Protokoll zum Treffen der DFN-Projekte DFN-PCA und AMBIX am 4. und 5.12. 1996

Am 4.12.1996, 14:00-18:00 Uhr und am 5.12, 9:00-13:00 Uhr trafen sich in Tübingen, Zentrum für Datenverarbeitung Stefan Kelm, Projekt DFN-PCA (Universität Hamburg), sowie Dr. Ralf Schneider und Karl-Peter Gietz vom Projekt AMBIX (Universität Tübingen), um die gemeinsame Zusammenarbeit bezüglich der Veröffentlichung von zertifizierten öffentlichen Schlüsseln im X.500 zu besprechen. Dr. Kurt Spanier, Projektleiter von AMBIX, konnte wegen Krankheit nicht teilnehmen. Vor dem Treffen wurden via Email gegenseitig Stichworte und Themen für das Treffen ausgemacht. Diese wurden Stück für Stück abgearbeitet.

Folgende Abkürzungen werden im Protokoll verwendet:

AMBIX	DFN-Projekt Aufnahme von MailBenutzern in das X.500-Verzeichnis
CA	Certification Authority
CRL	Certificate Revocation List
DN	Distinguished Name (innerhalb des X.500-Directory)
DSA	Directory System Agent
FTP	File Transfer Protocol
IETF	Internet Engineering Task Force
OA	Organisations Administrator (für AMBIX zuständig)
PCA	Policy Certification Authority (Die DFN-PCA in Hamburg)
PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy (Public Key System)
SigV	Signaturverordnung
SSH	Secure Shell
SSL	Secure Socket Layer
SDSI	Simple Distributed Security Infrastructure
SPKI	Simple Public Key Infrastructure
UCA	User Certification Authority (die von der PCA betriebene CA)

Welche Schlüssel sollen abgelegt werden?

Es wurde festgestellt, daß es im Augenblick für PEM- und PGP-Schlüssel einen Bedarf gibt, wobei davon ausgegangen werden kann, daß eine wesentlich größere Anzahl von PGP-Zertifikaten ausgestellt werden wird. Allerdings erklärten sich beide Seiten bereit, auf zukünftige Entwicklungen zu reagieren und weitere Schlüssel- bzw. Zertifikatformate zu berücksichtigen. Hier stehen insbesondere Zertifikate nach X.509v3 (z.B. SSL), SPKI, SDSI jetzt schon im Blickfeld; weitere könnten noch dazukommen. Auch die Integration neuartiger Widerrufslisten (z.B. CRLv2) ist zukünftig denkbar.

Die neue Gesetzgebung zur Telekommunikation

Im Gesetzesentwurf des Bundes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (IuKDG; plus entsprechender Verordnung zur digitalen Signatur, SigV) wird auch die elektronische Einverständniserklärung für die Veröffentlichung von Daten geregelt (Art. 2, §3, Abschn. 7). Der einzige, bisher nicht von AMBIX erfüllte Punkt lautet: *„Die Einwilligung kann auch elektronisch erklärt werden, wenn der Diensteanbieter sicherstellt, daß sie (...) nicht unerkennbar verändert werden (...) kann."* Die Teilnehmer waren sich einig, daß dieser Punkt durch eine PGP-Signierung der Benutzerformulare erfüllt werden könnte. Ob und in wie weit dieser Punkt jedoch für die Arbeit des AMBIX-Projektes rechtlich relevant ist, konnte wegen fehlender juristischer Kompetenz nicht entschieden werden - es besteht daher noch Klärungsbedarf.

PGP-Zertifikate

- **PGP-Zertifikate im X.500**

  Es wurde festgestellt, daß es im Augenblick noch keine standardisierte Möglichkeit gibt, PGP-Schlüssel und -Zertifikate im X.500 abzulegen. Ein im Februar 1996 veröffentlichter Internet-draft, welcher diese Problematik aufgreift, ist bereits abgelaufen. Die entsprechende IETF-Arbeitsgruppe wollte kurz nach dem Treffen tagen. AMBIX steht in Kontakt mit einem Teilnehmer, Roland Hedberg, der das Projekt auf dem Laufenden halten will. Alle waren sich einig, die Entwicklung innerhalb der IETF abzuwarten, bevor entschieden wird, ob die PGP-Zertifikate im X.500 diesem Standard entsprechend abgelegt werden sollen, oder eine in Tübingen schon praktizierte, proprietäre Lösung eingesetzt werden soll. In der Zwischenzeit wird die Verteilung direkt von der DFN-PCA vorgenommen.

- **PGP-UserID**

  Als weitere Schwierigkeit hierbei stellte sich heraus, daß - da die PGP-User-ID frei wählbar ist und nicht aus einem X.500-konformen DN besteht - die Zuordnung von Key und im X.500 eingetragenen Benutzer problematisch werden kann. Um eine solche Zuordnung dennoch, zumindest für die in der internen AMBIX-Datenbank gespeicherten Personen herstellen zu können, wurde beschlossen, die Zertifizierungsrichtlinien („Policy") der DFN-PCA dahingehend anzupassen, den Benutzern die Aufnahme der Emailadresse in die PGP-User-ID zu empfehlen. Dennoch ist es denkbar, daß bestimmte Benutzer aufgrund fehlender Emailadressen nicht durch AMBIX repräsentiert werden können.

- **Standardreferenz für PGP-Zertifikate**

  Standardreferenz für PGP-Zertifikate bleibt vorerst das weltweite PGP-Keyserver-System, an dem die DFN-PCA beteiligt sein wird. Derzeit wird von der DFN-PCA überprüft, ob der Betrieb eines „isolierten" PGP-Keyservers sinnvoll ist. Ein solcher Keyserver würde lediglich die Schlüssel der Teilnehmer aus der DFN-Hierarchie beinhalten und durch die erheblich kleinere Datenbank eine schnellere Möglichkeit der Abfrage bereitstellen.

- **Gültigkeit von PGP-Zertifikaten**

  Die derzeit eingesetzten PGP-Versionen unterstützen keine Gültigkeitsdauer für Zertifikate - dieses wird insbesondere aus der Sicht einer Zertifizierungsinstanz als Problem angesehen. Die zukünftige PGP-Version 3.0 wird Mechanismen, welche die Dauer der Gültigkeit regeln, enthalten und soll Anfang 1997 verfügbar sein.

- **Auswahl der zu speichernden Benutzer**

  Derzeit werden vom AMBIX-Projekt nur solche Benutzer im X.500 eingetragen, welche über eine „.de"-Emailadresse verfügen. Das PCA-Projekt kann jedoch prinzipiell auch Teilnehmer mit abweichenden Emailadressen (z.B. „.com") zertifizieren. Wie eine Veröffentlichung derartiger Benutzerdaten durchgeführt werden soll, wird im Einzelfall zu klären sein. Eventuell können zukünftig auch andere Benutzer in die AMBIX-Datenbank aufgenommen werden.

Zertifikate nach X.509

In diesem Abschnitt wird die Interaktion zwischen PCA und AMBIX bezüglich der X.509-Zertifikate behandelt. Diese Interaktion soll auch als Modell für die Organisationen, die selbst Daten im X.500 verwalten, dienen.

- **Zertifizierung von CAs durch die PCA**

  – Damit sichergestellt ist, daß die CAs ihre DNs und die der Benutzer X.500-konform bilden, ist folgendes Procedere beschlossen worden: Wenn sich eine CA bei der PCA zertifizieren lassen will, prüft die PCA vor der Zertifizierung durch einen entsprechenden Clientaufruf auf dem AMBIX-Rechner nach, ob für die jeweilige Organisation bereits eine X.500-Struktur angelegt worden ist.

    Die vom Client zurückgegebene Struktur wird von der PCA an die CA übermittelt, mit der Aufforderung, die User-DNs entsprechend dieser Struktur zu bilden. Die Details des entsprechenden Protokolls werden von den Mitarbeitern der PCA in Abstimmung mit AMBIX entwickelt.

  – Für den o.g. Clientaufruf, wird für die PCA ein AMBIX-Account eingerichtet, der ausschließlich über ein sicheres (sowohl authentisierendes wie verschlüsselndes) Kommunikations-Protokoll (SSH) von einem festgelegten PCA-Rechner aus benutzt werden darf. Über diesen Account legt die PCA die CA-Daten bei AMBIX ab und informiert AMBIX über diese Daten. AMBIX benachrichtigt die DFN-PCA per Email, sobald die CA-Daten im X.500 eingetragen wurden. Zu diesem Zweck reicht die Übermittlung einer Standardantwort aus.

  – Bei der Rückmeldung einer Organisationsstruktur ist es unerheblich, ob diese Struktur im Zuständigkeitsbereich von AMBIX angesiedelt ist, oder in einem sonstigen gepflegten X.500-Bereich liegt.

  - Ist für eine Organisation noch keine X.500-Struktur definiert worden, muß eine solche in Interaktion mit AMBIX erstellt werden, bevor die CA von der DFN-PCA zertifiziert werden kann.
  - Nach der Zertifizierung einer CA übermittelt die PCA Name, Email-Adresse, und Telefonnummer mindestens eines Ansprechpartners in der CA an AMBIX, um den Projektmitarbeitern den Kontakt mit der CA zu ermöglichen.
  - Bei der Zertifizierung von CAs gibt die PCA mit einem im Wortlaut noch abzusprechenden Standardbrief den CA-Administratoren bestimmte Informationen; z.B. über die Liefermodalitäten der Zertifikate an AMBIX.
  - Es soll u.a. der CA-Administrator aufgefordert werden, via Fax oder Briefpost eine schriftliche Bestätigung an AMBIX zu schicken, daß er von allen Benutzern die schriftliche Einwilligung für die Veröffentlichung der gelieferten Zertifikate im X.500 eingeholt hat. Nicht notwendig ist die Einwilligung jedes einzelnen Benutzers gegenüber AMBIX.
  - Bei CAs, die eine Zusammenarbeit mit AMBIX ablehnen, wird im mindestens anzulegenden Organisations-Kopfeintrag ein entsprechender Satz im Attribut „description“ abgelegt.

- **Die Lieferung der Zertifikate von den CAs an AMBIX**
  - Die Lieferung soll in dem von AMBIX für Personendatenlieferungen durch Organisationen vorgesehenen Format erfolgen. Folglich müssen den CA-Administratoren geeignete Hilfestellungen zur Verfügung gestellt werden (s.o.).
  - Generell werden AMBIX-seitig CAs wie an AMBIX aktiv teilnehmende Organisationen verwaltet, z.B. was die Registrierung von zuständigen Administratoren angeht.
  - Die Informationspolitik von AMBIX ist gegenüber CAs eine andere als bei OAs: es werden keine automatischen Datenlisten (von Selbsteinträgern bzw. Benutzerdatenänderungen) an die CAs geschickt.

- **Wer darf Zertifikate im X.500 eintragen/löschen?**
  - Durch CAs zertifizierte Schlüssel werden grundsätzlich nur von den CAs bzw. der DFN-PCA an AMBIX geliefert.
  - Zertifikate werden generell nur von solchen CAs angenommen, die sich in der Zertifizierungshierarchie unterhalb der DFN-PCA befinden.
  - Benutzer / OAs dürfen eigene, unzertifizierte (bzw. selbst-zertifizierte) Schlüssel ins X.500 eintragen.
  - CAs und OAs dürfen nur Einträge löschen, die kein gültiges Zertifikat eines Benutzers oder einer CA mehr enthalten (s.u.: „historischer DSA“). Einmal veröffentlichte CA-Zertifikate dürfen frühestens nach Ablauf der Gültigkeitsdauer aus dem X.500 entfernt werden, auch wenn ein Zertifikat zwischenzeitlich widerrufen wurde.

- Benutzer dürfen nach wie vor jederzeit ihren eigenen Eintrag löschen lassen, auch wenn dieser ein noch gültiges Zertifikat enthält.
- Ändert sich der DN eines eingetragenen Benutzers, ist der zuständige OA zu benachrichtigen.

- **Sonderstellung der User-CA**

  - Für eine Anlaufzeit, in der es noch wenige CAs gibt, sieht die PCA vor, eine eigene User-CA (UCA) aufzubauen, bei der sich beliebige Benutzer zertifizieren lassen können, solange noch keine flächendeckende Zertifizierungshierarchie existiert.
  - Da sich von der UCA zertifizierte Benutzer keiner Organisation zuordnen lassen, sollen diese unter dem X.500-Eintrag der PCA (unterhalb von *c=DE, o=DFN, ou=PCA, ou=User Certification Authority* oder *c=DE, o=DFN, ou=User Certification Authority* geplant) eingetragen werden.
  - Näheres zu oben beschriebenen DNs muß mit den Betreibern des DSAs des DFN-Vereins (Herr Jaretzki bzw. Frau Schröder) geregelt werden. AMBIX ist nicht unmittelbar für diese Einträge zuständig, es sei denn es wird vom DFN-Verein anders entschieden.
  - Da für die Zertifizierung eines Schlüssels durch die UCA in der Regel der persönliche Kontakt zwischen dem Benutzer und einem PCA-Mitarbeiter notwendig ist, ist nicht zu erwarten, daß hier erhebliche Datenmengen entstehen werden.
  - Die Frage, ob diesen Benutzern die Möglichkeit gegeben werden sollte, sich in die AMBIX-Struktur umzumelden, konnte noch nicht geklärt werden.

- **Widerrufslisten (CRLs)**

  - CRLs sollen regelmäßig von der PCA sowie den einzelnen CAs an AMBIX geliefert werden. AMBIX wird diese X.509-Konform im X.500 zur Verfügung stellen. Die Details des entsprechenden Protokolls werden von den Mitarbeitern der PCA in Abstimmung mit AMBIX entwickelt.
  - Die Möglichkeit der automatischen Auswertung dieser CRLs durch AMBIX und einer daraus resultierenden Kennzeichnung zurückgezogener Zertifikate im X.500 wurde angesprochen. Eine entsprechende Realisierung durch die Mitarbeiter des AMBIX-Projektes wurde jedoch nicht abschließend beschlossen.
  - CRLs sollen weder von Benutzern noch von OAs gelöscht werden können. Auch die Löschung einer CRL durch den verantwortlichen CA-Administrator sollte im Regelfall nicht ermöglicht werden. Bei Bedarf muß in jedem Fall Rücksprache mit einem PCA-Mitarbeiter gehalten werden.

- **Ein DSA für abgelaufene Zertifikate**

  Da nach dem aktuellen SigV-Entwurf Zertifikate über einen Zeitraum von mindestens 10 Jahren nach Ausstellung überprüfbar sein müssen, wird von

AMBIX für abgelaufene Zertifikate ein eigener X.500-Datenbestand aufgebaut und Recherche-Tools zur Verfügung gestellt, sofern sich hierfür ein Bedarf abzeichnet. Die Implementierung dieses „historischen DSA“ hat allerdings zunächst keine hohe Priorität, sondern ist eher als ein gegebenenfalls zusätzlich anzubietender Service zu betrachten. Nur Zertifikate, deren reguläre Gültigkeitsdauer abgelaufen ist - nicht aber via CRLs zurückgezogene Zertifikate - sollen in diesem historischen DSA abgelegt und aus dem aktuellen Datenbestand gelöscht werden.

Email-Schnittstelle für die Zertifikat-Recherche

Die Frage einer Email-Schnittstelle für Zertifikat-Recherche wurde kurz angesprochen. Falls sich ein Bedarf dafür abzeichnet, kann AMBIX eine entsprechende Schnittstelle zur Verfügung stellen. Allerdings dürfen auf diesem Weg lediglich das Zertifikat sowie die bei der Anfrage gelieferten Daten, nicht jedoch personenbezogene Daten, weitergegeben werden, da man den Absender einer Email-Anfrage ohne den Einsatz kryptographischer Hard- und Software nicht sicher identifizieren kann. Eine solche Identifikation ist jedoch Voraussetzung für die dem Projekt AMBIX vorgegebene Zugriffsbeschränkung auf Länder mit adäquaten Datenschutz. Für die PCA und somit für die Weitergabe der Zertifikate gibt es keine solche Beschränkungen.

Aufhebung des dem Projekt AMBIX vorgegebenen Minimalset

Ebenfalls aus Datenschutzgründen wurde AMBIX bisher lediglich erlaubt, ein Minimalset von personenbezogenen Daten (Name, Titel, Telefon, Fax, Emailadresse) zu sammeln. Da dieser Minimalset zukünftig durch *Public Keys* bzw. zugehörige Zertifikate ergänzt werden muß, stellt sich die Frage, ob darüber hinaus noch weitere Attribute zugelassen werden sollen und können, z.B. URL und Arbeitsgebiet, was von vielen Benutzern bereits mehrfach angeregt wurde. Selbstverständlich handelt es sich bei diesen zusätzlichen Attributen um freiwillige Angaben der Betroffenen. Bei Organisationslieferungen soll nur - im Falle der CAs - das Zertifikat zusätzlich erlaubt sein. Diese Fragen müssen mit dem DFN-Verein noch geklärt werden.

Beschreibung der internen AMBIX-Verarbeitung

Zur Information des PCA-Projektes wurde kurz das interne Vorgehen von AMBIX gezeigt, insbesondere die interne Datenhaltung und das Mailanalyseprogramm wurden vorgeführt.

Sicherheitsaspekte in der AMBIX-Arbeit

Schließlich wurde auch das Vorgehen von AMBIX in Bezug auf Sicherheitsfragen durch das PCA-Projekt kommentiert. Diesbezügliche Anregungen wurden gerne von AMBIX aufgenommen; beispielsweise die Einrichtung von unsichtbaren Unterverzeichnissen im „incoming“-Bereich des FTP-Servers, deren Namen nur die jeweils schreibberechtigte Organisation für die Ablage von X.500-Daten kennen soll. Ferner wurde besprochen, daß die Kommunikation mit den einzelnen Organisationen mittels PGP deutlich sicherer gemacht werden kann und soll.

Auch zukünftig sind die Mitarbeiter der DFN-PCA jederzeit gerne bereit, in Fragen der Rechner- und Netzwerksicherheit unterstützend tätig zu werden.

Schlußbemerkung

Insgesamt stellten alle Beteiligten des Treffens fest, daß in konzentrierter Arbeit alle wesentlichen Aspekte der Zusammenarbeit besprochen werden konnten. In jeder Hinsicht wurde eine gute Grundlage hierfür erstellt.

Karl-Peter Gietz
DFN-Projekt AMBIX
Zentrum für Datenverarbeitung
Universität Tübingen

Stefan Kelm
DFN-PCA
Fachbereich Informatik
Universität Hamburg