Einsatz der Lotus Domino-PKI 6

Secorvo White Paper

Version 1.0
Stand 27. Mai 2003

Dr. Markus Michels, Dr. Dörte Neundorf

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-500
Fax +49 721 6105-455

E-Mail info@secorvo.de
Internet http://www.secorvo.de

Inhaltsübersicht

1 Zusammenfassung 4
2 PKIs in Lotus Notes – welche Funktionalitäten gibt es? 5
3 Verwaltung von X.509-Zertifikaten mit der Domino-PKI 6 7
3.1 Administration der CA 7
3.2 Registrierung und Verteilung der Zertifikate 7
3.3 Sperrung von Zertifikaten und Verteilung der Sperrlisten 10
3.4 Ablage von Zertifikate und Sperrlisten im Domino-Directory 10
3.5 Cross-Zertifizierung 11
3.6 Schlüssel- und Zertifikatsmanagement im Notes-Client 12
3.7 Nutzung von Smartcards im Notes-Client 12
3.8 Möglichkeiten zur Wiedergewinnung privater Nutzerschlüssel 13
3.9 Schlüssel- und Zertifikatsmanagement im Notes-Web-Server 13
4 PKI-Anwendungsszenarien mit Notes-Mitteln 15
4.1 S/MIME-gesicherte E-Mail-Kommunikation mit Dritten 15
4.2 SSL-gesicherte Web-Zugriffe 17
5 Integrationsszenarien mit anderen PKI-Komponenten 20
5.1 Nutzung einer Fremd-PKI mit dem Notes-Client 20
5.2 Nutzung der Domino-PKI mit Anwendungen anderer Hersteller 21
6 Anhang: Formate 23
6.1 Zertifikatsformate 23
6.2 Sperrlistenformat 24

Abkürzungen

CA	Certification Authority
CDP	CRL Distribution Point
CRL	Certificate Revocation List
DNS	Domain Name System
DSS	Digital Signature Standard
ICL	Issued Certificate List
ISIS	Industrial Signature Interoperability Specification
ISIS-MTT	ISIS und MTT
LDAP	Lightweight Directory Access Protocol
MTT	MailTrusT
MD	Message Digest
MIME	Multipurpose Internet Mail Extensions
PAB	Persönliches Adressbuch
PIN	Persönliche Identifikationsnummer
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastruktur
PKIX	Public-Key Infrastructure X.509
RA	Registration Authority
RSA	Rivest, Shamir, Adleman
SCEP	Simple Certificate Enrollment Protocol
SHA	Secure Hash Algorithm
S/MIME	Secure MIME
SSL	Secure Socket Layer
URL	Uniform Resource Locator
VPN	Virtual Private Network

Historie

Version	Datum	Änderung	Autoren
1.0	27.5.2003	Erstellung des White-Papers	Michels, Neundorf

1 Zusammenfassung

In Unternehmen und Behörden bilden häufig Public Key Infrastrukturen (PKI) die Basis bei dem Aufbau von Sicherheitslösungen wie etwa der gesicherten E-Mail-Kommunikation, dem sicheren Web-Server-Zugriff oder der Sicherung von Virtual Private Networks (VPN). Wird Lotus Notes / Domino eingesetzt, so stellt sich die Frage, ob und falls ja, wie die vorhandenen Funktionalitäten in Lotus Notes / Domino Infrastruktur verwendet werden können.

In diesem White Paper wird beleuchtet, wie Lotus Notes / Domino in der Version 6 zur Realisierung von Sicherheitslösungen auf der Basis von X.509-konformen Zertifikaten verwendet werden kann. Ausgangspunkt sind die zwei folgenden Fragen:

- Unter welchen Voraussetzungen und für welche PKI-Anwendung ist es sinnvoll, ausschließlich die in Lotus Notes / Domino 6 integrierten PKI-Funktionalitäten auf Basis von X.509 zu verwenden?
- Unter welchen Voraussetzungen und für welche PKI-Anwendung ist es sinnvoll, einige der in Lotus Notes / Domino 6 integrierten PKI-Funktionalitäten auf Basis von X.509 zu verwenden und die übrigen durch Drittprodukte zu ersetzen?

Kapitel 3 beschreibt die Abläufe und Funktionen innerhalb der Domino-PKI 6 und die aus PKI-Sicht relevanten Eigenschaften des Notes-Clients und anderer Notes-Komponenten.

Kapitel 4 untersucht, ob und unter welchen Bedingungen die Absicherung der E-Mail-Kommunikation mit Externen sowie SSL-Zugriffe auf Webserver mit Notes-Komponenten realisiert werden können. In diesem Szenario wird ausschließlich die bereits in Notes enthaltene Funktion genutzt.

Kapitel 5 schließlich diskutiert, wie die Notes-Komponenten mit PKI-Komponenten anderer Hersteller zusammenarbeiten und wo dabei Probleme auftreten können. Dabei wird sowohl untersucht, wie die Zertifikate der Domino 6 PKI in Notes-fremde Anwendungen integriert werden können als auch wie der Notes-Client Zertifikate anderen PKIs nutzen kann.

Alle geschilderten Ergebnisse beruhen auf im Secorvo-Labor durchgeführten Tests.

Dieses White Paper richtet sich an Projektleiter und Mitarbeiter in Unternehmen und Behörden, die am Aufbau einer firmeneigenen PKI beteiligt und die bereits mit Grundbegriffen und Abläufen einer PKI und mit den Grundlagen von Lotus Notes vertraut sind.

2 PKIs in Lotus Notes – welche Funktionalitäten gibt es?

Lotus Notes wird in vielen großen Unternehmen schon lange als Basis für Messaging und Workflow eingesetzt. Diese Infrastruktur bietet u.a. PKI-basierte Sicherheitsmechanismen für die Authentifikation zwischen Notes-Clients und Notes-Server sowie für die Sicherung von E-Mails zwischen Nutzern einer Lotus-Notes-Infrastruktur. Bis zur Version 4 waren diese Mechanismen allerdings proprietär, so dass z. B. eine gesicherte E-Mail-Kommunikation mit Nutzern anderer Systeme nicht möglich war. Abhilfe konnte zu dieser Zeit nur mit sogenannten Plug-Ins anderer Hersteller geschaffen werden, mit deren Hilfe die erforderlichen Funktionen ergänzt wurden. Mit der Version 5 wurden die ersten standardkonformen Sicherheits-Funktionalitäten angeboten, die auch eine gesicherte Kommunikation mit Externen ermöglichen sollten. Der Funktionsumfang war allerdings im Vergleich zu anderen Produkten noch recht eingeschränkt. Im Oktober 2002 hat IBM die Version 6 von Lotus Notes / Domino auf den Markt gebracht, die unter anderem im Bereich Public Key Infrastrukturen (PKI) eine ganze Reihe neuer Funktionen bietet. Viele Unternehmen, die bereits über eine ausgerollte Lotus-Notes-Infrastruktur verfügen, haben daher ein großes Interesse daran, diese Funktionalitäten für bestimmte PKI-basierte Anwendungen zu nutzen und damit den finanziellen und organisatorischen Aufwand zur Einführung neuer Systeme einzusparen.

Lotus Notes / Domino besteht aus dem Domino-Server und verschiedenen Clients. Der Domino-Server stellt verschiedene Dienste zur Verfügung, u.a. Verzeichnisdienste, Replikationsdienste, ein Messaging-System, Sicherheitsdienste und Web-Server-Dienste. Der Notes-Client stellt Messaging- und Kalender-Funktionalitäten zur Verfügung und kann auch als Internet-Browser verwendet werden.

Lotus Notes / Domino enthält zwei verschiedene Public Key Infrastrukturen (PKI), die Notes-PKI und die Domino-PKI.

Die **Notes-PKI** ist die Grundlage der Notes-internen Authentifizierungs- und Verschlüsselungsfunktionen. Es werden sogenannte *Notes-Certifier* als Certification Authority (CA) eingerichtet. Basisfunktionen wie die Registrierung von Nutzern, das Ausstellen von Zertifikaten, das Schreiben der Zertifikate in das Domino-Directory und die Cross-Zertifizierung werden angeboten. Auf Basis der Notes-internen Schlüssel und Zertifikate kann ein Nutzer mit dem Notes-Client die Verschlüsselung und Signatur von Notes-internen E-Mails und Datenbanken sowie die Authentifizierung zum Notes-Server durchführen. Die Zertifikate der Notes-PKI basieren auf Lotus-spezifischen (proprietären) Formaten, so dass diese Zertifikate nicht in Lotus-fremde Applikationen importiert oder von ihnen interpretiert werden können.

Mit der **Domino-PKI** können *Domino-CA*s als Zertifizierungsstellen eingerichtet werden. Diese können X.509-Zertifikate ausstellen (in Lotus-Sprache "Internet-Zertifikate“ genannt). Diese Zertifikate können sowohl vom Notes-Client als auch von anderen PKI-Clients (z. B. Browser, andere E-Mail-Clients, Web-Server) genutzt werden.

Die Domino-CA und der Notes-Certifier interagieren an einigen Stellen miteinander. So werden etwa die Notes-internen Schlüssel und Zertifikate sowie die von der Domino-PKI ausgegebenen Schlüssel und Zertifikate beim Nutzer in derselben Datei, der NotesID, gespeichert. Dadurch kann bei einem Verlust dieser NotesID für die Wiedergewinnung der Schlüssel und Zertifikate dieselbe Notes-Server-Funktion verwendet werden. Soll die Handhabung der Domino-CAs und der Notes-Certifier vereinheitlicht werden, können sie in demselben Prozess – dem sogenannten CA-Prozess – integriert werden.

Die folgende Abbildung gibt einen Überblick über den Aufbau.

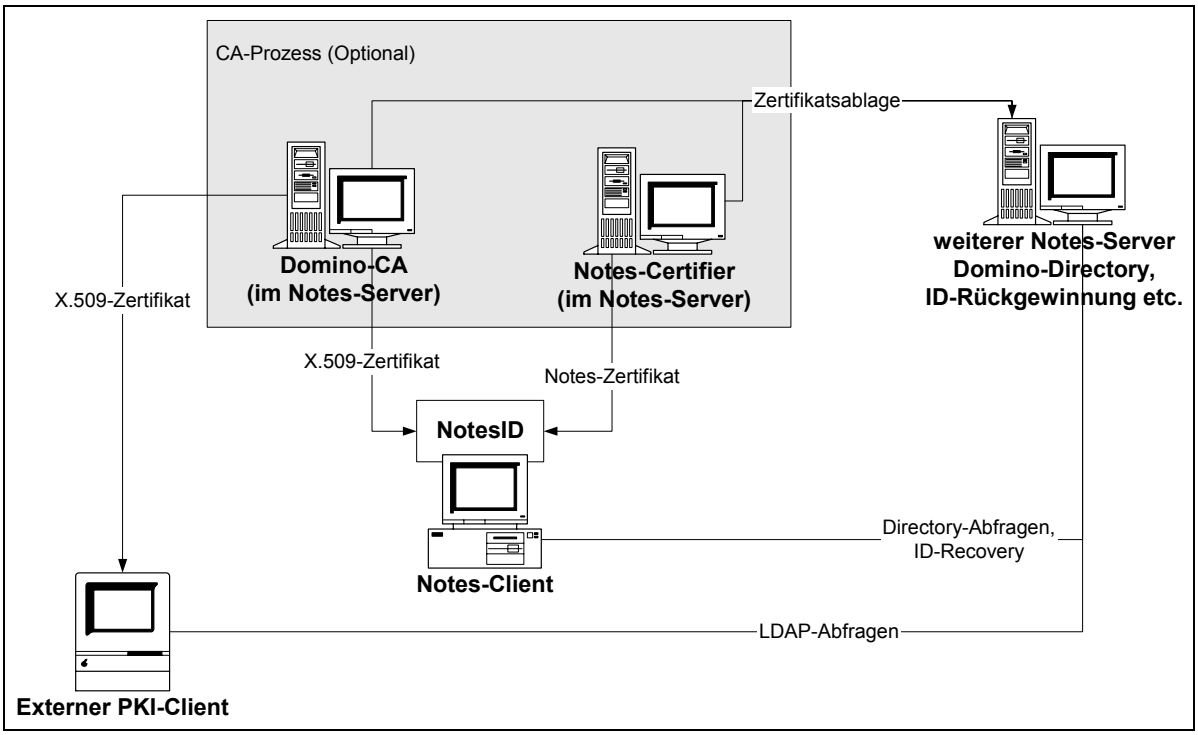

Abbildung 1: Aufbau und Kommunikation PKI-Elemente in Lotus Notes

3 Verwaltung von X.509-Zertifikaten mit der Domino-PKI 6

Dieses Kapitel gibt einen Überblick über die wesentlichen PKI-Funktionalitäten der Domino-PKI 6, um eine Bewertung der Eignung für bestimmte Anforderungsszenarien zu ermöglichen. Auf Basis dieser Funktionalitäten werden in Kapitel 4 und 5 verschiedene Anwendungsszenarien skizziert.

3.1 Administration der CA

Die Administration einer Domino-CA ist rollenbasiert. Die Domino-CA unterstützt zwei Rollen, den CA- und den RA-Administrator. Zusätzlich wird die Standard-Notes-Rolle „ID-Recovery-Administrator“ für die Schlüsselwiedergewinnung benötigt.

Der CA-Administrator hat die folgenden Aufgaben:

- Rollenverwaltung:
  Der CA-Administrator kann zu jeder Zeit in Notes registrierten Personen Rollen (CA- oder RA-Administrator) zuordnen. Weitere Rollen können nicht angelegt werden. (Insbesondere wird ein Vier-Augen-Prinzip technisch nicht unterstützt.)
- Festlegung des Inhalts des CA-Zertifikats (während der Initialisierung der CA):
  Dazu gehören der verwendete Signieralgorithmus, die Schlüssellänge, die Gültigkeit des Zertifikats sowie (optional) der alternative Name der CA.
- Konfiguration der Nutzerzertifikats- und Sperrlisten-Formate:
  Bei den Nutzerzertifikaten kann u.a. die Gültigkeitsdauer des Zertifikats sowie die Aufnahme einiger Erweiterungen eingestellt werden.[1] Für Sperrlisten kann jederzeit die Gültigkeitsdauer sowie die Häufigkeit der Neuausstellung (jeweils in Tagen) eingestellt werden.
- Konfiguration des Schutzes des CA-Schlüssels:
  Der CA-Schlüssel kann unverschlüsselt oder verschlüsselt in Software abgelegt werden. Hardware Security Module werden für die CA nicht unterstützt.

Der RA-Administrator ist für die Registrierung der Nutzer sowie die Sperrung von Zertifikaten verantwortlich. Innerhalb der vom CA-Administrator vorgegebenen Grenzen kann er zudem die Inhalte einzelner Zertifikate bestimmen.

3.2 Registrierung und Verteilung der Zertifikate

Es werden verschiedene Arten der Registrierung von Nutzern und Diensten (wie etwa Web-Servern) unterstützt:

- die Web-basierte Registrierung für Nutzer und Dienste,
- die zentrale Registrierung für Nutzer und
- ein zentraler Registrierungsprozess für den Notes-Web-Server.

---

[1] Dabei ist zu beachten, dass in der Default-Einstellung (in Abweichung zum Standard) für Key Usage das Flag DataEncipherment gesetzt ist, das Flag KeyEncipherment jedoch nicht. Es wird empfohlen, das Flag KeyEncipherment zu setzen. Nähere Informationen zu den Zertifikats- und Sperrlistenformaten sind im Anhang dargestellt.

Die Nutzer müssen sowohl für die Erstregistrierung als auch für die Erneuerung von Zertifikaten eine der Registrierungen durchlaufen, um neue Zertifikate zu erhalten. Es gibt keinen Mechanismus zur automatischen Erneuerung von Zertifikaten.

3.2.1 Web-Basierte Registrierung von Nutzern und Diensten

Bei der Web-basierten Registrierung gibt der Nutzer seine Daten in einem Web-Interface ein und sendet sie an die CA. Nach Zertifikatsausstellung erhält er eine E-Mail mit einem Link, über den er das Zertifikat beziehen kann. Für die Teilnahme an der Web-basierten Registrierung muss der Nutzer mit einem Notes-Client oder einem anderen Web-Browser ausgestattet sein. Die Web-basierte Registrierung läuft dann wie folgt ab:

1. Der Nutzer greift mittels eines Browsers auf eine Registrierungs-Webseite zu. Dort gibt er alle relevanten Daten und bei Beantragung eines Web-Server-Zertifikats auch den öffentlichen Schlüssel des Web-Servers ein. Bei Beantragung eines Nutzer-Zertifikats wird der private Schlüssel im Browser erzeugt; die relevanten Daten müssen für jeden Antrag erneut eingegeben werden.
2. In einem zwei-stufigen Prüfprozess kann der RA-Administrator den Antrag prüfen und ggf. die vom Nutzer eingetragenen Werte ändern. Dabei kann er konfigurieren, ob und ggf. in welches Domino-Directory das Zertifikat eingestellt werden soll, sofern für den Nutzer vorher ein Eintrag im Verzeichnis angelegt worden ist.[2]
3. Daraufhin wird das X.509-Zertifikat von der Domino-CA erstellt und in das Domino Directory geschrieben. Eventuell schon vorhandene X.509-Zertifikate werden nicht überschreiben.
4. Der Nutzer erhält per Mail eine URL und eine PIN. Durch Anklicken der URL oder Eingabe der PIN in ein Feld auf der Registrierungs-Web-Seite kann der Nutzer das Nutzerzertifikat automatisch in die NotesID (bei Verwendung des internen Notes-Browser im Notes-Client) oder in den Zertifikatsspeicher des Browsers (bei Verwendung eines externen Browsers) importieren.
   Dabei wird in diesem das Zertifikat in der NotesID nicht überschrieben; es ist also möglich, mehrere Zertifikate in der ID zu speichern

Die Identifizierung des Nutzers muss durch zusätzliche „out-of-band“-Maßnahmen erfolgen. Erfolgt der Zugriff mittels des Notes-Clients, kann etwa durch Beschränkung des Zugriffes auf die Registrierungs-Webseite ausgeschlossen werden, dass Unbefugte ein Zertifikat erhalten.

Dieses Verfahren unterstützt die lokale Schlüsselgenerierung beim Client und erlaubt das Ausstellen von mehreren Schlüsselpaaren für einen Nutzer. In der Praxis werden oft zwei Schlüsselpaare pro Nutzer verwendet, um Entschlüsselungs- und Signieroperationen mit getrennten Schlüsseln durchführen zu können. Die zu den Schlüsselpaaren gehörenden Zertifikate können gemeinsam im Directory-Nutzereintrag abgelegt werden.

Allerdings ist sowohl für den Nutzer als auch für die Administratoren durch die notwendigen manuellen Schritte im Vergleich zur im nächsten Abschnitt dargestellten zentralen Registrierung eher aufwändig. Eine Anbindung an ggf. vorhandene Daten der Nutzer ist nicht möglich; die Integration in vorhandene Notes-Prozesse ist gering.

---

[2] Für externe Benutzer muss daher vor der Zertifikatsausstellung ein Directory-Eintrag angelegt werden. Sinnvollerweise wird dies in den organisatorischen Ablauf der Akzeptanz des Antrags durch den Administrator integriert.

Insofern ist eine Nutzung dieses Verfahrens nur zur Registrierung einiger weniger Nutzer sinnvoll; sollen große Mengen von Zertifikaten ausgestellt werden, ist die Fehleranfälligkeit und der manuelle Aufwand meist zu hoch.

3.2.2 Zentrale Registrierung und Verteilung über das Notes-Login

Bei der zentralen Registrierung von Endbenutzern wird die Zertifikatsausstellung vom Notes-Administrator initiiert. Dieser gibt auch alle relevanten Daten ein. Die zentrale Registrierung baut auf der Notes-internen Registrierung auf. Voraussetzung für die Teilnahme an der zentralen Registrierung ist daher die vorherige Registrierung des Nutzers als Notes-Nutzer. Außerdem muss der Nutzer mit dem Notes-Client 6 ausgestattet sein. Die zentrale Registrierung läuft dann wie folgt ab:

1. Der CA-Administrator wählt aus der Liste der in Notes registrierten Personen diejenigen heraus, die ein Internet-Zertifikat erhalten sollen.
2. Für diese wird dann jeweils ein Zertifikat ausgestellt. Die CA stellt dabei das Zertifikat auf einen bereits in der NotesID vorhandenen und während der Generierung der NotesID erzeugten Schlüssel aus. Der Name im Zertifikat besteht aus dem Notes-Namen des Nutzers in X.500-Notation, ergänzt durch die E-Mail-Adresse.
3. Das Zertifikat wird in das Verzeichnis eingestellt; dabei wird ein bereits existierendes Zertifikat derselben CA überschrieben.
4. Meldet sich der Nutzer das nächste Mal beim Notes-Server an, so stellt der Notes-Server automatisch fest, dass in der zugehörigen NotesID des Nutzers das neu erstellte im Verzeichnis befindliche Zertifikat noch nicht vorhanden ist. Das Zertifikat wird an den Notes-Client gesendet und der NotesID automatisch hinzugefügt.

Da die zentrale Registrierung nur bereits in Notes registrierte Nutzer mit Internet-Zertifikaten ausstatten kann, ist eine erneute Identifikation der Nutzer nicht erforderlich. Dieses Registrierungsverfahren ist daher sowohl für den Nutzer und für die Administratoren sehr effizient. Eine Nutzung vorhandener Daten der Nutzer ist möglich.

Wird über die zentrale Registrierung ein zweites Internet-Zertifikat von derselben CA ausgestellt, so wird das vorhandene Zertifikat sowohl im Domino-Directory als auch in der NotesID des Nutzers überschrieben. Damit ist die Verwendung von getrennten Schlüsselpaaren (z. B. für Signierung, Entschlüsselung) von einer CA nicht möglich. Soll ein Nutzer mit mehr als einem Zertifikat ausgestattet werden, könnte eine weitere CA installiert und der Nutzer auch mit einem Zertifikat von dieser CA über die zentrale Registrierung ausgestattet werden. In diesem Falle wird dieses zusätzliche Zertifikat sowohl in der NotesID als auch im Domino-Directory zusätzlich zum bereits vorhandenen Zertifikat aufgenommen.

Alle Zertifikate für einen Nutzer sind bei Verwendung der zentralen Registrierung stets auf den gleichen in der NotesID vorhandenen Schlüssel ausgestellt. Dies ändert sich auch nicht, wenn die Notes-Schlüssel durch die in Notes integrierte Update-Funktionalität erneuert werden oder wenn das neue Zertifikat von einer anderen Domino-CA ausgestellt wird. Dies ist insbesondere dann problematisch, wenn ein Schlüsselwechsel – z. B. aufgrund einer Kompromittierung eines Schlüsselpaares – notwendig ist, da es das Sperren eines solchen Schlüssels faktisch unmöglich macht.

Eine Möglichkeit, neue Schlüssel zu erhalten, wäre die komplette Entfernung des Nutzers aus der Notes-Infrastruktur, um ihn dann erneut anzulegen. Mit einer neuen NotesID wird dann auch ein neuer Schlüssel erzeugt. Dies dürfte in der Realität allerdings nur selten praktikabel sein.

3.2.3 Registrierung des Notes-Web-Servers

Auf dem Domino-Server befindet sich ein Web-Server, der ein Web-Frontend für die Server-Funktionalitäten bereitstellt. Auch auf Notes-Datenbanken kann auf diese Weise grundsätzlich per Browser zugegriffen werden. Der Zugriff auf einzelne Web-Seiten kann beschränkt werden; insbesondere kann der Web-Server so konfiguriert werden, dass der Zugriff auf bestimmte Seiten nur über SSL erfolgen kann, wobei sich entweder nur der Web-Server oder auch der zugreifende Browser mit einem Zertifikat authentifizieren muss. Dafür besteht eine Notwendigkeit, den Web-Server mit Zertifikaten ausstatten zu können.

Für den Notes-internen Webserver können Zertifikate auf zwei verschiedene Arten ausgestellt werden.

- Ein Web-Server-Administrator generiert zunächst die Schlüssel für den Web-Server, die in einer passwortgeschützten Datei, dem sogenanntem Keyring (vgl. Kapitel 3.9), abgelegt werden. Dann erzeugt er einen Zertifikatsantrag. Über die Web-basierte Registrierung kann er mit Hilfe dieses Zertifikatsantrags ein X.509-Zertifikat für den Notes-Web-Server beantragen. Das ausgestellte Zertifikat und das Wurzelzertifikat der Domino-CA fügt er anschließend dem Keyring hinzu.
- Alternativ kann ein RA-Administrator den Keyring und den privaten Schlüssel erzeugen, ein Zertifikat ausstellen und den Keyring als Datei dem Web-Server-Administrator übergeben.

Um den Keyring zu nutzen, muss dieser in beiden Fällen (als Datei) so abgelegt werden, dass der Web-Server auf diesen zugreifen kann. Schließlich muss in der Web-Server-Konfiguration ein Verweis auf den Keyring gesetzt werden.

3.3 Sperrung von Zertifikaten und Verteilung der Sperrlisten

Der RA-Administrator kann Nutzer- und Server-Zertifikate sperren; die Angabe eines Sperrgrundes ist möglich.

Die Seriennummern der gesperrten Zertifikate sind Teil der Sperrliste (siehe Anhang), die von der Domino-CA regelmäßig entsprechend der Voreinstellungen neu erzeugt und in das Domino-Directory eingestellt wird. Von dort kann die Sperrliste von PKI-Clients zur Überprüfung von Zertifikaten geladen werden. Um zu gewährleisten, dass die Sperrung sofort Wirkung zeigt, kann der RA-Administrator auch Sperrlisten sofort in das Verzeichnis einstellen.

Der Notes-Client und der Web-Server verwenden die Sperrlisten allerdings nicht.

Ein gesperrtes Zertifikat wird sofort nach der Sperrung automatisch aus dem Directory gelöscht.

3.4 Ablage von Zertifikate und Sperrlisten im Domino-Directory

Die Domino-CA legt ihre eigenen Zertifikate und ihre Sperrlisten automatisch im Domino-Directory ab; die Konfiguration eines anderen Verzeichnisses ist nicht möglich. Für die Benutzer kann jeweils individuell ausgewählt werden, welches Directory verwendet wird. Für alle Notes-basierten Anwendungen erfolgt der Zugriff auch auf die X.509-Elemente mit Notes-Mitteln automatisch und problemlos.

Standardmäßig greifen PKI-Anwendungen anderer Hersteller per LDAP auf Directories zu. Durch Nutzung der vorhandenen LDAPv3-Schnitstelle des Domino-Directories ist ein solcher

Zugriff durch LDAP-Clients prinzipiell möglich. Die PKI-Informationen sind nach der folgenden im LDAP-Server sichtbaren Struktur abgelegt:[3]

- Benutzereinträge haben eine von `inetorgperson` abgeleitete strukturelle Objektklasse (`dominoPerson`); das Zertifikat liegt im Attribut `userCertificate`. Dies ist eine gängige Struktur, so dass keine Probleme zu erwarten sind. Sobald eine Internet-E-Mail-Adresse im Domino-Directory konfiguriert wird, ist diese über das LDAP-Attribut `mail` abzurufen. Auch dies ist ein übliches Vorgehen und erlaubt eine Suche nach gängigem Muster.
- CA-Entries haben die strukturelle Objektklasse `dominoInternetcertifier` mit der Hilfsklasse `certificationAuthority-V2`. Obwohl in dieser Hilfsklasse die Attribute `authorityRevocationList`, `certificateRevocationList` und `cACertificate` nach dem Standard X.521 (1997) für diese Hilfsklasse verpflichtend sind, sind sie im Eintrag der Domino-CA nicht alle belegt:
  - Die Sperrliste ist standardkonform im Attribut `certificateRevocationList` abgelegt.
  - Die Attribute `authorityRevocationList` und `cAcertificate` sind nicht vorhanden.

  Das CA-Zertifikat ist über `userCertificate` erreichbar und nicht über `cACertificate` wie im Standard X.509 (1997) gefordert. Insofern sind Probleme beim Download des CA-Zertifikats zu erwarten.

Das Domino-Directory unterstützt mehrere Einstiegspunkte. Insofern können mehrere Organisationen oder auch mehrere PKIs problemlos unterstützt werden. Auch Suchanfragen ohne Einstiegspunkt sind möglich.

Ein externer Schreibzugriff z. B. durch eine externe CA auf das Directory über LDAP ist möglich, wenn die Funktion aktiviert ist, und lief im Test problemlos. Allerdings muss die Rechtevergabe für den Schreibzugriff über die Access Control List (ACL) des Domino-Directories erfolgen; eine Konfiguration spezieller Zugriffsrechte per LDAP ist nicht vorgesehen. Somit ist eine Nutzung des Directories durch externe Anwendungen, die Daten oder Zertifikate ablegen, möglich.

Achtung: Im Test führten LDAP-Zugriffe von anderen PKI-Clients (z.B. verschiedene S/MIME Plug-Ins für Notes oder Outlook) auf die Sperrliste über den CRL Distribution Point (CDP) im Zertifikat zu einem Absturz des Domino Servers in den Versionen 6.0 und 6.01. Daher sollte der LDAP Service des Domino-Servers abgeschaltet werden, solange der Fehler nicht vom Hersteller behoben ist.

3.5 Cross-Zertifizierung

„Cross-Zertifizierung“ im klassischen Sinne – also die wechselseitige Zertifizierung von Zertifizierungsstellen – unterstützt die Domino CA nicht. Ebenso kann die Domino CA keine Zertifizierungsanfragen erzeugen oder von anderen Zertifizierungsausstellen für sich selbst ausgestellte Zertifikate importieren, mit denen eine Einbindung der Domino CA in eine übergeordnete PKI-Hierarchie außerhalb Lotus Notes möglich wäre.

---

[3] Das Schema des LDAP-Servers ist konfigurierbar; es wird hier die Standardkonfiguration beschrieben.

Die von Notes unterstützte „Cross-Zertifizierung“ ist abweichend von der normalerweise mit diesem Begriff bezeichneten Funktion: Ein Cross-Zertifikat ist ein vom Notes-Certifier oder vom Nutzer erstelltes Notes-Zertifikat, das ein anderes Zertifikat bestätigt und als vertrauenswürdig markiert. Dabei sind zur Verifizierung beide Zertifikate – das ursprüngliche und das Cross-Zertifikat – erforderlich. Es können Cross-Zertifikate auf Notes-Zertifikate und auf X.509-Zertifikate (CA-Zertifikate und Nutzer-Zertifikate) ausgestellt werden. Diese sind dann innerhalb einer Notes-Umgebung nutzbar.

Durch ein Cross-Zertifikat wird die Verwendung des cross-zertifizierten Zertifikates für den entsprechenden Geltungsbereich (lokal bei Cross-Zertifzierung durch den Benutzer, in der Domäne bei Cross-Zertifzierung durch den Notes-Certifier) zugelassen.

Eine Verwendung des Domino-CA-Zertifikats als vertrauenswürdiger Vertrauensanker im Notes-Client ist nur möglich, wenn ein Cross-Zertifikat für die Domino-CA vorliegt.

3.6 Schlüssel- und Zertifikatsmanagement im Notes-Client

Der Nutzer kann Schlüssel und Zertifikate im Notes-Client verwalten. Er kann eigene private Schlüssel und X.509-Zertifikate auf Basis des PKCS #12 Standards manuell importieren und (sofern sich der private Schlüssel nicht auf einer Smartcard befindet – siehe Kapitel 3.7) auch exportieren. Eigene X.509-Zertifikate können auf Basis üblicher Standard (PKCS #7, DER) exportiert werden. Fremde Zertifikate können auf Basis dieser Standards manuell in das Persönliche Adressbuch importiert werden. Sie können auch durch Zugriff auf das Domino-Directory oder auf konfigurierte LDAP-Directories dauerhaft oder temporär (für einmalige Verwendung) geladen werden. Damit sind alle für ein sinnvolles Zertifikatsmanagement erforderlichen Funktionen vorhanden.

Bei der Zertifikatsüberprüfung sucht der Notes-Client nach gültigen Zertifikatspfaden. Dabei muss eine Verbindung zum eigenen Notes-Certifier (über Cross-Zertifikate, siehe Kapitel 3.5) bestehen. Ist dies der Fall, können Benutzerzertifikate auch über mehrere Stufen erfolgreich überprüft werden (Da der Download der im Domino-Directory vorhandenen Cross-Zertifikate nicht automatisch erfolgt, ist ein gelegentliches Herunterladen aus dem Domino-Directory zu empfehlen). Alternativ kann der Benutzer selbst „Trust“ für Benutzerzertifikate und Zertifizierungsstellen setzen – durch Ausstellen eines Cross-Zertifikates. Eine Verwendung eines Zertifikates ohne „Trust“, d.h. ohne ein persönliches oder durch den Notes Certifier ausgestelltes Cross-Zertifikat - ist nicht möglich.

Eine Sperrlistenüberprüfung erfolgt bei der Zertifikatsprüfung nicht, und der Client überprüft auch nicht, ob das Zertifikat im Directory vorhanden ist. Somit besteht keine Möglichkeit, dem Notes-Client mitzuteilen, dass ein einmal ausgestelltes Zertifikat nicht mehr gültig ist.

3.7 Nutzung von Smartcards im Notes-Client

Smartcards werden vom Notes-Client mittels des PKCS #11–Standards (v2.01) unterstützt. Der Nutzer kann den Client so konfigurieren, dass die Smartcard zur Anmeldung in Notes erforderlich ist.

Der Nutzer gibt dann statt der Notes-PIN die Smartcard-PIN zur Authentifikation in den Notes-Client ein. Die NotesID muss allerdings nach wie vor als Datei vorhanden sein. Während einer Session muss sich die Karte im angeschlossenen Kartenleser befinden. Entfernt der Nutzer die Karte, so loggt sich der Notes-Client automatisch aus und erwartet eine erneute Authentifikation des Nutzers.

Die Smartcard kann zur Speicherung der den X.509-Zertifikaten zugrundeliegenden privaten Schlüsseln verwendet werden. Dazu kann der Nutzer – nach Erzeugung auf einem der geschilderten Wege – den zum Internet-Zertifikat zugehörigen privaten Schlüssel aus der NotesID auf die Karte auslagern. Die Signier- und Entschlüsselungsoperationen werden dann auf der Karte ausgeführt. Da sich die privaten Schlüssel nicht mehr in der NotesID befinden, ist ein Export des geheimen Schlüssels aus der NotesID dann nicht mehr möglich.

Die Sicherheit des Schlüssels wird durch Speicherung auf der Karte nur dann erhöht, wenn alle Kopien der ID, die vor dem Export erstellt wurden, sicher gelöscht werden.[4] Dies setzt in der Praxis mindestens voraus, dass der Export auf die Karte möglichst sofort nach der Erstellung der ID erfolgt. Sobald eine NotesID längere Zeit auf dem Benutzerrrechner gespeichert wurde, ist eine erhöhte Sicherheit durch Speicherung auf der Karte nicht mehr gegeben.

3.8 Möglichkeiten zur Wiedergewinnung privater Nutzerschlüssel

Notes bietet eine optionale Funktion zur Wiedergewinnung der NotesID und eines vergessenen Passworts an. Wird diese Funktion vom Notes-Administrator aktiviert, so wird die NotesID der Nutzer bei Erzeugung automatisch an zentraler Stelle abgelegt. Bei Änderungen (z. B. bei der Ausstellung eines X.509-Zertifikats mittels der zentralen Registrierung) wird die geänderte NotesID automatisch neu gespeichert. Bei Verlust der NotesID wird die letzte zentral gespeicherte Version an den Nutzer weitergeleitet (durch „out-of-band“-Maßnahmen).[5] Werden ihm von den ID-Recovery-Administratoren die Entsperr-Passwörter mitgeteilt, so ist er wieder in der Lage, sich in Notes anzumelden.

Verwendet der Nutzer eine Smartcard und kann sich aufgrund des Verlustes der Karte oder des Vergessens der Smartcard-PIN nicht einloggen, so kann der Nutzer ebenfalls auf den oben geschilderten Recovery-Prozess zurückgreifen. Der Nutzer bekommt von den Administratoren die letzte gespeicherte Version seiner ID (die auch die geheimen Schlüssel enthält) sowie die Entsperr-Passwörter ausgehändigt. Damit kann sich der Nutzer – allerdings ohne Smartcard-Unterstützung – wieder einloggen. Die Smartcard muss anschließend wieder lokal aktiviert werden.

Damit kann der in Notes übliche Recovery-Prozess ohne Änderungen auf die Wiedergewinnung von X.509-basierten Zertifikaten und dazugehörigen Schlüsseln ausgedehnt werden, sofern diese über die zentrale Registrierung ausgestellt wurden. Web-basiert ausgestellte Zertifikate und die dabei erzeugten privaten Schlüssel werden von dieser Recovery-Funktion nicht erfasst.

3.9 Schlüssel- und Zertifikatsmanagement im Notes-Web-Server

Auch der Notes-Web-Server kann ein von der Domino-CA ausgestelltes X-509-Zertifikat verwenden; er ist also ebenfalls ein „PKI-Client“.

Wie in Kapitel 3.2.3 ausgeführt, werden der private Schlüssel, das eigene Web-Server-Zertifikat, das eigene Wurzelzertifikat und ggf. andere Wurzelzertifikate kommerzieller PKI-

---

4 Soll ein Recovery möglich sein, ist die Sicherheit der zentralen Speicherung der NotesIDs entsprechend zu gewährleisten und eine dezentrale Speicherung zu vermeiden.

5 Eigene Tests und entsprechende Meldungen im Notes-6-Entwicklerforum weisen daraufhin, dass in der Domino/Notes 6.0 diese Funktion nur für solche Nutzer funktioniert, die explizit mittels des Notes-Certifiers und nicht mittels des CA-Prozesses in Notes registriert werden.

Betreiber in einem passwort-geschützten Keyring abgelegt. Bei Kenntnis des Passworts kann sich ein Web-Server-Administrator den Inhalt des Keyrings ansehen. Alle Wurzelzertifikate sind per Default als vertrauenswürdig markiert; die Vertrauenswürdigkeit kann vom Web-Server-Administrator geändert werden.

Es ist ferner möglich, Wurzelzertifikate zu löschen oder andere Wurzelzertifikate in den Keyring hinzuzufügen. Nutzer mit Zertifikaten von CAs mit vertrauenswürdigem Wurzelzertifikat können auf geschützte Web-Seiten des Web-Servers zugreifen. Daher sollte den im Keyring vorhandenen Wurzelzertifikaten, für die dies nicht erwünscht ist, das Vertrauen entzogen bzw. das Wurzelzertifikat gelöscht werden.

Es ist möglich, den Web-Server so zu konfigurieren, dass auf bestimmte Seiten auf Basis von SSL nur mit Client-Authentifikation zugegriffen werden kann. In diesem Falle prüft der Web-Server, ob das Client-Zertifikat von einer vertrauenswürdigen CA ausgestellt und im Domino-Directory (und ggf. in weiteren konfigurierten Verzeichnissen) vorhanden ist. Ist dies der Fall, wird der Benutzer zugelassen. Ist das Zertifikat nicht im Directory vorhanden, wird der Zugriff verweigert. Eine Prüfung gegen die von der Domino-CA ausgestellte Sperrliste erfolgt nicht.

4 PKI-Anwendungsszenarien mit Notes-Mitteln

Grundsätzlich ist die Nutzung der Domino-PKI und der von ihr ausgestellten Zertifikate aus allen Notes-basierten Anwendungen möglich, die auf die NotesID und die dort gespeicherten Zertifikate zugreifen können. Ggf. können zusätzlich auch andere Anwendungen durch Eigenentwicklungen und Anpassungen Zugriff auf die NotesID erhalten, so dass diese ebenfalls die von der Domino-PKI ausgestellten Zertifikate nutzen können.

Der Notes-Client kann ohne weitere Anpassungen X.509-Zertifikate zur E-Mail-Absicherung und für gesicherte Web-Verbindungen nutzen. Notes-Web-Server können Web-Verbindungen mit Zertifikaten sichern. Daher werden beiden Anwendungsszenarien „S/MIME-gesicherte E-Mail-Kommunikation mit Dritten“ und „SSL-gesicherte Web-Zugriffe“ hier näher untersucht.

4.1 S/MIME-gesicherte E-Mail-Kommunikation mit Dritten

Eines der häufigsten Einsatzgebiete von PKI ist die Absicherung von E-Mail, also das Verschlüsseln und Signieren von Nachrichten und Attachments.

Bei der Kommunikation innerhalb einer Notes-Infrastruktur können die zur Authentifizierung verwendeten Notes-internen Schlüssel ohne weitere Änderungen auch zur Verschlüsselung und Signatur von E-Mails verwendet werden. Anders sieht es jedoch aus, wenn der potentielle Empfänger nicht Mitglied der eigenen Notes-Infrastruktur ist:

- Verfügt er ebenfalls über eine Notes-Infrastruktur, ist es grundsätzlich möglich, die Notes-internen Sicherungsmechanismen weiter zu verwenden. Dies erfordert aber eine Reihe von manuellen Eingriffen der Administration und/oder des Benutzers und ist nur in Einzelfällen praktikabel, nicht aber, wenn eine große Zahl von Benutzern gesichert kommunizieren soll.
- Verwendet der Empfänger ein anderes E-Mail-Produkt (z. B. Microsoft Outlook), ist eine Interoperabilität mit den Notes-internen Sicherungsmechanismen in der Praxis nicht herzustellen.

Daher stellt sich die Frage, welches allgemein übliche und damit mit Dritten interoperable Protokoll zur Absicherung von E-Mails „nach extern“ verwendet werden kann. Sollen keine Fremdprodukte eingesetzt, sondern vorhandenen Notes-Funktionalitäten genutzt werden, ist dies am einfachsten mit S/MIME möglich.

S/MIME[6] wird von Lotus seit der Version 5 unterstützt, in der Version 6 sind eine Reihe von Funktionalitäten hinzugekommen. Die maximale Schlüssellänge ist 128 Bit symmetrisch und 1024 Bit asymmetrisch (im Vergleich zu 64 Bit symmetrisch und 630 Bit asymmetrisch bei der Verwendung der Notes-internen Verschlüsselung). Damit ist für die meisten Anwendungen eine ausreichende Schlüssellänge gewährleistet.

---

6 Secure MIME, eine Erweiterung des etablierten Mailstandards, der festlegt, wie signierte und verschlüsselte Daten in eine E-Mail "verpackt“ werden. Der geltende Standard ist S/MIME v3 (RFC 2630-2634).
Als Verschlüsselungs- und Signaturalgorithmus wird dort nahezu immer RSA verwendet, als Hash-Algorithmen sind SHA-1 und MD5 vorgesehen, als symmetrische Algorithmen kommen TripleDES (empfohlen) und RC-40 zum Einsatz.

Die S/MIME-Funktionalität selber – also die Möglichkeit, Inhalte zu verschlüsseln und oder zu signieren und im richtigen Format in die Nachricht zu codieren – ist im Client automatisch enthalten und erfordert keine weitere Installation. Zur Zertifikatsprüfung werden die in Kapitel 3.6 geschilderten Mechanismen genutzt (so ist u.a. keine Sperrlistenprüfung möglich). Auch auf der Mail-Server-Seite ist keine Installation zusätzlicher Software erforderlich; u.U. sind einige wenige Konfigurationen notwendig.

Zur Aktivierung der S/MIME-Funktionalität im Notes-Client muss ein X.509-Zertifikat in die NotesID importiert werden. Grundsätzlich ist ein manueller Import des X.509-Zertifikats möglich. Wird die Domino-PKI zur Ausstellung der X.509-Zertifikate verwendet, empfiehlt sich – aufgrund des geringeren manuellen Aufwands – die Verwendung der in 3.2 beschriebenen Prozesse[7], mit denen die erforderlichen Schlüssel und Zertifikate automatisch in die ID abgelegt werden.

Ein wesentlicher Punkt ist die **S/MIME-Interoperabilität** im praktischen Betrieb. Aufgrund der Notes-eigenen Formate und der deswegen erforderlichen MIME-Konvertierungen sind die notwendigen Einstellungen hier – auch bei der Verwendung von S/MIME-Plug-Ins – meist aufwändiger als bei MIME-basierten Systemen.

Tests gegen MS Outlook/Exchange und einige andere Produkte liefen an einem einfachen Testsystem jedoch problemlos. Für komplexere Mail-Server-Strukturen sind einige zusätzliche Aspekte zu beachten:

- Die PKCS-MIME-Typen müssen im Notes-Mail-Server eingetragen und freigeschaltet sein.
- Für interne Empfänger sollte das gewünschte Mail-Format „keine Präferenz“ oder „MIME“ sein, bei der Einstellung „Notes“ gibt es in einigen Fällen Schwierigkeiten.
- In der Praxis ist es möglich, dass beim Mailaustausch über S/MIME zusätzliche Probleme, z. B. aufgrund von automatisch angehängten Disclaimern oder der Firewallkonfiguration, entstehen können. Dies ist im Einzelfall zu prüfen (und unabhängig vom eingesetzten E-Mail-Produkt).

Neben der Interoperabilität des Austauschsformates spielt auch die Verfügbarkeit der **Zertifikate der externen Kommunikationspartner** in der Praxis eine wichtige Rolle.

Soll die Kommunikation mit Hilfe lokal gespeicherter Zertifikate erfolgen – z. B. weil das Directory des Kommunikationspartnern nicht öffentlich verfügbar ist oder weil häufiger Off-Line-Betrieb zu erwarten ist – kann der Import von externen Zertifikaten direkt aus einer S/MIME-signierten E-Mail in das Persönliche Adressbuch des Nutzers erfolgen.

Zusätzlich ist auch die Konfiguration weiterer LDAP-Directories im Notes-Client möglich; auch diese werden genauso wie das Domino-Directory automatisch nach den passenden Zertifikaten durchsucht.

Vor Verwendung eines Zertifikates prüft der Notes-Client, ob es vertrauenswürdig ist. Dazu versucht er, eine Verbindung („Zertifikatskette“) zu einem vertrauenswürdigen CA-Zertifikat herzustellen. Ist dies nicht der Fall, fordert er den Nutzer explizit zur Ausstellung eines Cross-Zertifikates zur Setzung des Vertrauens auf. Ohne eine erfolgreiche Verifikation kann das Zertifikat nicht verwendet werden.

---

7 Bei der Web-basierten Registrierung sollte der Notes-Browser verwendet werden, um den manuellen Aufwand für den Benutzer so klein wie möglich zu halten.

In der Praxis dürfte es sinnvoll sein, eine Cross-Zertifizierung durch den Benutzer nur in wenigen Einzelfällen zuzulassen[8] und möglichst für externe CAs zentral Cross-Zertifikate auszustellen.

Zusätzlich ist es erforderlich, auch die externen CA-Zertifikate selbst im Domino-Directory zur Verfügung zu stellen, da der Notes-Client diese – im Gegensatz zu Benutzerzertifikaten – nicht aus externen Verzeichnissen laden kann.

Damit lässt sich feststellen, dass eine S/MIME-Kommunikation mit Externen relativ problemlos möglich ist, sofern alle erforderlichen Zertifikate zur Prüfung vorhanden sind und Sperrlistenunterstützung nicht erforderlich ist.

Einschränkungen können sich ergeben durch die nicht vorhandene Sperrlistenunterstützung und die Schwierigkeiten, verschiedene Zertifikate einer CA für Signatur und Verschlüsselung zu verwenden (vgl. Kapitel 3.2.2). Außerdem findet der Notes-Client keine CA-Zertifikate in externen Directories, so dass diese im Domino-Directory bereitgestellt werden müssen.

Probleme entstehen dann, wenn eine Zertifikatsprüfung nur über Cross-Zertifikate möglich ist, da diese vom Notes-Client nicht zur Verifikation benutzt werden können.

Damit ist der Notes-Client zur S/MIME-Kommunikation in einer nahezu geschlossenen Umgebung mit eher niedrigen Sicherheitsanforderungen gut geeignet. Soll die Kommunikation mit einer Vielzahl von anderen Organisation erfolgen, ist erheblicher Zusatzaufwand für die Administration erforderlich, um für die Benutzer einen reibungslosen Ablauf zu gewährleisten. Ein hohes Sicherheitsniveau kann ohne die Unterstützung von Verfahren zur Sperrung von Zertifikaten nicht realistisch erreicht werden.

4.2 SSL-gesicherte Web-Zugriffe

Ein weiterer häufiger Einsatzbereich von X.509-Zertifikaten ist die Absicherung von Web-Verbindungen über SSL.

Im ersten Schritt wird dabei ein Web-Server mit einem Zertifikat ausgestattet. Baut dann ein Client eine SSL-Verbindung zum Web-Server auf, kann der Benutzer anhand des vorgelegten Zertifikats überprüfen, dass er mit dem richtigen Web-Server verbunden ist. Dabei muss der Name im Web-Server-Zertifikat mit dem DNS-Namen des Web-Servers übereinstimmen und der Browser des Benutzers der ausstellenden CA vertrauen. Außerdem werden die übertragenen Daten verschlüsselt und damit vor unbefugtem Mitlesen während der Übertragung geschützt.

Zusätzlich (und im SSL-Protokoll optional) kann sich auch der Client mittels eines Zertifikates im Rahmen des Verbindungsaufbaus authentifizieren.

Für Web-Server und Browser ist die Nutzung von Zertifikaten der Domino-PKI möglich, unabhängig davon, ob es sich um Notes-Komponenten oder Fremdprodukte handelt.

4.2.1 Web-Server-Authentifizierung

Soll nur der Webserver authentifiziert werden, sind zwei Dinge erforderlich:

- Der Web-Server muss über ein Zertifikat verfügen.

---

8 Da eine technische Deaktivierung der Cross-Zertifzierung im Client wegen zu großer Nebenwirkungen auf andere Notes-Funktionalitäten in den meisten Szenarien wenig Sinn macht, sind dazu organisatorische Maßnahmen erforderlich.

- Der Client muss dieses Zertifikat verifizieren können.

Die Registrierung von Web-Servern bei der Domino-PKI erfolgt über das in Kapitel 3.2.1 beschriebene Verfahren. Dabei ist die Registrierung von beliebigen Web-Servern möglich, nicht nur von Notes-Web-Servern. Für Notes-Web-Server kann alternativ der in Kapitel 3.2.3 beschriebene Weg verwendet werden.

Vor Nutzung der SSL-Funktion müssen alle betroffenen Browser das Zertifikat der ausstellenden CA importieren. Dazu gibt es verschiedene Wege:

- Besitzt der Client ein Zertifikat derselben PKI, ist das CA-Zertifikat bereits im Client vorhanden und meist automatisch als vertrauenswürdig markiert.
- Für Notes-Browser kann das CA-Zertifikat mittels Download des Zertifikats aus dem Domino-Directory importiert werden.
- Für andere Browser kann der Download über eine Webseite erfolgen. Hier ist auf eine ausreichende Überprüfung des Zertifikates vor der Vertrauenssetzung zu achten.
- Eine Verteilung außerhalb der eigenen Organisation – falls der Web-Server auch von Externen genutzt werden soll – ist dabei aufwändig (ganz unabhängig vom verwendeten PKI-Produkt), so dass in diesem Fall die Nutzung einer der bereits in den Browsern enthaltenen öffentlichen Zertifizierungsstellen erwogen werden sollte. (Auch der Notes-Browser verfügt über diese CAs.)

Der Notes-Browser prüft auch bei der Verifikation des Web-Server-Zertifikats keine Sperrlisten. Andere Browser können dies tun, wenn sie in der Lage sind, über den CDP die Sperrliste aus dem Notes-Directory abzurufen.

4.2.2 Client-Authentifikation

Soll zusätzlich auch eine Client-Authentifikation verwendet werden, sind zwei weitere Schritte notwendig:

- Die Clients müssen mit Zertifikaten ausgestattet werden.
- Die Web-Server müssen der Domino-CA vertrauen, die die Client-Zertifikate ausstellt.

Die Registrierung der Clients erfolgt – unabhängig vom Browser-Typ – wiederum über die in Kapitel 3.2 beschriebenen Registrierungsverfahren.

Wenn das Zertifikat der CA, die die Clients zertifiziert, nicht schon im Web-Server enthalten ist, muss es für einen erfolgreichen SSL-Verbindungsaufbau importiert und als vertrauenswürdig markiert werden. Dies erfolgt meist manuell, da es im Vergleich zur Anzahl der Clients nur wenige ausstellende CAs gibt und nur wenige Web-Server betroffen sind.

Der Notes-Web-Server prüft während der Zertifikatsprüfung zwar keine Sperrlisten; er prüft jedoch, ob das Client-Zertifikat im Notes-Directory vorhanden ist („aktive Sperrung“).Ist es nicht vorhanden, wird der Zugriff nicht erlaubt. Daher muss für jeden Nutzer für die Client-Authentifikation ein Directory-Eintrag angelegt werden, der das Zertifikat enthält.

4.2.3 Fazit

Die Domino CA kann aus technischer Sicht zur Ausstellung von Zertifikaten für Web-Server und/oder Web-Clients verwendet werden.

Zusammenfassend lässt sich feststellen, dass die Verwendung der Domino-PKI zur Ausstellung von Zertifikaten Web-Server problemlos möglich ist. Der Notes-Browser wertet keine

Sperrlisten aus, was abhängig von den vorliegenden Anforderungen eine Einschränkung bedeuten kann. Die Verteil- und Prüfproblematik der Zertifikate für externe Benutzer besteht auch hier, ist allerdings produktunabhängig und damit nicht Notes-spezifisch.

Notes-Client und Notes-Web-Server können dann sinnvoll für SSL-Verbindungen mit Client-Authentifizierung verwendet werden, wenn

- auf keiner Seite eine Sperrlistenprüfung erforderlich ist und
- wenn alle Client-Zertifikate in Directories für den Web-Server verfügbar sind.

In der Praxis dürfte dies in beiden Fällen bedeuten, dass eine Nutzung der Notes-Komponenten in einer geschlossenen Gruppe (z.B. in einem Unternehmen nur für interne Nutzung) bei nicht zu hohen Sicherheitsanforderungen sinnvoll ist. Ist die Umgebung heterogener oder die Sicherheitsanforderung höher, sollte die Nutzung anderer Komponenten erwogen werden.

5 Integrationsszenarien mit anderen PKI-Komponenten

Drittprodukte für Zertifizierungsstellen (CA) und PKI-Clients zeichnen sich gegenüber der Domino-PKI 6 z. T. durch erweiterte Fähigkeiten aus, z. B. hinsichtlich der Registrierung oder der Sperrlistenunterstützung beim PKI-Client. Anforderungen können dadurch möglicherweise besser erfüllt werden als bei ausschließlicher Nutzung der Domino-Funktionalität. Anderseits bietet die Domino-PKI eine gute Integration in Lotus-Notes-Abläufe, die wiederum in dieser Form nicht von allen Drittprodukten erreicht wird.

Neben den Alternativen, eine PKI-Lösung komplett auf Basis von Notes-internen Funktionalitäten oder komplett auf Basis von Drittanbieterprodukten zu realisieren, gibt es auch die Möglichkeit, Lotus Domino-PKI Funktionalitäten und von Drittanbieterprodukten zu kombinieren.

Hinsichtlich der Directory-Integration lässt sich dazu folgendes sagen:

- Die Nutzung des Domino-Directories durch eine externe PKI ist problemlos möglich. Konkret bedeutet dies, dass die externe CA – ausreichende Zugriffsrechte vorausgesetzt – ihre Informationen in das Domino-Directory schreiben kann. PKI-Clients können dies dann abrufen, sofern die externe CA ein passendes Schema verwendet.
- Die Nutzung eines externen Directories durch die Domino-PKI ist nicht direkt möglich; CA-Zertifikate und Sperrlisten werden immer in das Domino-Directory eingestellt. Eine Replikation in ein beliebiges LDAP-Directory mit der Hilfe von Skripten sollte jedoch unproblematisch sein; hierbei kann gleich die Korrektur des Schemas erfolgen, so dass externe PKI-Clients die Informationen dann korrekt abrufen können.

Für die weitere Integration von Lotus Domino Funktionalitäten mit PKI-Drittprodukten sind dann folgende Szenarien denkbar:

- Eine PKI eines Drittanbieters wird verwendet, um für Notes-Clients Zertifikate auszustellen. Dabei wird entweder das Domino-Directory oder ein externes Directory verwendet.
- Die Domino-PKI 6 wird verwendet, sie stellt jedoch Zertifikate für eine Anwendung eines Drittanbieters aus.

5.1 Nutzung einer Fremd-PKI mit dem Notes-Client

Die im Notes-Client vorhandenen PKI-Funktionalitäten (also das Zertifikatsmanagement, die S/MIME- und SSL-Funktionalitäten) können auch mit Zertifikaten einer Fremd-PKI genutzt werden. Ein solches Szenario ist insbesondere dann interessant, wenn in einer Organisation bereits eine PKI besteht (die z. B. über ein S/MIME-Plug-In für einen E-Mail-Client genutzt wird) und nun eine Migration auf den Notes-6-Client erfolgt.

Hinsichtlich der Anwendungsfunktionalität unterliegt man den in Kapitel 3.6 geschilderten Einschränkungen wie etwa der fehlenden Sperrlistenprüfung. Damit ist ein Einsatz nur bei eher niedrigen Sicherheitsanforderungen und einer „PKI-Landschaft“ ohne klassische Cross-Zertifikate sinnvoll.

Darüber hinaus sind die folgenden Integrationsfragen zu lösen:

- Wie kommen Schlüssel und Zertifikate in den Notes-Client?
- Ist die Nutzung eines externen Directories möglich?

Die für den Benutzer einfachste Registrierung ist auch hier Web-basiert. Allerdings ist dann sicherzustellen, dass die externe PKI eine webbasierte Registrierung mit dem Notes-Browser ermöglicht (In den meisten Fällen werden nur Netscape und Internet-Explorer von Fremd-PKIs unterstützt.). Ist eine solche Registrierung nicht möglich, ist ein Import über PKCS12-Dateien denkbar, allerdings in der Praxis recht aufwändig.

Eine Nutzung anderer Directories zum Auffinden von Nutzerzertifikaten ist möglich. Verwendet das externe Directory gängige Schemata, stehen die Chancen gut, dass der Notes-Client Nutzerzertifikate findet - sowohl bei manueller als auch bei automatischer Suche.

Für CA-Zertifikate sieht dies anders aus: Der Notes-Client sucht nicht automatisch; eine manuelle Suche findet zwar den passenden Entry, kann aber das Zertifikat nicht extrahieren. Diese Zertifikate müssen also manuell oder über den Umweg des Domino-Directories importiert werden.

Damit ergeben sich auch hieraus Einschränkungen bei inhomogenen und häufig wechselnden Kommunikationsbeziehungen; ist die Zertifikatslandschaft hingegen weitgehend statisch, können die fehlenden CA-Zertifikate manuell nachgepflegt werden.

5.2 Nutzung der Domino-PKI mit Anwendungen anderer Hersteller

Möchte man eine Domino-CA zur Ausstellung von Zertifikaten für Anwendungen nutzen, die nicht auf die NotesID und das Zertifikatsmanagement von Notes zugreifen können, stellen sich die folgenden Fragen:

- Wie kommt die Anwendung an die Schlüssel und Zertifikate?
- Welche Probleme sind bei der Nutzung des Domino-Directories durch die Anwendung zu erwarten?

Da die Anwendungen nicht auf die NotesID zugreifen können, ergeben sich die folgenden Möglichkeiten für die Registrierung:

- Kann die Anwendung kann auf den Zertifikatsspeicher eines Browsers zugreifen, so können die Zertifikate über die Web-basierte Registrierung ausgegeben werden.
- Verfügt der Nutzer über einen Notes-Client, können Schlüssel und Zertifikate zunächst mittels der zentralen oder der Web-basierten Registrierung in die NotesID des Nutzers geladen werden und daraus manuell im PKCS#12-Format exportiert werden. Die Schlüssel und Zertifikate können manuell in die Anwendung importiert werden, sofern die Anwendung das PKCS#12-Format für diesen Zweck unterstützt. Dieses Vorgehen ist allerdings sehr aufwändig und fehleranfällig und daher in der Praxis nicht für große Benutzerzahlen zu empfehlen.
- Andernfalls ist nach der Registrierung über einen Browser ein manueller Export (PKCS#12-Format) und ein Import in die Anwendung erforderlich. Wiederum muss die Anwendung das PKCS#12 Format für diesen Zweck unterstützen. Auch hier ist der manuelle Aufwand für die praktische Anwendung zu groß.

Andere Protokolle zur Registrierung – z. B. das Simple Certificate Enrollment Protocol (SCEP) für die Integration von Cisco VPN Produkten – werden nicht unterstützt.

Probleme können sich bei Verwendung des Domino-Directories aus der nicht-standardkonformen Ablage des CA-Zertifikats ergeben, die allerdings je nach Anwendung möglicher-

weise durch passende Konfiguration des LDAP-Searchfilters oder durch manuellen Import der CA-Zertifikate umgangen werden können.

Hinsichtlich der Nutzer-Zertifikate sind keine Probleme mit dem Verzeichnis zu erwarten. [9]

Zusammenfassend lässt sich damit feststellen, dass eine Nutzung der Domino-PKI 6 aus praktischen Gesichtspunkten nur mit Dritt-Anwendungen sinnvoll ist, die auf den Zertifikatsspeicher eines Standard-Internet-Browsers zugreifen können, über den direkte Registrierung bei der Domino-PKI möglich ist, da sonst der Registrierungsaufwand für die Nutzer unzumutbar ist. Außerdem ist in jedem Falle Zusatzaufwand für die Directory-Nachbearbeitung erforderlich.

9 Grundsätzlich ist von der Verwendung des LDAP-Servers abzuraten, solange der in Kapitel 3.4 beschriebene Fehler in Lotus Notes / Domino von IBM nicht behoben wurde.

6 Anhang: Formate

6.1 Zertifikatsformate

In der „Issued Certificate List - ICL[10]“ sind Formate für CA- und Nutzerzertifikate festgelegt. Es ist dort auch dargelegt, welche Einstellungen durch den CA-Administrator geändert werden können und welche nicht. Auf dieser Basis kann dann der CA-Administrator Zertifikatsformate definieren. Alle weiteren Ausführen gelten für das Standard ICL-Profil.

Für das CA-Zertifikat können während der Installation einige Einstellungen durch den CA-Administrator vorgenommen werden, insbesondere:

- der verwendete Algorithmus (RSA mit MD5, RSA mit SHA-1, DSS),
- die Schlüssellänge (1024 Bit oder 2048 Bit bei RSA und bei DSS) und
- alternative Namen der CA.

Das CA-Zertifikat ist X.509 v3 konform und enthält neben den Standardangaben (Versionsnummer, Seriennummer, Identifier des zur Erstellung des Zertifikats verwendeten Algorithmus, Name des Ausstellers, Gültigkeit, Name des Inhabers, der Public Key des Inhabers und der Identifier des zugehörigen Algorithmus) die folgenden Zertifikatserweiterungen:

- Die Basic Constraints Erweiterung mit Eintrag, dass dies ein CA-Zertifikat ist. Pfadlängen sind nicht enthalten. Die Erweiterung ist als „kritisch“ markiert.
- Die Key Usage Erweiterung mit gesetzten Flags DigitalSignature, CertificateSignature und CRLSignature. Die Erweiterung ist als „kritisch“ markiert.
- Optional die IssuerAltName Erweiterung. Die Erweiterung ist als „unkritisch“ markiert.

Andere Erweiterungen sind im CA Zertifikat nicht enthalten. Das Zertifikat ist weder konform zu den PKIX-Zertifikatsprofilen[11] (RFC 2459, 3280) noch zu ISIS-MTT[12], da die SubjectKeyIdentifier-Erweiterung im Zertifikat fehlt.

Das Nutzer-Zertifikat ist X.509 v3 konform und enthält neben den Standardangaben (wie beim CA Zertifikat) die folgenden Erweiterungen:

- Die issuerAltName Erweiterung, sofern sie auch im CA-Zertifikat vorhanden ist. Andernfalls fehlt diese Erweiterung. Die Erweiterung ist als „nicht-kritisch“ markiert.
- Optional die Key Usage Erweiterung mit den vom CA-Administrator festgelegten Flags. Die Erweiterung ist als „kritisch“ markiert.[13]

---

10 Erreichbar über den Konfigurations-Tab in der Server-Administration.

11 PKIX ist eine Arbeitsgruppe zur Entwicklung von Standards für X.509-basierte PKIs.

12 ISIS-MTT ist eine gemeinsame Spezifikation von TeleTrusT e.V. und der Arbeitsgruppe der signaturgesetzkonformen Trust Center (T7-Gruppe) für elektronische Signaturen, Verschlüsselung und Public-Key-Infrastrukturen. Die Spezifikation enthält auch Anforderungen an die Zertifikats- und Sperrlistenformate.

13 In der Default-Einstellung für Key Usage ist das Flag Data Encipherment gesetzt, aber Key Encipherment nicht. Dies führt zu Problemen bei der E-Mail-Verschlüsselung. Es wird empfohlen, das Flag Key Encipherment zu setzen.

- Optional die Extended Key Usage Erweiterung mit den vom CA-Administrator eingestellten Flags. Die Erweiterung ist als nicht-kritisch markiert.
- Optional den CRL Distribution Point. Der Eintrag des Distribution Point hat die Form `ldap://< Name des Servers>/<DN der CA>?certificateRevocationList`, wobei nur ein Eintrag möglich ist. Die Erweiterung ist als nicht-kritisch markiert.

Andere Erweiterungen sind im Nutzer-Zertifikat nicht enthalten. Das Zertifikat ist weder konform zu PKIX (RFC 2459, 3280) noch zu ISIS-MTT, da die AuthorityKeyIdentifier-Erweiterung im Zertifikat nicht enthalten ist.

Zu beachten ist, dass die E-Mail Adresse Teil des Inhabernamens (als EMAIL-Attribut als erstes Element des DN) und nicht in der (ohnehin nicht vorhandenen) SubjectAltName Erweiterung ist. Damit entspricht das Zertifikat nicht dem S/MIME-Standard. Bei den Tests mit Outlook führte dies nicht zu Problemen, Probleme mit anderen Clients sind aber nicht auszuschließen und ein Vorabtest in jedem Falle zu empfehlen.

Der Eintrag des CRL Distribution Point wird automatisch generiert. Es wird der Name des Notes-Servers eingetragen, auf dem die CA läuft. Läuft der LDAP-Server auf einem anderen Notes-Server, so kann dies zu Problemen führen.

6.2 Sperrlistenformat

Die ausgestellten Sperrlisten sind konform zum X.509v3 Standard. Sie enthalten die folgenden Angaben:

- die Versionsnummer
- den Algorithmen-Identifier
- Name des Ausstellers
- den Ausstellungszeitpunkt (thisUpdate)
- den nächste regulären Ausstellungszeitpunkt (nextUpdate)
- die Liste der gesperrten Zertifikate, wobei jedes gesperrte Zertifikat durch dessen Seriennummer und den Revozierungszeitpunkt ohne weitere optionale Erweiterungen repräsentiert wird

Erweiterungen (crlExtensions) sind in der Sperrliste nicht enthalten.

Die Sperrlisten sind nicht konform zu den PKIX-Zertifikatsprofilen (RFC 2459 oder RFC 3280), da in allen angegebenen Zeitpunkten die Zeit in UTCTime-Format mit Zeitdifferential angegeben wird. In PKIX darf in der Zeitangabe kein Zeitdifferential vorhanden sein. Die Sperrlisten sind daher auch nicht konform zu ISIS-MTT.

Zu erwähnen ist, dass der Distinguished Name des Ausstellers mit UTF8String angegeben wird, während der Subject Names des Ausstellers im zugehörigen CA-Zertifikat des Ausstellers das Format PrintableString verwendet wird. Während einer Zertifikatsprüfung wird u.a. geprüft, ob diese beiden Namen identisch sind. Schließt die Prüfung das Format der Kodierung mit ein, so würde die Prüfung fehlschlagen.