Nutzen und Chancen von Public-Key-Infrastrukturen

Dr. Norbert Pohlmann

Vorstandsvorsitzender des TeleTrusT e.V.

Vorstandsmitglied der Utimaco Safeware AG

06.2002

Inhaltsverzeichnis

Zusammenfassung

Immer mehr Geschäftsprozesse in Unternehmen und Organisationen werden – ganz oder teilweise – über elektronische Medien abgewickelt. Sowohl diese Prozesse als auch die dabei verarbeiteten oder generierten Daten stellen einen wesentlichen Unternehmenswert dar. Daher ist es wichtig, ausreichende Sicherheitsmechanismen zur Verfügung zu stellen, um diese Geschäftsprozesse adäquat zu schützen. Public-Key-Infrastrukturen (PKIs) und PKI-enabled Applications (PKAs) helfen, eine geeignete Sicherheitsbasis zu schaffen.

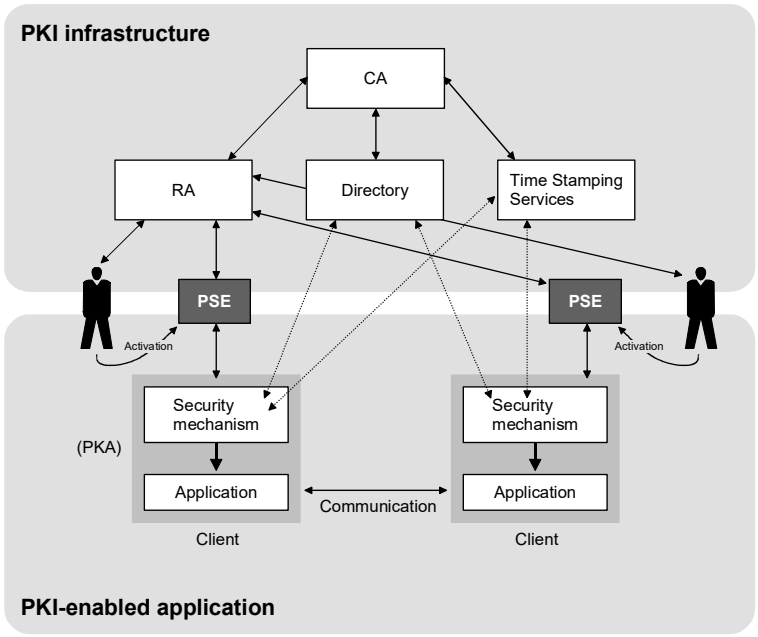
PKIs werden zur Zeit kontrovers diskutiert: Gegner behaupten, dass solche Systeme nicht einsetzbar seien, weil sie zu große Probleme und Veränderungen im Arbeitsablauf bewirkten. Konträr dazu steht die Forderung, PKIs in großem Umfang einzuführen, damit insbesondere bei organisationsübergreifenden Geschäftsprozessen eine angemessene Sicherheit erreicht werden kann.

Dieser Beitrag zeigt auf, was PKIs und PKAs leisten, welchen Nutzen sie in der heutigen Informations- und Wissensgesellschaft haben und welche Chancen sie bieten.

1 PKI und Anwendungsprinzipien

Eine PKI stellt zentrale Sicherheitsdienste zur Verfügung, schafft also die Voraussetzungen dafür, dass eine Anwendung vertrauenswürdig realisiert werden kann.

Das folgende Bild zeigt im oberen Teil den prinzipiellen Aufbau einer Public-Key-Infrastruktur sowie einige Kommunikationskanäle. Im unteren Bereich ist schematisch eine Anwendung abgebildet, die auf der PKI-Grundfunktionalität basiert.



PKI und PKA

1.1 Aufgaben und Komponenten einer PKI

Public-Key-Infrastrukturen bestehen aus Hardware, Software und einem abgestimmten Regelwerk, der **Policy.** Die Policy definiert, nach welchen Sicherheitsregeln die Dienstleistungen erbracht werden. Dazu zählt das Betriebskonzept der PKI, die Benutzerrichtlinien sowie Organisations- und Arbeitsanweisungen.

Im Allgemeinen ist es üblich, die Registrierung der Teilnehmer und die Zertifizierung der Schlüssel voneinander zu trennen und zum Teil auch an unterschiedlichen Orten vorzunehmen.

Die **Registration Authority (RA)** kann als private (innerhalb einer Organisation) oder öffentliche Einrichtung betrieben werden. Ihre Hauptaufgabe besteht darin, die Anträge auf Zertifizierung zu erfassen und die Identität der Antragsteller entsprechend der Policy zu prüfen. Die Identitätsprüfung kann sehr einfach, z.B. per E-Mail, oder auch aufwendiger und sicherer, z.B. durch persönliches Erscheinen und Vorlage des Ausweises, erfolgen.

Die Registration Authority bildet die Schnittstelle zwischen den Teilnehmern bzw. Antragstellern und der **Certification Authority (CA),** an die sie die Anträge weiterleitet.

Die **Certification Authority** vergibt eindeutige Identitäten und verwaltet für jeden Teilnehmer ein oder mehrere Schlüsselpaare mit den dazugehörigen Zertifikaten. Jedes von der CA erzeugte Zertifikat verbindet den öffentlichen Schlüssel des Teilnehmers mit dessen Namen und zusätzlichen Daten (Gültigkeitszeitraum, Seriennummer, evtl. weitere Attribute).
Die Certification Authority gibt die Zertifikate aus und verwaltet sie, damit die öffentlichen Schlüssel und Attribute (Position im Unternehmen, Rechte usw.) der Teilnehmer möglichst einfach verifiziert werden können.

Zur Verwaltung der Zertifikate unterhält jede PKI einen **Directory Service**. Hier werden die gültigen zertifizierten öffentlichen Schlüssel der Teilnehmer veröffentlicht. Zurückgezogene oder kompromittierte Schlüssel werden in einer Sperrliste (**"Certificate Revocation List", CRL**) zum Abruf bereitgehalten.

Ein **Zeitstempeldienst** dient dazu, gesicherte Zeitsignaturen gemäß der Policy zu erstellen. Damit wird ein Dokument oder eine Transaktion mit der aktuellen Zeitangabe verknüpft und diese Gesamtinformation anschließend digital signiert.

Das **Personal Security Environment (PSE)** ist die Sammlung aller sicherheitsrelevanten Daten eines Teilnehmers. Dazu gehören seine geheimen Schlüssel, die Zertifikate seiner Kommunikationspartner sowie der öffentliche Schlüssel der Zertifizierungsinstanz.

1.2 PKI-enabled Application (PKA)

Als "PKI-enabled Application" (PKA) wird eine Anwendung bezeichnet, die auf der Grundlage der von der PKI zur Verfügung gestellten Sicherheitsdienste (Zertifikate, Verzeichnisdienst etc.) eine vertrauenswürdige Nutzung ermöglicht. Eine PKA enthält selbst unterschiedliche Sicherheitsmechanismen (Authentisierung, Verschlüsselung, etc.), mit denen Vertrauenswürdigkeit (Authentizität, Integrität, Verbindlichkeit, Einmaligkeit und Vertraulichkeit) erzielt wird.

Eine PKI bildet die Sicherheitsgrundlage für die vertrauenswürdige Nutzung von Anwendungen wie

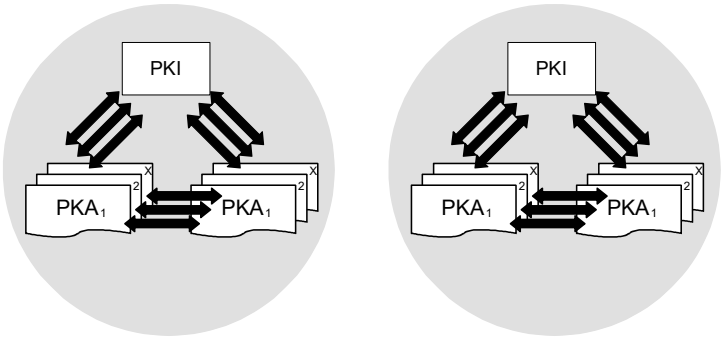
- E-Mail
- Dokumentverschlüsselung (z.B. von MS-Office-Dokumenten)
- Transaktionen im Finanzbereich (EDIFACT)
- XML Prozessen
- SSL-Kommunikation
- VPN-Kommunikation
- Identifikations- und Authentisierungsprozessen
- Zahlungssystemen

1.3 Modelle von Public-Key-Infrastrukturen

Es gibt verschiedene Modelle von Public-Key-Infrastrukturen, die im Folgenden kurz dargestellt werden:

Geschlossene Systeme

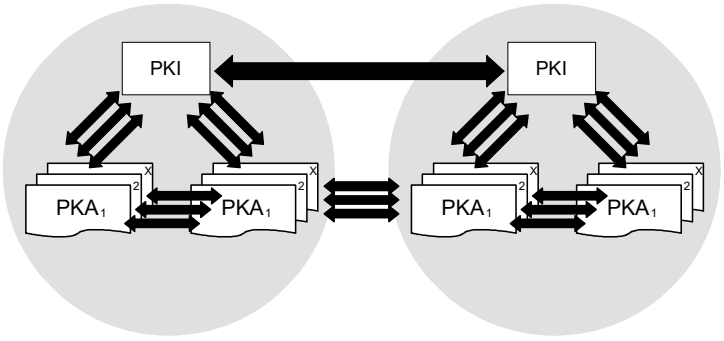
Eine Organisation betreibt eine PKI für eine oder mehrere Anwendungen (PKAs), die vollständig in ihrem eigenen Verantwortungsbereich liegen. Sicherheitsdienste wie z.B. gesicherte Kommunikation oder Authentisierung stehen nur innerhalb der Infrastruktur zur Verfügung.



Geschlossene PKI-Systeme

Offene Systeme

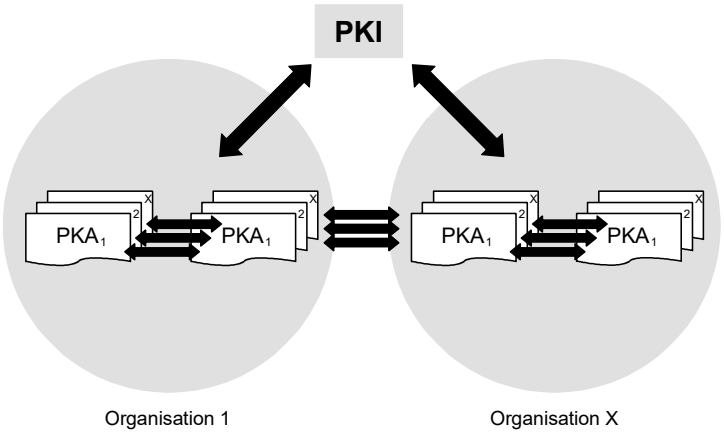
Mehrere Organisationen betreiben jeweils eigene PKIs für eine oder mehrere Anwendungen, die in den Verantwortungsbereichen der unterschiedlichen Organisationen liegen. So ist z.B. die gesicherte Kommunikation zwischen den Organisationen möglich. Der Austausch beruht auf gegenseitigem Vertrauen sowie auf kompatiblen Technologien und Verfahren.



Offene PKI-Systeme

Offene, zentrale Systeme

Ein PKI-Anbieter betreibt die PKI für eine oder mehrere Anwendungen, die in den jeweiligen Verantwortungsbereichen der darauf zurückgreifenden Organisationen liegen. Wenn die verschiedenen Organisationen der zentralen PKI vertrauen und kompatible Technologien bzw. Verfahren verwenden, kann eine vertrauenswürdige Kommunikation zwischen den Organisationen realisiert werden.



Zentral administriertes PKI-System

2 Probleme in der Praxis

Bei der Nutzung von PKIs gab und gibt es einige Probleme, die im Folgenden diskutiert werden.

Probleme bei geschlossenen Systemen

"Geschlossenes System" bedeutet, dass die PKI nur innerhalb einer Organisation verwendet wird und nicht für die Kommunikation nach außen genutzt werden kann. Da jedoch in der Praxis viele organisationsübergreifende Prozesse stattfinden, ist der Nutzen einer solchen PKI sehr eingeschränkt.

Probleme bei offenen Systemen

Bei offenen Systemen muss zum Aufbau einer organisationsübergreifenden Kommunikation ein Abgleich der verschiedenen organisationsspezifischen Policies erfolgen. Ziel ist ein gemeinsames "Level of Trust". Hier müssen geeignete Instrumente implementiert werden, um die organisatorischen sowie die IT-infrastrukturellen Konzeptionen zu bewerten, zu analysieren und zu gewichten.

Gerade bei der Nutzung für personenbezogene organisationsübergreifende Prozesse stellt sich aus ökonomischer Sicht und aus den tatsächlichen Anforderungen heraus die Frage, ob das Signaturgesetz die Grundlage für die PKI und die zum Einsatz kommenden PKAs bilden muss. Hierbei muss berücksichtigt werden, dass viele organisationsübergreifende Prozesse automatisiert sind und somit nicht mehr personenbezogen arbeiten. Die Kardinalfrage in diesem Zusammenhang ist, ob innerhalb des Sicherheitskonzepts der PKI beispielsweise die Verantwortlichkeit für von Servern erstellte Signaturen geregelt ist (Haftungsausschluss).

Hinzu kommt, dass eine Vielzahl von unterschiedlichen, teilweise sehr komplexen Standards existiert, die darüber hinaus ständig weiterentwickelt werden. Die Ursache hierfür liegt in der großen Vielfalt der Anwendungen (SSL, E-Mail etc.) und den daraus resultierenden besonderen Anforderungen.

Unterschiedliche Verantwortung für PKIs und PKAs in Unternehmen

Ein weiteres Problem, dem insbesondere große Organisationen gegenüberstehen, beruht darauf, dass die PKAs und PKIs zwar voneinander abhängig sind, aber häufig organisatorisch getrennt werden. In derartigen Fällen müssen sich beispielsweise verschiedene Abteilungen auf gemeinsame Ziele und Vorgehensweisen verständigen, um die entsprechenden technologischen Grundlagen zu erarbeiten.

"Henne-Ei-Problem"

Public-Key-Infrastrukturen sind nur dann ökonomisch sinnvoll, wenn der Einsatz dieser Strukturen und damit der vertrauenswürdige Ablauf von Geschäftsprozessen so umfassend wie möglich realisiert wird, d.h. wenn die gesicherte Kommunikation mit so vielen Partnern wie möglich stattfinden kann. Voraussetzung dafür ist der konsequente Einsatz der bestehenden Technologien und die Umsetzung der Security Policies.

Die Realität ist aber, dass sich die beteiligten Organisationen nur schwer auf den Abgleich ihrer individuellen Sicherheitskonzepte einigen können. Dadurch gestaltet sich der Aufbau eines gemeinsamen "Level of Trust" langwierig und längst fällige Entscheidungen werden nicht getroffen. Zu viele Beteiligte nehmen noch eine abwartende Haltung ein und der Ausbau der bestehenden PKIs stagniert.

Hoher personeller und organisatorischer Aufwand

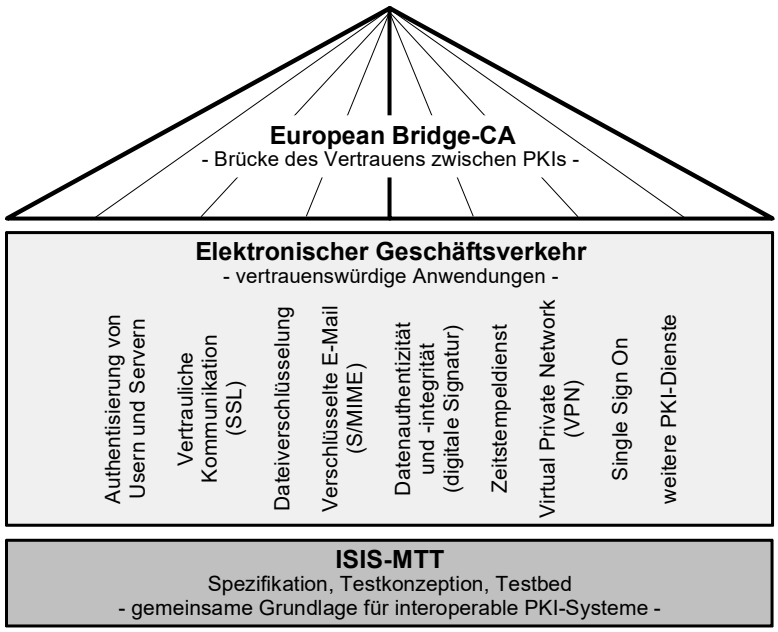
Die Einführung und der Betrieb einer Public-Key-Infrastruktur erfordert neben der technischen Umsetzung auch einen hohen personellen und organisatorischen Aufwand. Gerade in der Einführungsphase einer PKI ist die Sensibilisierung der Anwender für die IT-Sicherheit, die Schulung der Anwender auf die Produkte und die Planung und Durchführung des Roll-Out ein nicht zu vernachlässigender Faktor.

Key-Recovery bei der Verschlüsselung

Wenn Unternehmenswerte verschlüsselt werden, muss ein Verfahren realisiert werden, das bei technischen Defekten, bei einem PSE-Verlust oder beim Ausscheiden eines Mitarbeiters aus dem Unternehmen garantiert, dass die Unternehmenswerte sicher wieder entschlüsselt werden können.

3 Migration und Interoperabilität

In den letzten Jahren wurden in vielen Unternehmen PKIs eingerichtet. Zu Beginn dieser Entwicklung standen die Grundlagen von PKIs beim Anwender im Vordergrund. Gegenwärtig verschiebt sich der Akzent auf die Interoperabilität der Systeme, durch die ihr Nutzen erst voll ausgeschöpft werden kann. Bevor dieses Ziel erreicht werden kann, müssen jedoch noch einige technische und organisatorische (die Policies betreffende) Hürden überwunden werden. Zwei mögliche Lösungen hierfür werden im Folgenden beschrieben: die Spezifikation ISIS-MTT auf technischer und die Initiative "European Bridge-CA" auf organisatorischer Ebene.



Migration und Interoperabilität: ISIS-MTT und European Bridge-CA

3.1 ISIS-MTT

Die Bemühungen um Interoperabilität von PKI-Systemen werden durch die Vielfalt der Standards und ihrer Interpretationsmöglichkeiten erschwert. Um eine gemeinsame Grundlage zu schaffen, haben die Vereinigungen TeleTrusT e.V. und T7 e.V. mit Unterstützung durch das BMWi die Spezifikation **ISIS-MTT** ins Leben gerufen. Deren übergeordnetes Ziel ist eine schnelle flächendeckende Einführung PKI-gestützter Sicherheitstechnologie.

Folgende Kriterien werden hierbei zugrunde gelegt:

- Investitionssicherheit für Anwender und Anbieter durch Kompatibilität zu internationalen Standards und bereits verwendeten Zertifikatsformaten, durch langfristige Stabilität der Spezifikation und problemlose Interoperabilität von Produkten verschiedener Hersteller
- Anpassungsfähigkeit des Sicherheitsniveaus an die unterschiedlichen Anwendungsfelder

- Berücksichtigung aller für den elektronischen Geschäftsverkehr relevanten Formvorschriften (z.B. des Privat- und Verwaltungsrechts)

Die ISIS-MTT-Spezifikation basiert auf internationalen Standards (S/MIME, PKIX, PKCS, X.509, ETSI, CEN ESI etc.) und integriert die aus der bisherigen Anwendung gewonnenen Erfahrungen. Sie besteht aus einer Kernspezifikation, die die Grundanforderungen aller Anwendungskategorien abdeckt, und Erweiterungen für die verschiedenen Anwendungen (z.B. elektronische Signatur, E-Mail-Verschlüsselung). Darin werden ausschließlich Festlegungen getroffen, die in den bestehenden Standards nicht hinreichend eindeutig geregelt sind.

Um die Voraussetzungen für die Entwicklung interoperabler Anwendungen auf internationaler Ebene zu schaffen, wird die Akzeptanz von ISIS-MTT in den europäischen und weltweiten Standardisierungsgremien angestrebt. Auch die enge Verzahnung mit der Bridge-CA-Initiative bietet eine Möglichkeit, ISIS-MTT-Anwendungen schnell auf eine breite Basis zu stellen.

3.2 European Bridge-CA

Mit der zunehmenden Verbreitung von PKI-basierten Dienstleistungen erhalten die Anwender eine Vielzahl von verschiedenen Zertifikaten für spezielle Applikationen mit einem spezifischem Verwendungszweck und einem spezifischen Vertrauensmodell. Die Handhabung dieser Zertifikate in den verschiedenen Stadien ihres Lebenszyklus (Ausgabe, Nutzung, Verlängerung, Rücknahme) entwickelt sich zu einer zunehmend komplexen und aufwändigen Aufgabe.

Um diesen Aufwand zu verringern, ist die gegenseitige Akzeptanz von Zertifikaten der verschiedenen PKIs erstrebenswert. Dazu müssen nicht nur technische, sondern auch organisatorische (die Policy betreffende) Unterschiede überwunden werden. An dieser Stelle setzt die Initiative "European Bridge-CA" an, die sich das Ziel gesetzt hat, die Vertrauenslücken sowohl zwischen existierenden als auch zu noch einzurichtenden PKIs pragmatisch zu überbrücken. /Pohl2001/

Die Bridge-CA-Initiative wurde von der Deutschen Bank und der Deutschen Telekom ins Leben gerufen. Nach kurzer Zeit wurde die industrielle Vereinigung TeleTrusT Deutschland e.V. Betreiber der Initiative, die zur Zeit von über 20 großen Organisationen unterschiedlicher Industriezweige und der öffentlichen Verwaltung unterstützt wird. Im Zuge der gemeinsamen Standardisierung nimmt sie die Rolle eines neutralen Mittlers ein.

Das Ziel der europäischen Bridge-CA ist es, eine "Brücke des Vertrauens" zwischen verschiedenen PKIs weltweit herzustellen, indem sie minimale Policy-Anforderungen und technische Vorbedingungen definiert, die eine sichere Kommunikation über organisatorische Grenzen hinweg erlauben. Gleichzeitig gilt es, ein gemeinsames Verständnis für den Gebrauch von digitalen Signaturen bei allen Beteiligten sicherzustellen. Die Praktikabilität, die Flexibilität der vereinbarten Lösungen und der Schutz der getätigten Investitionen in die Sicherheits-infrastruktur stehen im Mittelpunkt der Aufmerksamkeit. Um das Ziel der PKI-Interoperabilität auch kurzfristig zu erreichen, wurde bei der Implementierung der Bridge-CA auf bereits verfügbare Technologie zurückgegriffen.

Ausgehend von der weiten Verbreitung der Kommunikation via E-Mail hat die Bridge-CA-Initiative ihre kurzfristigen Bemühungen auf diesen Bereich fokussiert.

Um die Nutzung von Verschlüsselung und digitalen Signaturen über die Grenzen von Organisationen hinaus praktikabel zu machen, müssen zwei Bedingungen erfüllt werden:

- Der Empfänger einer Nachricht muss in der Lage sein, die Gültigkeit des Zertifikats zu verifizieren. Folglich muss er auf die notwendigen Informationen der Zertifizierungsinstanz (CA) zugreifen können.
- Der Empfänger muss in der Lage sein, das Wurzelzertifikat der ausstellenden PKI zu identifizieren und darauf hin zu überprüfen, ob es gültig und vertrauenswürdig ist.

Die Bridge-CA ermöglicht dies, indem sie eine allgemeine Plattform zur Verfügung stellt, die die teilnehmenden CAs auf eine sichere, aber einfache Weise verbindet. Sie basiert auf einem standardisierten technischen und organisatorischen Regelwerk, das die Integration neuer CAs in die Bridge-CA-Infrastruktur erleichtert. Sobald ein neuer Teilnehmer sich anschließt, können alle Mitglieder seiner PKI mit allen Mitgliedern der anderen Bridge-CA-Partner sicher kommunizieren. Eine formale Prozedur für die Registrierung stellt sicher, dass alle Teilnehmer den Mindestanforderungen gerecht werden.

Um einer breiten Klientel den einfachen und schnellen Zugang zu ermöglichen, wurden die Teilnahmevoraussetzungen minimal gehalten:

- Persönliche Identifikation und Registrierung der Zertifikatsinhaber, um die eindeutige Koppelung zwischen einem öffentlichen Schlüssel und einer Person zu garantieren. Massenregistrierung ist nur zulässig, wenn die jeweiligen Datenquellen vertrauenswürdig genug sind.
- Zugang zu Statusinformationen des Zertifikats via CRLs oder OCSP sowohl für die Bridge-CA als auch für deren Teilnehmer.
- Die Distinguished Names in den Zertifikaten müssen eindeutig zugewiesen werden und dürfen sich nicht mit Namen anderer teilnehmender Organisationen überschneiden. Das ist für zukünftige Bridge-CA-Entwicklungen besonders wichtig, da diese die Verkettung von Verzeichnissen und die Kreuzzertifizierung beinhalten werden.
- RSA-Schlüssellänge von mindestens 1024 Bit.
- Schlüsselgebrauch ist "Signature" und/oder "Encryption".

Um der Bridge-CA als vertrauenswürdiger Partner beizutreten, muss ein zukünftiges Mitglied die folgenden Schritte absolvieren:

- Der erste Schritt ist die Überprüfung, ob die PKI des Beitrittskandidaten die minimalen Anforderungen an die Policy erfüllt, die vom Bridge-CA-Board definiert wurden.
- Sobald die Überprüfung erfolgreich abgeschlossen wurde, kann der zukünftige Teilnehmer mit den Bridge-CA-Executives in Kontakt treten.
  Ein Formular mit weiteren Informationen hierzu kann unter *http://www.bridge-ca.org*. bezogen werden.
- Der nächste größere Schritt sind technische Interoperabilitäts-Tests mit der Bridge-CA. Dieser Prozess wird vom Personal der Bridge-CA unterstützt und ist üblicherweise nicht sehr aufwändig.
- Wenn die komplette Interoperabilität aller Schlüsselelemente der PKI sichergestellt ist, kann der zukünftige Teilnehmer den formalen Beitritt durch die Unterzeichnung des Teilnehmer-vertrags vollziehen.
- Damit ist das neue Mitglied betriebsbereit und kann sicher mit allen anderen Teilnehmern der Bridge-CA kommunizieren. Dazu müssen die Root-Zertifikate der anderen Teilnehmer in die eigene PKI eingefügt werden.

Die Bridge-CA bietet somit eine praktikable Lösung für das Verbinden voneinander unabhängiger PKIs. Nutzer dieser PKI können sicher und ohne größeren Aufwand miteinander kommunizieren. Während dieser Artikel geschrieben wurde, waren bereits 300.000 Zertifikate von Teilnehmern der Bridge-CA im Einsatz. Die nächsten Schritte zur Weiterentwicklung sind die Einführung der Kreuzzertifizierung zwischen der Bridge-CA und ihren Teilnehmern, um den Verwaltungsüberhang zu reduzieren, und die Vereinfachung der Integration von zukünftigen Mitgliedern. Durch diese Entwicklung kann sich die Zahl der potenziellen Teilnehmer vergrößern und die Initiative somit einen weiteren Aufschwung erhalten.

4 Umsetzungskonzepte

Neben der Bereitstellung der notwendigen Technologien und der weitgehenden Lösung der Interoperabilitäts-Problematik sollte der Blick konsequent auf die tatsächlichen Anforderungen gerichtet werden. Pragmatische Ansätze sind gefragt, um die Einführung von Public-Key-Infrastrukturen zu beschleunigen.

Die folgenden vier Kernsätze können als Grundlage für die erfolgreiche Realisierung eines PKI-Systems gelten:

- Verschiedene Anwendungen haben unterschiedliche Sicherheitsbedürfnisse.
- Unterschiedliche Sicherheitsbedürfnisse lassen sich isoliert einfacher verwirklichen.
- Isolierte Lösungen haben einen klareren Fokus.
- Ein klarerer Fokus verringert die auftretenden Probleme und ermöglicht eine schnellere, einfachere und kostengünstigere Umsetzung.

Im Folgenden werden einige Umsetzungskonzepte exemplarisch dargestellt.

4.1 Umsetzungskonzept "SSL"

Bei Homebanking-Anwendungen, Depotabfragen etc. lautet eine explizite Datenschutz-anforderung, die Kommunikation zwischen Client und Server vertraulich zu gestalten, damit die ausgetauschten Daten weder mitgelesen noch manipuliert werden können.

Alle hierfür notwendigen Voraussetzungen sind gegeben. Die technische Infrastruktur ist bereits vorhanden: Web Server sind für die SSL Verschlüsselung vorbereitet, Clients (Browser) unterstützen den Standard und PKIs stehen zur Verfügung. Dem Markt stehen etablierte SSL-Bibliotheken als Open Source zur Verfügung und auch die Industrie hat den Markt erkannt: SSL-Accelerator-Lösungen für die Beschleunigung der gesicherten Verbindung stehen bereit.

Stellt man den Aspekt der leichten Anwendbarkeit (z.B. durch integrierte Zertifikate in Browsern) in den Mittelpunkt, müssen selbstverständlich die Sicherheitsanforderungen dagegen abgewogen werden. Nach Abschluss dieser Analyse wird eine Vielzahl von Organisationen feststellen, dass die Umsetzung der o.g. Anforderungen zeitnah und problemlos möglich ist.

4.2 Umsetzungskonzept "E-Mail-Sicherheit"

Zu schützende Unternehmensdaten sollen personenorientiert und vertraulich ausgetauscht werden. Das bedeutet, dass das gegenseitige Wissen um die Identität der Kommunikationspartner von zentraler Bedeutung ist. Insbesondere wenn via E-Mail Prozesse mit nachfolgenden Kosten (Bestellungen, Wareneinkauf ...) ausgelöst werden, liegt die Verbindlichkeit im Interesse der Unternehmen.

Mailprogramme sind den Nutzern bereits bekannt und vertraut. Sicherheitsrelevante Funktionen müssen so eingepasst werden, dass der Anwender sich nur einem Mindestmaß an neuen Funktionalitäten gegenüber sieht und jederzeit Klarheit über die nötigen Arbeitsschritte und ihre Folgen hat. Ihre Anwendung – d.h. die Einhaltung der Sicherheitskonzepte – sollte so einfach wie möglich gehalten werden. Dies ist eine Voraussetzung dafür, dass der Nutzer seine aktive Rolle (im Gegensatz zur passiven Rolle bei der gesicherten SSL-Kommunikation) konsequent wahrnehmen kann.

4.3 Umsetzungskonzept "Verbindlicher Austausch von Transaktionsdaten"

Transaktionsdaten stellen insofern 'besondere' Kommunikationsdaten dar, weil sich aus ihnen in der Regel Aktionen ableiten, die kostenrelevant sind. Für den Empfänger wie für den Sender steht die Verbindlichkeit im Mittelpunkt.

Diese Anwendungen sind meist firmen- bzw. gerätebezogen und basieren auf geschlossenen Systemen (z.B. der Austausch von Rechnungsdaten zwischen Telekommunikationsanbietern und ihren Partnerunternehmen). Die Bandbreite reicht von kleinen Datenmengen pro Monat bis hin zu einer hohen Anzahl von Transaktionen pro Minute.

Hier liegt der Fokus auf der möglichst nahtlosen Integration in bestehende Workflows, um zu einer praktikablen Lösung zu gelangen.

5 Fazit

Der Nutzen und die Chancen von Public-Key-Infrastrukturen liegen insbesondere in der Realisierung von vertrauenswürdigen elektronischen Geschäftsprozessen. Sowohl die technischen als auch die infrastrukturellen Voraussetzungen für ein übergreifendes PKI-Netzwerk sind gegeben oder in greifbare Nähe gerückt.

Das "Henne-Ei-Problem" bei organisationsübergreifenden Public-Key-Infrastrukturen können Anbieter und Anwender nur gemeinsam lösen. ISIS-MTT und Bridge-CA sind pragmatische Lösungsansätze auf der Grundlage zeitgemäßer Sicherheitstechnologien. Diesen Organisationen können Sie sich einfach anschließen.

Mit Public-Key-Infrastrukturen können wir ein Netz des Vertrauens spannen, damit wir alle in Zukunft die Vorteile der sicheren Kommunikation für unseren Erfolg nutzen können.

Literatur

/Pohl2001/ Norbert Pohlmann: Organisationshandbuch Netzwerksicherheit, laufend aktualisiertes Loseblattwerk mit über 2000 Seiten, INTEREST-Verlag, siehe: www.interest.de