Protokoll des Treffens der DFN-Projekte DFN-PCA und DFN-DSD am 2. und 3. März 1999 in Tübingen

Am 2. März 1999, 13:00 - 17:30 und am 3. März 1999, 9:00 - 12:30 wurde am Zentrum für Datenverarbeitung der Universität Tübingen ein Arbeitstreffen der DFN-Projekte *DFN-PCA* (Univ. Hamburg) und *DFN-DSD* (Univ. Tübingen) abgehalten. Die Teilnehmer waren Stefan Kelm von der DFN-PCA, sowie Dr. Kurt Spanier, Dr. Ralf Schneider, Bernhard Winkler und Dr. Markus Sauer von DFN-DSD.

Gegenstand der Besprechungen war die bereits beim letzten Arbeitstreffen im Dezember 1996 beschlossene Zusammenarbeit bei der Veröffentlichung von zertifizierten öffentlichen Schlüsseln im X.500. Via E-Mail wurde bereits im Vorfeld des Treffens eine Agenda festgelegt, welche im Verlauf der Gespräche abgearbeitet wurde.

Das hier vorliegende Protokoll wurde von den teilnehmenden Personen gemeinsam erstellt.

Agenda

1. Status des Projekts DFN-PCA
2. Status des Projekts DDSD
3. Diskussion des Protokolls der Sitzung vom Dezember 1996 [Pro96]
4. Vorstellung und Diskussion des Tübinger PGP-Schlüssel Modells für X.500
5. Planung eines gemeinsamen Plenums-Vortrags im Rahmen der 31. Betriebstagung des DFN im Oktober 1999 in Berlin
6. Festlegung nächster Schritte

Abkürzungen

Im nachfolgenden Protokoll werden folgende Abkürzungen verwendet:

AMBIX	DFN-Projekt Aufnahme von Mail-Benutzern in das X.500–Verzeichnis
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CRL	Certificate Revocation List
DIT	Directory Information Tree
DN	Distinguished Name (innerhalb des X.500-Directory)
DSA	Directory System Agent
DSD	Directory Services Deutschland
FTP	File Transfer Protocol
PCA	Policy Certification Authority (Die DFN-PCA in Hamburg)
PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy (Public Key System)
SigG/SigV	Signaturgesetz/Signaturverordnung
S/MIME	Secure Multipurpose Internet Mail Extension
SSH	Secure Shell
SSL	Secure Socket Layer
SDSI	Simple Distributed Security Infrastructure
SPKI	Simple Public Key Infrastructure
TLS	Transport Layer Security (RFC2246)

1 Status des Projekts DFN-PCA [1]

Die Laufzeit des Projektes DFN-PCA wurde vom DFN um weitere 2 Jahre bis Ende 2000 verlängert.

Die DFN-PCA hat bei der Regulierungsbehörde für Telekommunikation und Post (RegTP) einen Antrag auf Genehmigung als SigG-konforme Zertifizierungsstelle gestellt. Das Root-Zertifikat der Regulierungsbehörde für Telekommunikation ist seit dem 1. Jan. 1999 operabel. Es gilt jedoch zum jetzigen Zeitpunkt als unrealistisch, daß die PCA in der Lage sein wird, Zertifikate ausgeben zu können, die konform zu SigG/SigV [BSI] sein werden.

In diesem Zusammenhang stellte sich die Frage in wie weit DSD als Signaturgesetz-konformer Verzeichnisdienst geführt werden kann.

2 Status des Projekts DDSD [2]

Nach Ablauf des DFN-Projektes AMBIX am 30. April 98 wurde das Nachfolgeprojekt DFN - Directory Services Deutschland (DSD) aufgebaut. Das Projekt DSD setzt sich aus folgenden Teilprojekten zusammen:

Fortführung des ehemaligen DFN-Projektes AMBIX

Bereitstellung von ISODE-Software

Betrieb und Betreuung des zentralen DSAs für Deutschland (cn=Puma)

X.500-Directory Kompetenzzentrum

Die Laufzeit des Projektes DSD endet am 30. April 2000. Danach ist eine Umwandlung in ein angegliedertes Institut oder eine GmbH geplant.

[1] Bericht von Stefan Kelm
[2] Bericht von Dr. Ralf Schneider und Dr. Markus Sauer

3 Diskussion des Protokolls der Sitzung vom Dezember 1996

Übereinstimmend wurde festgestellt, daß die Themenpunkte des Arbeitstreffens im Dezember 1996 noch weitestgehend aktuell sind. Ausgehend von den Themenpunkten des vorliegenden Protokolls [Pro96] wurden nachfolgende Fragestellungen erörtert.

3.1 Welche Zertifikate / Schlüssel sind aktuell?

Beim Arbeitstreffen im Dezember 1996 wurde ein Bedarf sowohl für die Bereitstellung von PGP- als auch von PEM-Zertifikaten gesehen. Wie damals angenommen, wurden in der Folgezeit wesentlich mehr PGP- als PEM-Zertifikate ausgestellt. In der Praxis wird PEM kaum genutzt. Alle von der DFN-PCA ausgestellten PEM-Zertifikate sind mittlerweile abgelaufen und wurden nicht erneuert.

Ein großes Interesse besteht momentan an PGP und insbesondere an Zertifikaten nach dem X.509v3-Standard (z.B. für SSL und S/MIME). Der offizielle Nachfolger von SSLv3 ist seit kurzem als TLS standardisiert, S/MIMEv3 steht kurz davor zum Standard zu werden. Die neue Version 6 von PGP soll ebenfalls den X.509v3-Standard berücksichtigen.

Derzeit (Stand: März 1999) werden 26 CAs für PGP unterhalb der DFN-PCA betrieben. Es ist zum jetzigen Zeitpunkt nicht damit zu rechnen, daß die Anzahl an untergeordneten CAs noch wesentlich zunehmen wird. Zusammen mit den von der DFN-User-CA ausgestellten Benutzer-Zertifikaten sind die CA-Zertifikate auf einem hierfür eingerichteten *Light*-Keyserver in dem bewährten PGP-Keyserver-Format abgelegt. Die starke Frequentierung dieses *Light*-Keyserver zeigt die hohe Akzeptanz einer solchen Einrichtung.

Die Nachfrage nach SSL-Zertifikaten nimmt derzeit deutlich zu. Damit dürfte dann auch die Zahl der CAs, die SSL-Zertifikate ausstellen steigen.

SDSI- und SPKI-Zertifikate besitzen hingegen keine praktische Relevanz. Da sie nicht auf dem X.509v3-Standard aufsetzen können ihre Zukunftschancen als wahrscheinlich nur gering eingeschätzt werden.

Zur Zeit existieren im Prinzip keine Implementationen von CRLv2. CRLv2 wird daher bislang praktisch nicht genutzt. Es ist allerdings davon auszugehen, daß sich dies mit neueren Versionen von Servern, Browsern und CA-Tools ändern wird.

Die PCA unterstützt verschiedene Zertifikat-Erweiterungen für X.509v3, z.B. proprietäre Erweiterungen von Netscape. Problematisch ist derzeit jedoch, daß verschiedene Anwendungen diese proprietären Zertifikat-Erweiterungen unterschiedlich interpretieren und somit Interoperabilität nicht gewährleistet ist.

3.2 Eintrag von Zertifikaten ins X.500

Die Form des DNs, für den ein X.509-Zertifikat ausgestellt wird, ist in der Policy der PCA festgelegt.

Da die DFN-PCA bei der Ausgabe von X.509-Zertifikaten generell auch DNs akzeptiert, welche nicht konform zu dem im X.500 Verzeichnis unter c=DE angelegten DIT sind, wird die Ablage dieser Zertifikate im X.500 Directory zu Problemen führen.

Die bereits bei der DFN-PCA gemachten Erfahrungen mit zu zertifizierenden Einrichtungen und Personen haben jedoch deutlich gezeigt, daß sich inbesondere bzgl. des DNs nicht immer eine standardkonforme Namensgebung durchsetzen läßt. Es wird also seitens der DFN-PCA kaum Abweichungen bzgl. der Praxis der Namensgebung geben, auch wenn dies aus Sicht von DSD, bzw. der X.500-Betreiber sicherlich mehr als wünschenswert wäre. Unklar ist momentan auch, welche genauen Anforderungen der X.509-Standard an den DN stellt. Dieser Sachverhalt muß geklärt werden.

Ein möglicher Ausweg aus dem Problem nicht DIT-konformer DNs wäre eine eventuelle Umstrukturierung des X.500-Verzeichnisses auf Deutschlandebene, d.h. unterhalb c=DE. Die Bereitschaft der betroffenen Administratoren zu einer solchen Umstrukturierung erscheint allerdings fraglich.

Einen anderen Ausweg aus dem Problem nicht DIT-konformen DNs könnte auch das im nachfolgenden Abschnitt diskutierte Tübinger Modell eines X.500 basierten Server für PGP-Schlüssel, verallgemeinert für X509 Zertifikate, darstellen.

Von DSD ist im Zusammenhang mit der Veröffentlichung von Zertifikaten die Datenschutzfrage zu berücksichtigen. Um Zertifikate im X.500-Directory zur Verfügung zu stellen, muß das bereits etablierte *AMBIX-Minimalset* eines Benutzer-Eintrags zumindest um den *Public Key* erweitert werden. Zu klären ist in diesem Zusammenhang ob evtl. ein neues Datenschutz-Gutachten für DSD erstellt werden muß, oder ob dies dadurch entfallen könnte, daß die Personen ihre Zertifikate/Schlüssel freiwillig eintragen lassen.

3.3 Einrichtung eines "historischen DSA"

Die Einrichtung und der Betrieb eines "historischen DSA", in dem abgelaufene Zertifikate und CRLs abgelegt werden, ist nicht relevant, da hierfür bisher weder ein Bedarf noch eine Notwendigkeit besteht.

4 Vorstellung und Diskussion des Tübinger PGP-Schlüssel Modells für X.500

Grundlage der Diskussion war der Beitrag von Dr. K. Spanier zu den Proceedings des 6.CERT-Workshop [Spa99]. Bezüglich der Einzelheiten des Tübinger PGP-Schlüssel Modells sei an dieser Stelle auf dieses Papier verwiesen.

Grund für den Vorschlag dieser proprietären Lösung auf der Ebene c=DE für die Implementation von PGP-Schlüsseln in das X.500-Verzeichnis ist das offensichtlich geringe internationale Interesse an der Schaffung eines X.500-Standard für PGP-Schlüssel.

Das Modell definiert alle Objektklassen und Attribute, die für die Ablage von öffentlichen PGP-Schlüssel notwendig sind. Das verwendete Speicherschema erlaubt die Online-Rückverfolgung von CA-Signaturen durch alle Zertifizierungshierachieebenen bis hinauf zur höchsten Zertifizierungsinstanz der Top Level CA. Hierdurch wird der Aufbau eines Vertrauenspfades (sog. *Chain of Trust* oder *Certification Path*) für PGP-Schlüssel realisiert. Der Zugriff auf die auf dem DDSD PGP-Keyservers abgelegten Informationen ist weltweit über die Protokolle HTTP und LDAP möglich.

Diskutiert wurden im Anschluß die Vollständigkeit und die Flexibilität des Modells; besonderer Wert wurde während der gesamten Diskussion auf die praktische Umsetzbarkeit gelegt.

4.1 Vollständigkeit und Flexibilität des Modells

Von S. Kelm wurde die Hinzunahme eines Attributs *CA-CRL* in der Objektklasse *cAInformationObject* vorgeschlagen, das einen Verweis auf die (aktuelle) CRL der jeweiligen CA beinhaltet. Es wurde betont, daß es für DSD ausreicht, einen Verweis auf die von einer CA herausgegebenen CRL anzugeben. Die CRL muß nicht direkt bei DSD verfügbar sein.

Weiter wurde vorgeschlagen, den Inhalts des Attributs *pGPAlgorithm* (Objektklasse *pGPKeyContainer*) um die Information des verwendeten Hash-Algorithmus und den Inhalt des Attributs *keyCreationMode* (Objektklasse *cAInformationObject*) um den Mode *unknown* zu erweitern.

Zum Attribut *pGPKeyRevoked* (Objektklasse *pGPKeyContainer*) wurde angemerkt, daß der Status *0 := gültig* besser durch *0: = nicht zurückgezogen* ersetzt werden sollte. Die ebenfalls für das Attribut *pGPKeyRevoked* vorgeschlagenen Werte *2 := CA-Schlüssel zurückgezogen* und *3 := von Benutzer und CA zurückgezogen* existieren zumindest derzeit noch nicht. Eventuell werden jedoch bei PGPv6 weitere Zustände unterstützt, welche dann in dieses Modell eingebaut werden könnten.

Das Attribut *withPGPRevCert* (Objektklasse *cAInformationObject*), das die Information enthält ob ein Revocation Zertifikat hinterlegt wurde oder nicht, sollte eventuell weiter aufgeschlüsselt werden.

Anzumerken ist weiter, daß die Version 6 von PGP neue Features und Konzepte wie Master- und Subkeys bringen wird, und dadurch weitere Ergänzungen notwendig machen kann. Eine hinreichende Flexibilität des Modells ist daher von enormer Wichtigkeit.

4.2 Praktische Umsetzung

Die genauen Einzelheiten werden in der noch zu formulierenden Policy vom DSD definiert. Als relevante Punkte wurde Nachfolgendes diskutiert.

4.2.1 PGP-Keyserver

Geplant ist, die bei DSD abgelegten Schlüssel mittels eines Standalone LDAP-Servers zu verwalten. Die gespeicherten Attribute werden PGPv5-konform gewählt. Der Server soll dabei so konfiguriert sein, daß ein Benutzer mit seinen PGP-Anwendungsprogrammen über die LDAP-Schnittstelle direkt auf diesen LDAP-Server zugreifen kann. Zu klären ist in diesem Zusammenhang, wie die LDAP-Schnittstelle eines Keyservers definiert ist. Vermutlich wird diese Schnittstelle jedoch vom Hersteller NAI nicht oder nicht ausreichend dokumentiert sein.

4.2.2 Gateway-Software

Um die Rückverfolgung von Signaturen durch die Zertifizierungshierarchien zu realisieren ist eine Erweiterung des Tübinger WWW-X.500 Gateways TWEB notwendig, die ein Verfolgen von LDAP-URLs ermöglicht. Mit ersten Schritten in Bezug auf die Realierung dieser Erweiterung ist bis Mitte März zu rechnen. Aus praktischen Gründen besteht darüberhinaus evtl. auch die Notwendigkeit eine neuen Objektklasse für die LDAP-URL welche den Verweis auf ein Zertifikat enthält einzuführen. Dies wiederum würde die Generierung eines zugehörigen neuen TWEB-Displaytyps notwendig machen.

4.2.3 Format für die Ablage von Zertifikaten

Im Zusammenhang mit der Ablage von Zertifikaten stellt sich allgemein die Frage in welchem Format dies geschehen soll. Ursprünglich war die Speicherung sowohl in binärer als auch in ASCII-Form geplant. Es wäre dann dem Benutzer/Client überlassen welches Format er haben möchte. Ein Problem ist jedoch, daß zB. die unterschiedlichen Browser etwas unterschiedliches Binärformat (bzw. verschiedene MIME-Typen bei der Übertragung vom Server) für SSL-Zertifikate verlangen. Es müßte also durch die CAs für jeden Browser das entsprechende Binärformat bereitgestellt werden. Dies zu Realisieren erscheint sehr aufwendig.

Wie es zur Zeit scheint werden die Zertifate im ASCII-Format von allen Browsern und auch von allen PGP-Versionen verstanden. Speziell für DSD erscheint daher derzeit nur die Ablage von ASCII-armored PGP-Keys sinnvoll.

4.3 Eintragen/Löschen von Schlüsseln/Zertifikaten

Es wurde der Vorschlag gemacht, in einer Anfangsphase lediglich (P)CA-zertifizierte Schlüssel (also Teilnehmer der DFN-PKI) in den DSD PGPkeyserver aufzunehmen. Später könnte dann ein zweiter Keyserver eingerichtet werden, der die unzertifizierten Schlüssel hält. Diese Policy-Frage muß aber noch DSD-intern diskutiert werden.

Ganz allgemein sollte in Zukunft jeder Benutzer, der bei DSD eingetragen ist, seine(n) Schlüssel eintragen bzw. löschen lassen können; unabhängig davon, ob der/die Schlüssel von einer CA zertifiziert wurde(n) oder nicht (Das Tuebinger PGP-Modell läßt beides zu). Nicht CA-zertifizierte Schlüssel von Benutzern, welche nicht bei DSD eingetragen sind, sollen nicht aufgenommen werden. Das bedeutet auch, daß die Schlüssel eines Benutzers, der seinen Eintrag bei DSD entfernen läßt ebenfalls gelöscht werden. Alle Löschungen erfolgen nach Ablauf einer definierten Frist.

Ebenfalls diskutiert wurde das Löschen von abgelaufenen PGP-Schlüsseln, also von Schlüsseln, deren Gültigkeitsdatum überschritten ist. Geplant ist, diese abgelaufenen Schlüssel nach Ablauf einer festgelegten Frist (n Tage) automatisch vom DSD PGP-Keyserver zu entfernen. Schlüssel ohne Gültigkeitsdatum werden nur auf Anfrage des Benutzers / der CA gelöscht. Evtl. könnte auch ein Attribut *pGPExpirationTime* für diese Funktionalität definiert werden.

Beim Löschauftrag einer CA für ein von ihr ausgestelltes PGP-Zertifikat wird verlangt, daß der Auftrag von der CA signiert und verschlüsselt übermittelt wird. Beim Löschauftrag eines Benutzers wird zumindest eine Signatur des Benutzers verlangt. Sollte der Fall eintreten, daß der Benutzer keinen Zugang zu seinem geheimen Schlüssel mehr hat, wird das bewährte Mail-Reply-Verfahren mit einem Einmal-Schlüssel Anwendung finden.

4.4 Schnittstelle zwischen PCA/CA und DSD

Zu klären ist, wie die Lieferung von Daten, sprich PGP-Schlüssel von der PCA/CA an DSD erfolgt und welches Format diese Daten haben sollen. Es herrschte Einigkeit darüber, daß die Grundlage hierfür das herkömmliche DSD-Datenlieferungsformat sein muß, das entsprechend erweitert wird. Wie groß in diesem Zusammenhang der zusätzliche Arbeitsaufwand für die einzelnen CAs sein wird, müssen praktische Erfahrungen zeigen.

Alle Datenlieferungen sollen von der PCA/CA signiert und verschlüsselt via FTP an DSD geschickt werden.

4.4.1 Umfang der Datenlieferung

Ebenfalls diskutiert wurde, welche Informationen von der CA an DSD (außer der KeyID des Schlüssels) geschickt werden. Von Vorteil für DSD wäre dabei sicherlich, wenn die CA aus dem Key die zusätzlichen Informationen (z.B. den DN oder andere Schlüsseldaten) extrahieren und diese mitschicken würde. Da verschiedenste Software-Versionen (sowohl für PGP als auch für X.509) auf dem Markt sind, wäre dies für DSD selbst zu aufwendig. Es wurde festgehalten, daß ein entsprechendes Tool von/für die CAs entwickelt und zur Verfügung gestellt werden sollte. Ob und wo für eine solche Entwicklung die notwendigen Ressourcen zur Verfügung stehen würden, muß allerdings derzeit noch unklar bleiben, wenn es auch vielversprechende Ansätze (z.B. an der Univ. Stuttgart) gibt.

Zusätzlich könnte ein externer LDAP-Server als Protokoll-Server eingesetzt werden.

4.4.2 Handhabung von CRLs

Die Policy der DFN-PCA verlangt, daß jede CA eine CRL pflegt und diese öffentlich zugänglich macht. Die Ablage dieser CRL sollte u.a. auch im ASCII-Format erfolgen, da das CRL-Handling von Browsern (und Servern) noch nicht vollständig funktioniert. Für DSD ist es ausreichend, einen Verweis auf die jeweilige X.509-CRL der einzelnen CAs anzubieten. Unter Umständen ist es ferner sinnvoll, von jeder einzelnen Seite einen Link auf die aktuelle CRL der DFN-PCA (als oberster CA) einzurichten. Ansonsten werden die CRLs von DSD nicht weiterverarbeitet.

Es wird deutlich festgestellt, daß es Aufgabe des einzelnen Benutzers ist, die Gültigkeit eines Zertifikats zu überprüfen.

Da PGP nicht X.509-konform ist, gibt es für PGP keine CRLs im eigentlichen Sinne. Bietet eine CA jedoch eine CRL für PGP-Schlüssel an, wird mit dieser analog zu X.509-CRLs verfahren.

4.4.3 Ablage von X.509-Zertifikaten

Im Gegensatz zu PGP-Schlüsseln, die in der Regel direkt von den Benutzern abgerufen werden, erfolgt der Zugriff auf X.509-Zertifikate üblicherweise durch Applikationen wie z.B. Web-Browser. Eine Ablage der X.509-Zertifikate sowohl in Binär- als auch in ASCII-Form ist daher wünschenswert.

Die Suche im Datenbestand nach den Zertifikaten sollte anhand des DNs erfolgen, der im Zertifikat steht. Dies erfordert, daß der DN und die Seriennummer des Zertifikats extrahiert und separat abgelegt werden.

In Zukunft sollen die X.509-Zertifikate dann auch über LDAP abfragbar gemacht werden.

5 Planung eines gemeinsamen Plenums-Vortrags im Rahmen der 31. Betriebstagung des DFN im Oktober 1999 in Berlin

Allgemeine Zustimmung fand der Vorschlag eines gemeinsamen Plenums-Vortrags bei der kommenden 31. BT des DFN-Vereins. Der gemeinsame Vortrag soll auch nach außen hin die enge Zusammenarbeit der beiden Projekte dokumentieren. Als Dauer wurden 45 Minuten angesetzt; Wunschtermin ist direkt nach der Kaffeepause.

Themen:

- Vorstellung der Projekte (kurz)

- Möglichkeiten der Beteiligung an den Projekten
- Vorführung / Demonstration
- Vorstellen der Schlüsselverwaltung (Datenlieferung, Datenformat, Tü-X.500-PGP-Schlüssel Modell, etc)
- Vorstellen der Policies
- Neuigkeiten bei SSL
- Neuigkeiten bei Browsern
- evtl. 15-minütige Demonstration (off-line)

6 Festlegung weiterer Schritte

Für die nähere Zukunft wurden nachfolgend aufgeführte Vorhaben beschlossen

- Terminabsprache mit dem DFN-Verein für die kommende DFN-BT
- DSD gründet eigene CA zur Zertifizierung der PGP-Schlüssel der DSD-Mitarbeiter (PGPv5.5.3i wurde von S. Kelm empfohlen, PGPv2.6.2i ist jedoch ebenfalls akzeptabel).
- DSD wird einen Beitrag zu dem von der PCA geplanten PCA/CA-Tutorium liefern. Thema: Veröffentlichung von Zertifikaten. Der Termin steht noch nicht genau fest, vermutlich Ende 1999 / Anfang 2000.
- Setzen von WWW-Verweisen auf die jeweilige Homepage des anderen Projektes
- DSD: Studium von SSL, SSL-Servern, etc.

Literatur

[BSI] http://www.bsi.de/aufgaben/projekte/pbdigsig/

[Pro96] Protokoll zum Treffen der DFN-Projekte DFN-PCA und AMBIX am 4. und 5.12. 1996

[Spa99] K. Spanier, Proceedingsbeitrag 6.CERT-Workshop: LDAP und die Ablage von PGP-Schlüsseln im X.500-Directory