis, dass ein Webserver auch wirklich einem bestimmten Unternehmen oder Institution gehört.
- **VPN-Gateways und -Clients**
 - Nachweis, dass die Zugangskomponenten eines virtuellen privaten Netzes auch wirklich zum VPN gehören.

PKI - Authentifizierung von Personen und Objekten II

In der virtuellen Welt der offenen Netze ist Authentifikation eine zentrale Anforderung.

- **Datum/ Uhrzeit**
 - Nachweis, dass eine Willenserklärung auch wirklich zur genannten Zeit abgegeben wurde.
- **Software**
 - Nachweis der Herkunft und Unverfälschtheit von Software
- **Content**
 - Nachweis der Herkunft und Unverfälschtheit von Musik, Videos und textlichen Inhalten
- **Endgeräte/ (Devices)**
 - Nachweis der Identität von PCs, Handys, PDAs, Kabelmodems, Set-Top-Boxen,...für Funktionen, wie die Steuerung von Zugriffsrechten (Autorisierung), Copyright-Schutz und Leistungsabrechnung.

PKI - Die Optionen

PKIs können in vielfältigen Ausprägungsformen realisiert werden. Entscheidend sind die spezifischen Anforderungen des Unternehmens.

- Outsourcen oder Betrieb einer eigenen PKI?
- Signaturgesetz-Konformität: ja oder nein?
- Chipkarten-basierte versus Software-Lösungen?
- Vorkonfigurierte Standard-Lösung versus maßgeschneiderte Lösung?
- Internationale Interoperabilität versus firmeninterne Lösung?

PKI - Kosten und Nutzen

PKI begründet sich durch die Anwendungen. Eine Kosten-Nutzen-Betrachtungen sollte aus zwei Blickwinkeln erfolgen.

- Migration bestehender Verfahren für Authentifikation, Verschlüsselung und Security Management, die
- PKI als Teil der E-Business-Applikationen ist Bestandteil deren Kosten-Nutzen-Betrachtung.

Appendix

PKI - Der „Enabler“ für den E-Business

Eine PKI ist auf das engste mit dem E-Business und dessen Anwendungen verknüpft. Eine Einteilung nach den Leistungs- und Geschäftsbeziehungen ist zweckmäßig.

- **Business to Consumer (B2C)**
 - Beziehungen der Unternehmen und staatlichen Stellen mit Privatkunden, bzw. dem Bürger
- **Business to Business (B2B)**
 - Beziehungen zwischen Unternehmen und staatlichen Stellen mit Geschäftskunden, Lieferanten, Banken, Transportunternehmen und Kooperationspartnern
- **Business to Employee (B2E)**
 - Unternehmens- und Behörden-interne Leistungs- und Geschäftsbeziehungen zwischen Mitarbeitern an verschiedenen Standorten

Appendix

PKI - Business-to-Consumer (B2C) Anwendungen

- **Einsatzbeispiele für PKI-Lösungen**
 - Sichere E-Mail und Informationsübertragung
 - Sichere Kommunikation mit Webservern
 - Kundenkarten
 - Mobile Commerce
 - Sichere Zahlungssysteme
- **Branchen mit einem besonders hohen und spezifischen Bedarfspotential**
 - Finanzdienstleister,
 - Gesundheitswesen,
 - Staatliche Stellen (e-government),
 - Verkehr und
 - Software und Media.

Appendix

PKI - Business-to-Business (B2B) Anwendungen

- **Einsatzbeispiele für PKI-Lösungen**
 - Sichere E-Mail und Informationsübertragung
 - Sichere Kommunikation mit Webservern
 - Supply Chain Management, Web-EDI
 - Beschaffung, Elektronische Marktplätze
 - Zusammenarbeit (Collaboration)
 - IP-VPNs (Extranets)/ LAN-to-LAN -Kommunikation
- **Branchen mit hohem und spezifischem Bedarfspotential**
 - Finanzdienstleister,
 - Gesundheitswesen,
 - Staatliche Stellen (e-government),
 - Verkehr,
 - Maschinenbau und
 - Software.

Appendix

PKI - Business-to-Employee (B2E) Anwendungen

- **Einsatzbeispiele für PKI-Lösungen**
 - Sichere E-Mail und Informationsübertragung
 - Sichere Kommunikation mit Webservern
 - Zugangsschutz und Autorisierung (IT- und Netzwerkinfrastrukturen, Anwendungen, Daten)
 - Single-Sign-On
 - Mitarbeiterkarten
 - Dokumentenmanagement, archivierung, workflow
 - ERP (SAP,...)
 - Mobiler Zugang auf bestehende Online-Anwendungen
 - Zusammenarbeit in Arbeitsgruppen
 - IP-VPNs (Intranets)
 - LAN-to-LAN -Kommunikation
 - Remote Access (Vertrieb, Kundendienst, Management)

Appendix

PKI - Schnell wachsende Sicherheitstechnologie

PKI ist mit einer durchschnittlichen Wachstumsrate von über 40% eine der am schnellsten wachsenden Sicherheitstechnologien.

- Weltweite PKI-Markt wächst von 436 Mio.\$ in 2000 auf 3,4 Mrd. \$ im Jahr 2006*)
- USA und Europa ungefähr gleiche Bedeutung
- Das größte PKI-Marktsegment mit über 50% sind Zertifizierungsdienste (Insourcing, Outsourcing)
- In 2003 wird der Outsourcing-Anteil am PKI-Markt die 50%-Grenze überschreiten.

*) Quelle: Datamonitor