Prof. Dr. Norbert Pohlmann, Malte Hesse

Kryptographie: Von der Geheimwissenschaft zur alltäglichen Nutzanwendung (VII) – Vertrauensmodelle von Public-Key-Infrastrukturen

Im letzten Artikel haben wir PKI-Infrastrukturen und den Unterschied zwischen offenen und geschlossenen Systemen kennen gelernt. Diesmal wollen wir offene PKI-Systeme genauer betrachten, mit deren Hilfe mehrere Organisationen mit je eigener PKI über ihre Grenzen hinweg vertrauenswürdig mit anderen Organisationen kommunizieren.

Der organisationsübergreifende Einsatz von Public-Key-Infrastrukturen erfordert verbindliche Vertrauensmodelle, für die prinzipiell drei Ansätze existieren

Um dies zu ermöglichen, sind die verschiedenen organisationsspezifischen Leitlinien der beteiligten Public-Key-Infrastrukturen miteinander abzugleichen. Die Leitlinien beschreiben neben den verwendeten Technologien, Verfahren und Schnittstellen u. a. den für die User-Registrierung notwendigen Prozess, insbesondere Maßnahmen zur initialen Identifizierung und Authentifikation der Benutzer, die zum angestrebten Schutzniveau der PKI passen. So kann es in einem Fall notwendig sein, dass Personalausweise überprüft und Kopien für die Unterlagen gemacht werden, während in einem anderen die Stammdaten aus der Personalverwaltung für die Zertifikatserstellung ausreichen. Wichtig ist, dass die Geschäftspartner sich auf einen Mindeststandard einigen.

Zertifizierungshierarchie und Vertrauensmodelle

Mit der zunehmenden Verbreitung von PKI-basierten Dienstleistungen erhalten die Anwender eine Vielzahl von verschiedenen Zertifikaten für spezielle Applikationen. Zusätzlich gibt es sehr viele unterschiedliche Public-Key-Infrastrukturen. In der Praxis ist daher sicherzustellen, dass sich die unterschiedlichen Zertifikate auf ihre Gültigkeit und Richtigkeit sowie den passenden *Level of Trust* überprüfen lassen, damit die angestrebte vertrauenswürdige Kommunikation stattfinden kann. Dies wiederum lässt sich durch verschiedene Vertrauensmodelle für die Zusammenarbeit von Public-Key-Infrastrukturen erreichen.

Vertrauensmodell A: Übergeordnete CA (Wurzel-CA, Root CA)

Eine Methode ist die Schaffung einer übergeordneten CA, welche die Wurzelzertifikate der untergeordneten CAs aufnimmt (s. Abb. 1). Wurzelzertifikate sind Zertifikate mit den öffentlichen Schlüsseln der CAs.

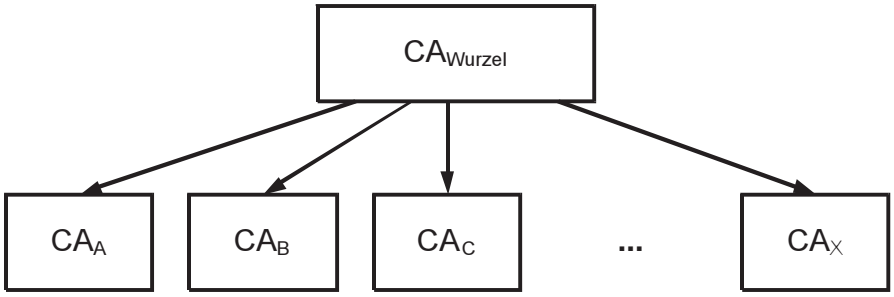

ABB. 1: Vertrauensmodell einer Wurzel-CA

Ablauf: Die CA_{Wurzel} generiert Zertifikate der öffentlichen Schlüssel der untergeordneten CAs. Der öffentliche Schlüssel der CA_{Wurzel} ist im Personal Security Environment (z. B. auf einer Smartcard) untergebracht oder wird für einen einfachen Abruf als Zertifikat der untergeordneten CAs zur Verfügung gestellt. Damit ist jeder Teilnehmer einer speziellen untergeordneten CA in der Lage, die öffentlichen Schlüssel einer anderen untergeordneten CA zu verifizieren und auch die Zertifikate mit den öffentlichen Schlüsseln der Teilnehmer der entsprechenden untergeordneten CAs zu überprüfen.

Bewertung: In den meisten Fällen akzeptieren Unternehmen, Organisationen oder Länder keine derartige Unterordnung, da sie zu große Abhängigkeiten von einer zentralen Autorität schafft: Im Extremfall würde eine für alle verbindliche „Welt-CA“ eingerichtet. Da dieses Maß an Zentralisierung meist weder nötig noch realisierbar ist, hat sich das Modell der Wurzel-CA nur in großen, geschlossenen PKI-Systemen etabliert, die nicht für eine organisationsübergreifende Kommunikation konzipiert wurden.

Vertrauensmodell B: n:n-Cross-Zertifizierung

Ein weiterer Ansatz ist, dass jede CA ihre öffentlichen Schlüssel selbstständig mit jeder anderen CA austauscht (s. Abb. 2).

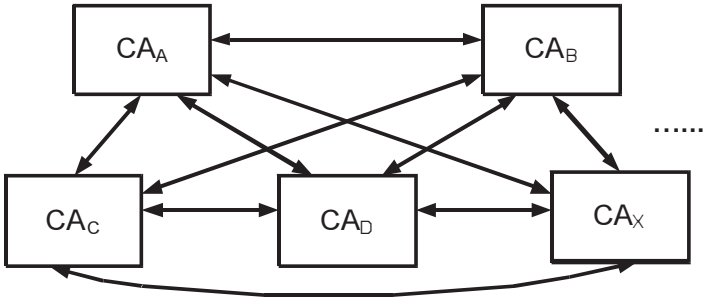

ABB. 2: Vertrauensmodell einer n:n-Cross-Zertifizierung

Ablauf: Jede CA stellt jeder anderen ihre eigenen öffentlichen Schlüssel zur Verfügung und übernimmt deren Zertifikate bzw. erkennt sie an. Dieser Prozess ist sehr aufwändig, weil der authentische Austausch der öffentlichen Schlüssel in der Regel ein persönliches Treffen der beteiligten PKI-Betreiber notwendig macht.

Bewertung: Dieses Vertrauensmodell erfordert multiple Vertragsverhandlungen und ermöglicht abweichende Verträge und Vereinbarungen zwischen den beteiligten PKI-Betreibern. Bei einer Vielzahl von Beteiligten wird die daraus entstehende Infrastruktur jedoch schnell sehr komplex und lässt sich nur schwer verwalten. Daher hat sich dieses Vertrauensmodell nur bei kleinen Gruppen unabhängiger PKI-Betreiber durchgesetzt, und auch dort nur in abgegrenzten Geschäftsprozessen.

Vertrauensmodell C: 1:n Cross-Zertifizierung (Bridge CA)

In der Praxis durchgesetzt hat sich das Modell der 1:n-Cross-Zertifizierung, das den PKI-Betreibern die größtmögliche Entscheidungsfreiheit bei der Wahl der Vertrauenskette lässt

Ein viel versprechendes Konzept stellt demgegenüber der Bridge-CA-Ansatz dar, weil er zum einen den Verwaltungsaufwand klein hält, zum anderen den angeschlossenen CAs die Entscheidungsfreiheit über die passende Vertrauenskette lässt. Erreicht wird dies durch eine neue, sehr einfach gehaltene Struktur, bei der alle nachgeordneten CAs authentisch ihre öffentlichen Schlüssel an die Bridge CA übergeben, die ihrerseits als eine zentrale Vermittlungsinstanz zwischen den beteiligten Organisationen fungiert (s. Abb. 3).

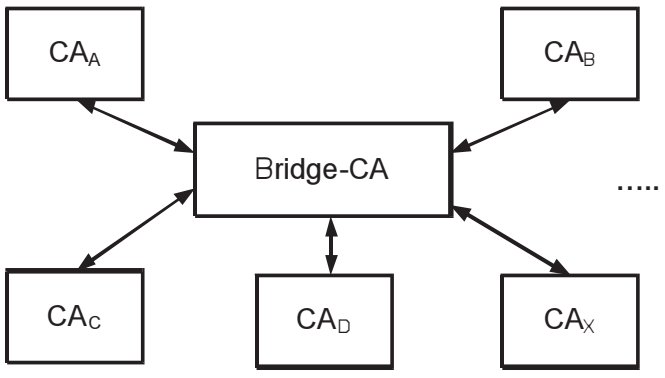

ABB. 3: Vertrauensmodell einer 1:n-Cross-Zertifizierung am Beispiel einer Bridge CA

Ablauf: Die CAs übergeben authentisch ihre öffentlichen Schlüssel an eine zentrale Bridge CA. Diese signiert eine Tabelle der öffentlichen Schlüssel aller beteiligten CAs. Die eigene CA stellt dann all ihren Teilnehmern den öffentlichen Schlüssel der Bridge CA als Zertifikat zur Verfügung.

Bewertung: Bei der 1:n-Cross-Zertifizierung gibt es für jede CA nur einen Vertragspartner, die Bridge-CA. Das reduziert den Abstimmungsaufwand und ermöglicht dennoch, in jedem Fall ein passendes Vertrauensmodell einzuführen. Die Kunst einer erfolgreichen Bridge CA besteht darin, eine Policy zu erarbeiten, die möglichst viele PKI-Betreiber politisch wollen und technisch erfüllen können.

Ein Beispiel für dieses Vertrauensmodell ist die vom *TeleTrusT e. V.* betriebene European Bridge CA, die sich zum Ziel gesetzt hat, eine „Brücke des Vertrauens" zwischen verschiedenen PKIs weltweit herzustellen. Zu diesem Zweck hat *TeleTrusT* pragmatische Leitlinien-Anforderungen und technische Vorbedingungen definiert, die eine vertrauenswürdige Kommunikation über organisatorische Grenzen hinweg erlauben. Gleichzeitig gilt es, bei allen Beteiligten ein gemeinsames Verständnis für den Nutzen und den korrekten Einsatz digitaler Signaturen herzustellen. Die Praktikabilität, die Flexibilität der vereinbarten Lösungen und der Schutz der getätigten Investitionen in die Sicherheitsinfrastruktur stehen im Vordergrund.

Die European Bridge CA stellt eine allgemeine Plattform dafür zur Verfügung, die die teilnehmenden CAs auf eine vertrauenswürdige, aber einfache Weise verbindet. Ein standardisiertes technisches und organisatorisches Regelwerk erleichtert die Integration neuer CAs in die Infrastruktur. Sobald sich ein neuer Teilnehmer anschließt, können alle Mitglieder seiner PKI mit allen Mitgliedern der anderen Bridge-CA-Partner vertrauenswürdig kommunizieren. Eine einheitliche formale Registrierungsprozedur stellt dabei sicher, dass alle Teilnehmer den Mindestanforderungen gerecht werden (s. dazu die Webseite www.bridge-ca.org).

Interoperabilität

An der Schaffung international verbindlicher Standards wird zurzeit noch gearbeitet

Leider hat eine Vielzahl unterschiedlicher, teilweise sehr komplexer Standards und Anforderungen die Entstehung übergreifender, verbindlicher Public-Key-Infrastrukturen bislang behindert. Um Interoperabilität zu erreichen, wird daher versucht, technische und organisatorische Hürden so weit wie möglich zu überwinden. Eine wichtige Lösung dabei ist die Spezifikation ISIS-MTT, die *TeleTrusT* und *T7 e.V.* mit Unterstützung des Bundeswirtschaftsministeriums ins Leben gerufen haben. ISIS-MTT legt eindeutig fest, welche Attribute existierende PKI-Standards aufweisen müssen, um international einsatzfähig zu sein, und schafft damit letztlich die Grundlage für Modelle wie die European Bridge CA (s. Abb. 4).

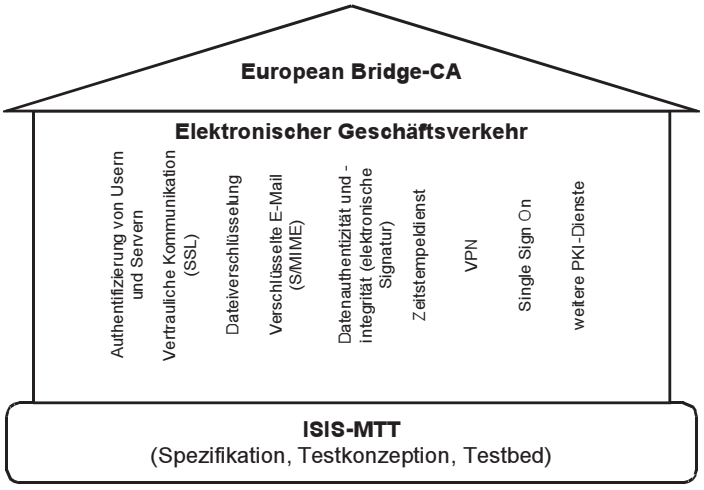

ABB. 4: Die Spezifikation ISIS-MTT gibt eindeutige Merkmale für internationale PKI-Standards wie die European Bridge CA vor.

Fazit

Die größten Probleme bei der flächendeckenden Einführung von PKI-Systemen ergeben sich aus teils inkompatiblen, teils für den praktischen Einsatz zu komplexen Standards und wenig geeigneten Vetrauensmodellen. Konzepte wie die European Bridge CA und Spezifikationen wie ISIS-MTT können helfen, diese zu lösen. Allerdings werden auch in Zukunft weitere Anstrengungen, nötig sein, um einen verbindlichen, organisations-, länder- und kulturübergreifenden *Level of Trust* zu schaffen, der die Einführung international verbindlicher Modelle gestattet.

Zu den Autoren: Prof. Dr. Norbert Pohlmann ist Geschäftsführender Direktor des Instituts für Internet-Sicherheit der Fachhochschule Gelsenkirchen. E-Mail-Kontakt: norbert.pohlmann@informatik.fh-gelsenkirchen.de

Malte Hesse ist Mitarbeiter am Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen. E-Mail-Kontakt: hesse@internet-sicherheit.de