DFN-PCA – Sicherheit im Netz

Das Pilotprojekt "Policy Certification Authority" – PCA *

Stefan Kelm
kelm@pca.dfn.de

Britta Liedtke
liedtke@pca.dfn.de

29. Februar 1996

Zusammenfassung

Verschlüsselungsprogramme wie PGP erfahren im Internet eine zunehmende Verbreitung. Grundlage solcher Programme sind asymmetrische Verschlüsselungsalgorithmen, die sog. Public Key-Verfahren, die es jedem Benutzer ermöglichen, vertrauliche Nachrichten an andere Benutzer zu senden, ohne vorher geheime Schlüssel ausgetauscht zu haben. Um einen Mißbrauch von Public Key-Verfahren zu verhindern, ist jedoch der Einsatz von Zertifizierungsinstanzen erforderlich. Am Fachbereich Informatik der Universität Hamburg wird daher innerhalb eines 18-monatigen DFN-Pilotprojekts eine solche Zertifizierungsinstanz für das WiN aufgebaut, welche schwerpunktmäßig Zertifikate für Instanzen der DFN-Einrichtungen erstellen wird.

*Dieser Artikel ist in gleicher Form auch in den DFN-Mitteilungen, Heft 40 – März 1996 veröffentlicht worden. Die Abbildungen befinden sich im Anhang dieses Artikels.

Einleitung

Das Versenden von elektronischer Post (*Email*) stellt heute neben der Benutzung von Informationssystemen wie WWW und FTP die am häufigsten genutzte Anwendung innerhalb des Internets dar. Die Zahl der auf elektronischem Wege ausgetauschten und archivierten Dokumente steigt ständig.

Die dabei zugrunde liegenden Kommunikationssysteme bieten jedoch noch immer keine Mechanismen zum Schutz der zu übermittelnden Nachrichten: die unberechtigte Einsichtnahme oder die unbefugte Veränderung fremder Nachrichten läßt sich nicht verhindern. Trotz dieser Tatsache werden immer häufiger auch sensitive Daten innerhalb des Internets versendet, was die Notwendigkeit von Sicherheitsdiensten und -mechanismen im Bereich der Rechnerkommunikation deutlich macht.

Verschlüsselungsverfahren

Die vertrauliche Kommunikation über offene Rechnernetze erfordert den Einsatz kryptographischer Methoden (z.B. einer Verschlüsselung), wobei generell zwischen symmetrischen ("Secret Key") und asymmetrischen ("Public Key") Verfahren unterschieden werden kann. Die bedeutenderen asymmetrischen Verfahren – z.B. RSA – zeichnen sich dadurch aus, daß jeder Teilnehmer über ein Paar aus mathematisch voneinander abhängigen Schlüsseln verfügt, wobei einer der beiden Schlüssel, der Public Key, öffentlich verteilt werden kann, während der andere, der Private Key, geheimgehalten werden muß. Offensichtlich darf also der Private Key unter keinen Umständen aus dem Public Key ableitbar sein. Üblicherweise wird dann der Public Key eines Benutzers verwendet, um diesem vertrauliche Nachrichten zu senden; nur der Benutzer kann mit seinem entsprechenden Private Key den Originaltext erzeugen.

Problematisch bei der Anwendung von Public Key-Verfahren ist, daß zunächst keine eindeutige Bindung zwischen einem Public Key und dem jeweiligen Benutzer besteht: es gibt keine Möglichkeit festzustellen, ob ein bestimmter Public Key wirklich zu einem Benutzer gehört oder nicht. Soll dennoch die Authentizität eines Schlüssel nachgewiesen werden, werden digitale *Zertifikate* benötigt, welche – von übergeordneten Zertifizierungsinstanzen (*Certification Authority, CA*) erstellt – eine eindeutige Verbindung zwischen einem kryptographischen Schlüssel und einer bestimmten Person herstellen.

Nur durch die Benutzung solcher Zertifikate kann ausgeschlossen werden, daß öffentliche Schlüssel von anderen Benutzern mißbraucht werden, da ohne Zertifikate ein Schlüssel unter falschem Namen erzeugt werden könnte (s. Abb. 1).

Zertifizierungsinstanzen

Jeder Benutzer, der sich zertifizieren lassen möchte, um die Sicherheitsdienste zu nutzen, kann - z.B. durch Vorlage seines Personalausweises - seine Identität gegenüber der entsprechenden CA beweisen, um ein Zertifikat zu erhalten. Alle anderen Benutzer sind dann mit Hilfe eines solchen Zertifikates in der Lage, die Echtheit dieses Schlüssels einwandfrei zu verifizieren – sie können diesen Schlüssel anschließend verwenden, um vertrauliche Nachrichten an den Besitzer dieses Schlüssels zu versenden. Zertifikate unterliegen einer festgelegten Gültigkeitsdauer, können jedoch jederzeit von der zertifizierenden Instanz für ungültig erklärt werden.

CAs operieren anhand festgelegter Richtlinien und werden ihrerseits von übergeordneten Instanzen, den sog. PCAs (Policy Certification Authority) zertifiziert, so daß eine baumförmige Hierarchie von Instanzen entsteht. Die Zertifizierungsrichtlinien einer PCA werden öffentlich bekanntgegeben und an die untergeordneten Instanzen vererbt. Die Wurzel dieser Hierarchie wird dabei von der *Internet Policy Registration Authority* (IPRA) gebildet.

Bisher existiert im Internet keine wirklich funktionierende Hierarchie von CAs. Es werden zwar einige lokal operierende CAs betrieben; eine flächendeckende Struktur von CAs ist bisher jedoch noch nicht abzusehen. Auch die IPRA, die momentan vom MIT in Boston angeboten wird, befindet sich noch im Anfangsstadium ihres Betriebes. Speziell der Aufbau und Betrieb von landes- und netzwerkweiten PCAs hat daher eine besondere Bedeutung, da eine existierende PCA den Aufbau weiterer, untergeordneter CAs unterstützen und somit die Bildung einer Hierarchie motivieren könnte.

Für die Nutzer des Deutschen Forschungsnetzes wird jetzt eine zentrale Anlaufstelle eingerichtet, bei der sie kompetente Unterstützung für den Aufbau und den Betrieb eigener Zertifizierungsinstanzen erhalten: Die DFN-PCA wird Zertifikate für organisations-eigene CAs erstellen und bei deren Aufbau unterstützend tätig sein.

Anwendung von Zertifikaten

Durch den Einsatz von kryptographischen Verfahren lassen sich wichtige Sicherheitsdienste wie Integrität, Authentizität und Vertraulichkeit bei der elektronischen Kommunikation in Netzwerken realisieren. Speziell die Verwendung von Public Key-Verfahren ermöglicht die sichere Kommunikation über bekanntermaßen unsichere Netzwerke wie dem Internet, ohne daß vorher ein Austausch von geheimen Schlüsseln notwendig ist.

Zu den Hauptanwendungsgebieten digitaler Zertifikate gehören Anwendungen, die eine elektronische Kommunikation unter Zuhilfenahme kryptographischer Verfahren sicherer machen können. Insbesondere Programme wie PEM ("Privacy Enhanced Mail") und PGP ("Pretty Good Privacy") stehen auf FTP-Servern weltweit zur Verfügung, haben jedoch bis heute keine globale Verbreitung erfahren. Auch zukünftige Anwendungsgebiete werden momentan in diversen Arbeitsgruppen international diskutiert; hierzu gehören vor allem Konzepte zur Sicherung des WWW ("Secure WWW"), die Einbindung von PEM-Diensten in MIME ("MOSS"), sowie elektronische Bezahlungsmöglichkeiten über das Internet ("Electronic Cash"). Diese Anwendungen sind allerdings noch als proprietär oder als im Experimentierstadium befindlich einzustufen.

Obwohl verschiedene Experten eine gegensätzliche Meinung vertreten, werden die auf Anwenderseite notwendigen kryptographischen Schlüssel nicht von der DFN-PCA erzeugt, sondern bleiben in der Verantwortung des Benutzers. Das häufig zitierte "big brother"-Problem ist also nicht relevant, da die CA keinerlei private Schlüssel der Anwender besitzt.

Die Wurzel einer DFN-weiten Zertifizierungshierarchie kann von der DFN-PCA gebildet werden; das Zertifikat der DFN-PCA, welches auch deren Public Key enthält, ist demnach ausreichend vor Mißbrauch zu schützen und öffentlich zu verteilen, z.B. in den DFN-Mitteilungen. Mit dem öffentlich bekannten Public Key der DFN-PCA kann anschließend jeder Teilnehmer der DFN-Zertifizierungshierarchie alle anderen zertifizierten Benutzer eindeutig identifizieren und somit sicher kommunizieren (s. Abb. 2). Es sei jedoch ausdrücklich darauf hingewiesen, daß durch eine Zertifizierung keinerlei rechtliche Ansprüche an die DFN-PCA entstehen.

Eine PCA für das DFN

Mit der Ausschreibung des Projekts "PCA im DFN – Aufbau einer Policy Certification Authority (PCA) für das Deutsche Forschungsnetz" trug der DFN-Verein der zunehmenden Bedeutung kryptographischer Verfahren in Netzwerken Rechnung. Die Arbeit des Projektteams an der Universität Hamburg begann am 1. Januar 1996 und läuft über einen Zeitraum von 18 Monaten. Praktische Untersuchungen und Forschungen sollen auch im Rahmen von Studien- und Diplomarbeiten durchgeführt werden. Die Aufgaben des Projekts sind:

- *Aufbau und Betrieb einer PCA*

  Die DFN-PCA soll in erster Linie Zertifikate für organisations-weite CAs erstellen, aber auch Netzwerkmanager und Systemadministratoren bei der Einrichtung eigener CAs unterstützen.

- *Betreuung und Unterstützung*

  Die Betreuung der Anwender durch die DFN-PCA gliedert sich in drei verschiedene Bereiche:

  - allgemeine Grundlagen und Fragen zu Zertifizierung, Zertifizierungsinstanzen, kryptographischen Verfahren, digitalen Signaturen, etc.
  - Zertifizierung untergeordneter Organisations-CAs durch die DFN-PCA
  - Zertifizierung von End-Anwender durch eine vorübergehend betriebene zusätzliche CA unterhalb der DFN-PCA

- *Kooperation mit anderen Gruppen*

  Durch den Aufbau einer DFN-PCA und der Kooperation mit anderen deutschen PCAs (ähnliche Projekte werden von der Deutschen Telekom und im kommerziellen Bereich geplant; im Rahmen von TERENA werden Bestrebungen für eine europäische Infrastruktur vorangetrieben) könnte die Kommunikation zwischen DFN-Mitgliedern und weiteren Anwenderkreisen unterstützt werden.

- *Untersuchungen und Forschungen*

  Untersuchungen beinhalten vor allem praktische Tests relevanter Softwarepakete für den Einsatz innerhalb einer CA/PCA, sowie Analysen von neuen Programmen und Konzepten.

PCAs können mit unterschiedlich starken Sicherheitsanforderungen ("Policies") betrieben werden. Die Regeln einer Policy lassen sich dabei grob in die Klassen "High-Level", "Medium-Level" und "Low-Level" einordnen und werden an die von der PCA zertifizierten CAs weitergegeben. Während der Laufzeit des DFN-Projektes wird davon ausgegangen, daß kein breiter Bedarf für eine PCA mit höchsten Sicherheitsanforderungen bestehen wird; sinnvoll erscheint daher der Betrieb zweier PCAs mit unterschiedlichen Policies ("Medium-Level" und "Low-Level").

Dienstangebote des Projekts

Die Dienste einer PCA richten sich an einen bestimmten Anwenderkreis, welcher in erster Linie aus Administratoren von CAs besteht. Aber auch End-Anwender werden von einer PCA angesprochen, da zentrale Informationen von der PCA verteilt werden, die für die End-Anwender relevant sind, z.B. Listen mit ungültig gewordenen Zertifikaten, die sog. "Certification Revocation Lists" (CRL).

Durch die von der DFN-PCA angebotenen Dienstleistungen wird ein hohes Sicherheitsniveau vor allem bei der elektronischen Kommunikation erreicht. Von besonderer Bedeutung ist hierbei auch der direkte Kontakt zwischen den DFN-Teilnehmern und den Mitarbeitern der DFN-PCA; durch die Aufklärung und Bereitstellung von Informationen werden Kenntnisse über Bedrohungen und Sicherheitsmaßnahmen verbreitet.

Speziell wird der Einsatz von Anwendungen empfohlen, welche eine Absicherung der Kommunikation durch die Verwendung von Public-Key-Verfahren erlauben. Für die notwendige Garantie einer authentischen Bindung zwischen öffentlichem Schlüssel und Schlüsselbesitzer wird die Zertifizierung als eine Hauptdienstleistung angeboten. Damit in engem Zusammenhang stehen andere Aufgaben wie die Schlüssel- und Zertifikatsverteilung, die Pflege und Verteilung der CRLs, sowie die Festlegung der damit verbundenen Policies.

Fragen und Probleme können jederzeit an die Projektmitarbeiter herangetragen werden; mit der DFN-PCA existiert ein kompetenter Ansprechpartner, welcher die Klärung offener Fragen und Probleme beim Betrieb einer eigenen lokalen CA anbietet. Die Anwender können also gezielt ihre Erwartungen und Wünsche an die DFN-PCA richten.

Ausblick

Durch die praktische Arbeit des Projektes werden wichtige Erfahrungen in den Bereichen Public Key-Verschlüsselung, Zertifizierung, sowie den damit verbundenen Anwendungen entstehen. Aus diesen Erfahrungen können dann wesentliche Leitlinien für zukünftige Projekte in diesem Bereich abgeleitet werden. Abhängig von den Entwicklungen und der geplanten Zusammenarbeit mit vergleichbaren Projekten in dem Bereich kann dann beispielsweise eine Spezialisierung der bereits bestehenden Dienstangebote, oder eine Erweiterung der Angebote auf neue Anwendungen berücksichtigt werden.

Das Projekt wird sich auf der 24. Betriebstagung vorstellen und dort auch im Arbeitskreis “Security” vertreten sein. Gelegenheit zu aktiver Diskussion besteht jederzeit. Über wichtige Entwicklungen und Ergebnisse aus dem Projekt wird auch an dieser Stelle berichtet werden. Alle DFN-Mitglieder werden gebeten, das Leistungsangebot in Anspruch zu nehmen, sowie konstruktive Kritik und Vorschläge einzubringen.

Kontaktadressen

Direkte Anfragen an die DFN-PCA sind erwünscht. Sie erreichen das Projekt unter folgender Email-Adresse:

`dfnpca@pca.dfn.de`

oder über:

DFN-PCA
Universität Hamburg
Fachbereich Informatik – RZ
Vogt-Kölln-Str. 30
22527 Hamburg
Tel. (040) 54715-262
Fax. (040) 54715-241

Die Informationsdienste der DFN-PCA sind bereits installiert; es werden zur Zeit die Server des DFN-CERT mitbenutzt:

`ftp://ftp.pca.dfn.de/pub/`
`http://www.pca.dfn.de`

Der WWW-Server bietet ergänzend die Möglichkeit einer Volltext-Recherche in sämtlichen Dokumenten des Servers.

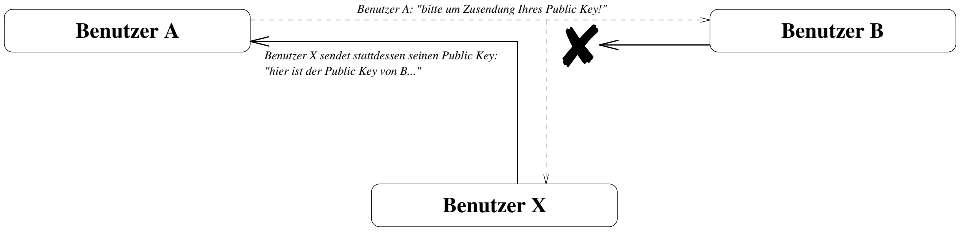

Abb. 1: Benutzer X kann sich ohne Zertifikate für Benutzer B ausgeben.

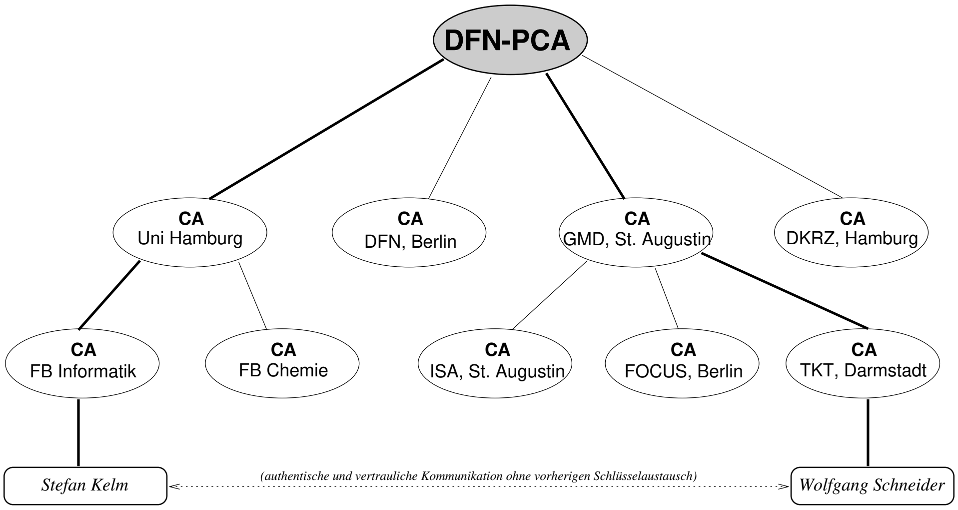

Abb. 2: Gesicherte Kommunikation innerhalb der Zertifizierungshierarchie