BERUFSAKADEMIE | MANNHEIM
university of cooperative education | staatliche studienakademie

Ausarbeitung zum Referat

Public - Key – Infrastruktur mit OpenSSL / OpenCA

von

Christiane Hein (Matr.Nr. 192215)

und

Madlen Behlert (Matr.Nr. 148495)

Vorlesung: Seminar Informationstechnik
Dozent: Herr Prof. Tischhauser

Inhaltsverzeichnis

1 Grundlagen

1.1 Public-Key

Public-Key Infrastruktur (engl.: "public key infrastructure"; PKI) ermöglicht den sicheren Austausch vom digitalen Signaturen, verschlüsselten Dokumenten, Authentifizierung und Autorisierung, auch wenn mehrere Kommunikationspartner betroffen sind.

Die folgenden Elemente bilden die PKI:

- Certificate Authority (CA)
- Registration Authority (RA)
- Directory Service[1]

Die verwendeten Schlüssel können u.a. für Server, Clients, Benutzer von der PKI erstellt, gesperrt, gesucht und verifiziert werden, zur Signierung und

Verschlüsselung von E-Mail und anderen Daten. [2]

Schlüssel existieren immer als Paar:

- Privater Schlüssel (private key)
- Öffentlicher Schlüssel (public key)

Vorteil gegenüber herkömmlicher Verschlüsselung: Keine geheime Übermittlung von Schlüsseln nötig.

Problem: Der öffentliche Schlüssel muss zweifelsfrei dem Eigentümer zuordenbar sein.[3]

1.2 Certification-Authority (CA)

Die Certification-Authority ist verantwortlich für die Ausgabe und Verwaltung der digitalen Zertifikate und übernimmt hierfür folgende Aufgaben:

- Zertifizierung des öffentlichen Schlüssels des Benutzers
- Veröffentlichung des Zertifikates
- Ausgabe von Zertifikatswiderrufliste (Certification Revocation Lists - CRLs)[1]

CA hat folgende Vorteile:

- Weniger Arbeit für den Anwender

[1] WWW.SPENNEBERG.ORG/VPN-BOOK/VPN_KAP8.PDF
[2] WWW.KFUNIGRAZ.AC.AT/ZID/SICHERHEIT/INFRASTRUKTUR/ UNIGRAZ-PKI-PROJEKTPLAN_V1.3.1.PDF
[3] WWW.FRANKEN.DE/DE/VERANSTALTUNGEN/ KONGRESS/2000/KNF-CA.PDF

- Zertifikatswege leichter handhabbar
- Bekannte Zertifizierungsrichtlinien

CA hat folgende Nachteile:

- Starre Struktur
- Von zentralen Instanzen abhängig
- Fest im Browser eingebaut == vertrauenswürdig[4]

1.3 Registration-Authority (RA)

Die Informationen, welche die CA benötigt, wird von der Registration-Authority aufgezeichnet und überprüft. Für die Unterzeichnung des Zertifikates ist die Überprüfung der Identität des Benutzers besonders wichtig. In der Regel erfolgt die Identitätsüberprüfung durch die Kontrolle des Ausweises.[1]

1.4 Directory Service

Directory Service ist ein Verzeichnisdienst, der die Aufgabe hat die gültigen Zertifikate aller Benutzer in einem zentralen Repositorium zu speichern und zu veröffentlichen. So kann jeder Benutzer auf die Zertifikate der anderen Benutzer zugreifen. Das Directory Service veröffentlicht zusätzlich die Zertifikatswiderrufslisten (CRLs) oder erlaubt eine Überprüfung der Zertifikate mit dem Online Certificate Status Protocol (OCSP).[1]

1.5 OpenCA

OpenCA ist ein Open Source Projekt das 1999 gestartet wurde, um eine Open Source Trust Center Software für UNIX zu erschaffen. Hauptsächlich besteht die OpenCA aus einem Web Interface, welches in Perl geschrieben wurde, OpenSSL für die kryptografischen Operationen und einer Datenbank, in der die Schlüssel, Zertifikate und Widerrufslisten gespeichert werden.

Die Voraussetzung für OpenCA ist die Verwendung von x509 basierten Zertifikaten in z.B. Email oder VPN.

Durch OpenCA wird eine einheitliche Zertifikationsverwaltung realisiert, die in unterschiedliche Sicherheitsbereiche und administrativen Berechtigungen aufgeteilt ist, dessen Zugriffe über Zertifikation oder weitere Berechtigungsinformationen geregelt ist.

[4] WWW.FRANKEN.DE/DE/VERANSTALTUNGEN/ KONGRESS/2000/KNF-CA.PDF

Es herrscht eine funktionale Trennung zwischen der öffentlichen Schnittstelle (engl. Interface) zur Schlüsselgenerierung, Zertifikatsantragsstellung und nichtöffentlichen Bereichen der Registration- und Certification-Authority.[5]

OpenCA wird von allen Plattformen mit Unterstützung von oben Apache, OpenSSL, OpenLDAP und Perl unterstützt.

Es kommt hauptsächlich beim Aufbau einer unternehmensweiten CA-Hierarchie mit umfassender PKI zu Einsatz. Hierbei wird die Zertifikatsverwaltung auf Ebenen unterschiedlicher Organisationen unter Anbindung bestehender Daten realisiert.

OpenCA wird noch weiterentwickelt und unterstützt bereits folgende Funktionen:

- Verschiedene Schnittstellen: LDAP, RA, CA und die Protokolle SCEP und OCSP
- Anmeldung mit Kennwort und Zertifikat
- Flexible Steuerung der Certificate Subjects und der X.509.v3 Erweiterung
- Rückruf der Zertifikate gesteuert durch PIN Nummern oder mit digitalen Signaturen
- Warnung bei Ablauf eines Zertifikates
- usw.[1]

Die Zertifikatsverwaltung besteht aus verschiedenen Interfaces (Public, LDAP, RA und CA). Je nach Sicherheitsanforderungen können alle Komponenten auf verschiedenen Rechnern in unterschiedlichen Netzwerken betrieben werden und unterschiedliche Authentifikationsmechanismen implementieren.[5]

1.6 OpenSSL

OpenSSL ist ein Tool für kryptografische Aufgaben bei der Verschlüsselung und Authentifizierung digitaler Dokumente.

Die starke Kryptografie basiert auf einer freien Implementierung, wobei der Code sicherheitstechnisch extrem überwacht ist.

OpenSSL stellt Bibliotheksfunktionen zur Nutzung von kryptographischen Funktionen zur Verfügung und unterstützt die Generierung von RSA-Public/Private-Key's und die Anfertigung von x509-basierten Zertifikaten.

Der Werkzeugsatz besteht im Kern aus zwei Bibliotheken und dem Kommandozeilenwerkzeug "openssl". Die Bibliothek "libssl.a" implementiert SSL (Secure Socket Layer) und TLS (Transport Layer Security) in verschiedenen

[5] http://www.xtelligent.de/wissen/steckbriefe/oss_openca.htm

Versionen und die Bibliothek "libcrypto.a" implementiert verschiedenste kryptografische Funktionen (Cipher, Hash-Funktionen, Public Key Management, Management von x509-Zertifikaten).[6]

1.7 Gesetzliche Vorgaben

1.7.1 Signaturgesetz SigG

Ziel der gesetzlichen Vorgaben ist es Rahmenbedingungen für elektronische Signaturen zu schaffen. Herrscht keine gesetzliche Pflicht eine elektronische Signatur zu benutzen, bleibt dem Anwender der Gebrauch freigestellt.

Durch rechtliche Vorschriften für die öffentliche Verwaltungstätigkeit kann bestimmt werden, dass die elektronischen Signaturen weitere Anforderungen erfüllen müssen, die objektiv, verhältnismäßig und nicht diskriminierend sein dürfen und sich auf spezifische Merkmale der Anwendung beziehen.

Das Gesetz definiert eine elektronische Signatur als eine Art Unterschrift, die den Eigentümer elektronischer Daten eindeutig authentifiziert. Diese kann nur vom Besitzer selbst oder automatisch, unter Berücksichtigung beglaubigter Zertifikat erstellt werden und hat den Stellenwert einer handgeschriebenen Unterschrift. Sie ist einmalig und jegliche Veränderung ihrer ursprünglichen Form wird erkannt.

Die Überprüfung der Einhaltung der gesetzlichen Vorgaben obliegt der Behörde des Telekommunikationsgesetzes.

Der Betrieb eines Zertifizierungsdienstes ist im Rahmen der Gesetze genehmigungsfrei, jedoch darf nur der einen Zertifizierungsdienst betreiben, der die Zuverlässigkeit und Fachkunde sowie eine Deckungsvorschrift erfüllt. Der Betrieb ist der zuständigen Behörde darzulegen.

Ein Zertifikat enthält Angaben über den Antragsteller. Es kann aber auch Angaben über eine Vertretungsmacht enthalten. Diese Angaben müssen vor der Erstellung eines Zertifikats sorgfaltig auf ihre Richtigkeit geprüft werden. Diese dürfen jedoch nur mit Einwilligung des Antragstellers in das Zertifikat aufgenommen werden. Wünsch der Antragsteller z.B. ein Pseudonym für seinen Namen, ist diesem nachzukommen.

Inhalt eines Zertifikats:

- eindeutige Identifizierungsdaten, sei es der Name oder ein Pseudonym, des Inhabers
- den zugeordneten Signaturprüfschlüssel,

[6] http://www.xtelligent.de/wissen/steckbriefe/oss_openssl.htm

- Beschreibung wie der Signaturprüfschlüssel des Inhabers als auch des Zertifizierungsdienstanbieters benutzt werden kann
- die laufende Nummer des Zertifikates,
- Gültigkeitszeitraum des Zertifikates,
- den Namen des Zertifizierungsdienstanbieters und des Staates, in dem er niedergelassen ist,
- Angaben über Beschränktheit des Signaturschlüssels auf bestimmte Anwendungen,
- Angaben, dass es sich um ein qualifiziertes Zertifikat handelt, und
- nach Bedarf Attribute des Signaturschlüssel-Inhabers.

Es ist die Pflicht des Zertifizierungsdienstes dafür Sorge zu tragen, eine Verfälschung der Zertifikate unmöglich zu machen. Außerdem ist er für die Geheimhaltung des Signaturschlüssels verantwortlich. Dieses beinhaltet, dass der Schlüssel nur vom Zertifizierungsdienst selbst an einem sicheren Ort gespeichert werden darf.

Neben dem Zertifikat selbst muss auch die dazugehörige Dokumentation eindeutig sein. Auch sie darf im Nachhinein nicht Änderbar und muss jeder Zeit einsehbar sein.

Es herrscht jedoch strengster Datenschutz bei den Daten des Antragstellers, sodass Unbefugten der Zugriff verweigert werden muss.[7]

1.7.2 Signaturverordnung – SigV

Durch den Erlass des Signaturgesetzes vom 22. Juli 1997 trat diese Verordnung am 1. November 1997 in Kraft. Diese Verordnung umfasst z.B. die Verfahren bei Erteilung, Rücknahme und Widerruf von Genehmigungen, die Kosten, die Antragsverfahren bei Vergabe von Zertifikaten, die Erzeugung und Speicherung von Signaturschlüsseln und Identifikationsdaten, die Übergabe von Signaturschlüsseln und Identifikationsdaten, die Gültigkeitsdauer von Zertifikaten, die Öffentliche Verzeichnisse von Zertifikaten, die Verfahren zur Sperrung von Zertifikaten, die Zuverlässigkeit des Personals, den Schutz der technischen Komponenten, ein Sicherheitskonzept, die Dokumentation, die Anforderungen und Prüfung der technischen Komponenten usw.

Der Paragraph für die Erzeugung und Speicherung von Signaturschlüsseln und Identifikationsdaten schreibt dem Erzeuger eines Signaturschlüssel-Inhaber vor, die Zertifizierungsstelle zu überzeugen, dass der Inhaber des Signaturschlüssel für die Speicherung und Anwendung geeignet ist. Des Weiteren muss der Inhaber

[7] http://www.netlaw.de/gesetze/sigg.htm

geeignete technische Komponenten nach dem Signaturgesetz und dieser Verordnung einsetzen.

Der Paragraph über die Gültigkeit eines Zertifikates lässt die Lebensdauer eines Zertifikates nach fünf Jahren enden. Wenn die Gültigkeit des Signaturschlüssel-Zertifikates abgelaufen ist, endet daraus resultierend auch die Gültigkeit aller zugehörigen Attribut-Zertifikate.

Der Paragraph zur Dokumentation schreibt vor, dass die entstandene Dokumentation nach §10 des Signaturgesetzes für eine Dauer von 35 Jahren nach Ausstellung des Signaturschlüssels zu speichern ist.

Im Paragraph zur Kontrolle der Zertifizierungsstelle wird vorgeschrieben, dass die besagte Stelle eine Prüfung alle zwei Jahre veranlassen und den daraus entstandene Prüfungsbericht an die zuständige Behörde weiterleiten muss.[8]

2 Zusammenwirken / Konzeption (Entwurf)

Bei der Public-Key Verschlüsselung kommen zwei Arten von Schlüsseln zum Einsatz. Sowohl der Empfänger als auch der Sender besitzen einen Public- und einen Private-Key. Der Public-Key vom Empfänger der verschlüsselten Nachricht, wird dem Sender zur Verfügung gestellt. Dieser verschlüsselt die Nachricht mit dem Public-Key des Empfängers. Um diese wieder entschlüsseln zu können wird der Private-Key des Empfängers benötigt. Dadurch kann niemand anderes als der Empfänger die Nachricht wieder entschlüsseln, auch nicht der Sender, da ihm der Private-Key fehlt.

Das Arbeiten mit zwei unterschiedlichen Schlüsseln zum Ver-und Entschlüsseln nennt man asymmetrisches Verschlüsselungsverfahren. Diese „…sind derzeit kaum zu knacken, da die besten Verfahren auf Schlüsseln basieren, die durch Primzahlzerlegung 200stelliger Zahlen erzeugt werden. Selbst Superrechner brauchen für das Neuberechnen der Schlüssel aus dem Schlüsseltext viele Jahre.“[9]

Neben dem Verschlüsseln, wird die PKI auch zur digitalen Signatur benutzt, welche dem Empfänger es erlaubt den Sender der Nachricht zu authentifizieren.

Bei der Identifikation an Systemen stellt sich immer wieder die Frage, ob wahre Identität mit der vorgegebenen übereinstimmt. Um dieses sicher zu stellen gibt es Zertifikate. Bei einem Zertifikat handelt es sich um einen Public-Key bei dem eine dritte Partei mit ihrer digitalen Unterschrift bestätigt, dass die angegebene Identität korrekt ist. Diese dritte Partei ist die Certifikation-Authority (CA).

Für die CA haben sich die von der International Telecommunications Union (ITU) und der ISO standardisierten x509-Zertifikate etabliert. Ein x509-Zertifikat stellt eine

[8] http://www.online-recht.de/vorges.html?SigV
[9] http://www.net-lexikon.de/Public-Key-Verschluesselung.html

Verbindung zwischen einer Identität in Form eines ‘x500 Distinguished Name’ (DN) und einem Public Key her. Durch die digitale Signatur einer x509 Certification Authority (CA) wird diese Verbindung beglaubigt.[10]

3 Organisations-Modelle

3.1 Root-CA

Durch die Einführung des PKI in Unternehmen sowie in den öffentlichen Behörden entstanden in der Regel hierarchisch strukturierte PKIs. Die Root-CA stellt hierbei die Wurzel der Vertrauensbasis dar, denn die Gültigkeitsprüfung der Zertifikate hängt von der Gültigkeit des Root CA-Zertifikats ab.

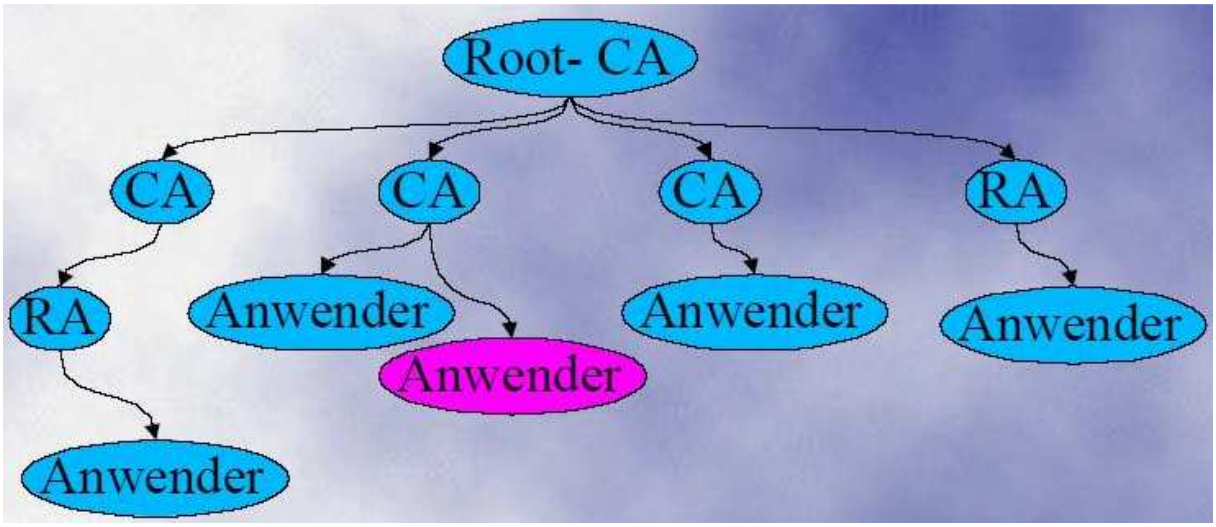

Abbildung 1: Root CA

Diese Stammzertifizierungsstelle ist getrennt vom Netz. Die Daten werden verschlüsselt gehalten und können gegebenenfalls in CA und RA unterschieden werden (Bsp. OpenCA). Der Datenaustausch zu niedrigeren Ebenen erfolgt über Wechselmedien (z.B. USB-Stick). Durch die Getrennte Haltung des Root-CAs ist die Zertifikatlebensdauer sehr hoch.[11]

Die Root-CA signiert die Sub-CA eine Ebene tiefer. Diese Sub-CA erhält das Root-CA bzw. dessen „Fingerprint“ in Form einer persönlichen Registrierung und Ausstellung seines Teilnehmerzertifikates. Dieses Root-CA-Zertifikat ist in der Regel in der Anwendungssoftware mit enthalten und wird damit ausgeliefert und installiert. Durch die Nutzerregistrierung bzw. die Auslieferung der Anwendungssoftware auf einem Wechselmedium kann die Authentizität des Root-CA-Zertifikats sichergestellt werden. Somit kann eine sichere Übertragung stattfinden.[12]

[10] http://www.heise.de/ct/02/05/216/)
[11] www.iid.de/rahmen/sigv.pdf
[12] www.gwdg.de/forschung/veranstaltungen/workshops/ security_ws_2003/pki-vortrag.pdf

3.2 Bridge-CA

Bestehende Public-Key-Infrastrukturen der einzelnen Organisationen werden miteinander verknüpft, indem bereits ausgegebene Zertifikate eingebunden werden. Ein Unternehmen meldet sich an und kann nach seiner Aufnahme sofort mit allen anderen Teilnehmern sicher kommunizieren - ohne mit jedem einzelnen Unternehmen langwierige Gespräche zu führen oder Verträge schließen zu müssen. Damit erlaubt die European Bridge-CA organisationsübergreifende PKI-Lösungen. Eine Anwendung hierfür ist der Austausch von signierten und verschlüsselten E-Mails.

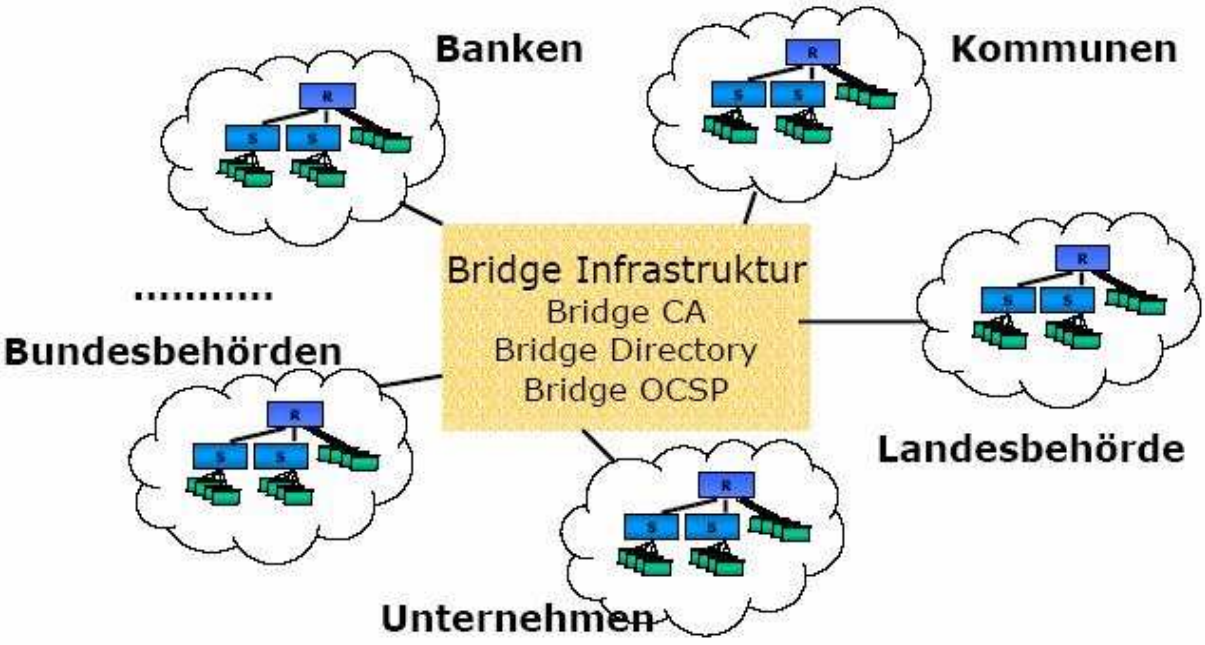

Abbildung 2: Bridge CA

Ein neutrales Gremium entscheidet über die Anbindung einer bestehenden Public-Key-Infrastruktur an die European Bridge-CA. Sowohl Hardware- als auch Software-Zertifikate sind zulässig. Langfristig wird ein Übergang auf Chipkarten angestrebt, um auch den Anforderungen des Signaturgesetzes zu genügen. Das Gremium vertritt pragmatisch die Interessen der Mitglieder und Anwender. Da die vorhandene PKI und bereits ausgegebene Zertifikate weiterhin genutzt werden können, sind diesbezüglich im Unternehmen getätigte Investitionen geschützt.

Gleichzeitig ist das Gremium ein Forum für den Austausch von Erfahrungen. Diese Plattform eignet sich auch für Organisationen, die noch keine Public-Key-Infrastruktur haben, vor allem bei Aufbau und Betrieb einer solchen.[13]

Der Zugriff auf Teilernehmer- bzw. User-Zertifikaten erfolgt über das Bridge Directory Service.

[13] http://www.bridge-ca.de/

Die Validierung der Zertifikate wird über den Bridge OCSP Service geregelt.

Die Bridge Infrastruktur erfordert für die Organisation einen Bridge Service und eine Standardisierung (ISIS-MTT; ETSI) der verschiedenen PKIen. Daraus folgt eine flexible Anbindung der verschiedenen PKIs untereinander.[14]

3.3 Broker-Modell

In der Praxis ist es nicht vorstellbar, dass alle untereinander Roaming-Abkommen abschließen. Als Lösung bieten sich Broker Modelle (Broker, engl. Vermittler) an. Diese erlauben den lokalen Servern im Extremfall ihre Sicherheitsbeziehungen auf eine einzige zum Broker zu reduzieren. Denkbar sind auch mehrstufige Broker-Architekturen, damit die Skalierbarkeit in großen Netzwerken gewährleistet bleibt.

Kritisch beim Einsatz von Brokern ist die Garantie von Sicherheit bei der Übertragung. Sie kann entweder durch hop-by-hop- oder Ende-zu-Ende-Sicherheitsbeziehungen realisiert werden. Hop-By-hop bedeutet, dass jeder Knoten nur den Port des nächsten Knoten weiß.

In jedem Fall steigt die Zahl der benötigten Bestätigungen bevor mit dem Datenaustausch begonnen werden kann, was zu höherer Latenz führt. Dies ist bei zeitkritischen Anwendungen unbedingt zu beachten.

Der Broker ermöglicht ein Zusammenarbeiten zwischen den Servern, ohne dass eine direkte Sicherheitsbeziehungen zwischen diesen bestehen muss. Damit kann die geforderte Skalierbarkeit zwischen unabhängigen Domänen erreicht werden.

Die Aufgabe des Brokers ist eine Vertrauensbasis zwischen fremden Domänen zu schaffen.

Für Informationsdaten, die einen substantiellen Paketverlust erfahren können, müssen Übertragungswiederholungen an Zwischenstationen vorgesehen werden, um Verzögerungen zu vermeiden.

Obwohl für den Transport zwischen den Servern ein Broker eingeschaltet wird, muss die Ende-zu-Ende-Sicherheit erhalten bleiben.

Auch der Transport verschlüsselter Daten, wie Schlüssel, zwischen den Servern muss garantiert werden.[15]

[14] WWW.SECUMEDIA.DE/ITSA/HANDOUT/2003/ BL_DI_14_30_STOERTKUHL.PDF
[15] HTTP://WWW.UBKA.UNI-KARLSRUHE.DE/VVV/IRA/2001/13/13.PDF

4 Glossar

CA	Certificate Authority
Cipher	engl. Chiffrierung; Chiffre (frz: Ziffer, Kennwort bzw. Geheimzeichen)
ETSI	European Telecommunications Standards Institute, Standardisierung von Zertifikatsprofilen [Europa]
ITU	International Telecommunications Union
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
PKI	Public-Key Infrastruktur
RA	Registration Authority
SSL	Secure Socket Layer
TLS	Transport Layer Security

5 Quellenverzeichnis

[1] WWW.SPENNEBERG.ORG/VPN-BOOK/VPN_KAP8.PDF

[2] WWW.KFUNIGRAZ.AC.AT/ZID/SICHERHEIT/INFRASTRUKTUR/ UNIGRAZ-PKI-PROJEKTPLAN_V1.3.1.PDF

[3] WWW.FRANKEN.DE/DE/VERANSTALTUNGEN/ KONGRESS/2000/KNF-CA.PDF

[4] WWW.FRANKEN.DE/DE/VERANSTALTUNGEN/ KONGRESS/2000/KNF-CA.PDF

[5] http://www.xtelligent.de/wissen/steckbriefe/oss_openca.htm

[6] http://www.xtelligent.de/wissen/steckbriefe/oss_openssl.htm

[7] http://www.netlaw.de/gesetze/sigg.htm

[8] http://www.online-recht.de/vorges.html?SigV

[9] http://www.net-lexikon.de/Public-Key-Verschluesselung.html

[10] http://www.heise.de/ct/02/05/216/)

[11] www.iid.de/rahmen/sigv.pdf

[12] www.gwdg.de/forschung/veranstaltungen/workshops/ security_ws_2003/pki-vortrag.pdf

[13] http://www.bridge-ca.de/

[14] WWW.SECUMEDIA.DE/ITSA/HANDOUT/2003/ BL_DI_14_30_STOERTKUHL.PDF

[15] HTTP://WWW.UBKA.UNI-KARLSRUHE.DE/VVV/IRA/2001/13/13.PDF