DuD
Datenschutz und Datensicherheit

Einsatz der Lotus Domino 6 PKI

Markus Michels, Dörte Neundorf

Lotus Notes ist in vielen großen Unternehmen die Basis für Messaging- und Workflow-Anwendungen. Der vorliegende Beitrag beleuchtet, wie Lotus Notes/Domino in der Version 6 zur Realisierung von Sicherheitslösungen auf der Basis von X.509-konformen Zertifikaten verwendet werden kann.[1]

Dr. Markus Michels

Security Consultant, Secorvo Security Consulting GmbH. Arbeitsschwerpunkt: PKI, Sicherheitskonzepte.

E-Mail: michels@secorvo.de

Dr. Dörte Neundorf

war Security Consultant bei Secorvo und ist jetzt bei der BMW AG tätig.

E-Mail: Doerte.Neundorf@bmw.de

1 Einleitung

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 bzw. wie die vorhandenen Funktionalitäten in der Lotus Notes / Domino Infrastruktur verwendet werden können. Der Beitrag 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 beiden 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 realisiert werden kann. 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-PKI in Notes-fremde Anwendungen integriert werden können, als auch, wie der Notes-Client Zertifikate anderer PKIs nutzen kann.

2 PKI-Funktionalität in Lotus Notes

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.

Lotus Notes / Domino enthält (ab Version 4.6) zwei verschiedene Public Key Infrastrukturen, 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-CAs als Zertifizierungsstellen eingerichtet werden.
  Diese können X.509-Zertifikate ausstellen, die auch als „Internet-Zertifikate“ bezeichnet werden, um sie von Zertifikaten der Notes-PKI zu unterscheiden. X.509-Zertifikate können sowohl vom Notes-Client als auch von anderen PKI-Clients (z. B. Browser, andere E-Mail-Clients, Web-Server) genutzt werden.

[1] Der Beitrag ist eine gekürzte und überarbeitete Version von [MiNe03].

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 einem Prozess – dem sogenannten CA-Prozess – integriert werden. Abbildung 1 gibt einen Überblick über den Aufbau.

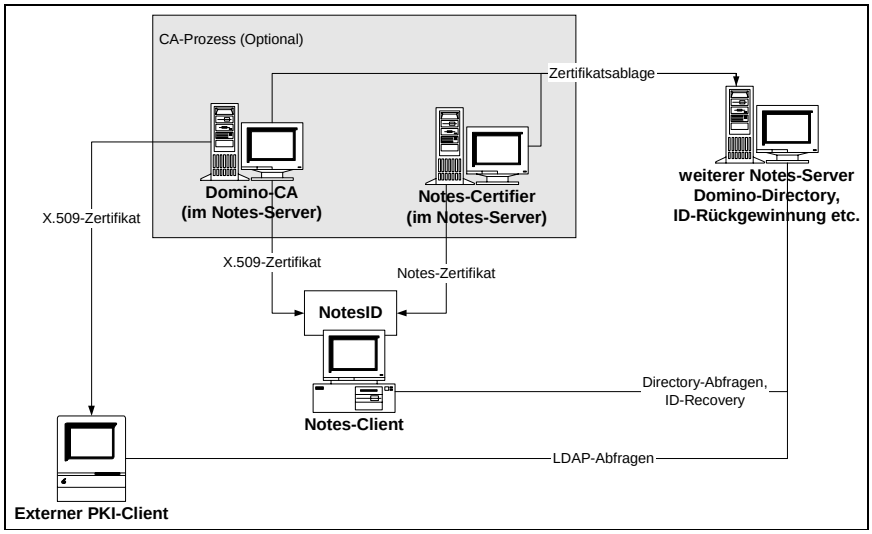

Abbildung 1: Aufbau und Kommunikation PKI-Elemente in Lotus Notes

3 Domino-PKI 6

Im Folgenden geben wir einen Überblick über die wesentlichen PKI-Funktionalitäten der Domino-PKI 6, um eine Bewertung der Eignung für bestimmte Anwendungsszenarien zu ermöglichen.

3.1 Registrierung und Verteilung der Zertifikate

Durch die Domino-PKI werden verschiedene Arten der Registrierung von Nutzern und Diensten (wie etwa Web-Servern) unterstützt:

- die Web-basierte Registrierung für Nutzer und Dienste und
- die zentrale Registrierung für Nutzer.

Die Nutzer müssen sowohl für die Erstregistrierung als auch für die Erneuerung von Zertifikaten eine der beiden Registrierungen verwenden. Es gibt keinen Mechanismus zur automatischen Erneuerung von Zertifikaten. Darüber hinaus gibt es einen zentralen Registrierungsprozess für den auf dem Domino-Server befindlichen Notes-Web-Server.

Web-basierte Registrierung von Nutzern und Diensten

Bei der Web-basierten Registrierung greift der Nutzer mittels eines Browsers auf eine Registrierungs-Webseite zu. Dort gibt er alle relevanten Daten ein (bei Beantragung eines Web-Server-Zertifikats auch den öffentlichen Schlüssel des Web-Servers). Bei Beantragung eines Nutzer-Zertifikats wird der private Schlüssel im Browser erzeugt; die relevanten Daten müssen für jeden Antrag erneut eingegeben werden.

Der RA-Administrator kann 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 ein Eintrag im Verzeichnis vorhanden ist.

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 überschrieben.

Der Nutzer erhält per Mail eine URL und eine PIN. Durch Anklicken der URL oder Eingabe der PIN in ein Feld auf der Registrierungs-Webseite 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 das Zertifikat in der NotesID nicht überschrieben; es ist also möglich, mehrere Zertifikate in der ID zu speichern.

Die Authentifikation 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.

Die web-basierte Registrierung unterstützt die lokale Schlüsselgenerierung beim Client und erlaubt die Verwendung 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 dieses Vorgehen 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.

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

Zentrale Registrierung und Verteilung über das Notes-Login

Voraussetzung für die zentrale Registrierung ist, dass der Nutzer mit dem Notes-Client 6 ausgestattet ist. Die zentrale Registrierung baut auf der Notes-internen Registrierung auf. Bei der zentralen Registrierung von Endbenutzern wird die Zertifikatsausstellung vom Notes-Administrator initiiert, in dem in der Liste der in Notes registrierten Personen diejenigen markiert werden, die ein Internet-Zertifikat erhalten sollen.

Für diese wird dann 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. Das Zertifikat

wird in das Verzeichnis eingestellt; dabei wird ein bereits existierendes Zertifikat derselben CA überschrieben.

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. Daher ist die Verwendung von getrennten Schlüsselpaaren (z. B. für Signierung, Entschlüsselung) mit Zertifikaten von einer CA nicht möglich.

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 Schlüssel-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.

Neue Schlüssel könnten durch die komplette Neuregistrierung des Nutzers in Lotus Notes erhalten werden. Dies dürfte in der Realität allerdings nur selten praktikabel sein.

3.2 Ablage von Zertifikaten und Sperrlisten

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-PKI-Informationen 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 externe LDAP-Clients prinzipiell möglich.

Benutzereinträge und Sperrlisten sind (aus LDAP-Sicht) standardkonform abgelegt; CA-Entries jedoch nicht: Das CA-Zertifikat ist über userCertificate erreichbar und nicht über cACertificate wie im Standard X.509 gefordert. Insofern sind Probleme beim Download des CA-Zertifikats zu erwarten.

Ein externer Schreibzugriff z. B. durch eine externe CA auf das Directory über LDAP ist möglich. 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.[2]

3.3 Cross-Zertifizierung

„Cross-Zertifizierung“ im klassischen Sinne – also die wechselseitige Zertifizierung von Zertifizierungsstellen[3] – 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.

Die von Notes unterstützte „Cross-Zertifizierung“ weicht von der normalerweise mit diesem Begriff bezeichneten Funktion ab: 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 zu Notes-Zertifikaten und zu X.509-Zertifikaten (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-Zertifizierung durch den Benutzer, in der Domäne bei Cross-Zertifizierung 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.

3.4 Schlüssel- und Zertifikatsmanagement im 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) auch exportieren. Eigene X.509-Zertifikate können auf Basis üblicher Standards (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 oben) 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“,

[2] 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 6.0.1. In entsprechenden Tests mit der Version 6.0.2 trat der Fehler nicht mehr auf.

[3] Zum Begriff des Cross-Zertifikats siehe Fox, Gateway, DuD 2/2001, S. 105, sowie ausführlicher Hammer, *Cross-Zertifikate verbinden*, DuD 2/2001, S. 65-70.

d. h. ohne ein persönliches oder durch den Notes Certifier ausgestelltes Cross-Zertifikat, ist nicht möglich.

Eine Sperrlistenüberprüfung erfolgt bei der Zertifikatsprüfung nicht. 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.

3.5 Weitere Funktionen

- **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 ist für die Rollenverwaltung, Festlegung des Inhalts des CA-Zertifikats und die Konfiguration der Nutzerzertifikats- und Sperrlisten-Formate verantwortlich.
- **Sperrung von Zertifikaten und Verteilung der Sperrlisten**: Der RA-Administrator kann Nutzer- und Server-Zertifikate sperren; die Angabe eines Sperrgrundes ist möglich.
  Ein gesperrtes Zertifikat wird sofort nach der Sperrung automatisch aus dem Directory gelöscht und in die Sperrliste eingetragen, die im Notes Directory veröffentlicht wird. Der Notes-Client und der Notes Web-Server verwenden die Sperrlisten allerdings nicht.
- **Unterstützung von Smartcards**: Eine Smartcard kann sowohl für die Authentifikation in den Notes-Client als auch zur Speicherung der den X.509-Zertifikaten zugrundeliegenden privaten Schlüsseln verwendet werden.
  Dazu kann der Nutzer den zum Internet-Zertifikat gehörigen privaten Schlüssel aus der NotesID auf die Karte auslagern. Die Signier- und Entschlüsselungsoperationen werden dann auf der Karte ausgeführt.
- **Wiedergewinnung privater Nutzerschlüssel**: Notes bietet eine optionale Funktion zur Wiedergewinnung der NotesID und eines vergessenen Passworts.
  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). Werden ihm von den ID-Recovery-Administratoren die Entsperr-Passwörter mitgeteilt, so ist er wieder in der Lage, sich in Notes anzumelden.

4 PKI-Anwendungsszenarien

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.

Notes-Web-Server können Web-Verbindungen mit Zertifikaten sichern. Die Verwendung der Domino-PKI zur Ausstellung von Web-Server-Zertifikaten ist problemlos möglich. Der Notes-Browser wertet bei der Überprüfung eines Web-Server-Zertifikats allerdings keine Sperrlisten aus. Dies kann abhängig von den vorliegenden Anforderungen eine Einschränkung bedeuten. Notes-Clients können durch die Domino-PKI mit Zertifikaten für SSL-Verbindungen mit Client-Authentifizierung (Web-Zertifikate für Clients) ausgestattet werden. Bei der Überprüfung des Client-Zertifikats nutzt der Notes Web-Server allerdings keine Sperrlisten, sondern akzeptiert das Client-Zertifikat nur dann, wenn es in für den Web-Server verfügbaren Directories vorhanden ist.

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. Für die Kommunikation mit Externen, die nicht Teil der Notes-Infrastruktur sind oder ein anderes E-Mail-Produkt (z. B. Microsoft Outlook) verwenden, ist dies jedoch nicht möglich.

Sollen keine Fremdprodukte eingesetzt, sondern vorhandene Notes-Funktionalitäten genutzt werden, ist die Kommunikation mit Externen am einfachsten auf der Basis von S/MIME möglich. S/MIME wird von Lotus ab der Version 5 unterstützt. Die maximale Schlüssellänge beträgt 128 bit (symmetrisch) und 1024 bit (asymmetrisch). Damit ist für die meisten Anwendungen eine ausreichende Schlüssellänge gewährleistet. Die Domino-PKI unterstützt die Ausgabe von Zertifkaten zur sicheren E-Mail-Kommunikation auf der Basis von S/MIME.

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 oben 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 3.1 beschriebenen Prozesse, mit denen die erforderlichen Schlüssel und Zertifikate automatisch in der NotesID abgelegt werden.

Ein wesentlicher Punkt im praktischen Betrieb ist die S/MIME-Interoperabilität. 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 mit MS Outlook/Exchange und einigen anderen Produkten liefen an einem einfachen Testsystem jedoch problemlos. Für komplexere Mail-Server-Strukturen sind zusätzliche Aspekte zu beachten:

- Die PKCS-MIME-Typen müssen im Notes-Mail-Server eingetragen und freigeschaltet sein.
- Für interne Empfänger sollte das in Notes konfiguierte 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 unabhängig vom eingesetzten E-

Mail-Produkt und im Einzelfall zu prüfen.

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 Zertifikats 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.

In der Praxis dürfte es allerdings sinnvoll sein, eine Cross-Zertifizierung durch den Benutzer nur in wenigen Einzelfällen zuzulassen 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.

Zusammenfassend 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 durch die nicht vorhandene Sperrlistenunterstützung und die Schwierigkeiten, verschiedene Zertifikate derselben CA für Signatur und Verschlüsselung zu verwenden ergeben. 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 „echte“ 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.

5 Integration externer 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 Drittanbieterprodukte zu kombinieren. Eine Möglichkeit ist die Directory-Nutzung:

- 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 diese 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 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 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 eingesetzt.
- 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 Client 6 erfolgt.

Hinsichtlich der Anwendungsfunktionalität unterliegt man den oben 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 web-basierte Registrierung mit dem Notes-Browser ermöglicht.[4] Ist eine solche Registrierung nicht möglich, ist ein Import über PKCS #12-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

[4] In den meisten Fällen werden nur Netscape und Internet-Explorer von Fremd-PKIs unterstützt.

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.

5.2 Nutzung der Domino-PKI mit Anwendungen anderer Hersteller

Soll eine Domino-CA zur Ausstellung von Zertifikaten für Anwendungen genutzt werden, 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 auf den Zertifikatsspeicher eines Browsers zugreifen, so können die Zertifikate über die Web-basierte Registrierung ausgegeben werden.

  Eine zentrale Wiedergewinnung von Schlüsseln ist jedoch praktisch nicht möglich, da dieser Mechanismus die NotesID voraussetzt.
- 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.

Probleme können sich bei Verwendung des Domino-Directories aus der nicht-Standard-konformen Ablage des CA-Zertifikats ergeben, die allerdings je nach Anwendung möglicherweise 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.

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.

Literatur

[MINe03] M. Michels, D. Neundorf, *Einsatz der Lotus Domino-PKI 6*, Secorvo White Paper, Version 1.0, 23.05.2003, http://www.secorvo.de/whitepapers/, 24 Seiten.