Zertifizierungs-infrastruktur für die PKI-1-Verwaltung

Umsetzungskonzept für die Anwendung von SSL

Version 1.4
Stand 10.12.2002

Hans-Joachim Knobloch
Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
knobloch@secorvo.de

Dr. Andreas Schmidt
Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
D-53175 Bonn
Andreas.Schmidt@bsi.bund.de

Inhaltsübersicht

Abkürzungen

ADV	Automatisierte Datenverarbeitung
AES	Advanced Encryption Standard
AG	Arbeitsgruppe
ASN.1	Abstract Syntax Notation Number 1
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CBC	Cipher Block Chaining
CDP	CRL Distribution Point
CN	Common Name
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DN	Distinguished Name
DNS	Domain Name Service
DAS	Digital Signature Algorithm
HSM	Hardware Security Modul
HTTP	HyperText Transfer Protocol
ISIS	Industrial Signature Interoperability Specification
KoopA ADV	Kooperationsausschuss ADV Bund/Länder/Kommunaler Bereich
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest No. 5
MTT	MailTrusT
OID	Object Identifier (nach ASN.1)
OCSP	Online Certificate Status Protocol
PCA	Policy Certification Authority
PKCS	Public Key Cryptography Standard (Industriestandards der RSA Security Inc.)
PIN	Persönliche Identifikations-Nummer
PKI	Public Key Infrastruktur

PSE	Personal Security Environment
RC4	Ron's Cipher No. 4, Verschlüsselungsalgorithmus nach Ron Rivest
RFC	Request For Comments
RSA	Kryptoverfahren nach Rivest, Shamir und Adleman
SHA	Secure Hash Algorithm
SPKAC	Signed Public Key And Challenge
SSL	Secure Sockets Layer
TAN	Transaktions-Nummer
TLS	Transport Layer Security
VS	Verschlusssache
VS-NfD	Verschlusssache – NUR FÜR DEN DIENSTGEBRAUCH

Änderungshistorie

Version	Datum	Änderung	Autor
1.0	30.09.02	Erste vollständige Version	Knobloch
1.1	15.10.02	Einarbeitung Anmerkungen Herr Schmidt (BSI) Aufgeteilt in „Umsetzungskonzept für die Anwendung von SSL" und „Regelungen für die Anwendung von SSL"	Knobloch
1.2	17.10.02	Einarbeitung Anmerkungen Herr Schmidt (BSI)	Knobloch
1.3	21.11.02	Einarbeitung Anmerkungen aus der internen Kommentierung durch das BSI	Knobloch
1.4	10.12.02	Einfügen Anmerkungen von Herrn Jeß, Finanzbehörde, Hamburg	Andreas Schmidt (Ref. I 1.3, BSI)

1 Einleitung

In diesem Dokument werden das Konzept zur technischen und organisatorischen Umsetzung der Verwendung von SSL-Zertifikaten innerhalb der PKI-1-Verwaltung und die daraus folgenden Regelungen dargestellt. Dieses Konzept umfasst folgende Punkte:

- Generische Verfahren zur Verteilung der Zertifikate an die Clients und Server. Hier werden Möglichkeiten zur Verteilung und zum Import von Zertifikaten sowie zur Löschung nicht mehr benötigter Zertifikate betrachtet.
- Ein Realisierungskonzept zur Bereitstellung der SSL-Funktionalitäten für die beiden Referenzszenarien „WWW-Client-Server-Kommunikation mit einseitiger Authentisierung“ und „WWW-Client-Server-Kommunikation mit beidseitiger Authentisierung“.
- Eine Einführungsstrategie (Roll-Out-Grobkonzept) für SSL. Dieses Grobkonzept gibt einen Überblick über notwendige Maßnahmen und Voraussetzungen, die erfüllt sein müssen, um SSL-Zertifikate verwenden zu können.

Die Regelungen für die Anwendung von SSL [Regelungen] wurden aus dem vorliegenden Umsetzungskonzept gewonnen. Zur besseren Lesbarkeit wurden textliche Übereinstimmungen beibehalten und nicht durch Querverweise ersetzt. Bei künftigen Änderungen und ggf. abweichenden Formulierungen sind jedoch allein die Regelungen für die Anwendung von SSL in der jeweils aktuellen Version maßgeblich.

2 Verwaltung von Zertifikaten und geheimen Schlüsseln

Damit ein Server und ein Client per SSL gesichert kommunizieren können, ist es nicht erforderlich, dass der Client das Serverzertifikat vorab kennt und umgekehrt, da die Zertifikate beim SSL-Verbindungsaufbau ausgetauscht werden.

Damit die ausgetauschten Zertifikate allerdings geeignet überprüft werden können, müssen bestimmte Wurzel- und CA-Zertifikate vorab verteilt werden. Außerdem muss natürlich jeder Client und jeder Server sein eigenes Zertifikat installiert haben. Je nach Ort der Schlüsselgenerierung ist außerdem eine gesicherte Verteilung der geheimen Schlüssel erforderlich.

Die Verteilung von Zertifikaten kann getrennt nach Server und Client betrachtet werden. Während für die Installation bzw. Löschung von Zertifikaten auf Servern in der Regel Fachpersonal zur Verfügung steht und vergleichsweise wenige Systeme betroffen sind, betrifft die Verteilung von Zertifikaten an Clients potenziell eine Vielzahl von Systemen, von deren Benutzern keine besonderen Vorkenntnisse vorausgesetzt werden können.

2.1 Verteilung von Zertifikaten an Server

Jeder SSL-Webserver benötigt einen geheimen Schlüssel, sein zugehöriges Serverzertifikat und die dazugehörige Kette von CA-Zertifikaten bis zum Wurzelzertifikat. Falls eine Anwendung auf dem betreffenden Server eine SSL-Clientauthentisierung erfordert, müssen darüber hinaus die Wurzelzertifikate zu den Clientzertifikaten importiert werden.

2.1.1 Serverzertifikate und Schlüssel

Die technischen Abläufe bei der Verteilung von Serverzertifikaten und Schlüsseln müssen sich nach den individuellen Gegebenheiten der jeweiligen Zertifizierungsinstanz und des jeweiligen Servers richten und können hier nicht verbindlich festgelegt werden. Es müssen aber in jedem Fall die für

Gruppenzertifikate festgelegten Regelungen (vgl. [GrReg]) zum Schutz der geheimen Schlüssel bei Transport und Speicherung zur Anwendung kommen.

In der Regel wird einer der folgenden Mechanismen zum Einsatz kommen:

- Falls die Schlüssel von der Zertifizierungsinstanz generiert werden, werden geheimer Schlüssel, Serverzertifikat und Zertifikatskette in Form einer passwortgeschützten PKCS#12-Datei an den Schlüsselinhaber (Server-Administrator) übermittelt. Dieses Datenformat kann dann in den Webserver (beispielsweise Microsoft IIS oder Apache/mod_SSL) importiert werden.
  Bei der Übermittlung des Transportpassworts zu der PKCS#12-Datei sollte genau so verfahren werden, wie dies auch im Fall von E-Mail-Zertifikaten vorgesehen ist.
- Falls die Schlüssel vom Schlüsselinhaber (Server-Administrator) mittels der Server-Software generiert werden, wird ein Zertifizierungsantrag im PKCS#10-Format erzeugt, der an die Zertifizierungsinstanz übermittelt wird. Diese übermittelt das ausgestellte Serverzertifikat und die zugehörige Zertifikatskette als PKCS#7-Datei, die in den Webserver (beispielsweise Microsoft IIS, SunONE/iPlanet oder Apache/mod_SSL) importiert werden kann.

2.1.2 Gültigkeitsdauer von Serverzertifikaten

Die Gültigkeit der SSL-Serverzertifikate ist auf maximal ein Jahr beschränkt.

Die generelle Verpflichtung zur Feststellung der Sperrung von Serverzertifikaten auf Seiten des SSL-Clients bleibt hiervon unberührt.

2.1.3 Sperrung von Serverzertifikaten und Löschen von geheimen Schlüsseln

Der Schlüsselverantwortliche (bei Serverzertifikaten in der Regel der Server-Administrator) veranlasst bei Vorliegen eines Sperrgrunds (vgl. [Policy, Kapitel 5.4.1] und [GrReg, Kapitel 3.2 und 3.4]) die Sperrung des jeweiligen Server-zertifikats durch Meldung bei der betreffenden Zertifizierungsstelle.

Der Schlüsselverantwortliche ist dazu verpflichtet, bei Benachrichtigung über die Sperrung seines Serverzertifikats das Zertifikat und den zugehörigen geheimen Schlüssel unverzüglich aus dem Webserver zu löschen und alle zugehörigen Hardware-PSEs (Smartcard, Token) einzuziehen.

2.1.4 Feststellung der Sperrung von Serverzertifikaten

Grundsätzlich sind die Verantwortlichen für den Einsatz von SSL-Clients (Browsern) zur Feststellung der Sperrung von SSL-Serverzertifikaten anhand von Sperrlisten der jeweiligen Zertifizierungsstellen verpflichtet. Eine automatisierte Auswertung von Sperrlisten wird von den derzeit verfügbaren Browsern jedoch nur unzureichend unterstützt. Daher wird folgende Regelung getroffen:

- Wenn eine automatisierte Verarbeitung von Sperrlisten vom Browser unterstützt wird (z.B. vom Microsoft Internet Explorer unter Windows 2000 mit einem LDAP-Verzeichnis oder unter Windows NT mit einem Active-Directory-Verzeichnis), ist diese einzusetzen.
- Andernfalls muss abhängig von den individuellen Gegebenheiten der jeweiligen System- und Netzwerkumgebung eine andere Lösung eingerichtet werden:
    - Soweit möglich sollte der Systemadministrator die aktuellen Sperrlisten über Netzwerk in den fertig installierten Browser eines Benutzers einspielen (z.B. durch Überschreiben der Datei „cert7.db“ beim Netscape-Browser oder durch Verteilung über das Active Directory einer Windows 2000 Domäne beim Microsoft Internet Explorer).
    - Falls der Systemadministrator diese Möglichkeit nicht hat, muss dem Endanwender der Download und die manuelle Installation der aktuellen Sperrlisten ermöglicht werden (z.B. über HTTP-Link und eine Wizard-Oberfläche des Netscape Navigator oder durch Download und Nutzung der Importfunktion des Zertifikatsmanagements beim Internet Explorer). Es liegt dann in der Verantwortung des Endanwenders, diese

Sperrlisten zu nutzen. Sobald der verantwortliche Systemadministrator Kenntnis von der Sperrung eines Serverzertifikats erlangt, sollte er die betroffenen Endanwender (z.B. per E-Mail) informieren und zur Installation der betreffenden Sperrliste im Browser auffordern.

Darüber hinaus können und sollten sensibilisierten Endanwendern von der jeweiligen Zertifizierungsstelle je nach Anwenderkreis mehrere, zum Bürger hin möglichst alle der im folgenden aufgelisteten Möglichkeiten für eine Abfrage des Zertifikatsstatus angeboten werden:

- automatischer Sperrlistenimport via CDP-Erweiterung mit LDAP-URL (z.B. beim Internet Explorer),
- künftig ggf. automatische Sperranfrage via OCSP (derzeit nur vom Netscape Browser ab Version 6.1 unterstützt) und
- manueller Sperrlistenimport via HTTP (z.B. über HTTP-Link und eine Wizard-Oberfläche des Netscape Navigator oder durch Download und Nutzung der Importfunktion des Zertifikatsmanagements beim Internet Explorer).

2.1.5 Import von weiteren Wurzelzertifikaten in Server

Sofern Server- und Clientzertifikate auf dasselbe vertrauenswürdige Wurzelzertifikat zurückgehen (im Regelfall ein Wurzelzertifikat der PCA-1-Verwaltung), wird dies bei der Einrichtung des Serverzertifikats mit importiert und kann auch für die Clientauthentisierung mit verwendet werden. Je nach verwendeter Server-Software (z.B. bei SunONE/iPlanet oder Apache/mod_SSL) muss das jeweilige Wurzelzertifikat dazu in der jeweiligen Server-Konfiguration speziell für die Clientauthentisierung freigegeben werden.

In jedem Fall liegt es in der Verantwortung des Server-Administrators sich (z.B. durch Vergleich eines Fingerprints) von der Authentizität des entsprechenden Wurzelzertifikats zu überzeugen, bevor es für eine Clientauthentisierung eingesetzt wird.

2.2 Verteilung von Zertifikaten an Clients

SSL-Clients (Browser), die für eine Clientauthentisierung verwendet werden sollen, benötigen einen geheimen Schlüssel, das zugehörige Clientzertifikat und die dazugehörige Kette von CA-Zertifikaten bis zum Wurzelzertifikat, einem Zertifikat der PCA. Dies ist im Regelfall gleichzeitig das Wurzelzertifikat für die Serverauthentisierung.

Clients, die ausschließlich für Anwendungen ohne Clientauthentisierung verwendet werden, benötigen lediglich die PCA-Wurzelzertifikate, auf die die Serverzertifikate zurückgehen.

2.2.1 Clientzertifikate und Schlüssel

Die technischen Abläufe bei der Verteilung von Clientzertifikaten und Schlüsseln müssen sich nach den individuellen Gegebenheiten der jeweiligen Zertifizierungsinstanz und des jeweiligen Clients richten und können hier nicht verbindlich festgelegt werden. Es wird jedoch empfohlen, falls möglich wie folgt vorzugehen:

- Die Schlüssel werden von der Zertifizierungsinstanz generiert und zusammen mit dem Clientzertifikat und der Zertifikatskette (inklusive Wurzelzertifikaten) als passwortgeschützte PKCS#12-Datei an den Zertifikatsinhaber übermittelt, der diese in seinen Browser (beispielweise Microsoft Internet Explorer, Netscape oder Opera) importieren kann.
  Die bei dieser Vorgehensweise mit installierten Wurzelzertifikate der PCA-1-Verwaltung dienen gleichzeitig als Vertrauensanker für die Serverauthentisierung.
  Bei der Übermittlung des Transportpassworts zu der PKCS#12-Datei sollte genau so verfahren werden, wie dies auch im Fall von E-Mail-Zertifikaten vorgesehen ist.
- Die Schlüssel werden im Browser generiert und online über ein von der Zertifizierungsstelle angebotenes Web-Formular ein Zertifizierungsantrag (Format PKCS#10 bei Microsoft Internet Explorer, SPKAC bei Netscape und

Opera) gestellt. Das daraufhin ausgestellte Clientzertifikat und die Zertifikatskette werden dann ebenfalls online per HTTP zum Download angeboten (i. d. R. im Format PKCS#7). Um die Authentizität der auf diesem Wege installierten Zertifikate zu sichern, sollte der Zertifikatsdownload über eine SSL-Verbindung mit Serverauthentisierung erfolgen.
D.h. bei dieser Vorgehensweise müssen die Wurzelzertifikate der PCA-1-Verwaltung als Vertrauensanker für die Serverauthentisierung bereits im Browser installiert sein.

2.2.2 Feststellung der Sperrung von Clientzertifikaten

Im Rahmen der SSL-Clientauthentisierung muss ein SSL-Server feststellen, ob das vorgelegte Clientzertifikat gesperrt ist. Die Feststellung der Sperrung der Clientzertifikate auf der Seite des Serverbetreibers erfolgt durch die Auswertung von Sperrlisten der jeweiligen Zertifizierungsinstanzen auf dem Webserver, der die Clientauthentisierung realisiert. Es liegt in der Verantwortung des jeweiligen Server-Administrators, dass die jeweils gültigen Sperrlisten zur Verarbeitung vorliegen.

Dies kann auf mehrere Arten realisiert werden:

- Sofern vom eingesetzten Produkt unterstützt (z.B. Microsoft IIS) können die Sperrlisten automatisch per LDAP über eine in der CDP-Erweiterung der Zertifikate angegebene URL bezogen werden.
  Dazu muss allerdings der Zugriff auf das im CDP referenzierte Verzeichnis gegeben sein.
- Andernfalls muss der Server-Administrator einen Prozess einrichten, um jeweils rechtzeitig vor Ablauf der vorliegenden Sperrliste (oder häufiger) die aktuellen Sperrlisten aus einem Verzeichnis zu beziehen, in das die jeweilige Zertifizierungsstelle diese eingestellt hat, und in den Server zu importieren. Dabei können die Sperrlisten grundsätzlich über das bestehende LDAP-Verzeichnis oder den HTTP-Server entsprechend dem Verzeichnisdienstkonzept der PKI-1-Verwaltung bezogen werden.

Es bietet sich an, diesen Prozess der Sperrlistenaktualisierung zu automatisieren (z.B. über Skripte etc.).

2.2.3 Wurzelzertifikate zu Serverzertifikaten

Sofern die zu den Serverzertifikaten gehörigen Wurzelzertifikate nicht bei der Installation des Clientzertifikates mit installiert wurden (z.B. weil der betreffende Browser ausschließlich in Anwendungen ohne Clientauthentisierung verwendet wird), müssen sie auf andere Weise importiert werden. Soweit möglich soll der Endanwender nicht mit der vertrauenswürdigen Installation von Wurzelzertifikaten belastet werden. Wie dies umgesetzt werden kann, richtet sich nach den individuellen Gegebenheiten der jeweiligen System- und Netzwerkumgebung und kann hier nicht eindeutig festgelegt werden. Folgende Mechanismen könnten ggf. verwendet werden (in der anwendenden Organisation werden hierzu geeignete Regelungen erlassen):

- Die Wurzelzertifikate können vom Systemadministrator über Netzwerk in den fertig installierten Browser eines Benutzers eingespielt werden (z.B. durch Überschreiben der Datei „cert7.db“ beim Netscape-Browser, die die installierten Zertifikate enthält, oder durch Verteilung über das Active Directory einer Windows 2000 Domäne beim Microsoft Internet Explorer).
- Die Wurzelzertifikate werden über ein Software-Managementsystem innerhalb eines Administrationsbereichs (Rechnernetzes) verteilt, das eine „Muster-Installation“ des passend konfigurierten Browsers auf den angeschlossenen Systemen repliziert.
- Die Wurzelzertifikate werden in eine installationsfähige (d.h. aus Setup-Dateien bestehende) angepasste Version des Browsers („Corporate Edition“) eingebracht und im Zuge der normalen Browser-Installation automatisch mit installiert.

  Eine solche Corporate Edition kann für den Microsoft Internet Explorer mit dem „Internet Explorer Administration Kit“ zusammengestellt werden.

In jedem Fall muss der ausführende Systemadministrator besondere Sorgfalt auf die Verifikation der Authentizität der zu installierenden Wurzelzertifikate legen.

Als Rückfallmöglichkeit muss der Endanwender in die Lage versetzt werden, die Wurzelzertifikate selbst zu installieren. Dazu ist für Clients innerhalb und außerhalb des Bereichs der öffentlichern Verwaltung eine Möglichkeit zum Download der Wurzelzertifikate per HTTP zu schaffen. Alle gängigen Browser beherrschen den Import von Zertifikaten per Download in den Formaten DER oder PKCS#7. Die zugehörigen Fingerprints zur Prüfung der Authentizität der Wurzelzertifikate sind bereits an diversen Stellen publiziert.

3 Realisierungskonzept

Im Folgenden wird das Realisierungskonzept zur Bereitstellung der SSL-Funktionalitäten für die beiden Referenzszenarien „WWW-Client-Server-Kommunikation mit einseitiger Authentisierung“ und „WWW-Client-Server-Kommunikation mit beidseitiger Authentisierung“ dargestellt, insbesondere Anforderungen und Empfehlungen, die sich aus den Sicherheitsvorgaben der PKI-1-Verwaltung ableiten.

3.1 Szenario „WWW-Client-Server-Kommunikation mit einseitiger Authentisierung“

Betrachtet wird in diesem Szenario der gesicherte Datenaustausch zwischen Behörde und Kommunikationspartner (Bürger, Wirtschaft, Behörde) über eine verschlüsselte WWW-Client-Server-Verbindung in einer heterogenen offenen Netzlandschaft. Dabei findet eine einseitige Authentisierung des Behörden-Servers gegenüber dem Client des Kommunikationspartners statt, damit sich dieser davon überzeugen kann, dass er tatsächlich mit dem Behörden-Server verbunden ist. Gewahrt werden soll dabei die Vertraulichkeit und Integrität der übertragenen Daten sowie die Authentizität des Datenursprungs (Server).

3.1.1 Allgemeine Sicherheit des SSL-Servers

Als eine Grundlage der Sicherheit von SSL-Anwendungen ist die allgemeine logische und physikalische Sicherheit des SSL-Servers zu gewährleisten (insbesondere mit Blick auf den Schutz des geheimen SSL-Schlüssels). Die hierfür zu ergreifenden Maßnahmen hängen stark von individuellen Gegebenheiten ab und können hier nicht allgemein festgelegt werden. Es wird empfohlen, insbesondere folgende Punkte zu beachten:

- Grundsätzlich müssen Aufbau, Umgebung und Betrieb des Servers zumindest IT-Grundschutzniveau (siehe [GSHB]) genügen. Je nach Anwendung sind darüber hinaus ggf. weitere Regelungen und

Sicherheitsanforderungen (z.B. für Daten des VS-Grads VS-NfD) im Sicherheitskonzept für das jeweilige LAN zu beachten.

- Je nach Anwendung, Aufbau oder Einbindung des SSL-Servers kann es erforderlich sein, den SSL-Server mit einer Firewall, Filterung aktiver Inhalte und /oder einem Virenschutz zu koppeln, z.B.
  - wenn von den Clients beliebige Informationen auf dem Server abgelegt werden können oder
  - wenn der Kreis der berechtigten Nutzer schlecht überschaubar oder mit vorsätzlichen Handlungen der Nutzer zu rechnen ist (z.B. bei Servern, die über das Internet erreicht werden können).
- Bei Servern mit erhöhtem Schutzbedarf wird empfohlen, den Server ausschließlich für die SSL-Anwendung einzusetzen.

3.1.2 Anforderungen an Server-Produkte

Es dürfen nur solche SSL-Server von CAs der PKI-1-Verwaltung zertifiziert werden, die SSL-Server-Produkte verwenden, die (ggf. unter Berücksichtigung des Betriebssystems) folgende Mindestanforderungen erfüllen:

- Der geheime Schlüssel des Servers muss so verschlüsselt abgespeichert werden, dass er gegen unbefugtes Auslesen geschützt ist (z.B. mit einem von einem Benutzerpasswort abgeleiteten Schlüssel).
  Für Anwendungen mit erhöhtem Sicherheitsbedarf wird empfohlen, eine Smartcard oder ein Hardware Security Modul (HSM) zur Speicherung und Anwendung des geheimen Schlüssels einzusetzen.
- Grundsätzlich muss der Gebrauch des geheimen Schlüssels von einem Mitglied der zugeordneten Gruppe (im Sinne des Gruppenzertifikats; hier in der Regel die Gruppe der Administratoren des betreffenden Servers) beim Start des Servers durch Eingabe eines Passworts autorisiert werden. Das einzusetzende Produkt muss diese Freigabe durch Passwort unterstützen.
  Nur dann, wenn im Einzelfall gemäß [GrReg, Kapitel 3.4] eine Regelung getroffen wird, die einen automatisierten Zugriff auf den geheimen Schlüssel

erlaubt, kann auch ein Produkt eingesetzt werden, das keine derartige Freigabe-Funktionalität unterstützt.

- Server, die für Anwendungen mit Clientauthentisierung verwendet werden, müssen die Verwendung von Sperrlisten der Version CRLv2 zur Prüfung der Gültigkeit von Clientzertifikaten unterstützen.
- Der Server muss SSL 3.0 und/oder TLS 1.0 und mindestens eine der für den jeweiligen Anwendungsbereich zulässigen Cipher Suites (siehe Tabelle 1) unterstützen. Im Sinne einer breiten Interoperabilität muss zumindest die Cipher Suite TLS_RSA_WITH_3DES_EDE_CBC_SHA und darüber hinaus möglichst viele weitere geeignete Cipher Suites unterstützt werden.

Beim Betrieb von SSL-Servern sollten unbedingt regelmäßig alle sicherheitsrelevanten Patches – insbesondere solche, die die Sicherheit der SSL-Implementierung bzw. die Auswertung von SSL-Zertifikaten betreffen – eingespielt werden.

Zulässige SSL/TLS Cipher Suites für IT- Grundschutzniveau	Zulässige SSL/TLS Cipher Suites für die Übertragung von Inhalten des VS-Grades VS-NUR FÜR DEN DIENSTGEBRAUCH[1]
TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_RC4_128_SHA	TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_AES_128_CBC_SHA	TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA	TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_RC4_128_MD5	

Tabelle 1: Zulässige Cipher Suites. Die zu verwendende RSA-Schlüssellänge ergibt sich implizit aus der Schlüssellänge im verwendeten Zertifikat. Hierfür gelten die in [Policy] getroffenen Regelungen zur Schlüssellänge.

Die Eignung einiger verbreiteter Server-Produkte kann der folgenden Tabelle entnommen werden:

[1] Neben der angegebenen grundsätzlichen Eignung der Algorithmen für VS-NfD ist für die Übertragung von Inhalten des VS-Grades VS-NfD über SSL-Verbindungen eine Zulassung oder Einsatzempfehlung des BSI für die Produkte erforderlich

Kriterium	Microsoft Internet Information Server 5.0 unter Windows 2000	Sun ONE Web Server 6.0 (vormals iPlanet WebServer Enterprise)	Apache 1.3.26 mit mod_SSL 2.8.10
Ausreichender Schutz des geheimen Schlüssels	Wird unterstützt. Allerdings ist ein Zugriff auf den geheimen Schlüssel auch für den Windows-Domänen-administrator möglich. Sofern dies im Einzelfall gegen Sicherheits-anforderungen verstößt, muss eine Smartcard oder HSM eingesetzt werden	Wird unterstützt.	Wird unterstützt.
Freigabe des geheimen Schlüssels durch Passwort	Wird nicht unterstützt. Sofern im Einzelfall benötigt, muss eine Smartcard oder HSM mit Freigabe durch PIN eingesetzt werden.	Wird unterstützt.	Wird unterstützt.
CRLv2 Sperrlisten für Clientzertifikate	Wird unterstützt.	Wird unterstützt.	Wird unterstützt.
SSL 3.0/TLS 1.0	Wird unterstützt. Allerdings ist eine Einschränkung auf SSL 3.0 bzw. TLS 1.0 nicht möglich[2].	Wird unterstützt. Eine Einschränkung auf SSL 3.0 bzw. TLS 1.0 ist möglich.	Wird unterstützt. Eine Einschränkung auf SSL 3.0 bzw. TLS 1.0 ist möglich.
Zulässige Cipher Suites	Wird unterstützt. Allerdings kann nicht zwischen Cipher Suites mit MD5 und Cipher Suites mit SHA-1 differenziert werden[3].	Wird unterstützt.	Wird unterstützt.

Tabelle 2: Eignung verschiedener Server-Produkte

3.1.3 Konfiguration des SSL-Servers

Am SSL-Server sind die folgenden Einstellungen vorzunehmen:

- Soweit möglich ist die Verwendung von SSL auf SSL 3.0 und/oder TLS 1.0 zu beschränken.
- Die Auswahl an Cipher Suites ist auf solche zu beschränken, die nach Tabelle 1 zulässig sind.

---

[2] D.h. abhängig von der Konfiguration des Browsers wird möglicherweise SSL 2.0 verwendet.

[3] D.h. es kann serverseitig nicht sichergestellt werden, dass nur die in Tabelle 1 für VS-NfD angegebenen Cipher Suites benutzt werden. Abhängig von der Konfiguration des Browsers kann stattdessen auch die Cipher Suite TLS_RSA_WITH_RC4_128_MD5 benutzt werden. Bei einigen Browsern wird dies in Standard-Konfiguration stets der Fall sein.

- Serverzertifikat, Schlüssel und zugehörige Zertifikatskette müssen installiert werden.
- Soweit erforderlich ist einzustellen, dass der geheime Schlüssel des Servers beim Server-Start durch Passworteingabe freigegeben werden muss.

Darüber hinaus ist die allgemeine logische Sicherheit des SSL-Servers zu gewährleisten (insbesondere mit Blick auf den Schutz des geheimen SSL-Schlüssels). Die hierfür zu ergreifenden Maßnahmen hängen stark von individuellen Gegebenheiten ab und können hier nicht allgemein festgelegt werden. Es wird empfohlen, insbesondere folgende Punkte zu beachten:

- Es wird grundsätzlich empfohlen, den Server ausschließlich für die SSL-Anwendung einzusetzen. Wo dies anwendungsbedingt nicht möglich ist, sollte die Gesamtanordnung mittels eines Sicherheitskonzeptes abgesichert werden.
- Daneben sind generell zumindest die Vorgaben des IT-Grundschutzes ([GSHB]) zu beachten. Im individuellen Fall ggf. höhere Sicherheitsanforderungen sind im Sicherheitskonzept für das jeweilige LAN zu beachten.

3.1.4 Konfiguration der SSL-Clients

Auf den SSL-Clients sind in diesem Szenario lediglich die Wurzelzertifikate zu installieren (vgl. Abschnitt 2.2.3).

Hinweis: Sofern Probleme beim SSL-Verbindungsaufbau auftreten, kann evtl. dadurch Abhilfe geschaffen werden, dass auch die Zertifikate der zwischengelagerten Zertifizierungsstellen in den Client importiert werden.

Siehe hierzu auch die weiteren Sicherheitshinweise im folgenden Abschnitt.

3.1.5 Weitere Sicherheitshinweise

Sofern SSL-Clients über eine Firewall auf SSL-Server zugreifen, ist zu beachten, dass aktive Inhalte (Java, Javascript, ActiveX etc.) und Viren

aufgrund von Verschlüsselung und Integritätsschutz durch SSL – anders als bei unverschlüsselten HTTP-Verbindungen – nicht durch die Firewall blockiert werden können. Es wird daher empfohlen, zusätzliche Sicherheitsmaßnahmen wie z.B. die folgenden zu treffen:

- Deaktivierung der Ausführung aktiver Inhalte in den betroffenen Browsern, soweit möglich durch Vorgabe geeigneter Sicherheitseinstellungen, die von den Endnutzern nicht verändert werden können.
- Realisierung eines umfassenden Virenschutzes für die SSL-fähigen Client-Rechner.
- Einschränkung der über die Firewall zulässigen SSL-Verbindungen auf bestimmte Client-Rechner und auf bestimmte, hinsichtlich der Verwendung aktiver Inhalte und der Verbreitung von Viren hinreichend vertrauenswürdige SSL-Server.

Von der Verwendung von Proxy-Lösungen, die keine durchgängige Transport-Sicherheit zwischen Client und Server gewährleisten, sondern die SSL-Verbindungen an der Firewall terminieren, ist grundsätzlich abzusehen, da hierdurch die Sicherheitsziele von SSL (siehe Abschnitt 3.1.6) unterlaufen werden und zusätzlich im weiteren Szenario mit Clientauthentisierung die geheimen Schlüssel der Clients im Proxy vorliegen müssten. Wenn im Einzelfall doch solche SSL-Proxies eingesetzt werden, weil durch Maßnahmen auf den Endsystemen keine ausreichende Sicherheit gegen aktive Inhalte erzielt werden kann, so muss das Sicherheitskonzept der betreffenden Lösung sicherstellen, dass Benutzer durch dessen Verwendung nicht gegen das Verbot der Weitergabe von geheimen Schlüsseln und zugehörigen PINs bzw. Passwörtern [Policy, Kapitel 3.3] verstoßen.

3.1.6 Erreichte Sicherheitsziele

In diesem Szenario werden die folgenden Sicherheitsziele umgesetzt:

- Authentizität der Servers

- Integrität der vom Server angebotenen Daten (Webseiten, Formulare, Dokumente, Binärdateien etc.)
- Vertraulichkeit und Integrität der vom Client übertragenen Daten (insbesondere ausgefüllte Formulare, Passworte, TANs etc.)

Nicht erreicht werden hingegen:

- Authentizität des Clients (hierzu wäre eine SSL-Clientauthentisierung erforderlich; ggf. kann die Authentizität des Clients jedoch durch alternative Mechanismen wie die Abfrage von Benutzernamen und Passwort, PINs/TANs unter dem Schutz der SSL-Verbindung sichergestellt werden)
- Vertraulichkeit der vom Server angebotenen Daten (da sich prinzipiell jeder Client mit dem Server verbinden kann)

3.2 Szenario „WWW-Client-Server-Kommunikation mit beidseitiger Authentisierung“

Die beidseitige Authentisierung baut auf das Szenario „WWW-Client-Server-Kommunikation mit einseitiger Authentisierung“ auf. Die nachfolgend angegebenen Anforderungen und Schritte verstehen sich daher als Ergänzung zu den oben angegebenen.

3.2.1 Anforderungen an Client-Produkte

Es dürfen nur solche Clients mit Zertifikaten der PKI-1-ausgestattet werden, die die folgenden Mindestanforderungen erfüllen:

- Der geheime Schlüssel des Anwenders muss so verschlüsselt abgespeichert werden, dass er gegen unbefugtes Auslesen geschützt ist (z.B. verschlüsselt mit einem von einem Benutzerpasswort abgeleiteten Schlüssel).

  Für Anwendungen mit besonderen Sicherheitsanforderungen wird empfohlen, eine Smartcard zu verwenden, in der der geheime Schlüssel auslesegeschützt gespeichert und angewendet wird, oder zumindest für

SSL Schlüssel und Zertifikate zu verwenden, die nicht gleichzeitig zum Schutz von E-Mail eingesetzt werden können.

- Der Gebrauch des geheimen Schlüssels muss vom Benutzer durch Eingabe eines Passworts autorisiert werden (mindestens ein Mal pro Browser-Sitzung, besser bei jedem Gebrauch, d.h. bei jeder neuen SSL-Sitzung).
- Es wird empfohlen, den Client so zu konfigurieren, dass ein Import weiterer vertrauenswürdiger Wurzelzertifikate nicht durch den Benutzer, sondern nur durch Administrationspersonal möglich ist (siehe unten). Ist der Import auch durch den Benutzer möglich, darf der Client neue vertrauenswürdige Wurzelzertifikate nicht ohne Autorisierung durch den Benutzer installieren. Der Benutzer muss die Möglichkeit haben, ein vertrauenswürdiges Wurzelzertifikat eindeutig zu identifizieren, z. B. anhand eines Fingerprints.
- Der Client muss SSL 3.0 und/oder TLS 1.0 und mindestens eine der für den jeweiligen Anwendungsbereich zulässigen Cipher Suites (siehe Tabelle 1) unterstützen. Im Sinne einer breiten Interoperabilität sollte zumindest die Cipher Suite TLS_RSA_WITH_3DES_EDE_CBC_SHA unterstützt werden. Je nach Anwendung können darüber hinaus weitere geeignete Cipher Suites unterstützt werden.

Beim Betrieb von SSL-Clients (Browsern) sollten unbedingt regelmäßig alle sicherheitsrelevanten Patches – insbesondere solche, die die Sicherheit der SSL-Implementierung bzw. die Auswertung von SSL-Zertifikaten betreffen – eingespielt werden.

Die Eignung einiger verbreiteter Browser kann der folgenden Tabelle entnommen werden:

Kriterium	Microsoft Internet Explorer 5.5 oder 6.0 unter Windows NT oder Windows 2000	Netscape Communicator 4.79 und Netscape 6	Opera 6.04
Ausreichender Schutz des geheimen Schlüssels[4]	Wird unterstützt. Es muss für den Schutz des geheimen Schlüssels Sicherheitsstufe „hoch“ gewählt und ein zusätzliches Passwort vergeben werden. Ansonsten ist ein Zugriff auf den geheimen Schlüssel auch für den Windows-Domänenadministrator möglich.	Wird unterstützt.	Wird unterstützt.
Freigabe des geheimen Schlüssels durch Passwort	Wird unterstützt.	Wird unterstützt.	Wird unterstützt.
Schutz beim Import von Wurzelzertifikaten	Wird unterstützt.	Wird unterstützt.	Wird unterstützt.
SSL 3.0/TLS 1.0	Wird unterstützt. Eine Einschränkung auf SSL 3.0 bzw. TLS 1.0 ist möglich.	Wird unterstützt (von Netscape 4.79 nur SSL 3.0). Eine Einschränkung auf SSL 3.0 bzw. TLS 1.0 ist möglich.	Wird unterstützt. Eine Einschränkung auf SSL 3.0 bzw. TLS 1.0 ist möglich.
Zulässige Cipher Suites	Wird unterstützt. Allerdings kann nicht zwischen einzelnen Cipher Suites differenziert werden. Die ist jedoch nicht kritisch, da bereits serverseitig die Cipher Suites festgelegt werden.	Wird unterstützt.	Wird unterstützt.
Weiteres	Keine Anmerkungen.	Netscape 4.79 unterstützt keine Umlaute in Distiguished Names von Client- und Serverzertifikaten und verstößt somit gegen die Anforderungen des Namenskonzepts ([Namen]).	Opera unterstützt keine Sperrung von Serverzertifikaten über Sperrlisten und ist daher nur für Anwendungen mit entsprechend niedrigen Sicherheitsanforderungen geeignet.

Tabelle 3: Eignung verschiedener Client-Produkte

3.2.2 Konfiguration des SSL-Clients

Am SSL-Client sind die folgenden Einstellungen vorzunehmen:

[4] Es wurden nur die Sicherheitsfunktionen betrachtet, nicht jedoch die Art und Eignung der konkreten Implementierung in den Browsern.

- Soweit möglich ist die Verwendung von SSL auf SSL 3.0 und/oder TLS 1.0 zu beschränken (siehe Tabelle 3).
- Soweit möglich ist die Auswahl an Cipher Suites auf solche zu beschränken, die nach Tabelle 1 zulässig sind. (Falls dies nicht möglich ist, bestehen jedoch keine Sicherheitsprobleme, da die Server bereits entsprechend konfiguriert sind).
- Clientzertifikat, Schlüssel und zugehörige Zertifikatskette müssen installiert werden.
- Es ist einzustellen, dass der geheime Schlüssel des Clients beim Gebrauch durch Passworteingabe freigegeben werden muss.

Darüber hinaus ist die allgemeine logische Sicherheit des Client-Rechners zu gewährleisten (insbesondere mit Blick auf den Schutz des geheimen SSL-Schlüssels). Die hierfür zu ergreifenden Maßnahmen hängen stark von individuellen Gegebenheiten ab und können hier nicht allgemein festgelegt werden. Es ist jedoch insbesondere auf die in Abschnitt 3.1.5 genannten Aspekte des Schutzes gegen Viren und bösartige aktive Inhalte zu achten.

3.2.3 Konfiguration des SSL-Servers

Auf der Seite des SSL-Servers sind für den Einsatz einer SSL-Clientauthentisierung folgende Einstellungen vorzunehmen:

- Die SSL-Clientauthentisierung muss aktiviert werden. Ob eine Clientauthentisierung obligatorisch oder optional verlangt wird, richtet sich nach den Gegebenheiten des Server-Produkts und den Erfordernissen der einzelnen Anwendung.
- Ggf. muss ein Wurzelzertifikat als Vertrauensanker für die Clientzertifikate installiert oder ein schon installiertes dafür freigegeben werden.
- Es muss eine Prozedur zur Feststellung der Sperrung von Clientzertifikaten durch die Auswertung von Sperrlisten eingerichtet werden.

Damit ist eine SSL-Clientauthentisierung zwischen Browser und Server möglich. Als nächster Schritt muss ggf. auf dem Webserver oder auf nachgeordneten Application Servern die Autorisation, Zugriffsbeschränkung, Ablaufsteuerung und Protokollierung abhängig von dem bei dieser Authentisierung benutzten Clientzertifikat konfiguriert werden. Dieser Schritt muss sich nach den individuellen Erfordernissen der jeweiligen Anwendung richten und wird an dieser Stelle nicht näher betrachtet.

3.2.4 Erreichte Sicherheitsziele

In diesem Szenario werden die folgenden Sicherheitsziele umgesetzt:

- Authentizität der Servers
- Integrität der vom Server angebotenen Daten (Webseiten, Formulare, Dokumente, Binärdateien etc.)
- Vertraulichkeit der vom Server angebotenen Daten (sofern bei nicht erfolgreicher Clientauthentisierung ein Zugriff verweigert wird)
- Authentizität des Clients
- Vertraulichkeit und Integrität der vom Client übertragenen Daten (insbesondere ausgefüllte Formulare, Passworte, TANs etc.)

Nicht erreicht wird hingegen:

- Nichtabstreitbarkeit der vom Client übertragenen Daten (da nicht die übertragenen Dateninhalte vom Client signiert werden, sondern lediglich Schlüsselaustauschdaten beim SSL-Verbindungsaufbau). Eine Nichtabstreitbarkeit kann über SSL generell nicht erreicht werden; sie muss bei Bedarf auf Anwendungsebene sicher gestellt werden und wird hier nicht weiter betrachtet.

4 Roll-Out-Grobkonzept

Da für die Einführung von SSL keine wesentlichen technischen Änderungen an bestehenden CA-Komponenten oder Zertifikaten der PKI-1-Verwaltung erforderlich ist, sind keine Maßnahmen zur technischen Migration erforderlich.

Es müssen lediglich die organisatorischen Regelungen angepasst und entsprechende Maßnahmen zum Roll-Out der neuen Zertifikate ergriffen werden.

4.1 Migration der organisatorischen Regelungen

Die Ausstellung von SSL-Zertifikaten durch die PKI-1-Verwaltung erfordert als vorbereitende Schritte

- die Anpassung der Dokumente der PKI-1-Verwaltung ([Policy],[Namen], [GrReg] und [Formate]) an die Erfordernisse der SSL-Anwendung und
- die Abstimmung dieser angepassten Dokumente mit allen angeschlossenen Zertifizierungsinstanzen (d.h. insbesondere Änderung der Verträge etc.).

Dies sind im wesentlichen organisatorische Schritte; besondere technische Voraussetzungen brauchen nicht geschaffen zu werden.

Verantwortlich für diesen Schritt ist die PCA, die anhand der zur Änderung der Dokumente festgelegten Verfahren die Änderungen an die beteiligten CAs kommunizieren muss.

4.2 Ausstellung von Zertifikaten

4.2.1 Ausstellung neuer SSL-Zertifikate

Vor der Ausstellung von Zertifikaten müssen die CAs die geänderten Regelungen ggf. in ihre lokalen Regelungen und Policies umsetzen.

Anschließend kann jede angeschlossene CA unmittelbar mit der Ausstellung von SSL-Serverzertifikaten und ggf. SSL-Clientzertifikaten (für die ausschließliche Verwendung mit SSL) beginnen.

Die Prozesse zur Ausstellung der Zertifikate und Übermittlung der Schlüssel und Zertifikate an die Endanwender sind grundsätzlich identisch mit denen für die bestehenden persönlichen E-Mail-Zertifikate bzw. die E-Mail-Gruppenzertifikate.

Es steht den einzelnen CAs dabei frei, ob und an wen sie SSL-Zertifikate ausgeben und ob sie über die hier definierten Regelungen hinaus weitere Festlegungen treffen will.

4.2.2 Verwendung von E-Mail-Zertifikaten als SSL-Clientzertifikat

Ein besonders wichtiger Sicherheitsaspekt bei der Benutzung von E-Mail-Zertifikaten und Schlüsseln für die SSL-Clientauthentisierung ist der Schutz der privaten Schlüssel in den jeweils eingesetzten Produkten.

Ein privater Schlüssel, der im Rahmen der SSL-Anwendung durch unzureichende Schutzmechanismen eines SSL-Produkts kompromittiert wird, kann selbstverständlich auch nicht mehr zur Sicherung von E-Mail verwendet werden. Als besonders kritisch ist der Fall einzustufen, dass eine Schlüsselkompromittierung über längere Zeit unbemerkt bleibt.

Um in dieser Hinsicht keine neuartigen Risiken einzugehen, sollten SSL-Clients zum Schutz von privaten Schlüsseln gleichwertige Sicherheitsmechanismen einsetzen wie die bereits im Einsatz befindlichen E-Mail-Produkte. Eine entsprechende Überprüfung gestaltet sich jedoch in der Praxis bedingt durch lückenhafte Information und proprietäre Lösungen der Hersteller sehr schwierig.

Die Verwendung von vorhandenen E-Mail-Zertifikaten und -Schlüsseln für die SSL-Clientauthentisierung soll daher nach einem Beschluss der AG Kommunikation und Sicherheit des KoopA ADV so lange zurückgestellt werden, bis durch die zuständigen Stellen des BSI abschließend geklärt ist, dass das Sicherheitsniveau der zu verwendenden SSL-Clients (Browser) hinsichtlich des

Schutzes der geheimen Schlüssel äquivalent zu dem der eingesetzten E-Mail-Clients (Plugins) ist. Bis dahin sollten nur für SSL bestimmte Zertifikate, sogenannte „SSL-only“-Zertifikate, verwendet werden, die nicht gleichzeitig zur Sicherung von E-Mail dienen. Die Kennzeichnung als ausschließliches SSL-Zertifikat geschieht durch Setzen der entsprechenden Zertifikatserweiterungen (siehe hierzu die SSL-Zertifikatsprofile in [Formate-neu]) und ggf. einen einschränkenden Namens-Zusatz entsprechend den Regelungen in [Namen]. Unabhängig davon, ob Schlüssel zentral oder dezentral generiert werden, muss die zuständige Zertifizierungsinstanz durch organisatorische Maßnahmen zuverlässig feststellen, ob ein SSL-Zertifikat beantragt wurde und das Zertifikat als solches wie oben angesprochen kennzeichnen. Diese Feststellung kann bei zentraler Schlüsselgenerierung z.B. durch einen Vermerk auf dem Antragsformular der Zertifizierungsinstanz erfolgen, bei dezentraler Schlüssel-generierung z.B. implizit aufgrund der Tatsache, dass der Zertifizierungsantrag über eine Web-Schnittstelle aus einem Browser heraus gestellt wurde.

4.3 Einsatz von Zertifikaten

Der Einsatz von SSL-Zertifikaten richtet sich hauptsächlich nach dem auftretenden Bedarf durch konkrete Anwendungen. Welche Anwendungen dies sind und welches der beiden geschilderten Szenarios zum Einsatz kommt, liegt im Verantwortungsbereich der jeweiligen Behörden und CAs.

Für die Einbringung von Wurzelzertifikaten zur Serverauthentisierung in SSL-Clients bietet sich ein zweigleisiges Vorgehen an:

- Die Wurzelzertifikate werden gezielt auf den Client-Rechnern installiert, die für eine bestimmte Anwendung SSL-Serverauthentisierung benötigen.
- Daneben können die Wurzelzertifikate auch ohne direkten Anlass durch eine konkrete Anwendung, sozusagen „vorsorglich“, bei ohnehin anfallenden Updates bzw. Neuinstallationen von Browsern im Bereich der Verwaltung mit installiert werden.

Eine Umstellung von bestehenden Anwendungen mit Passwort-basierter Authentisierung auf SSL-Clientauthentisierung kann in folgenden Migrationsschritten vollzogen werden:

- Nach der Umstellung einer bestehenden Anwendung auf eine web-basierte Benutzerschnittstelle kann diese im Szenario der SSL-Serverauthentisierung genutzt werden, indem die Authentifikation der Anwender über die vorhandenen Benutzernamen und Passworte (unter dem Schutz der SSL-Verbindung) realisiert wird.
  Hierzu muss lediglich das jeweilige Wurzelzertifikat an die betroffenen Web-Clients verteilt werden.
- Im nächsten Ausbauschritt kann eine SSL-Clientauthentisierung optional für die Clients bzw. Anwender eingerichtet werden, die bereits mit Clientzertifikaten ausgestattet sind. Die übrigen Anwender authentisieren sich weiterhin mit Benutzername und Passwort.
- Sobald alle Anwender mit Clientzertifikaten ausgestattet sind, kann die SSL-Clientauthentisierung obligatorisch verlangt werden.

4.4 Unterstützende Maßnahmen der einsetzenden Behörde

Für beide Szenarien sollte die SSL einsetzende Behörde parallel zur technischen Umsetzung alle Beteiligten über die neue Anwendung informieren.

Dabei ist insbesondere darauf zu achten, dass Benutzer ausreichend über den Umgang mit SSL (hier insbesondere über eine ggf. erforderliche Zertifikats-prüfung und über den Umgang mit Fehlermeldungen) informiert werden, damit nicht durch Fehlbedienung das Sicherheitsniveau entscheidend gesenkt wird.

Dazu ist die Erstellung einer Kurzanleitung zu empfehlen, die den konkret verwendeten Browser und die lokale Konfiguration berücksichtigt.

4.5 Unterstützende Maßnahmen der PCA

Unterstützend für einen breiten Einsatz von SSL-Anwendungen mit Zertifikaten der PKI-1-Verwaltung können noch folgende Maßnahmen seitens der PCA in Betracht gezogen werden:

- Eine gezielte Information von System-Administratoren, Betreibern und Anwendungs-Verantwortlichen (z.B. E-Government-Teams) über Möglichkeiten und Regelungen des SSL-Einsatzes in der PKI-1-Verwaltung.
- Die Erstellung bzw. Zusammenstellung von detaillierten Konfigurationshinweisen und Beispielkonfigurationen für verbreitete Server-Systeme als Vorlage für Server-Administratoren.
- Die Erstellung bzw. Zusammenstellung von detaillierten Konfigurationshinweisen für verbreitete Browser als Vorlage für System-Administratoren oder Endanwender.
- Die Bereitstellung eines installierbaren, passend vorkonfigurierten Browsers in Form einer „Corporate Edition“.
- Die Schaffung von Testmöglichkeiten (z.B. Referenz-Server, Testzertifikate) zum Zweck der Validierung einer korrekten Konfiguration von SSL-Komponenten durch deren Betreiber.

5 Referenzen

[GrReg]	Secorvo, BSI: „Regelungen für Gruppenzertifikate“, Version 1.3, Dezember 2002
[Namen]	Secorvo, BSI: „Namensregeln und –formate“, Version 1.3, November 2002
[Formate]	Secorvo, BSI: „Technische Grundlagen der Wurzelzertifizierungsstelle – Formate und Protokolle nach MTTv2“, Version 1.01, 08.03.2001
[Formate-neu]	Secorvo, BSI: „Technische Grundlagen der Wurzelzertifizierungsstelle – Formate und Protokolle nach MTTv2“, Version 2.0, überarbeitete Version für SSL
[Policy]	BSI: „Sicherheitsleitlinien der Wurzelzertifizierungsinstanz der Verwaltung“, Version 3.0, November 2002
[VZK2002]	Secorvo, BSI: V. Hammer, D. Neundorf, A. Rosenhauer: „Zertifizierungsinfrastruktur für die PKI-1-Verwaltung – Verzeichnisdienstkonzept“, Version 1.2, 07.05.2002
[GSHB]	BSI: „IT-Grundschutzhandbuch“, Ausgabe Mai 2002
[Regelungen]	Secorvo, BSI: „Regelungen für den Einsatz von SSL“, Version 1.5, Dezember 2002