BADEN-
WÜRTTEMBERG

Verschlüsselung zur Sicherung des WWW- und Email-Dienstes im Intranet-Verbund öffentlicher Verwaltungen

Abschlußbericht

Forschungsinstitut für anwendungsorientierte
Wissensverarbeitung, Ulm

Dezember 1997

Erstellt im Auftrag des Landes Baden-Württemberg
vertreten durch die
Stabsstelle für Verwaltungsreform im Innenministerium

FAW Ulm

INNEN-
MINISTERIUM

Titel	Verschlüsselung zur Sicherung des WWW- und Email-Dienstes im Intranet-Verbund öffentlicher Verwaltungen
Herausgeber	Forschungsinstitut für anwendungsorientierte Wissensverarbeitung (FAW)
Erstellt durch	*Dr. W.-F. Riekert (Bereichsleiter Umweltinformationssysteme)* *Ahmet Arslan (Projektleiter), Sören Schilling* Forschungsinstitut für anwendungsorientierte Wissensverarbeitung (FAW), Helmholtzstraße 16 89081 Ulm Internet-Mail: arslan@faw.uni-ulm.de *Peer Wichmann* Europäisches Institut für Systemtechnik (E.I.S.S.) an der Universität Karlsruhe Internet-Mail: wichmann@ira.uka.de
Auftraggeber	Land Baden-Württemberg vertreten durch die Stabsstelle für Verwaltungsreform im Innenministerium Dipl.-Math. G. Schäfer, Internet-Mail: Schaefer@sik.im.bwl.de
Hinweise	Die Bewertung und Beschreibung der genannten Techniken und Produkte erfolgt nach sorgfältiger Analyse und ohne Nennung von Handels- und Urheberrechten. Dennoch können sich bei der Komplexität der behandelten Materie Fehler eingeschlichen haben. Der Verfasser, das FAW (Auftragnehmer) und das Innenministerium Baden-Württemberg (Auftraggeber) können deshalb keine Gewähr für die Richtigkeit aller gemachten Aussagen übernehmen.
Copyright © 1997	

Zusammenfassung

Die öffentliche Verwaltung nutzt zunehmend die Internet-Technik im Rahmen eines Zusammenschlusses ihres Intranets, weil diese Technik die Autonomie der Kommunikationspartner wahrt, zuverlässig und kostengünstig ist. Problematisch war bislang das Fehlen einer flexiblen, zuverlässigen und auch bei Massenbetrieb praktikablen und billigen Sicherheitstechnik, die auf der Basis von Verschlüsselung

- Identifikation und Authentifikation gewährleistet,

- WWW-Zugriffe differenziert zuläßt und Inhalte beim Transport verschlüsselt,

- Email verschlüsselt und soweit sinnvoll digital signiert.

Dieses Sicherheitsproblem ist jetzt gelöst und die Lösung ist nachfolgend beschrieben.

Die WWW-Technologie bietet eine bequeme Möglichkeit Dokumente und ähnliches für viele Nutzer verfügbar zu machen. Allerdings existieren Dokumente bzw. Informationen, die nicht jedem sondern nur einer bestimmten Personengruppe verfügbar gemacht werden sollen. Beispielsweise dürfen EU-Ratspapiere nicht für jedermann zugänglich sein. Nur ein bestimmter Personenkreis darf auf diese Informationen zugreifen. Somit muß über entsprechende Mechanismen gewährleistet sein, daß der Nutzer beim Zugriff auf solche Dokumente sich sicher identifiziert und in Abhängigkeit von dieser Authentifizierung ein Zugriff gestattet bzw. verweigert wird. So wie sich der Server von der Authentizität des Nutzers überzeugt, muß auch der Nutzer den Server authentifizieren können, damit er die Gewißheit hat, daß die Dokumente bzw. Informationen tatsächlich vom gewünschten Anbieter abgerufen werden und nicht gefälschte Dokumente von jemand anders.

Zur Absicherung entsprechender Server wurde bisher der Basic-Authentification-Mechanismus verwendet. Hierbei wird der Zugriff auf Ressourcen durch eine einfache Paßwort-Abfrage geschützt. Dieser Mechanismus bietet keine große Sicherheit, da die Paßwörter unverschlüsselt über das Netz übertragen und abgehört werden können. Weiterhin werden die Nutzer im Intra- bzw. Internet mit einer Vielzahl von Paßwörtern konfrontiert, was zur Verwendung von einfachen bzw. identischen Paßwörtern, für viele verschiedene Server, führt.

Durch eine einmalige Anmeldung des Nutzers mit einem einzigen sicheren Paßwort, womit der Zugriff auf alle Ressourcen, die eine Authentifikation erfordern, ermöglicht wird, läßt sich dieses Problem lösen. Diese Technologie wird als Einzelanmeldung bzw. single-sign-on bezeichnet. Die Verwirklichung dieser Einzelanmeldung basiert auf der Verwendung von Zertifikaten, womit sich die Nutzer gegenüber Servern authentifizieren. Das Single-sign-on-Prinzip impliziert die Verwendung von SSL (Secure Socket Layer), womit die verschlüsselte Übertragung aller Informationen vom Nutzer zum Server und zurück sichergestellt wird. Mit SSL wird die Authentizität (Identität des Kommunikationspartners), Integrität (Unverfälschtheit der Daten) sowie Vertraulichkeit (Unzugänglichkeit der Daten für Dritte) sichergestellt.

Ein Weiterer Vorteil des Single-sign-on-Prinzips ist die Verwendbarkeit der existierenden Zertifikate für die Sicherung des Email-Dienstes. Nutzer können

verfaßte Nachrichten mit Hilfe des öffentlichen Schlüssels des Empfänger verschlüsseln und damit die Möglichkeit der Manipulation der Nachricht verhindern. Zusätzlich kann die Identität des Absenders über eine Signatur (Fingerabdruck), die an die Email angehängt wird, sichergestellt werden. Dies geschieht durch Bilden einer Quersumme (Hashing) der zu übermittelnden Nachricht. Diese Quersumme wird mit dem privaten Schlüssel des Absenders verschlüsselt und an die Email angehängt. Nun ist es dem Empfänger möglich, diese Signatur über den öffentlichen Schlüssel des Absenders zu entschlüsseln, ebenfalls eine Quersumme über die empfangene Nachricht zu bilden, und die Gleichheit dieser beiden Quersummen zu überprüfen. Somit werden Vertraulichkeit, Integrität und Authentizität der Nachricht sichergestellt.

Die Generierung bzw. Nutzung eines Zertifikats ist relativ einfach. Hierzu muß der Nutzer mit Hilfe seines Browsers ein Schlüsselpaar (öffentlich, privat) generieren. Der private Schlüssel wird in eine lokalen Datenbank des Browser abgelegt und über ein Paßwort geschützt. Der öffentliche Teil wird einer Zertifizierungsinstanz (Trust Center) übermittelt, die die Identität des Nutzers übermittelt und gegebenenfalls den öffentlichen Schlüssel signiert. Der signierte öffentlichen Schlüssel (Zertifikat) kann nun bei folgenden Verbindungen mit Servern, die eine Authentifikation des Nutzers über Zertifikate erfordern, verwendet werden. Der Nutzer muß vor der Übermittlung seines Zertifikats das Paßwort der Datenbank für die privaten Schlüssel eingeben und kann sich somit über ein Paßwort auf beliebig vielen Servern authentifizieren.

WWW-Server, die Client-Authentifizierung ermöglichen gestatten die Zuordnung von Zertifikaten auf entsprechende Dateistrukturen bis hin zu einzelnen Dateien (Certificate-Mapping), um notwendige Zugriffsbeschränkungen festzulegen. Somit lassen sich auch über Zertifikate sehr fein granulierte Zugriffsbeschränkungen definieren.

Innerhalb dieses Projektes wurden verschiedene Softwarepakete, die die Verwaltung und Erstellung von Zertifikaten unterstützen, evaluiert und jeweils eine Testinstallation durchgeführt. Durch die hervorstechenden Vorteile des Netscape Certificate-Servers fiel im Rahmen dieser Politisierung die Entscheidung auf dieses Softwarepaket. Dies ist keine Vorentscheidung für Netscape. Die Mitbewerberprodukte werden - so die Planung - auch noch untersucht. Netscape erlaubt die Verwaltung beliebig vieler Zertifikate, da dabei zur Datenhaltung auf die relationale Datenbank Informix aufgesetzt wird. Weiterhin bietet der Netscape Certificate-Server durch sein Nutzerinterface, das komplett auf WWW-Techniken basiert, eine einfache Bedienung.

Damit ist eine Lösung für die geschilderten Probleme gefunden. Eine Kostenuntersuchung zeigt, daß mit geringem Mitteleinsatz hohe Sicherheit realisiert werden kann.

Inhaltsverzeichnis

1 Aufgabe und Lösung

Der sichere Zusammenschluß von Intranets der öffentlichen Verwaltung ist unverzichtbar. Beispiele für diese Aufgabe sind:

- ressortübergreifender sicherer Austausch von Informationen
- sichere Übertragung von Email.

1.1 Austausch elektronischer EU-Ratsdokumente

Im Rahmen des Austauschs elektronischer EU-Ratsdokumente wäre es vorteilhaft, wenn die Dokumente möglichst verschlüsselt übertragen und ein sicherer Zugriff auf einen WWW-Dokumenten-Server beim BMWi (Bundesministerium für Wirtschaft) eingerichtet werden könnten.

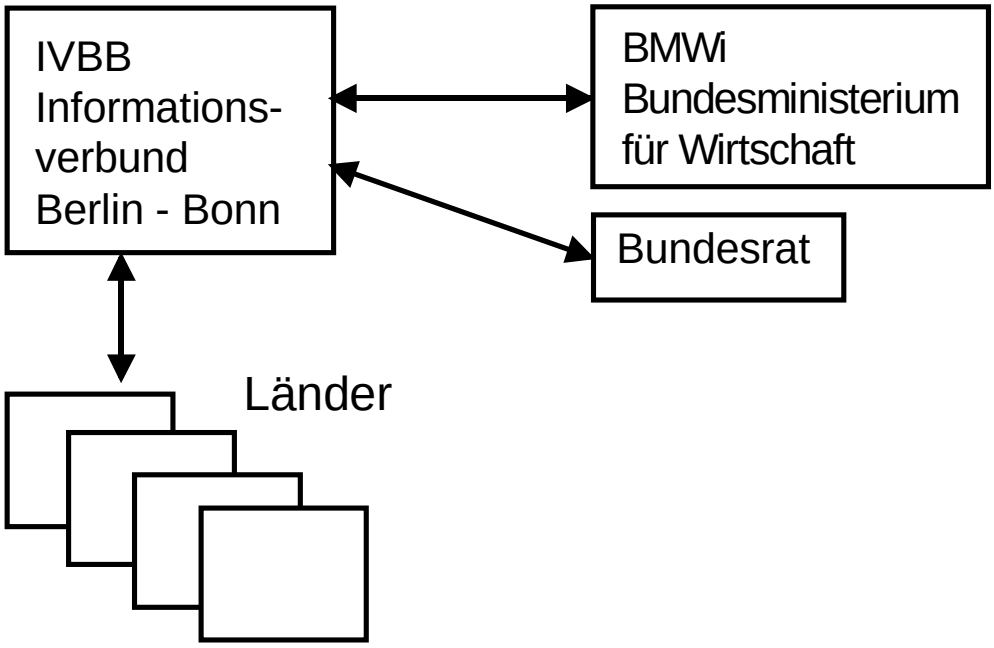
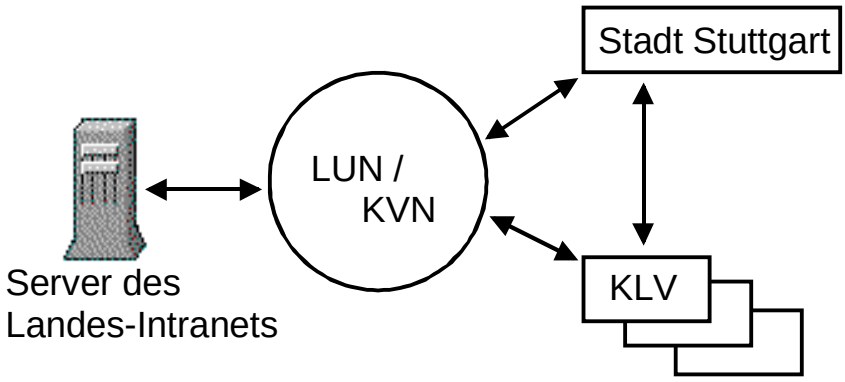


Abbildung 1: Austausch von EU-Ratsdokumenten

1.2 Zusammenschluß von Intranets der öffentlichen Verwaltung

Beim Zusammenschluß des Landes-Intranets[1] Baden-Württemberg mit Intranets des kommunalen Verwaltungsnetzes Baden-Württemberg, von Städten und Verbänden (z.B. kommunale Landesverbände) müssen differenzierte Zugriffsberechtigungen realisiert und elektronischen Dokumente möglichst auch verschlüsselt werden.



LVN = Landesverwaltungsnetz
KVN = Kommunales Verwaltungsnetz
KLV = Kommunale Landesverbände

Abbildung 2: Verbund von Intranets der Verwaltungen

1.3 Integration des Landtags in das Landes-Intranet

Der Landtag Baden-Württemberg muß als Anbieter und Nutzer des Landes-Intranets Baden-Württemberg integriert werden, um eine Vielzahl von Verwaltungsvorgängen (z.B. Recherche der Tagesordnungen und Landtagsdrucksachen) rationeller zu gestalten. Dadurch dürfen aber das verfassungsrechtlich festgelegte Informationsrecht des Landtags und die Autonomie der Landesverwaltung und Landesregierung nicht verändert werden.

Für diese und vergleichbare Anwendungen sind folgende Sicherheitsmechanismen notwendig:

- Verschlüsselung der übertragenen Informationen
- Möglichkeit von differenzierten WWW-Zugriffen
- Gewährleistung der Identifikation und Authentifikation.
- Verschlüsselte Email-Übertragung und soweit sinnvoll digitale Signierung.

Diese Sicherheitsfunktionen müssen auch bei mehreren Tausend Nutzern (Massenbetrieb) kostengünstig realisiert werden können. Zudem müssen sie auf eine WWW-Dateistruktur abgebildet werden können, bei der möglichst nicht nur Unterbäume eines hierarchisch gegliederten WWW-Informationsbaums sondern auch Teile aus dieser Informationsstruktur einer differenzierten Zugriffsregelung

[1] Das ist ein logisches Subnetz des Landesverwaltungsnetzes Baden-Württemberg

unterworfen werden. Weiter sollten mehrere autonome Trust Center in so einem Intranet-Verbund parallel betrieben werden können.

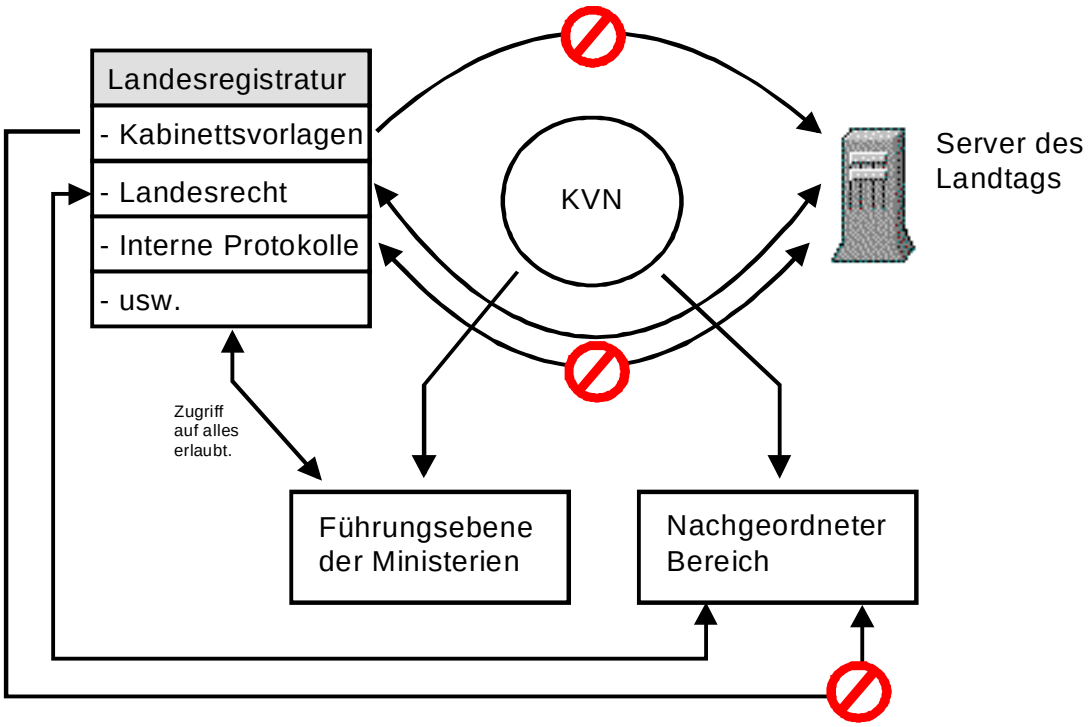


Abbildung 3: Differenzierte Zugriffsrechte auf die Landesregistratur

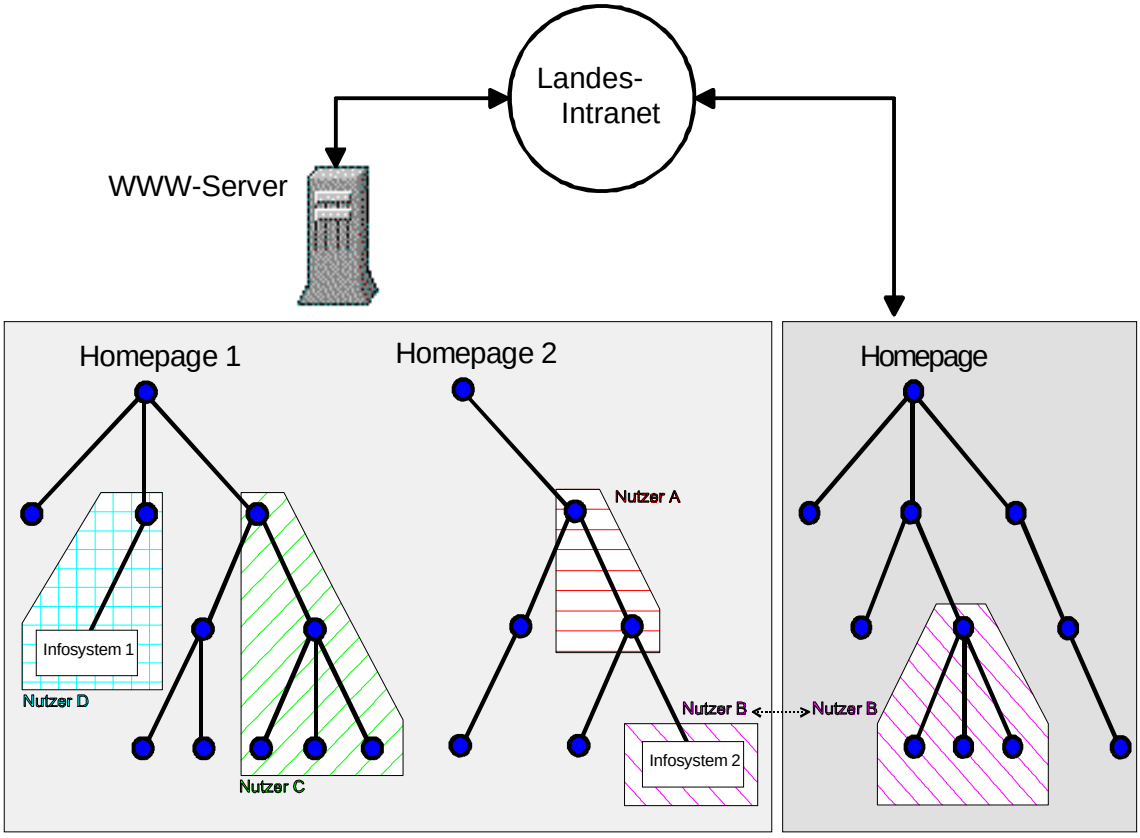


Abbildung 4: Informationsbäume im WWW und differenzierte Zugriffsregelung

1.4 Lösung

Die Lösung erfolgt durch

- ein oder mehrere Trust Center, die auf der Basis der weltweit verbreiteten Sicherheitsarchitektur SSL V3 arbeiten,
- sowie durch Standard Browser (Netscape Navigator, Microsoft Explorer) und Standard Webserver des Internets (Netscape Enterprise bzw. FastTrack Server, Microsoft Internet Information Server), die SSL V3 nutzen können.

Welche sicherheitsbezogenen Überlegungen diesem Ansatz zugrunde liegen, kann (Schäfer,1997)[2] entnommen werden. Welche Sicherheitstechniken in den Browsern verfügbar sind, kann (IM, 1997)[2] entnommen werden

SSL unterliegt zwar der amerikanischen Exportbeschränkung zu kryptographischen Produkten. Diese Einschränkung wurde im Rahmen der vorliegenden Studie so bewertet:

- Eine 40 Bitverschlüsselung, wie sie für den Export aus den USA freigegeben ist, und im vorliegenden Projekt genutzt wurde, ist bereits ein großes Hindernis für Angreifer. Deshalb wird auch das eingeschränkte SSL V.3 das Sicherheitsniveau spürbar verbessern.
- In der Vergangenheit erhielt die Landesverwaltung bereits eine uneingeschränkte Verschlüsselungstechnik. Man kann davon ausgehen, daß eine solche Ausnahme der Exportbeschränkung erneut möglich ist.
- Die Lösung der Sicherheitsprobleme beim Zusammenschalten von Intranets wurde hier ausführlich beschrieben. Wenn Verwaltungen dennoch externe Unterstützung für eine Implementierung von SSL benötigen, ist das FAW Ulm gerne hierzu bereit.

Kontaktadresse: FAW Ulm
Dr. Wolf-Fritz Rickert
Helmholtzstr. 16
89081 Ulm
Tel.: 0731 501 500
Fax: 0731 501 999
Internet-Mail: rickert@faw.uni-ulm.de

[2] vgl. Literaturverzeichnis

2 Grundlagen

Innerhalb des World-Wide-Web werden derzeit zwei verschiedene Verfahren (Basic-Authentification, single-sign-on bzw. SSL) eingesetzt, um Sicherheitsanforderungen gerecht zu werden. Im folgenden werden die Verfahren Basic-Authentification und single-sign-on näher erläutert.

2.1 Basic Authentification

Fordert ein Nutzer Informationen von einem Server an, der eine Authentifikation des Clients voraussetzt, bekommt der Client (Browser) vom Server eine Aufforderung zur Authentifizierung des Nutzers. Der Client öffnet eine Dialog-Box, die zur Eingabe des Namens bzw. Paßworts auffordert. Der Client sendet diese Informationen unverschlüsselt im Header der Anforderung zum Server, der damit den Nutzer identifizieren und abhängig von den Zugriffsrechten, die für ihn gelten, die Informationen zurückliefern oder verweigern kann. Die Daten wie Name des Nutzers und Paßwort werden lediglich im Base64-Verfahren kodiert und bieten bei einem gezielten Lauschangriff keinerlei ernsthaften Widerstand. Ein Hacker braucht lediglich die übertragene Sequenz mitzuschneiden und die Base64-Kodierung rückgängig zu machen. Die notwendige Software ist bei jedem Metamail-Paket z.B. mmencode enthalten.

Die Verwaltung der Zugriffsrechte für die Nutzer erfolgt in entsprechenden Zugriffslisten (ACL / Access Control List). Da Name und Paßwort bei jedem Zugriff des Nutzers quasi unverschlüsselt über das Netz übertragen werden, besteht ein enormes Sicherheitsrisiko, da die Paßwörter abgefangen und mißbräuchlich verwendet werden können. Somit können alle, die physikalischen Zugriff auf das Übertragungsmedium besitzen, die Daten abhören. Hierzu zählen beispielsweise Internet-Provider oder aber Knotenrechner über die Datenpakete laufen. Weiterhin bietet Basic-Authentification keinerlei Verschlüsselung der übertragenen Dokumente selbst. Nach der Authentifikation des Nutzers sendet der Server die angeforderten Dokumente im Klartext, wie jedes andere auch. Folgende Abbildung zeigt den generellen Ablauf der Client-Authentifizierung:

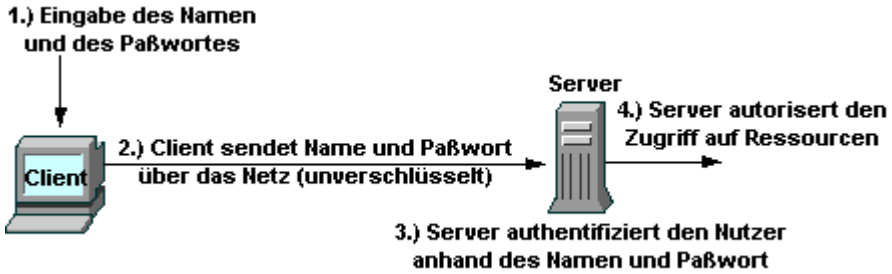


Abbildung 5: Basic Authentification

2.2 Single-sign-on und Trust Center

Beim Single-sign-on werden im Gegensatz zur Basic Authentification keine Namen und Paßwörter zur Authentifizierung über das Netz geschickt sondern Zertifikate, wobei auf das SSL (Secure Socket Layer)-Protokoll aufgesetzt wird.

SSL ist ein Protokoll, das den Austausch von verschlüsselten Informationen über das Internet erlaubt. SSL ist zwischen der Transport- und Anwendungsebene integriert, womit sie für Applikationen transparent erscheint. Somit können bestehende Applikationen ohne große Modifikation auf eine sichere Übertragung zurückgreifen.

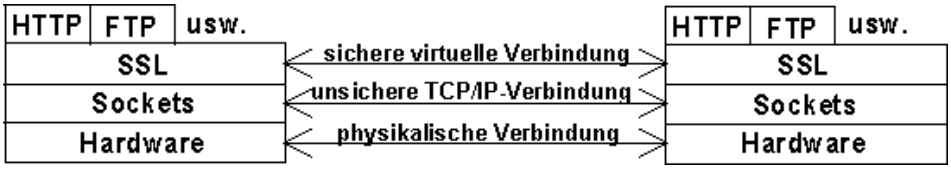


Abbildung 6: SSL-Aufbau

Bei Verwendung von SSL laufen vor der eigentlichen Datenübertragung folgende Interaktionen zwischen dem Client und dem Server ab:

In der sogenannten Hallo-Phase baut der Client eine Verbindung zum Server auf und teilt ihm mit, welche Kryptographie-Algorithmen er unterstützt. Der Server wählt daraus ein Public-Key/Private-Key- und ein Hash-Verfahren aus, die für nachfolgende Verschlüsselungen verwendet werden. Gleichzeitig sendet der Server ein Zertifikat zum Client, das die Kennung des Servers und seinen öffentlichen Schlüssel enthält. Zertifikate sind im allgemeinen Dateien, die die Identität einer Person (oder eines Unternehmens) entsprechend einem Paß oder Personalausweis, bestätigen. Hierzu sind jedoch Zertifikatsbehörden (Trust Center) erforderlich, die die Zertifizierung d.h. die Garantie für die Echtheit der Angaben, übernehmen. Die Zertifizierung können unabhängige externe Firmen (z.B.: Verisign) oder auch eine interne Organisation eines Unternehmens übernehmen.

Die Übertragung des Zertifikats zum Client ist jedoch für die Identifikation des Servers nicht ausreichend, da das Zertifikat möglicherweise aus einer anderen Verbindung kopiert worden sein könnte. Der Client generiert daraufhin einen Sitzungsschlüssel (Session Key) für einen Datenaustausch mit dem Private-Key-Verfahren. Dieser wird nun mit dem öffentlichen Schlüssel des Servers verschlüsselt. Diesen chiffrierten Schlüssel schickt der Client an den Server, der mit seinem geheimen Schlüssel den Sitzungsschlüssel entschlüsseln kann. In der abschließenden Authentifizierungs-Phase authentifiziert der Client den Server, indem er ihm eine Reihe von mit dem Sitzungsschlüssel chiffrierten zufälligen Testnachrichten schickt. Der Server kann diese Testnachrichten nur dann korrekt dechiffrieren und bestätigen, wenn er im Besitz des geheimen Serverschlüssels ist und somit der echte Server ist.

Optional kann der Server auf vergleichbare Weise den Client authentifizieren. Bevor der Nutzer sich bei einem mit SSL abgesicherten Server authentifizieren kann, muß er ein Zertifikat anfordern. Hierzu generiert er mit Hilfe des Clients ein Schlüsselpaar (geheimer / öffentlicher Schlüssel). Der generierte öffentliche Schlüssel wird der Zertifikatsbehörde übermittelt, die die Daten des Nutzers überprüft und gegebenenfalls den öffentlichen Schlüssel zertifiziert und zurückschickt. Sowohl der private Schlüssel als auch der öffentliche Schlüssel werden in einer Datenbank des Clients abgelegt. Der private Schlüssel bzw. die Datenbank für die privaten Schlüssel wird zusätzlich mit einem Paßwort geschützt, um einen Mißbrauch zu verhindern.

Werden Daten von einem Server abgerufen, der eine Authentifizierung des Clients über Zertifikate erfordert, bekommt der Client vom Server eine Aufforderung zur Authentifizierung des Nutzers. Da der private Schlüssel über ein Paßwort geschützt ist, wird der Nutzer durch den Browser zur Eingabe des Paßworts für die Datenbank aufgefordert. Mit Hilfe des Paßwortes kann der Client auf die Datenbank der geheimen Schlüssel zugreifen. Zur eindeutigen Authentifizierung des Clients verschlüsselt der Client einige zufällig generierte Daten und schickt sie an den Server, der wiederum mit dem Zertifikat bzw. öffentlichen Schlüssel des Clients diese Daten entschlüsseln und somit den Client authentifizieren kann. Der Server versucht anhand des Zertifikats den Nutzer einem bestimmten Eintrag in der Nutzer-Datenbank zuzuordnen. Gelingt ihm das so kann er abhängig von den Zugriffsrechten, die für den Nutzer gelten, die Informationen zurückliefern oder verweigern. Der Nutzer muß sich somit nur das Paßwort für die Datenbank merken und kann mit seinem Zertifikat sich auf jedem Server, der Client-Authentifizierung über Zertifikate unterstützt, authentifizieren. Folgende Abbildung zeigt den generellen Ablauf der Client-Authentifizierung:

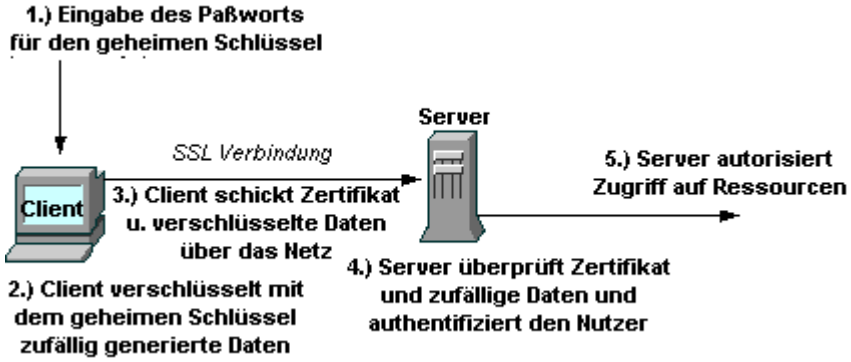


Abbildung 7: Authentifizierung des Nutzers über Zertifikate

Ein entsprechende single-sign-on Lösung wäre natürlich mit einer Chipkarten-Lösung ebenfalls möglich. Hier könnte der Nutzer über eine ihn ausweisende Chipkarte eine einmalige Authentifikation im System erreichen. Diese Technologie wurde jedoch in diesem Umfeld nicht untersucht.

2.3 Vorteile des single sign-on Prinzips für Nutzer und Systemverwalter

- Komfortabel

  Der Nutzer braucht sich nur einmal über ein Paßwort anzumelden und kann sich über sein Zertifikat auf beliebig vielen Servern authentifizieren ohne durch lästige Paßwort-Eingaben unterbrochen zu werden.

- Sichere Übertragung

  Da die Authentifizierung über Zertifikate auf der Basis von SSL läuft, ist immer eine verschlüsselte Verbindung zwischen Client und Server gegeben. Damit wird die Authentizität des Servers sowie des Clients, die Integrität und Vertraulichkeit der Informationen, sichergestellt. Des weiteren ist nur ein lokales Paßwort für die Zugangsberechtigung zur Datenbank der geheimen Schlüssel notwendig, das nicht über das Netz verschickt werden muß und somit die Gefahr der Ausspähung verhindert.

- Einfachere Verwaltung

  Systemverwalter können sehr einfach über die Liste von Zertifizierungsbehörden in Clients bzw. Servern festlegen, welcher Client auf welchen Server zugreifen darf. Des weiteren existieren bereits Softwarepakete (Directory Server von Netscape), die eine zentrale Verwaltung von Nutzern, deren Zertifikate und Zugangsberechtigungen ermöglichen. Existierende Server können über ein genormtes Protokoll (LDAP[3]) auf diesen Dienst zugreifen und aktuelle Informationen über die Zugangsberechtigung eines Nutzers beziehen. Beispielsweise braucht der Systemverwalter eines Unternehmens beim Ausscheiden eines Mitarbeiters nur an einer zentralen Stelle die Zugangsberechtigungen bzw. das Zertifikat zu revidieren, damit der Mitarbeiter auf keine Server im Unternehmen zugreifen kann. Die bisherige Technologie erforderte das Austragen der Nutzer in jedem einzelnen existierenden Server.

- Problemlose Integration in vorhandenen Umgebungen

  Das single-sign-on-Prinzip läßt sich problemlos in vorhandene Umgebungen integrieren. Voraussetzung ist die Verwendung von Server-Produkten, die das SSL 3.0 Protokoll unterstützen. Optional kann eine lokale Zertifizierungsbehörde eingerichtet werden oder auf eine der bereits existierenden unabhängigen Zertifizierungsbehörden (z.B.: Verisign[4]) zurückgegriffen werden. Bereits vergebene bzw. aktive Zugangskontrolleinstellungen, die innerhalb einer Basic-Authentification-Umgebung bereits existieren, können ohne Änderungen in eine single-sign-on Lösung überführt werden.

---

[3] LDAP ist eine Abkürzung für Lightweight Directory Access Protocol, auf deutsch: "Leichtes Verzeichnis-Zugangs-Protokoll." Dabei handelt es sich um einen offenen Standard im Internet, ursprünglich entwickelt an der Michigan State University (MSU), der es erlaubt, auf gewisse standardisierte Verzeichnisdienste im Netz zuzugreifen. Vor allem werden Verzeichnisse unterstützt, die den X.500-Standard benutzen.

[4] Siehe http://www.verisign.com

Des weiteren können existierende Zertifikate zur Sicherung des Email-Dienstes verwendet werden. Somit können Nachrichten verschlüsselt bzw. signiert übertragen werden. Damit wird die Vertraulichkeit, Integrität und Authentizität der Email gewahrt.

3 Vergleich verschiedener Zertifizierungssoftwarepakete

Im Rahmen dieses Projektes wurden die Zertifizierungssoftwarepakete der Firmen Netscape, Microsoft und ein Public-Domain Produkt evaluiert. Die Ergebnisse der Evaluation sind in folgender Tabelle aufgeführt:

Name	**Netscape Certificate Server**	**Microsoft Certificate Server**	**SSLeay**
Hersteller	Netscape	Microsoft	Internet-Gemeinde Eric Young
Vertrieb	über Netscape direkt oder Vertragshändler	über Microsoft direkt oder Vertragshändler	über FTP-Server (ftp://ftp.cert.dfn.de/pub/tools/crypt/sslea y)
Internet Adresse	http://home.netscape.com/	http://www.microsoft.de/	z.B.: http://www.camb.opengroup.org/RI/www/prism/wwwj/
Version	1.02	beta	0.8.1
Unterstützung für NT	ja	ja	ja
Unterstützung für UNIX	ja	nein	ja
Unterstützung für Netscape Clients (Browser)	ja	nein	ja, muß selbst implementiert werden
Unterstützung für Microsoft Clients	ja, jedoch fehlerhaft	ja	ja, muß selbst implementiert werden
Schlüssellängen-begrenzung	ja, nur 40 Bit Schlüssel wegen Exportbeschränkungen der USA	ja, nur 40 Bit Schlüssel wegen Exportbeschränkungen der USA	nein, beliebig lange Schlüssellängen

Unterstützung von Zertifikaten nach X509 v3 - Standard	ja	ja	ja
Unterstützung von Certificate Revocation Listen	ja	ja	ja
Unterstützung von hierarchischen Zertifizierungs-behörden	ja	ja	ja
Unterstützung von S/MIME zur verschl. Email Übertragung	ja	ja	nein
Unterstützung des LDAP Protokolls	ja	ja	nein
Datenhaltung	relationale Datenbank	Datenbank über ODBC	Filesystem
Dokumentation	sehr gut	wenig	sehr gut
Testlizenz	verfügbar, 60 Tage	Beta-Test möglich	ja
Installation	einfach	kompliziert, Abbruch mit Fehlern	Sourcen müssen explizit kompiliert werden
Bedienung	einfach, über WWW-Nutzerinterface	keine Testmöglichkeit, da Installation immer wieder abgebrochen	kompliziert, da kein Nutzerinterface
Inhaber des Urheberrechts	Netscape	Microsoft	Eric Young
Weitere benötigte Produkte	keine	Internet Information Server	keine
Preis	995 $	k. A.	kostenlos

Aufgrund der Vorteile des Netscape Certificate-Servers wurden alle weiteren Tests bzw. Installationen auf der Basis des Netscape-Produktes realisiert.

4 Installation des Netscape Certificate-Servers

4.1 Die Informix-Datenbank

Die Informix-Datenbank wird innerhalb des Netscape Certificate-Servers zur Speicherung der Zertifikate verwendet. Unter anderem werden zusätzlich folgende Informationen abgelegt:

- Gültigkeitsdauer des Zertifikat
- Ausstellungsdatum
- Aussteller
- Liste der Widerrufe

Zur Datenbank Betreuung sind keine weiteren Kenntnisse erforderlich, da sämtliche Datenbankzugriffe bzw. Aufgaben zur Instandhaltung über die Schnittstelle des Certificate-Servers abgehandelt werden können.

4.1.1 Was muß vor der Installation beachtet werden

Bevor die Installation der Informix-Datenbank durchgeführt werden kann, müssen folgende Punkte beachtet werden:

- Die Installation muß durch einen Administrator des Systems durchgeführt werden.
- Vor der Installation muß bei der Netzwerkkonfiguration unter TCP/IP Einstellungen DHCP deaktiviert sein.
- Installation muß auf dem Laufwerk *C* erfolgen.
- Die Installationpartition muß im NTFS-Format formatiert sein.
- Zur Installation muß folgender Speicherplatz zur Verfügung stehen:
  - 20 MB für die Informix-Programme
  - für die Verwaltung von je 1000 Zertifikaten müssen 6 MB Speicherplatz eingeplant werden.

4.1.2 Installation der Informix-Datenbank

Die Installation der Informix-Datenbank wird durch Starten von *Setup.exe* angestoßen. Bei der Aufforderung zur Eingabe der Art der Installation (Typical, Custom oder Minimal) sollte die Custom-Installation ausgewählt werden. Im nächsten Eingabefeld ist die Eingabe der Datenbankgröße erforderlich. Hier kann grob 6MB pro 1000 zu verwaltenden Zertifikate berechnet werden. Die weitere Installation geht folgendermaßen vonstatten:

- Vergabe eines Namens für den Datenbank-Server. Hier kann ein beliebiger Name gewählt werden.

- Vergabe eines Administrationspaßwortes für die Informix-Datenbank. Als Informix-Datenbank-Nutzer wird standardmäßig *informix* vorgeschlagen. Dieser Nutzer kann übernommen werden. Jedoch sollte ein neues Paßwort vergeben werden. Nachdem Sie dieses Paßwort eingegeben haben wird in ihrem System beim nächsten Start im NT-System ein neues Nutzer-Profil installiert, das für die Administration der Informix-Datenbank verwendet wird.
- Neustart des Systems.

Nach dem Neustart des Systems muß der *Command-Center* der Informix-Gruppe über das "Start"-Menü "Programme" "INFORMIX OnlineWorkgroup Server" "CommandCenter" gestartet werden. Über den Menüpunkt "Server" "Select" muß der neue Datenbank-Server ausgewählt werden und über Menüpunkt *"General"* auf *On-Line* gestellt werden, womit die Datenbank aktiviert wird. Bei Aufforderung muß hier der Benutzername sowie das während der Installation gesetzte Paßwort eingegeben werden. Der Command-Center kann nun geschlossen werden, da der Datenbankprozeß im Hintergrund weiterläuft. Die Informix-Datenbank ist nun fertig installiert, aktiviert und konfiguriert.

4.2 Der Certificate-Server

Der Netscape Certificate Server dient zum Erstellen, Unterzeichnen und Verwalten von Zertifikaten. Unternehmen können somit den Certificate Server zur Verwaltung ihrer eigenen Zertifikatsinfrastruktur mit öffentlichen Schlüsseln verwenden, anstatt den Dienst einer öffentlichen Zertifikatsbehörde in Anspruch zu nehmen.

4.2.1 Was muß vor der Installation beachtet werden

Bevor die Installation der Informix-Datenbank durchgeführt werden kann, müssen folgende Punkte beachtet werden:

- Die Installation des Certificate-Servers muß auf dem Laufwerk *C* erfolgen.
- Die Installations-Partition muß im NTFS-Format formatiert sein.
- Die Installation des Certificate-Servers erfordert ca. 25 MB Speicherplatz auf dem Laufwerk.
- Der Netscape Navigator 3.0 oder eine neuere Version muß bereits installiert sein.

4.2.2 Installation des Administration-Servers

Der Netscape Certificate Server besteht aus zwei verschiedenen Servern, einem Administration-Server und dem eigentlichen Certificate Server. Über den Administration-Server lassen sich eigene Einstellungen verändern und neue Certificate Server installieren bzw. deinstallieren.

Nach dem Start des Installationsprogramms muß ein Installationspfad eingegeben werden. Hier sollte das Installationsverzeichnis *C:\Netscape* angegeben werden. Der Administrations-Server ist nun fertig installiert und es kann ein Certificate Server installiert werden.

4.2.3 Installation des Certificate-Servers

Die Installation des Certificate-Servers läuft über den Administration-Server. Dieser muß über das Start-Menü, *„Programme“, „Netscape“, „Administer Netscape Servers“* gestartet werden. Durch anklicken der Schaltfläche *„Install a new Certificate-Server“* erfolgt jetzt die abschließende Installation.

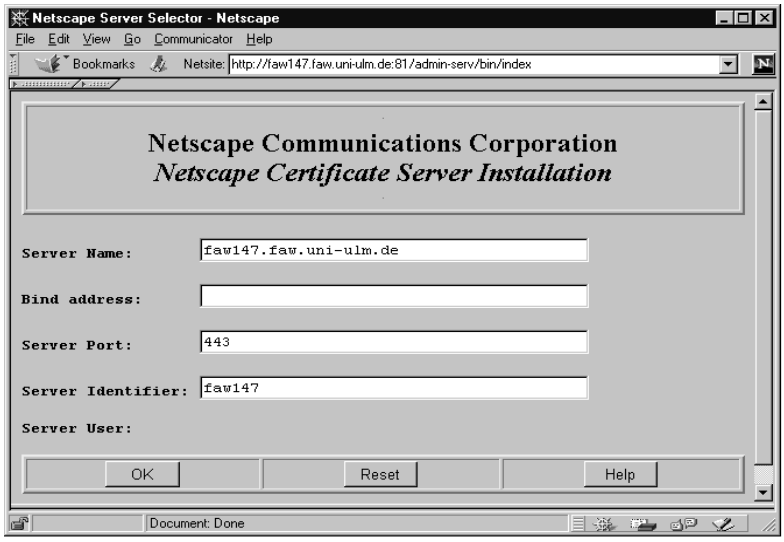


Abbildung 8: Netscape Certificate-Server Installation

In den nächsten Eingabefeldern sollten alle Vorgaben zutreffen und können übernommen werden. Folgende Parameter werden gesetzt (siehe Abbildung):

- Server Name: Der Name Ihres Rechners plus Domäne (getrennt durch einen Punkt).
- Bind address: Ist nur erforderlich falls sie eine weitere Netzwerkkarte installiert haben und diese separat ansprechen möchten.
- Server Port: Gibt den zu verwendenden Port für den Server an. Hier kann ein beliebig freier Port, der zwischen 1 und 65535 liegen kann, gewählt werden. Der Standardport ist auf 80 vordefiniert.
- Server Identifier: Hier kann dem neuen Server ein Alias-Name zugeordnet werden, unter dem ein Zugriff auf den Server möglich sein soll.

Nach Überprüfung der Parameter kann über den OK-Schaltknopf die Eingaben übernommen werden. Nach erfolgreicher Abarbeitung erscheint eine Erfolgsmeldung und die bisher eingestellten Konfigurationsdaten des Servers werden angezeigt.

Durch Klicken auf *„Configure more about your new server“* wird automatisch ein Fenster geöffnet, der sämtliche Schritte, die zur Erzeugung einer neuen Zertifizierungsstelle erforderlich sind, anzeigt und durch den Nutzer bearbeiten läßt. Gleichzeitig sind zu jedem Punkt erläuternde Hilfetexte vorhanden.

Im folgenden werden die Schritte einzeln erläutert:

- Generierung eines Schlüsselpaares (öffentlicher und privater Schlüssel) das zur späteren Signierung der Zertifikate dient.

  Über das „Start"-Menü „Programme" „Eingabeaufforderung" muß ein DOS-Eingabefenster geöffnet werden. Hier muß in das Verzeichnis *C:\Netscape\Server\bin\cms\admin\bin* gewechselt werden und das Programm *„gen-sgnkey"* mit den Parametern *„-k 1024"* aufgerufen werden. Das Programm *„gen-sgnkey"* generiert einen privaten sowie öffentlichen Schlüssel für den Certificate-Server. Es erscheint ein Dialog der zur Eingabe eines Verzeichnisses auffordert, indem das Schlüsselpaar gespeichert werden soll. Hier kann entweder die bei Punkt 4, des Installation Wizard´s, angegebene Verzeichnis übernommen werden oder ein eigenes angegeben werden. Im nächsten Dialog muß durch ein Paßwort das generierte Schlüsselpaar geschützt werden. Eine zweite Aufforderung erscheint, wo die Paßworteingabe wiederholt werden muß, um eventuelle Tippfehler auszuschließen.

  Achtung: Die Eingabe dieses Paßworts ist bei jedem Neustart des Certificate-Servers
  erforderlich. Somit darf dieses Paßwort nicht vergessen werden. Das vergebene Paßwort muß nochmals innerhalb des Eingabefeldes im Formular beim Installations-Wizard eingegeben und mit *OK* bestätigt werden.

- Generierung eine Schlüsselpaares für die SSL-Kommunikation des Certificate-Servers

  Über das „Start"-Menü „Programme" „Eingabeaufforderung" muß ebenfalls ein DOS-Eingabefenster geöffnet und in das Verzeichnis *C:\Netscape\Server\bin\cms\admin\bin* gewechselt werden. In diesem Verzeichnis muß das Programm *seckey* gestartet werden, das ebenfalls ein Schlüsselpaar generiert, das für die SSL-Kommunikation des Certificate-Servers notwendig ist. Es erscheint ein Dialog der zur Eingabe eines Verzeichnisses auffordert, indem das Schlüsselpaar gespeichert werden soll. Hier kann entweder die bei Punkt 4, des Installation-Wizard´s angegebene Verzeichnis übernommen werden oder ein anderes angegeben werden.

  Es erscheint ein Dialog der zufällige Daten anhand der Mausbewegungen sammelt. Diese zufälligen Daten werden zur Generierung der Schlüssel verwendet. Im nächsten Dialog muß durch ein Paßwort das generierte Schlüsselpaar geschützt werden. Eine zweite Aufforderung erscheint, wo die Paßworteingabe wiederholt werden muß, um eventuelle Tippfehler auszuschließen.

  Achtung: Die Eingabe dieses Paßworts ist bei jedem Neustart des Certificate-Servers
  erforderlich. Somit darf dieses Paßwort ebenfalls nicht vergessen werden. Das vergebene Paßwort muß nochmals innerhalb des Eingabefeldes im Formular beim Installations-Wizard eingegeben und mit *OK* bestätigt werden.

- Konfiguration des Zugriffs auf die Informix-Datenbank

Im nächsten Schritt müssen die Parameter für den Zugriff des Certificate-Servers auf die Informix-Datenbank konfiguriert werden.

- In das Eingabefeld „*Database Server*“ muß der bei der Informix-Installation vergebenen Name für den Datenbank-Server angegeben werden.
- In das Eingabefeld „*Database Name*“ muß der bei der Informix-Installation vergebenen Name für den Datenbank-Namen angegeben werden.
- In das Eingabefeld „*Database User*“ muß „informix“ eingetragen werden.
- In das Eingabefeld „*Database Password*“ muß das zum Benutzer „informix“ gehörende Paßwort eingetragen werden und das Formular durch klicken auf „OK“ bestätigt werden.

- Daten über die Zertifizierungsinstanz eintragen

  Hier müssen allgemeine Daten über die Zertifizierungsinstanz eingegeben werden.

  - unter „*Common Name*“ muß ein allgemeiner Name für die Zertifizierungsinstanz eingegeben werden, z.B.: Zertifizierungsstelle Innenministerium.
  - unter „*Organization Unit*“ muß der Name der Abteilung eingegeben werden, z.B.: Stabsstelle.
  - unter „*Organization*“ muß der Name der Organisation eingegeben werden, z.B.:Innenministerium
  - unter „*Country*“ muß die Länderkennung eingegeben werden (für Deutschland = de)
  - Das Eingabefeld „*Issuing Authority's Distinguished Name*“ darf nicht geändert werden, da diese Informationen aus den zuvor angegebenen Werten automatisch generiert werden.
  - Über „*Length of Validity Period*“ läßt sich die Dauer der Gültigkeit des Zertifikates der Zertifizierungsinstanz einstellen. Falls ein professioneller Einsatz geplant ist, sollte die Dauer lang gewählt werden, da sonst vor dem Ablauf alle Zertifikate durch ein neues ersetzt werden müssen.
  - unter „*Start Serial Number*“ kann der Startwert der Seriennummer gesetzt werden. Jedem ausgestellten Zertifikat wird eine eindeutige Seriennummer zugewiesen.
  - die Checkbox „*Enable X.509 v3 certificate extensions*“ muß mit einem Häkchen markiert sein, um Zertifikate nach dem neuen X.509v3-Standard zu unterstützen. Über das Auswahlfenster „*Select Signature Algorithm*“ kann ein Verschlüsselungsalgorithmus aus einer Liste ausgewählt werden. Hier sollte der Standardalgorithmus („MD5 With RSA Encryption“) eingestellt werden.
  - das „*Database Password*“ und „*Signing Key Password*“ werden automatisch eingetragen und müssen nicht explizit eingegeben werden.

Nach Beenden der Eingaben kann das Formular durch Betätigen des OK-Knopfes beendet werden.

- Informationen zum SSL-Server-Zertifikat

  In diesem Formular müssen entsprechend dem Zertifikat für die Zertifizierungsinstanz für das Zertifikat des SSL-Servers allgemeine Daten wie Common Name, Organization Unit, Organization und Country eingegeben werden. Die Eingaben müssen ebenfalls über den OK-Knopf bestätigt werden.

- Certificate-Server-Administrator Zertifikat

  Zur Authentifikation beim Certificate-Server wird ein spezielles Administrator-Zertifikat angelegt. Über dieses wird der Zugriff auf privilegierte Bereiche des Certificate-Servers ermöglicht. Zur Einrichtung eines solchen Zertifikats sind folgende Daten erforderlich:

  – unter *„Your Username“* muß ein individueller Benutzernamen angeben werden, z.B.: Schäfer

  – unter *„Common Name“* muß ein allgemeiner Name angegeben werden, der das Zertifikat beschreibt z.B.: Administratorzertifikat des Servers im Innenministerium

  – unter *„Organization Unit“* muß der Name ihrer Abteilung angegeben werden, z.B.: Stabsstelle.

  – unter *„Organization“* muß der Name der Organisation angegeben werden, z.B.: Innenministerium.

  – unter *„Country“* muß die Länderkennung angegeben werden (für Deutschland = de).

  – Das Eingabefeld *„Service Administrator´s Distinguished Name“* darf nicht geändert werden, da es automatisch aus den obigen Werten generiert wird.

  – unter *„Key size“* kann die Länge des öffentlichen Schlüssels ausgewählt werden. Derzeit wird nur eine Schlüssellänge von 512 Bit bei der Exportversion der Software unterstützt.

  – die Dauer der Gültigkeit des Zertifikates kann bei *„Length of Validity Period“* eingestellt werden. **Achtung:** Die Gültigkeitsdauer des Administratorzertifikats sollte die der Zertifizierungsinstanz nicht überschreiten!

  – das *„Database Password“* und *„Signing Key Password“* werden von den vorigen Eingaben übernommen und brauchen deshalb nicht erneut eingegeben werden.

  Nach Beendigung der Eingaben muß das Formular durch Bestätigen mit OK abgeschickt werden.

- Administrator-Zertifikat in den Netscape Navigator importieren

Hier wird das neu generierte Administrator-Zertifikat in den Navigator eingebettet, um später bei Operationen für privilegierte Nutzer zur Client-Authentifizierung an den Server geschickt werden zu können.

Durch Klicken auf *„Import Certificate“* kann das Administrator-Zertifikat in den Navigator importiert werden. Anschließend erscheint eine Bestätigung, daß das Administrator-Zertifikat erfolgreich importiert werden konnte. Hier haben Sie zugleich noch die Möglichkeit, Ihre bisherigen Einstellungen bzgl. der Wertezuweisung während der Installation für *„Common Name“, „Organization Unit*“, usw. zu überprüfen und gegebenenfalls zu ändern. Über *„more Info“* können Informationen über das aktuelle Zertifikat angesehen werden. Nach dem Bestätigen mit OK erscheint eine Aufforderung zur Eingabe eines Paßworts durch den Navigator. Mit diesem Paßwort wird die Datenbank, der geheimen Schlüssel, gesperrt. Bei Zugriffen auf diese Datenbank muß jeweils dieses Paßwort eingegeben werden. Das zugewiesene Zertifikat kann zur Sicherung in einer Datei abgelegt werden, um bei Systemabstürzen gegebenenfalls, in einen anderen Browser (diese Zertifikate) importieren zu können.

- Nach Drücken des Close-Knopfes ist die Installation des Certificate-Servers abgeschlossen.

5 Bedienung

Die Handhabung des Netscape Certificate-Servers gestaltet sich einfach, da die gesamte Bedienung über einen Netscape Browser, über entsprechende Formulare des Servers, ermöglicht wird. Generell unterscheidet der Certificate-Server zwei Nutzergruppen: Public User (Öffentliche Nutzer) und Privileged User (Privilegierte Nutzer). Im folgenden werden jeweils die wichtigsten Aktionen, die durch die einzelnen Nutzergruppen angestoßen werden können, erläutert.

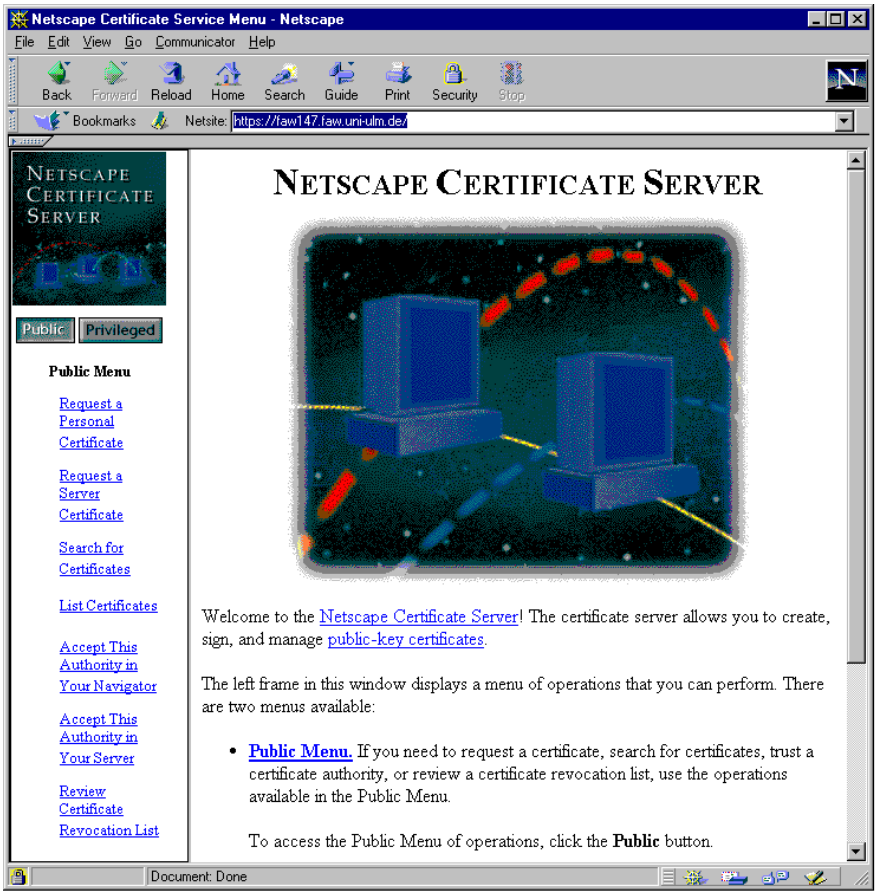


Abbildung 9: Startseite des Certificate-Servers

5.1 Nutzergruppe: Public User (Öffentliche Nutzer)

Diese Nutzergruppe gibt allen, mit Netscape Browsern arbeitenden Nutzern, die Möglichkeit, öffentliche Schlüssel zertifizieren zu lassen bzw. über bereits revidierte Zertifikate Informationen einzuholen. Hierzu stellt der Certificate-Server folgende Menüpunkte zur Verfügung:

- **Request a Personal Certificate (Anfordern eines persönlichen Zertifikats)**

  Hier kann der Nutzer ein persönliches Zertifikat anfordern, daß später zur Authentifizierung gegenüber anderen Instanzen verwendet werden kann. Hierzu ist es erforderlich, einige Angaben über seine Person zu machen. Aus diesen

Angaben wird eine Zeichenkette, die auch als Distinguished Name bezeichnet wird, generiert. Damit kann dieser Nutzer immer eindeutig identifiziert werden. Beim Abschicken der Anforderung über *Submit Request* wird automatisch der Netscape Navigator zur Generierung eines Schlüsselpaares (privater sowie öffentlicher Schlüssel) veranlaßt. Der generierte öffentliche Schlüssel wird über cgi-Skripts dem Certificate-Server übergeben, während der private Schlüssel lokal in einer Datenbank gespeichert wird. Der Certificate-Server fügt die Anforderung in ein Liste der zu signierenden öffentlichen Schlüssel ein. Gleichzeitig wird dieser Anforderung eine eindeutige Seriennummer zugeordnet, über diese später der signierte öffentliche Schlüssel abgerufen werden kann. Bis zur Signierung durch eine für die Zertifizierung privilegierte Person verbleibt dieser Schlüssel in der Warteschlange. Zur Auftragsbestätigung wird seitens des Certificate-Servers ein Formular zurückgeschickt, das alle entgegengenommenen Daten sowie die zugeordnete Seriennummer enthält. Diese eingegangene Anforderung kann nun durch einen privilegierten Nutzer bearbeitet (signiert) werden und das somit generierte Zertifikat über Email, Post etc. zurückgesandt werden.

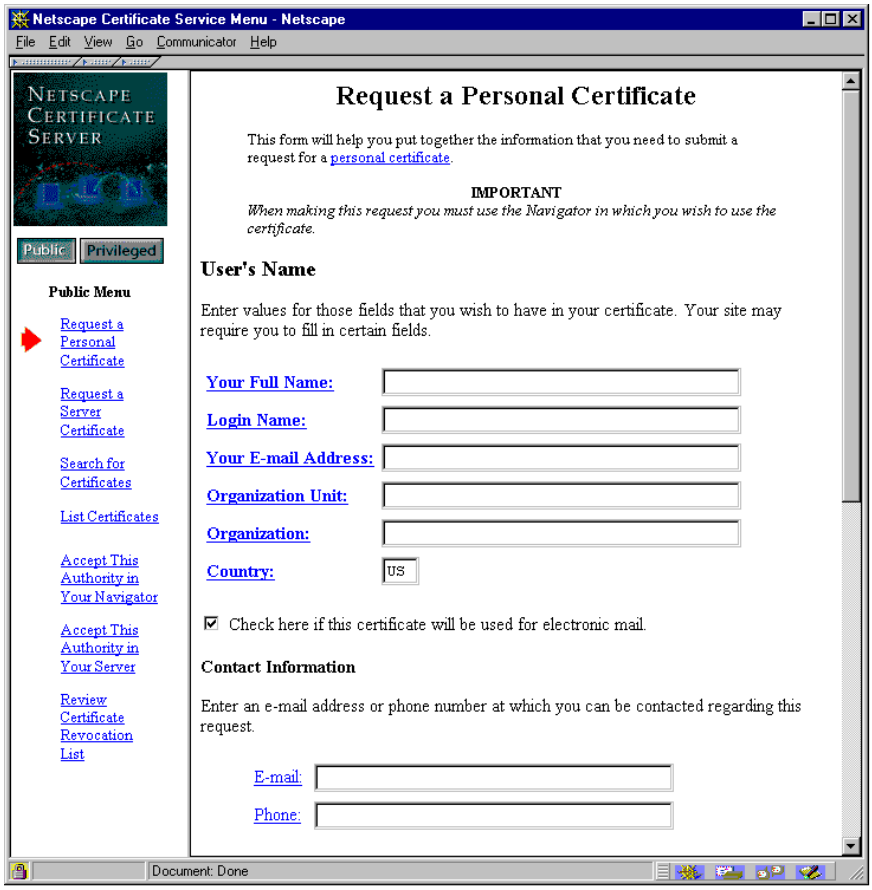


Abbildung 10: Anfordern eines persönlichen Zertifikats

- **Request a Server Certificate (Anfordern eines Server Zertifikats)**

  Die Zertifizierung eines Server-Schlüsselpaares, welche erforderlich ist um Verbindungen über SSL aufbauen zu können, wird über diesen Menüpunkt angestoßen.

  Die Zertifizierung eines Schlüsselpaares eines Servers, um Verbindungen über SSL aufbauen zu können, wird über diesen Menüpunkt angestoßen. Zuvor muß jedoch im entsprechenden Server ein Schlüsselpaar generiert werden. Für Netscape-WWW-Server sind im allgemeinen folgende Schritte notwendig:

  – Über die Option „Request Server Certificate“, muß ein Schlüsselpaar generiert werden.

  – Markieren und Kopieren des Textes zwischen **** BEGIN NEW CERTIFICATE REQUEST **** und **** END NEW CERTIFICATE REQUEST ***.*

  – Einfügen des kopierten Bereiches in das dafür vorgesehene Fenster unter *Server Certificate Request* des Certificate-Servers.

  – Abschicken der Anforderung über *Submit Request.*

  Die Anforderung wird ebenfalls mit einer Seriennummer versehen und in eine Warteschlange aufgenommen. Sie kann durch einen privilegierten Nutzer bearbeitet (signiert) werden und das somit generierte Zertifikat über Email, Post etc. zurückgesandt werden.

Abbildung 11: Anfordern eines Server-Zertifikats

- **Accept this Authority in Your Navigator (Akzeptieren der Zertifizierungsinstanz im Netscape Navigator)**

  Damit der Browser Zertifikate die von einer bestimmten Zertifizierungsstelle ausgestellt wurden, erkennen kann, muß das Zertifikat der Zertifizierungsinstanz installiert werden. Des weiteren kann zusätzlich über die Option „*I want to trust all certificate authorities that share the same root authority*“, sämtliche von dieser Instanz signierten Zertifizierungsinstanzen akzeptieren.

Abbildung 12: Akzeptieren der Zertifizierungsinstanz im Netscape Navigator

- **Accept This Authority in Your Server (Akzeptieren der Zertifizierungsinstanz im Server)**

  Um eine Zertifizierungsstelle dem Server bekannt zu machen sind zusätzliche Schritte erforderlich. Durch Ausführen dieses Formulars wird das Zertifikat der Zertifizierungsstelle angezeigt. Über die Option „*I want to trust all certificate authorities that share the same root authority*“, können sämtliche von dieser Instanz signierten Zertifizierungsinstanzen akzeptiert werden. Zur Übernahme des Zertifikats in den Server muß der Bereich zwischen *** *BEGIN CERTIFICATE* *** und *** *END CERTIFICATE* *** markiert und in die Zwischenablage kopiert werden. Über den Menüpunkt „*Install CA Certificate*“ des Servers, der ein Fenster zur Verfügung stellt, wo der kopierte Bereich eingefügt werden muß. Nach abschicken des Formulars wird das entsprechende Zertifikat zu der Liste aller Zertifizierungsstellen, die dem Server bekannt sind, hinzugefügt.

Abbildung 13: Akzeptieren der Zertifizierungsinstanz im Server

- **Review Certificate Revocation List (Anzeigen der widerrufenen Zertifikate)**

  Privilegierte Nutzer haben die Möglichkeit, bereits zugewiesene Zertifikate zu revidieren, um Nutzern einen weiteren Zugriff auf Ressourcen zu verweigern. Die Überprüfung, ob ein Zertifikat seine Gültigkeit verloren hat oder widerrufen worden ist, kann über den Menüpunkt *„Review Certificate Revocation List“* des Certificate-Servers erfolgen. Damit ein Server bzw. der Browser überhaupt Kenntnis über die revidierten Zertifikate bekommt, muß die Certificate-Revocation-List (CRL) in den Server bzw. Browser importiert werden. Dabei vergleicht der Browser die Liste aller ihm bekannten Zertifikate mit denen, die widerrufen worden sind, und setzt übereinstimmende auf ungültig.

Abbildung 14: Anzeigen der widerrufenen Zertifikate

5.2 Nutzergruppe: Privileged User (Privilegierte Nutzer)

Diese Nutzergruppe hat Zugriff auf alle administrativen Funktionen wie z.B.: Zertifikate signieren bzw. widerrufen. Während der Installation des Certificate-Servers wird ein Client-Zertifikat generiert, über den die Authentifizierung als privilegierter Nutzer erfolgt. Versucht man auf Formulare zuzugreifen, die für privilegierte Nutzer bestimmt sind, so erwartet der Certificate-Server die Authentifizierung über ein Zertifikat und erlaubt nur bei erfolgreicher Authentifikation den Zugriff auf administrative Funktionen. Im folgenden werden alle möglichen administrativen Funktionen bzw. Aufgaben der privilegierten Nutzer erläutert:

- **List Certificate Signing Requests (Anzeige der Liste der zu signierenden Zertifikate)**

  Ein privilegierter Nutzer kann hier durch klicken auf „*Run Query*“, die Liste der in die Warteschlange aufgenommen Zertifizierungsanforderungen anzeigen lassen. Jedoch muß das Auswahlkästchen „*Show waiting requests*“ im entsprechenden Formular markiert sein. Der Server zeigt daraufhin alle wartenden Anforderungen, sortiert nach Seriennummer, an. Um eine Anforderung zu bearbeiten, muß auf die jeweilige Seriennummer geklickt werden. Der Server stellt die Anforderung dar und über den Link „*Assign To Me*“ wird die Anforderungen aus der Warteschlange herausgenommen und diesem privilegierten Nutzer zugeordnet. Da es prinzipiell möglich ist, mehrere privilegierte Nutzer zu haben, kann über die Zuordnung im nachhinein festgestellt werden, wer eine Anforderung bearbeitet hat und ob es z.B.: zu Unrecht bearbeitet wurde. Weiterhin kann auf diesem Formular über „*Length of Validity Period*“ die Gültigkeitsdauer des ausgestellten Zertifikats (z.B.: 30 Tage) und der Verwendungszweck eingestellt werden. Hier wird zwischen Client, Server, Email sowie Software unterschieden. Um die Eindeutigkeit des aktuellen öffentliche Schlüssel zu garantieren muß die Option „*Check to override public key uniqueness requirement*“ aktiviert werden. Damit wird der zu signierende öffentliche Schlüssel mit allen bereits signierten öffentlichen Schlüsseln verglichen. Bei Gleichheit bzw. Übereinstimmung mit einem bereits signierten öffentlichen Schlüssel, wird die weitere Bearbeitung der Anforderung abgebrochen. Durch aktivieren der Schaltfläche „*x509v3-Certicates*“ wird das erstellte Zertifikate um weitere Informationen erweitert, um dem x509v3-Standard zu entsprechen. Weiterhin kann auf diesem Formular der Verwendungszweck des ausgestellten Zertifikats eingestellt werden. Dabei stehen folgende Auswahlmöglichkeiten zur Verfügung:

  - *SSL Client*: Verwendung als Zertifikat zur Authentifizierung gegenüber Servern
  - *SSL Server*: Verwendung als Server-Zertifikat
  - *Secure Email*: Verwendung zur sicheren Übertragung von Email
  - *Object Singning*: Verwendung als Zertifikat zum signieren von Programmen wie z.B.: Java-Applets, Javascript-Elemente oder ähnliches.

  Um vor Ablauf des Zertifikats der Zertifizierungsstelle bereits einen neu generierten öffentlichen Schlüssel der Zertifizierungsstelle bei Zertifizierungen

mit einzubinden kann über die Optionen „*Include Authority Key Identifier*“ und „*Include Subject Key Identifier*“ erreicht werden.

Das Verfahren zur Erstellung der Signatur kann unter „*Select Signature Algorithm*“ eingestellt werden, wobei die Standardverfahren verwendet werden sollten, da es von gängigen SSL-Servern und -Browsern unterstützt wird.

Nach der Überprüfung der Angaben des Antragstellers kann das Zertifikat über das Menü „*Select An Operation To Perform on This Request*“ entweder geprüft, ausgegeben, abgebrochen, entfernt oder zurückgesetzt werden. Direkt über die Wahl „*Issue This Certificate*“ und abschließendes klicken auf „*Perform Selected Operation*“ wird die Anforderung bearbeitet und der öffentliche Schlüssel signiert somit ein Zertifikat erstellt. Das erstellte Zertifikat kann nun über Email, speichern auf Diskette und verschicken per Post oder durch Übermittlung des unter „*Importing This Certificate To a Navigator*“ angegeben HTML-Adresse zugestellt werden.

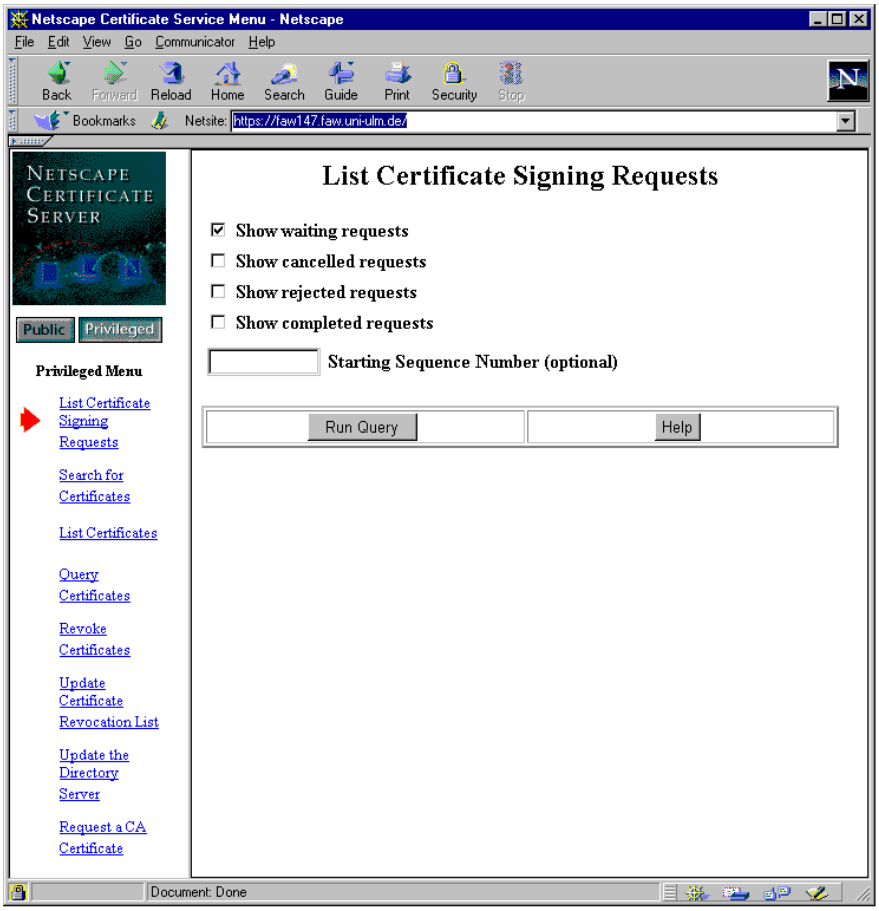


Abbildung 15: Anzeigen der Liste der zu signierenden Zertifikate

- **Revoke Certificates (Widerrufen von Zertifikaten)**

  Über diesen Menüpunkt lassen sich bereits zugestellte Zertifikate widerrufen und werden somit für ungültig erklärt. Dies kann firmeninterne Gründe (z.B.: Kündigung eines Mitarbeiters) haben oder auch bei Verlust bzw. Offenbarung des privaten Schlüssels eines Nutzers notwendig werden. Ein entprechendes Formular stellt hier verschiedene Suchoptionen bereit, über die entsprechenden Zertifikate aus dem aktuellen Zertifikatsbestand herausgefiltert werden und entsprechend revidiert werden können.

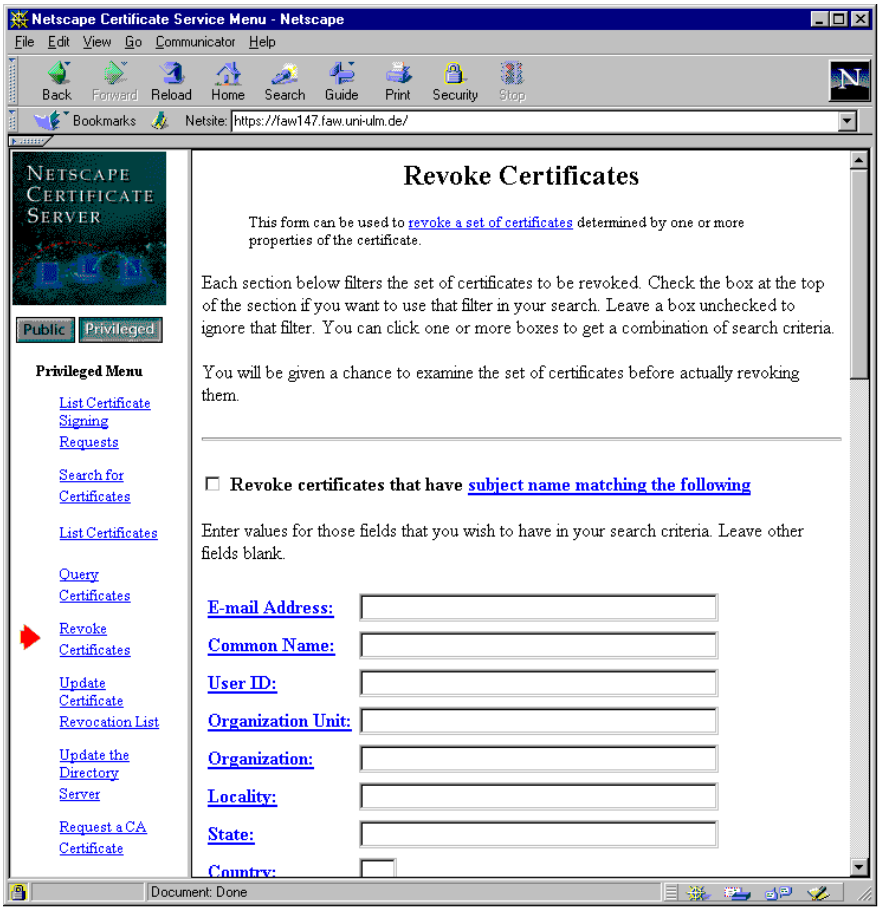


Abbildung 16: Widerrufen von Zertifikaten

- **Update Certificate Revocation List (Aktualisieren der Liste der widerrufenen Zertifikate)**

  Aktuelle widerrufene Zertifikate werden nicht automatisch in die Certificate-Revocation-List (CRL), d.h. die Liste mit den revidierten Zertifikaten, aufgenommen. Somit muß nach jedem Widerruf eines Zertifikats die CRL über „*Update Certificate Revocation List*“ aktualisiert werden.

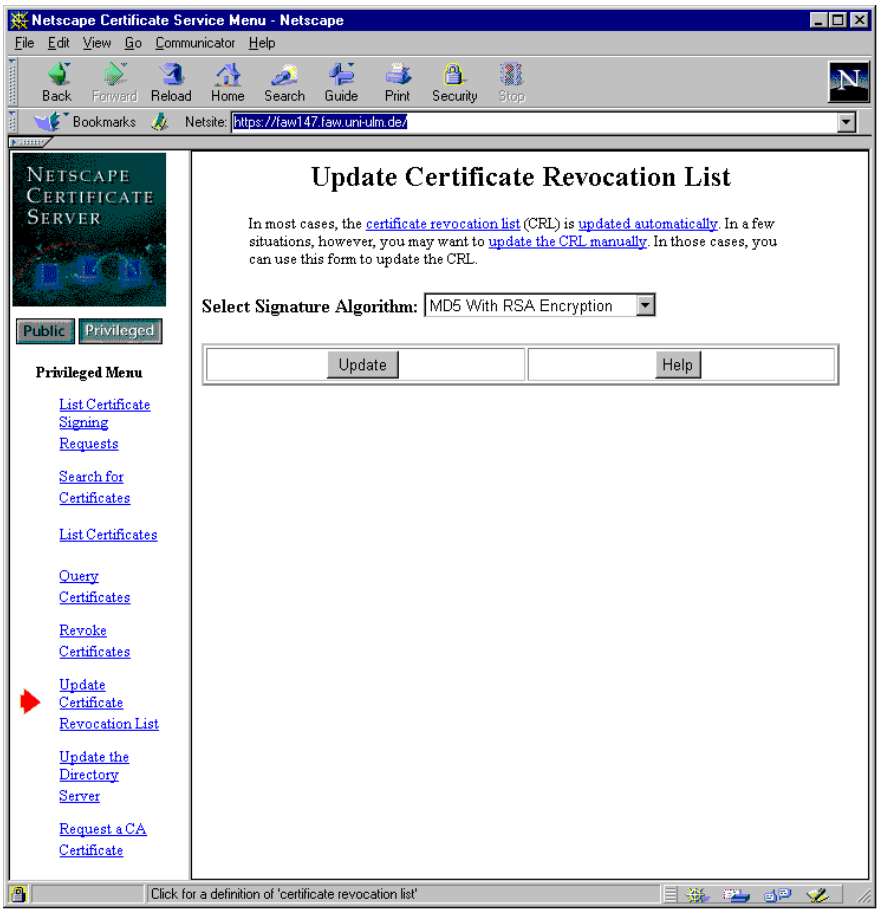


Abbildung 17: Aktualisieren der Liste der widerrufenen Zertifikate

6 Kostenabschätzung

Die folgende Kostenschätzung bezieht sich auf den Betrieb und die Einführung des single sign-on Prinzips. Hierbei wird die Zertifizierungssoftware sowie die Client-Software (Netscape Navigator) der Firma Netscape als Grundlage genommen. Die Kostenabschätzung wird auf der Basis von einem Nutzer erstellt. Der Administrationsaufwand wird für die Einführungsphase (ca. 1 Monat) höher angesetzt, da die Installation bzw. erste Einführung mehr Supportleistung für die Nutzer erfordert.

Posten	**Kosten bzw. Aufwand**
Zertifizierungssoftware (Netscape Certificate Server 1.01) für Windows NT (Verwaltung bzw. Speicherung von beliebig vielen Zertifikaten)	995 $
Client-Software (Navigator 4) CD-Version für Windows NT bzw. Client-Software (Navigator 4) Download Version für Windows NT	39 $ 26.99 $
Administrationsaufwand für die Einführungsphase	1 Mannmonat
folgender Administrationsaufwand	10 Stunden / Monat

7 Sicherheitsbewertung

Im folgenden Kapitel soll die erreichte Sicherheit der erarbeiteten Lösung näher betrachtet werden. Um hier eine korrekte Einschätzung zu ermöglichen wird zunächst auf die einzelnen verwendeten Mechanismen und deren Möglichkeiten und Beschränkungen eingegangen. Danach werden die konkret eingesetzten Mechanismen und vorgeschlagenen Verfahren beurteilt.

7.1 Verwendete Mechanismen

Die in den vorgeschlagenen Werkzeugen eingesetzten Algorithmen und Protokolle sind weitestgehend standardisiert. Die einzelnen Verfahren unterliegen, soweit die Produkte aus den USA kommen, den dortigen Regulierungen für Waffen- und Munitionsexporte. Die derzeitigen Regulierungen besagen, daß Verschlüsselungsalgorithmen nur bis zu einer Schlüssellänge von 40 Bit exportierbar sind. Eine Ausnahme hiervon sind Applikationen im Banken- und Regierungsbereich. Für diese Bereiche kann die Begrenzung durch eine Sondergenehmigung aufgehoben werden. Jüngste Pressemeldungen (New York Times) deuten jedoch darauf hin, daß die Exportbeschränkungen zukünftig strenger und restriktiver gehandhabt werden sollen (zumindest im Bankenbereich). Für Authentifikations- und Idetifikationszwecke existieren gegenwärtig keine Beschränkungen der verwendbaren Schlüssel.

7.1.1 SSL / SSLeay

Das SSL-Protokoll, das auch in SSLeay eingesetzt wird, stellt eine reine Absicherung der Kommunikationsverbindung gegen Abhören dar. Der Partner wird authentisiert und die Daten werden verschlüsselt übertragen. Es wird keine später nachweisbare Signatur unter die Daten generiert. Der gesamte Verkehr könnte daher auch von einer der beiden Parteien ohne Mitwirkung der anderen Partei erzeugt worden sein.

Das SSL-Protokoll, in der Version wie es von WWW-Browsern eingesetzt wird, unterstützt eine Authentifikation mittels RSA und eine anschließende Verschlüsselung der Daten mit den Algorithmen Tripel-DES, RC2 oder RC4. Eine weitergehende Beschreibung der Algorithmen kann in (MOV, 97) nachgelesen werden. Die Schlüssellängen sind auf 40 Bit beschränkt, wenn kein Zertifikat eines Servers mit Sondergenehmigung vorliegt, das die Beschränkung aufhebt.

SLL existiert in verschiedenen Versionen. Momentan ist nur die Version 3.0 allgemein als sicher anerkannt. Die Kompatibilität zu Version 2.0, die oft eingestellt ist, ergibt einen beträchtlichen Sicherheitsverlust und sollte unbedingt vermieden werden. Der entsprechende Fehler im Handshake-Protokoll wurde in Version 3.0 behoben.

Die verwendeten Chiffren bieten bei uneingeschränkter Schlüssellänge einen sehr guten Schutz gegen einen Bruch der Vertraulichkeit. Wird die exportfähige 40-Bit Version eingesetzt, so kann ein Schlüssel von engagierten Gruppen oder

Einzelpersonen mit mäßigem Hardwareaufwand (einige PCs) rekonstriert werden. Ein derartiger Angriff muß jedoch bei jeder einzelnen Nachricht neu ausgeführt werden. Die Mechanismen zur Identifikation und Authentifikation basieren (in der Exportversion) auf RSA mit 512 Bit Schlüssellänge und sind als hinreichend stark für die meisten Applikationen einzustufen.

7.1.2 S/MIME

Bei S/MIME werden die Basismechanismen von SSL eingesetzt um vertrauliche, integere und authentische email zu implementieren. Durch die Mechanismen wird ein permanent bestehender Unterschriftstatus erzielt. Eine S/MIME mail kann daher abgespeichert werden und später als Beweismittel eingesetzt werden, wenn die verwendeten Protokolle und Komponenten dies im Rahmen des Signaturgesetzes zulassen.

S/MIME verwendet die gleichen Chiffriersysteme wie das oben beschriebene SSL-Protokoll. Die Chiffren sind in der Exportversion jedoch ständig auf 40 Bit Schlüssellänge beschränkt. In diesem Fall existiert auch keine Ausnahmeregelung für Banken- und Regierungsanwendungen.

Die verwendeten Signaturalgorithmen sind Standardalgorithmen und bieten eine gute Sicherheit. Die Vertraulichkeit der Nachrichten kann nicht unbedingt garantiert werden, da die verwendeten Chiffren mit 40 Bit Schlüssellänge im Einzelfall (s.o.) gebrochen werden können (siehe auch (Eurosign, 97)).

7.2 WWW-Sicherheit

Das Hypertext-Protokoll (http), das von den Web-Browsern wie Netscape Navigator oder Internet Explorer verwendet wird, ist nicht in erster Linie für Sicherheit ausgelegt, sondern nur zur einfachen Erbringung des Endergebnisses. Daher wurden zu dem bestehenden Protokoll Sicherheitsmechanismen hinzugefügt. Der gebräuchlichste ist die Erweiterung HTTPS, die eine Transportsicherung über das Secure Socket Layer (SSL) Protokoll erzielt. Es werden jedoch weiterhin alle Teile einer Seite mit getrennten Requests vom Server geholt. Der Browser baut daher im Extremfall für jedes Teilbild eine eigene SSL-Verbindung zum Server auf. Während jede einzelne SSL-Verbindung für sich vertraulich und authentisch ist, ergibt sich die Frage, ob alle Daten vom **gleichen** Server stammen. Dies kann der Benutzer nur herausfinden, indem er sich die Zertifikatsinformation (Security, Security Info, OpenPageInfo) der Seite ansieht und überprüft, ob alle Datenverbindungen mit dem selben Zertifikat durchgeführt wurden. Auch, wenn einige Teile der Seite von einem anderen Host kommen, oder mit einem anderen Zertifikat gesendet wurden, der Schlüssel oder das Schloß, das eine sichere Verbindung andeuten soll, an der unteren Ecke des Bildschirmes ist in diesem Fall die ganze Zeit über aktiv, obwohl die Sicherheit nicht gewährleistet ist.

Um dieses Problem zu umgehen, besteht die Möglichkeit einen eigenen Certificate Server aufzusetzen und nur dessen Zertifikat im Browser zu speichern. Löscht man nun alle fremden Zertifikate anderer Certificate Server, so kann der Browser nur noch Server authentifizieren, die vom eigenen Certificate Server autorisiert wurden.

Soll ein Serverzertifikat von Verisign verwendet, um die Längenbeschränkungen der Schlüssel aufzuheben, so sollte nur das eigentliche Server-Zertifikat im Browser abgespeichert werden. Alle anderen Zertifikate sollten gelöscht werden oder es sollte ihnen zumindest die Berechtigung zum Ausstellen von Serverzertifikaten im Browser aberkannt werden (Security Info, Certificates, Signers, Accept this Certificate Authority for Certifying network sites).

Diese Maßnahmen implizieren jedoch eine eingeschränkte Funktionalität, da der Browser dann nicht mehr fähig ist mit allen Servern zu kommunizieren. Wird eine Verbindung zu einem anderen https-Server geöffnet, so wird der Benutzer gefragt, ob das Zertifikat zur Zertifikatliste hinzugefügt werden soll. Akzeptiert der Benutzer dies, so wird die Sicherheit des eigenen Servers wieder reduziert, da wieder mehrere Server-Zertifikate eingetragen sind. Eine andere Möglichkeit ist es, im Browser dafür zu sorgen, daß ein Alarm ausgelöst wird, sobald ein Request an einen anderen als den zuletzt authentifizierten Host geschick wird. Dies kann bei neueren Netscape Navigator Versionen (ab Version 4.0.3) unter Security, Navigator, Leaving an encrypted site eingestellt werden. Der Benutzer müßte jedoch nach dem Eintritt in des sicheren Host immernoch dessen Identität durch eine Überprüfung der Sicherheitsinformationen kontrollieren. Die angesprochene Einstellmöglichkeit existiert nicht bei allen Versionen des Netscape Navigator. Es ist daher zu sicherzustellen, daß die verwendete Version dieses Feature unterstützt.

Ein weiteres Problem ist die angesprochene Kompatibilität zu SLL-Version 2.0. Diese sollte beim Browser unbedingt entfernt werden (unter Security, Navigator, Enable SLL v2). Ebenfalls unter Security, Navigator sollten alle verfügbaren Warnungen (bis auf Entering an encrypted site) eingeschaltet werden. Bei einem bestimmungsgemäßen Einsatz und Verwendung von nur einem sicheren Server sollten dann keine Warnungen auftreten.Werden mehrere Server verwendet, so tritt jeweils beim Wechsel zwischen zwei Servern die Meldung auf. Existiert eine Ausnahmegenehmigung der US-Behörden, so kann ebenfalls unter Security, Navigator, Configure SSL v3 die Verwendung von 40-Bit Chiffren unterbunden werden.

7.3 Sicherheit von Certificate- und Administration-Server

Die beiden Server sind ein kritischer Bestandteil des Gesamtsystems. Sowohl auf den Certificate- als auch auf dem Administration Servern sollte unter keinen Umständen anderer Benutzerverkehr zugelassen werden. Ebenfalls sollten die Passworte (nicht nur die Passworte für Certificate- und Administration-Server) sehr sorgältig gewählt werden. Der Rechner sollte **keinerlei andere Services** nach außen zur Verfügung stellen (shares etc.). Da der Administrator-share nicht abgestellt werden kann, ist hier mit besonderer Sorgfalt vorzugehen. Die entsprechenden Logfiles sollten daher ebenfalls regelmäßig überprüft werden.

Der Administration-Server sollte nicht online am Netz betrieben werden. Er wird ohnehin nur zur Einrichtung und Verwaltung von Certificat-Servern eingesetzt. Um Sicherheitsrisiken auszuschließen kann er auf einem separaten Rechner installiert werden und die geheimen Daten sollten auf Diskette gehalten werden.

Die sicherste Installation eines Certificate-Servers ist ebenfalls nicht online am Netz verfügbar. Die Benutzer werden persönlich beim Administrator vorstellig und erhalten ihr Zertifikat auf Diskette. Das Zertifikat kann dann in den Zielrechner importiert werden. Aus organisatorischen Gründen wird dieses Vorgehen jedoch nicht immer durchführbar sein. Muß der Server am Netz gehalten werden, so sollten die Geheidaten des Servers und der privilegierten Nutzer nicht auf der Festplatte des Servers abgelgt werden. Auch nicht in verschlüsselter Form. Die Daten sollten auf Diskette gehalten und nur bei Bedarf in den Rechner eingelegt werden.

8 Literatur

(IM, 94) Innenministerium Baden-Württemberg, Schäfer, Georg; Datenschutz- und Sicherheitskonzept für das LVN-OSI, Az.: S-0278-LVN/30

(IM, 96) Innenministerium Baden-Württemberg, Schäfer, Georg; Einsatz der Verschlüsselung in der Landesverwaltung Baden-Württemberg, Konzeption, Az.: S-0275.0/11

(IM, 97/1) Innenministerium Baden-Württemberg, Schäfer, Georg; Einsatz der Intranet-Technik in der Landesverwaltung Baden-Württemberg, Konzeption, Az.: S-0278-LVN/58

(IM, 97/2) Innenministerium Baden-Württemberg, Schäfer, Georg; Datenschutz und Datensicherheit bei Client - Server - Systemen, Entwurf, Az.: S-0275.0/12

(IM, 97/3) FAW Ulm; Sicherheit für Benutzer der Internet-Technologie, Studie für das IM, 1997

(Schäfer, 97) Schäfer, Georg; Mit Sicherheit erfolgreich - Ein Leitfaden zur Sicherung moderner Informations- und Kommunikationssysteme, R.v. Decker Verlag, 1997, ISBN 3-7685-4796-5

(Netscape, 97) Informationen zu Netscape-Produkten, http://www.netscape.com

(MOV, 97) Menezes, Alfred, van Oorschot, Paul, Vanstone, Scott; Handbook of applied cryptography, CRC Press, 1997, ISBN 0-8493-8523-7

(Eurosign, 97) Bewertung von 40 Bit Chiffren; http://eurosign.com/help/policy/isitsec