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, Zweigstelle Morgenstelle Stefan Kelm, Projekt DFN-PCA, Universität Hamburg und 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, Prjektleiter von AMBIX, konnte wegen Krankheit leider 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
IETF	Internet Engineering Task Force
OA	Organisations Administrator (für AMBIX zuständig)
PCA	Policy Certification Authority (Die DFN-PCA in Hamburg)
PGP	Pretty Good Privacy (Public Key System)
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. Allerdings erklärten sich beide Seiten bereit auf zukünftige Entwicklungen zu reagieren und weitere Schlüssel bzw. Zertifikate zu berücksichtigen. Hier stehen z.B. Schlüssel nach X.509v3, SSL, SPKI, SDSI jetzt schon im Blickfeld, andere können noch dazukommen.

- **Die neue Gesetztgebung zur Telekommunikation**
  Im Gesetzt des Bundes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste mit Verordnung zur digitalen Signatur wird auch elektronische Einverständniserklärung für die Veröffentlichung von Daten geregelt (Art. 2 Par. 3 Abschn. 7). Der einzige bisher nicht von AMBIX erfüllte Punkt (Nr. 2) lautet: Die Einwilligung kann auch elektronisch erklärt werden, wenn der Diensteanbieter sicherstellt, daß 2. sie nicht unerkennbar verändert werden kann. Die Teilnehmer waren sich einig, daß dieser Punkt durch eine PGP-Signierung der Benutzerformulare erfüllt werden kann. Ob AMBIX dazu verpflichtet werden kann, konnte wegen fehlender juristischer Kompetenz nicht entschieden werden.

- **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. Das entsprechende Internet-draft ist abgelaufen. Die entsprechende IETF 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 diese Entwicklung abzuwarten, bevor man sich entscheidet, wie die PGP-Zertifikate im X.500 abgelegt werden sollen.
  - **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 schwierig wird. Um eine solche Zuordnung dennoch, wenigstens für die in der internen Datenbank von AMBIX gespeicherten Personen herstellen zu können, wurde beschlossen zu empfehlen, die Emailadresse in die PGP-User-ID mit einzubringen.
  - **Standardreferenz für PGP-Zertifikate**
    Standardreferenz für PGP-Zertifikate bleibt vorerst das PGP-Keyserver-System.
  - **Gültigkeit von PGP-Zertifikaten**
    PGP-Zertifikate der augenblicklichen PGP-Version haben kein Gültigkeitsablauf. Dieses wird als Problem angesehen. Die zukünftige PGP-Version 3.0 wird Mechanismen, die die Dauer der Gültigkeit regeln enthalten.

- **Zertifikate nach X.509**

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

  - **Zertifizierung von CAs durch die PCA**
    - Damit sichergestellt ist, daß die CAs die DNs der User X.500-konform bilden, ist folgendes Procedere beschlossen worden: Wenn sich eine CA bei der PCA zertifizieren läßt, prüft die PCA durch einen entsprechenden Clientaufruf auf der AMBIX-Maschine nach, ob für die jeweilige Organisation bereits im X.500 eine 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.
    - Für den erwähnten Clientaufruf, wird von AMBIX der PCA ein account eingerichtet, der über 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 schreibt eine EMail zurück, nachdem Die CA-Daten im X.500 eingetragen wurden.

  * Bei der Rückmeldung der Organisationsstruktur ist es unerheblich, ob diese Struktur im Zuständigkeitsbereich von AMBIX angesiedelt ist, oder in einem sonstigen gepflegten X.500-Bereich liegt.
  * Ist keine Struktur definiert, muß eine solche in Interaktion mit AMBIX erstellt werden, bevor die CA zertifiziert werden kann.
  * Nach der Zertifizierung einer CA, übermittelt die PCA Name, Email-Adresse, und Telefonnummer mindestens eines Ansprechpartners in der CA an AMBIX.
  * Bei der Zertifizierung der CAs gibt die PCA mit einem im Wortlaut noch abzusprechenden Standardbrief an die CA-Administratoren Informationen auch über die Liefermodalitäten der Zertifikate an AMBIX.
  * Hierbei soll u.a. der CA-Administrator aufgefordert werden, an AMBIX via Fax oder Briefpost eine schriftliche Bestätigung schicken, daß er von allen Benutzern der gelieferten Zertifikaten die schriftliche Einwilligung für die Veröffentlichung der Daten im X.500 eingeholt hat.
  * Bei CAs die eine Zusammenarbeit mit AMBIX verweigern, wird im mindestens anzulegenden Organisations Kopfeintrag ein entsprechender Satz im Attribut „description“ abgelegt.

- **Die Lieferung der Zertifikate von den CAs an AMBIX**
  * Die Lieferung erfolgt in dem von AMBIX für Personendatenlieferungen durch Organisationen vorgesehenen Format.
  * Generell werden AMBIX-seitig CAs wie an AMBIX aktiv teilnehmende Organisationen verwaltet, z.B. was die Registrierung von zuständigen Administratoren angeht.
  * Nur die Informationspolitik ist gegenüber CAs eine andere als bei OAs: Es werden keine automatischen Datenlisten (von Selbsteinträgern bzw. Userdatenänderungen) an die CAs geschickt.
- **Wer darf Zertifikate eintragen/löschen**
  * Zertifizierte Schlüssel werden grundsätzlich nur von den CAs geliefert.
  * Zertifikate werden nur von PCA-Zertifizierten CAs angenommen
  * User/ OAs dürfen eigene unzertifizierte Schlüssel ins X.500 eintragen
  * CAs und OAs dürfen nur Einträge löschen, die kein gültiges Zertifikat mehr haben
  * User dürfen nach wie vor jederzeit ihren Eintrag löschen lassen, auch wenn dieser ein noch gültiges Zertifikast enthält.
- **Sonderstellung der UCA**
  * Für eine Anlaufzeit, in der es noch wenige CAs gibt, sieht die PCA vor eine eigene UCA aufzubauen, bei der sich beliebige User Zertifizieren lassen können.

    * Da sich diese User CA-mäßig keiner Organisation zuordnen lassen, sollen diese unter dem X.500-Eintrag der PCA (unter c=DE, o=DFN, ou=PCA, ou=User Certification Authority) eingetragen werden.
    * Näheres muß mit den Betreiber des DSAs des DFN-Vereins (Herr Jaretzki bzw. Frau Schröder) geregelt werden. AMBIX ist nicht für diese Einträge zuständig, es sei denn es wird vom DFN-Verein anders entschieden.
    * Weil für die Zertifizierung eines Schlüssels durch die UCA eine persönliche Anwesenheit in Hamburg notwendig ist, ist es 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, wurde noch nicht geklärt.
  - **CRLs**
    * CRLs werden regelmäßig von den CAs an AMBIX geliefert. AMBIX stellt diese X.509-Konform im X.500 zur Verfügung.
    * Die Möglichkeit der automatischen Auswertung dieser CRLs durch AMBIX und der Kennzeichnung zurückgezogener Zertifikate wurde angesprochen. Eine Realisierung hiervon wurde aber nicht verpflichtend beschlossen.
  - **Ein DSA für abgelaufene Zertifikate**

    Da ein Zertifikat noch 33 Jahre nach Austellung überprüfbar sein muß, wird von AMBIX für abgelaufene Zertifikate ein eigener X.500 Datenbestand aufgebaut und Recherchetools zur Verfügung gestellt, sofern hierfür sich ein Bedarf abzeichnet. Die Implementierung dieses „historischen DSA" hat allerdings keine hohe Priorität. Nur Zertifikate, deren Gültigkeitsdauer abgelaufen sind, nicht aber via CRLs zurückgezogene Zertifikate werden in diesem historischen DSA abgelegt und aus dem aktuellen Datenbestand gelöscht.

- **Email-Schnittstelle für Zertifikatrecherche**

  Die Frage einer Email-Schnittstelle für Zertifikatrecherche wurde kurz besprochen. Falls sich ein Bedarf dafür abzeichnet kann AMBIX es zur Verfügung stellen. Allerdings dürfen auf diesem Weg keine Personenbezogenen Daten, außer den bei der Anfrage gelieferten und dem Zertifikat weitergegeben werden, da man über EMail den Abfrager nicht sicher identifizieren kann, was wiederum Vorraussetzung für die dem Projekt AMBIX vorgegebene Zugriffsbeschränkung auf Länder mit adäquaten Datenschutz.

- **Aufhebung des dem Projekt AMBIX vorgegebenen Minimalset**

  Ebenfalls aus Datenschutzgründen wurde AMBIX nur erlaubt einen Minimalset von personenbezogenen Daten (Name, Titel, Telefon, Fax, Emailadresse) zu sammeln. Da dieser Minimalset durch *Public Keys* bzw,. deren Zertifikate aufgehoben werden muß, stellt sich die Frage, ob nicht noch weitere Attribute zugelassen werden sollen, z.B. URL und Arbeitsgebiet, was von vielen

Benutzern schon angeregt worden ist. Selbstverständlich handelt es sich bei allen diesen Attributen um freiwillige der Betroffenen. Bei Organisationslieferungen soll nur, im Falle der CAs das Zertifikat zusätzlich erlaubt sein. Die Frage muß mit dem DFN-Verein geklärt werden.

- **Beschreibung der internen AMBIX-Verarbeitung**

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

- **Sicherheitsaspekte in der AMBIX-Arbeit**

  Schließlich wurde das Vorgehen von AMBIX in Bezug auf Sicherheitsfragen von seiten des PCA-Projektes kommentiert. Diesbezügiche Anregungen wurden gerne von AMBIX aufgenommen, zum Beispiel die Einrichtung von unsichtbaren Unterverzeichnissen im incomming-Bereich des FTP-Servers, deren Namen nur die jeweilige Organisation kennt. Ebenfalls wurde besprochen, daß die Kommunikation mit den Organisationen mittels PGP sicherer gemacht werden kann.

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