

Signaturbündnis

Vorgaben und Konvergenzziele für das Signaturbündnis

Version 1.2

Stand 19. März 2003

Inhaltsübersicht

1	Einleitung	3
2	Übersicht der Vorgaben und Konvergenzziele für das Signaturlbündnis	7
3	Vorgaben und Konvergenzziele	10
3.1	Grundsätzliches Sicherheitsniveau	11
3.2	Technische Anforderungen	12
3.2.1	Anforderungen an die Signaturkarte	12
3.2.2	Anforderungen an den Verzeichnisdienst	12
3.2.2.1	Zugriff auf Signaturprüfchlüssel von Endteilnehmern	12
3.2.2.2	Zugriff auf Verschlüsselungszertifikate von Endteilnehmern	13
3.2.2.3	Zugriff auf Zertifikate von Zertifizierungsdiensteanbietern	13
3.2.2.4	Bereitstellung von Sperrinformationen	14
3.2.2.5	Verteilung von Zertifikaten (oder öffentlichen Schlüsseln) von Wurzelzertifizierungsstellen.....	14
3.2.2.6	Gültigkeitsmodell.....	15
3.3	Organisatorische Anforderungen.....	15
3.3.1	Registrierung und Identifikation des Schlüsselinhabers	15
3.3.2	Ausgabe von Chipkarte und PIN.....	15
3.3.3	Sperrung	16
4	Abkürzungen.....	17
5	Referenzen	19

Ansprechpartner

Dr. Albrecht Rosenhauer, Bundesministerium des Innern, Projektgruppe BundOnline 2005,
Tel. 01888 681-4388, Albrecht.Rosenhauer@bmi.bund.de

1 Einleitung

Zweck des Signaturbündnisses ist es, die Anwendung, Verbreitung und Einführung chipkartenbasierter elektronischer Signaturen und anderer PKI-Anwendungen zu fördern. Hierzu verpflichten sich die Bündnispartner, eine stabile Grundlage für interoperable Infrastrukturen auf der Basis gemeinsam akzeptierter Standards zu entwickeln. Dabei sollen offene Fragen geklärt werden, die eine Verbreitung der elektronischen Signaturen beeinflussen können.

Im Kern geht es darum, eine Reihe von PKI-Funktionen in standardisierter Art und Weise zu unterstützen. Dies kommt auch E-Business, E-Commerce- und E-Government-Anwendungen zu Gute, die neben elektronischen Signaturen auch eine verschlüsselte Kommunikation mit dem Bürger bzw. Kunden und sichere Internetverbindungen benötigen. Dem Karteninhaber erschließt sich auf diese Weise ein breites Anwendungsspektrum.

In dem vorliegenden Dokument werden die notwendigen (Vorgaben) und angestrebten (Konvergenzziele) technisch-organisatorischen Eigenschaften einer Signaturkarteninfrastruktur beschrieben. Es adressiert Institutionen und Unternehmen, die eine Chipkarte für Signaturanwendungen herausgeben oder nutzen wollen und im Signaturbündnis mitarbeiten wollen. Durch das Setzen von Vorgaben und Konvergenzziele verfolgt das Signaturbündnis die Absicht, die Vielzahl unterschiedlicher Ausprägungen von Signaturlösungen (und anderen PKI-Anwendungen) zu reduzieren und in einen Konvergenzkorridor zu bringen, an dessen Ende vom Markt wenige, vereinheitlichte Infrastrukturstandards angeboten werden.

Bei den Signaturanwendungen wird zwischen zwei Kategorien unterschieden:

- Anwendungen der qualifizierten Signatur gemäß Signaturgesetz, die formwahrende Transaktionen ermöglichen und
- Anwendungen von fortgeschrittenen Signaturen, die zur Sicherung von Authentizität und Integrität Verwendung finden.

Das erforderliche Sicherheitsniveau für diese Kategorien ist verschieden. Das erforderliche Sicherheitsniveau für Anwendungen der qualifizierten Signatur wird durch Gesetz und Verordnung in der jeweils gelten Fassung sowie durch das zugrundeliegende EU-Recht bestimmt. Im Signaturbündnis werden Fragen, die sich aus der Umsetzung von Gesetz und Verordnung ergeben, sowie gegebenenfalls notwendig erscheinende Modifikationen der rechtlichen Rahmenbedingungen diskutiert und hierzu Lösungsvorschläge erarbeitet.

Für fortgeschrittene Signaturen ist ein Grundschutzniveau anzustreben, das durch geringere Sicherheitsanforderungen definiert wird. Dieses Niveau soll auch für die Zwecke der Verschlüsselung und sicherer Internetverbindungen zugrunde gelegt werden.

Das Grundschutzniveau ist noch nicht abschließend bestimmt. Das vorliegende Dokument enthält Empfehlungen für Vorgaben, die jedoch noch nicht alle relevanten Aspekte berücksichtigen.

Chipkarten, die mehr als eine PKI-Funktion aufweisen, werden als „multifunktionale Chipkarte“ bezeichnet und können Schlüssel für folgende Anwendungskategorien speichern:

- herausgeberspezifische Anwendungen je nach Anforderungsprofil (z. B. Betriebsausweis),
- bis zu drei allgemeine PKI-Anwendungen (für fortgeschrittene Signaturen, Verschlüsselung und SSL-Authentisierung) und
- qualifizierte Signaturen im Sinne des Signaturgesetzes.

Im folgenden wird der Begriff „Chipkarte“ generell für „sichere Signaturerstellungseinheit“ verwendet.

Als „herausgeberspezifisch“ werden die Anwendungen bezeichnet, die der Kartenherausgeber für seine eigenen Zwecke verwendet. Kartenherausgeber ist die Organisation, die Chipkarten an ihre Mitarbeiter oder Kunden ausgibt und für diese und ggf. auch für Dritte die erforderlichen PKI-Dienstleistungen erbringt. Im Falle von herausgeberspezifischen Anwendungen werden die PKI-Dienstleistungen ausschließlich für die eigenen Mitarbeiter oder Kunden erbracht.

Mit „allgemein“ werden die PKI-Anwendungen bezeichnet, die nicht herausgeberspezifisch sind und die keine qualifizierten Signaturen im Sinne des Signaturgesetzes verwenden. Qualifizierte Signaturen im Sinne des Signaturgesetzes bilden eine eigene Kategorie.

Die Mitglieder des Signaturbündnisses haben das gemeinsame Ziel, dass mit einer beliebigen Chipkarte in Kombination mit beliebigen Chipkartenleser-Lesern jeweils mit geeignetem Sicherheitsniveau möglichst viele dieser PKI-Anwendungen genutzt werden können.

Voraussetzungen für die Mitgliedschaft im Signaturbündnis

Mitglied im Signaturbündnis kann jeder Herausgeber von Chipkarten und Anbieter von Dienstleistungen werden, der solche Geräte für Signaturanwendungen mit mindestens fortgeschrittenen Signaturen nutzen will. Anstelle der Chipkarte können auch andere Technologien wie zum Beispiel USB-Token herausgegeben oder genutzt werden, soweit sie die gleiche Sicherheit und Funktionalität bietet. Als weitere Voraussetzung müssen die Vorgaben erfüllt werden, die im vorliegenden Dokument definiert sind.

Konvergenzziele des Signaturlbündnisses

Die Ziele des Signaturlbündnisses orientieren sich am grundlegenden Gedanken, die Vielzahl unterschiedlicher Ausprägungen von Signaturlösungen (und anderen PKI-Anwendungen) zu reduzieren und in einen Konvergenzkorridor zu bringen, an dessen Ende vom Markt wenige vereinheitlichte Infrastrukturstandards angeboten werden. Zu den Konvergenzzielen, zu denen sich die Mitglieder des Signaturlbündnisses bekennen, gehören:

- **Standardkonformität der Komponenten**

Durch geeignete Maßnahmen soll sichergestellt werden, dass die Standardkonformität von PKI-Diensten, Chipkarten, Chipkartenlesern und PKI-Anwendungen erreicht wird. Die Erfüllung der im vorliegenden Dokument als Vorgaben bezeichneten Standards ist Voraussetzung für den Beitritt zum Signaturlbündnis. Eine hinreichend vereinheitlichte Standardkonformität wird jedoch erst dann erreicht, wenn auch die als Konvergenzziele bezeichneten Standards von den Teilnehmern des Signaturlbündnisses unterstützt werden.

Mit der Forderung nach Standardkonformität ist insbesondere auch das Ziel verbunden, eine verbesserte Interoperabilität der Komponenten zu erreichen.

- **Multifunktionale Chipkarte**

Durch geeignete Maßnahmen soll sichergestellt werden, dass die Chipkarte für verschiedene Anwendungen genutzt werden kann.

- **Einheitliche Sicherheitsniveaus**

Für die herausgeberspezifischen Anwendungen legen die Kartenherausgeber ihr Sicherheitsniveau nach eigenem Bedarf fest. Die beiden anderen Kategorien von PKI-Anwendungen sollen die folgenden Sicherheitsniveaus erreichen:

- Für die **allgemeinen PKI-Anwendungen** (fortgeschrittene Signatur, Verschlüsselung und Authentisierung) muss Grundschatz realisiert werden, vergleichbar dem der PKI-Verwaltung der Bundesbehörden (PKI-1-Verwaltung).
- Die **qualifizierten Signaturen halten** das Sicherheitsniveau nach SigG und SigV ein.

- **Ermöglichung des Einsatzes qualifizierter Signaturen**

Die Verbreitung von Chipkarten, die kryptographische Schlüssell für qualifizierte elektronische Signaturen aufnehmen können, wird angestrebt.

Konvergenzphase des Signaturlbündnisses

Das Signaturlbündnis soll Anfang 2003 gegründet werden und seine Ziele bis Ende 2005 erreicht haben. Dieser Zeitraum wird als Konvergenzphase bezeichnet, in der sich die Bündnisteilnehmer den Konvergenzzielen Schritt für Schritt nähern sollen.

Die Teilnehmer des Signaturlbündnisses entscheiden selbst, wie und in welchen Schritten sie die Konvergenzziele erreichen wollen. Abhängig von der weiteren Entwicklung der Standardisierung, des Marktes für PKI-Komponenten und anderer Einflüsse entscheiden die Teilnehmer ggf. auch über Anpassungen der Konvergenzziele.

Bezüge zu anderen Initiativen

Derzeit arbeiten verschiedene andere Initiativen an der Weiterverbreitung von Anwendungen zur elektronischen Signatur und zum E-Government:

- Das BMF hat, abgestimmt mit der Kreditwirtschaft, in der StDÜV eine (fortgeschrittene) Signatur mit zusätzlichen Sicherheitsanforderungen aus dem Kriterienkatalog der qualifizierten elektronischen Signatur gemäß SigG definiert, um die Umsetzung erleichtern. Diese Signatur kann für eine Übergangszeit bis zum 31. Dezember 2005 für formgebundenen elektronischen Datenaustausch mit der Finanzverwaltung verwendet werden.
- Die Ergebnisse der D21 Arbeitsgruppe 5: „Sicherheit und Vertrauen im Internet - Projektgruppe Smartcards“ sind für das Signaturbündnis von besonderem Interesse.
- Es besteht notwendigerweise eine weitgehende Übereinstimmung zwischen den Standards des Signaturbündnisses und dem E-Government-Standard SAGA. Auf der einen Seite muss SAGA bei der Definition der Standards des Signaturbündnisses Berücksichtigung finden. Auf der anderen Seite müssen die Vereinbarungen des Signaturbündnisses in den E-Government-Standard SAGA einfließen.

Aufbau des Dokuments

Kapitel 2 stellt in einer Übersicht dar, welche Eintrittsvoraussetzungen von den Mitgliedern erfüllt werden müssen und welche Ziele für die Konvergenzphase vereinbart werden.

Kapitel 3 erläutert im Einzelnen, welche Vorgaben und Konvergenzziele für das Signaturbündnis gelten.

2 Übersicht der Vorgaben und Konvergenzziele für das Signaturbündnis

Die folgende Tabelle ermöglicht den Mitgliedern des Signaturbündnisses einen Überblick bezüglich der Mindestanforderungen und Ziele. Dabei ist zu beachten:

- Die Spalte „Vorgaben“ stellt die Mindestanforderungen dar, die mit dem Eintritt in das Signaturbündnis zu erfüllen sind. Übergangsregelungen können im Einzelfall vereinbart werden.
- Die Spalte „Konvergenzziele“ stellt die Ziele dar, die vom Signaturbündnis erreicht werden sollen. Abschließende Entscheidungen müssen jedoch im Signaturbündnis getroffen werden.
- Über die Mindestanforderungen hinaus können die Mitglieder des Signaturbündnisses weitere Dienste anbieten oder höhere Sicherheitsanforderungen einhalten.
- Die Ausgabe von Chipkarten mit qualifizierter Signaturfunktion ist keine Beitrittsvoraussetzung. Werden jedoch Chipkarten mit qualifizierter Signaturfunktion ausgegeben, gelten insoweit für die Vorgaben aus SigG/SigV. In den Konvergenzzielen werden teilweise Vorschläge gemacht, die sich auf qualifizierte Signaturen beziehen. Mit diesen Vorschlägen wird das Ziel verfolgt, die von Mitgliedern des Signaturbündnis angestrebte Signaturkarteninfrastruktur und die gesetzlichen Anforderungen an eine Infrastruktur für die qualifizierte elektronische Signatur in Einklang zu bringen.

Gegenstand	Vorgaben	Konvergenzziele
Sicherheitsniveau	Maßgebend für das Sicherheitsniveau des Kartenherausgebers sind die IT-Grundschutzregeln. Dieses Niveau ist z. B. bei der PKI-1-Verwaltung realisiert.	Vereinheitlichung des vom Markt angebotenen Sicherheitsniveaus auf zwei Stufen für allgemeine und qualifizierte Zertifikate. Allgemeine Zertifikate sind Zertifikate für die allgemeinen PKI-Funktionen Verschlüsselung, Authentifizierung und fortgeschrittene Signatur. Existierende Prozesse von Kartenherausgebern erlangen, wo möglich, rechtliche Anerkennung für die Ausgabe qualifizierter Signaturen.
Chipkarte	Die Karte bietet mindestens ein Schlüsselpaar für fortgeschrittene Signaturen. Der Kartenherausgeber bietet zu seinen Chipkarten Kartenleser und die passende Middleware an.	In der Regel werden mehrere Schlüsselpaare auf einer Chipkarte personalisiert. Die Ausstattung mit der Funktion „Qualifizierte Signatur“ wird angestrebt. Standardisiertes Filesystem und Standardkommandos auf der Karte
Verzeichnisdienst	Veröffentlichung von Zertifikaten in Verzeichnissen oder Unterstützung des bilateralen Schlüsselaustauschs Bereitstellung von Sperrlisten bzw. OCSP-Auskünften	Einheitliches Verzeichnisdienstkonzept für die Veröffentlichung von Zertifikaten und Sperrlisten neben der Unterstützung des bilateralen Schlüsselaustauschs
Wurzel-Zertifizierungsinstanzen	Vorgaben sind noch festzulegen	Gesicherte Übergabe und Speicherung von Wurzelzertifikaten (oder des öffentlichen Schlüssels der Wurzel) über Chipkarte Festlegung eines Verfahrens zur gesicherten Verteilung von Wurzelzertifikaten (oder des öffentlichen Schlüssels der Wurzel) an Teilnehmer ohne Karte
Gültigkeitsmodell	Gültigkeitsmodell nach ISIS-MTT für allgemeine PKI-Anwendungen (Schalenmodell gemäß PKIX)	
Registrierung	Vorgaben sind noch festzulegen	Vereinheitlichtes Namenskonzept Ausgabe allgemeiner Zertifikate auf der Basis marktgängiger Registrierungsverfahren Prüfung der Eignung dieser Verfahren für die Ausgabe qualifizierter Zertifikate; Klärung von Einzelfragen.
Ausgabe von Karte und PIN	Vorgaben sind noch festzulegen	Einheitliche Übergabeverfahren mit definierter Sicherheit Prüfung der Eignung dieser Verfahren für die Ausgabe sicherer Signaturerstellungseinheit gemäß SigG; Klärung von Einzelfragen.

Gegenstand	Vorgaben	Konvergenzziele
Sperrdienst	Durch Kartenherausgeber. Reaktionszeit und Verfügbarkeit im Rahmen üblicher Arbeits- und Bürozeiten. Neben dem Karteninhaber muss mindestens eine weitere Instanz Sperrberechtigung haben.	Verbesserung der Reaktionszeit und Verfügbarkeit des Sperrdienstes für allgemeine Zertifikate

Tabelle 1: Übersicht der Vorgaben und Ziele des Signaturbündnisses

3 Vorgaben und Konvergenzziele

Die in Kapitel 2 tabellarisch aufgeführten Voraussetzungen für die Mitarbeit im Signaturbündnis (Vorgaben) sowie die vom Bündnis verfolgten Ziele (Konvergenzziele) werden in diesem Kapitel ausführlicher erläutert.

Bei den Vorgaben beschränkt sich das Signaturbündnis auf die allgemeinen PKI-Funktionen (Verschlüsselung, Authentifizierung und fortgeschrittene Signatur) sowie allgemeine, für alle Funktionen gleiche technische Interoperabilitätsaspekte. Sofern der Kartenherausgeber die Funktion „qualifizierte Signatur“ anbietet, gelten die zusätzlichen Anforderungen aus Gesetz und Verordnung in seiner jeweils geltenden Fassung.

Die Ziele des Signaturbündnisses orientieren sich an zwei Kategorien von Signaturanwendungen:

- Anwendungen der qualifizierten Signatur gemäß SigG, die formwahrende Transaktionen ermöglichen und
- Anwendungen von fortgeschrittenen Signaturen, die zur Sicherung des Datenschutzes und zur starken Authentifizierungen und/oder zur Sicherung der Integrität eingesetzt werden.

In beiden Kategorien gibt es zur Zeit eine Reihe unterschiedlicher Ausprägungen:

Im Bereich der qualifizierten Signatur gibt es Angebote und Festlegungen für qualifizierte Signaturen mit Anbieterakkreditierung gemäß SigG, sowie solche ohne Anbieterakkreditierung. Im Bereich der Finanzverwaltung wird eine fortgeschrittene Signatur mit zusätzlichen Sicherheitsanforderungen aus dem Kriterienkatalog der qualifizierten elektronischen Signatur eingesetzt. Diese kann für das Steuerdatenübermittlungsverfahren formwahrend eingesetzt werden.

Die im Bereich der Finanzverwaltung verwendete Signatur soll mit den gesetzlichen Anforderungen an eine Infrastruktur für die qualifizierte elektronische Signatur in Einklang gebracht werden und diesen in der Konvergenzphase entsprechen.

Im Bereich der fortgeschrittenen Signatur bietet der Markt eine Vielfalt von Lösungen an, die sich in den technischen Schnittstellen und dem angebotenen Sicherheitsniveau erheblich unterscheiden. Die z. B. in Unternehmen im Einsatz befindlichen Lösungen spiegeln diese Vielfalt wieder. Das Signaturbündnis wird für die fortgeschrittene Signatur Mindestanforderungen festlegen, die zu technischer Interoperabilität und vergleichbarer Sicherheit in diesem Bereich führen sollen, um die Einsetzbarkeit der Lösungen für E-Government-Anwendungen sicherzustellen.

Die Mindestanforderungen sollen sich an den Festlegungen der „European Bridge-CA“-Initiative, der PKI-1-Verwaltung des Bundes, sowie den Festlegungen kommerzieller Zertifizierungsdiensteanbieter für „Class 3“ Zertifikate (die Policies von Dienstleistern wie z. B. Verisign, TC Trustcenter HH oder der „Digital Certificate Working Group“ können hier als Referenz dienen) orientieren. Die exakte Bestimmung der geeigneten Mindestanforderungen bleibt den Bündnisteilnehmern überlassen.

Die in diesem Kapitel aufgeführten Eigenschaften der Infrastruktur unterteilen sich in Vorgaben und Ziele des Signaturbündnisses. Die Vorgaben orientieren sich an bestehenden gesetzlichen Vorgaben und etablierten Verfahren (best practices). Die Festlegungen zu den Konvergenzzielen des Signaturbündnisses orientieren sich am grundlegenden Gedanken, die Vielzahl unterschiedlicher Ausprägungen von Signaturlösungen zu reduzieren und in ei-

nen Konvergenzkorridor zu bringen, an dessen Ende vom Markt wenige, vereinheitlichte Infrastrukturstandards angeboten werden.

Die Anforderungen an die Infrastruktur werden aus Sicht der Anwendungen beschrieben. Damit stehen die Schnittstellen zwischen Anwendung und Infrastruktur, sowie das von der Infrastruktur angebotene Sicherheitsniveau im Zentrum der Betrachtungen.

Die betrachteten Schnittstellen sind die Signaturkarte einschließlich APIs sowie der Verzeichnisdienst mit den Zertifikaten und Statusinformationen. Die Standardisierung dieser Schnittstellen ist wesentlich für die technische Interoperabilität zwischen Anwendungen und Infrastruktur.

Für das angebotene Sicherheitsniveau sind neben den Sicherheitseigenschaften der Schnittstellen weitere organisatorische Aspekte wesentlich, insbesondere die Maßnahmen, die zur Sicherstellung der Vertrauenswürdigkeit von Zertifikaten ergriffen werden (Verfahren zur Identitätsüberprüfung, sichere Ausgabe von Karten bzw. Besitzfeststellung bzgl. privater Schlüssel, Verfügbarkeit und Zuverlässigkeit von Sperrdiensten und Statusauskünften).

Es steht den Infrastrukturbetreibern frei, die für ihr jeweiliges Angebot günstigste Realisierung umzusetzen, solange die in diesem Dokument genannten Sicherheitsanforderungen gewahrt bleiben und die Infrastruktur ihre Dienste (Schlüssel, Zertifikatsformate und Verzeichnisdienst und Sperrauskunft, Wurzel-Schlüsselmanagement) den Anwendungen in vergleichbarer Art und Weise bereitstellt.

3.1 Grundsätzliches Sicherheitsniveau

Das Sicherheitsniveau für qualifizierte Signaturen ergibt sich aus dem SigG. Im Zuge der Aktivitäten des Signaturbündnisses ist ein definiertes Sicherheitsniveau für fortgeschrittene Signaturlösungen und allgemeine PKI-Anwendungen zu schaffen.

Vorgabe:

- Das Sicherheitsniveau für das Key-Management für allgemeine Schlüsselpaare wird am IT-Grundschutz orientiert. Als beispielhafte Vorgabe werden die Maßnahmen der PKI-1-Verwaltung herangezogen.

Konvergenzziel:

- Einzelfragen, die sich aus der Prüfung existierender Prozesse bei Kartenherausgebern hinsichtlich ihrer Eignung für die Ausgabe qualifizierter Zertifikate ergeben, werden im Bündnis diskutiert und hierzu Lösungsvorschläge erarbeitet.

3.2 Technische Anforderungen

3.2.1 Anforderungen an die Signaturkarte

Basis der vom Signaturlösungsverbund angestrebten Lösung ist eine Chipkarte, die mehrere PKI-Anwendungen mit unterschiedlichen Verwendungszwecken (Verschlüsselung, Authentifizierung, Signatur etc.) tragen kann.

Vorgaben:

- Das Signaturlösungsverbund unterstützt ausschließlich chipkartenbasierte Lösungen, die mindestens die Funktion der fortgeschrittenen Signatur bereitstellen. Die Unterstützung der fortgeschrittenen Signatur mit erweiterten Sicherheitsanforderungen, wie sie im Steuerdatenübermittlungsverfahren eingesetzt wird, sowie der qualifizierten Signatur ist erwünscht.
- Zum Beitrittszeitpunkt genügt es, wenn die Chipkarten, Kartenleser und die passende Middleware von den Kartenherausgebern bereitgestellt werden. Dabei muss die Middleware der Anwendung entweder eine PKCS#11- oder eine CryptoAPI-Schnittstelle zur Verfügung stellen, über die mehrere Anwendungen auf den jeweiligen Bereich der Karte zugreifen können.

Konvergenzziele:

- Die Chipkarte stellt Schlüssel für allgemeine PKI-Anwendungen auf einem vom Signaturlösungsverbund definierten Sicherheitsniveau zur Verfügung. Die Unterstützung der qualifizierten Signatur gemäß SigG/SigV wird angestrebt.
- Zum Konvergenzzeitpunkt muss die Chipkarte zusätzlich über ein standardisiertes Datenformat (Filesystem) und einen standardisierten Kommandosatz verfügen, so dass die Middleware unterschiedlicher Hersteller auf die Datenobjekte der Karte zugreifen kann, sofern sie die gleichen Kartenleser und Chipkarten unterstützt. Dadurch ist ein Bundle von Chipkartenleser und Middleware ausreichend, um mit verschiedenen Chipkarten unterschiedliche Anwendungen zu nutzen.
- Die Verwendung des Schlüssels für die qualifizierte Signatur muss durch eine PIN oder ein anderes (z. B. ein gleichwertiges biometrisches) Verfahren gesichert sein. Die Karte muss es erlauben, die PIN für die qualifizierte Signaturfunktion auf einen von PINs für andere Funktionen der Karte abweichenden Wert zu setzen. Entscheidend ist, dass durch das den Signaturlösungsverbund schützende Verfahren die Ausübung eines Willensaktes „Signatur“ eindeutig sichergestellt werden kann.

3.2.2 Anforderungen an den Verzeichnisdienst

3.2.2.1 Zugriff auf Signaturprüfchlüssel von Endteilnehmern

Die Partner, die an einer gesicherten elektronischen Kommunikation teilnehmen, müssen auf Zertifikate mit den öffentlichen Schlüsseln zugreifen können. Dazu sind drei Fälle zu unterscheiden: Zertifikate von Endteilnehmern für die Prüfung elektronischer Signaturen, Zertifikate von Zertifizierungsdiensteanbietern für die Bildung von Zertifikatsketten und die Prüfung von Sperllisten sowie die Suche nach Verschlüsselungsschlüsseln. In diesem und den folgenden Kapiteln wird auf diese Fälle gesondert eingegangen.

Vorgabe:

- Die für die Prüfung elektronisch signierter Dokumente gängige Praxis, das Unterzeichnerzertifikat dem Dokument anzufügen (z. B. bei der Verwendung von S/MIME für elektronische Mail) erscheint aus heutiger Sicht ausreichend. Unterzeichnerzertifikate müssen daher nicht notwendigerweise in einem Verzeichnisdienst veröffentlicht werden. Zur Unterstützung des bilateralen Schlüsselaustausches muss das Unterzeichnerzertifikat von der Chipkarte geladen werden können.

Konvergenzziel:

- Zur Unterstützung von Signaturverfahren, bei denen die Unterzeichnerzertifikate nicht dem Dokument beigelegt werden können, muss vom Signaturbündnis ein Verzeichnisdienstkonzept für den Abruf von Unterzeichnerzertifikaten bereit gestellt und von den Beteiligten eingesetzt werden. Die Möglichkeit des bilateralen Schlüsselaustausches muss aus datenschutzrechtlichen Gründen erhalten bleiben.

3.2.2.2 Zugriff auf Verschlüsselungszertifikate von Endteilnehmern

Für die Verschlüsselung von Dokumenten muss der Absender über den öffentlichen Schlüssel des Empfängers verfügen. Dieser kann als Zertifikat aus Verzeichnisdiensten effizient abgefragt werden.

Nach Stand der Technik fragen Anwendungen zur Zeit lokal konfigurierte Verzeichnisdienstadressen nacheinander, teilweise automatisch, ab. Einige Verschlüsselungsanwendungen unterstützen auch den „bilateralen“ Schlüsselaustausch, bei dem die Teilnehmer ihre Verschlüsselungszertifikate individuell an andere Kommunikationspartner per E-Mail verteilen. Diese Situation ist unbefriedigend.

Vorgabe:

- Wenn Verschlüsselungsanwendungen vom Kartenherausgeber angeboten werden, muss zumindest der bilaterale Schlüsselaustausch unterstützt werden. Zur Unterstützung des bilateralen Schlüsselaustausches muss das Verschlüsselungszertifikat von der Chipkarte geladen werden können.

Konvergenzziele:

- Im Signaturbündnis wird ein domänenübergreifendes Verzeichnisdienstkonzept festgelegt, durch das die Verschlüsselungs-Zertifikate der Teilnehmer in einheitlicher Art und Weise (Art der Abfrage) öffentlich abrufbar gehalten werden können. Basis des Verzeichnisdienstkonzepts sind die Standards LDAP und X.509v3-Formate für Zertifikate und Sperrlisten. Die Mitglieder des Signaturbündnisses verpflichten sich, dieses Verzeichnisdienstkonzept in der Konvergenzphase umzusetzen. Die Möglichkeit des bilateralen Schlüsselaustausches muss aus datenschutzrechtlichen Gründen erhalten bleiben.
- Anwendungen müssen bei der Suche nach Teilnehmerzertifikaten ggf. mehrere Dienst Anfragen absetzen. Während der Konvergenzphase ist zu prüfen, inwiefern eine Vernetzung der Verzeichnisdienste möglich ist, um Mehrfachanfragen zu vermeiden.

3.2.2.3 Zugriff auf Zertifikate von Zertifizierungsdiensteanbietern

Zertifikate der Zertifizierungsdiensteanbieter stehen nicht immer zur Verfügung. Nach Stand der Technik werden Zertifikate von Zertifizierungsdiensteanbietern zur Zeit von Anwendungen lokal gespeichert (relevant vor allem für Zertifikate von Wurzelzertifizierungsstellen, Empfehlungen hierzu siehe 3.2.2.5) bzw. aus übermittelten Dokumenten entnommen. Ein einheitliches Verteilverfahren für Zertifikate von Zertifizierungsdiensteanbietern fehlt.

Vorgabe:

- In der Einführungsphase werden Verfahren unterstützt, bei denen die zur Prüfung von Zertifikaten und Sperrlisten benötigten Zertifikate von Zertifizierungsdiensteanbietern überbrachten Dokumenten beigelegt werden.

Konvergenzziel:

- Ein Ziel der Konvergenzphase wird die Festlegung und Umsetzung von effizienten Verteilungsverfahren für Zertifikate von Zertifizierungsdiensteanbietern sein. Damit können auch Verfahren unterstützt werden, bei denen keine Zertifikate übermittelt werden.

3.2.2.4 Bereitstellung von Sperrinformationen

Sperrinformationen über Zertifikate müssen bereitgestellt werden, um die einwandfreie Funktionalität von PKI-basierten Sicherheitsverfahren zu garantieren. Problematisch ist die uneinheitliche Art und Weise, in der PKI-Anwendungen Sperrinformationen abfragen. Ziel des Signaturlbündnisses ist es, hier zügig ein einheitliches Angebot zu schaffen, das möglichst viele Anwendungen sofort nutzen können und auf das sich weitere Anwendungsentwicklungen stützen können.

Vorgabe:

- Für die allgemeinen Zertifikate müssen die Sperrinformationen mindestens in Form einfacher Sperrlisten nach X.509 in einem LDAP-Verzeichnis bereitgestellt werden. Als Dienst zur Bereitstellung kann prinzipiell der gleiche Verzeichnisdienst verwendet werden, der auch Zertifikate der Endteilnehmer veröffentlicht (vgl. Kapitel 3.2.2.1). Alternativ ist die Unterstützung von Sperrabfragen durch OCSP zulässig.

3.2.2.5 Verteilung von Zertifikaten (oder öffentlichen Schlüsseln) von Wurzelzertifizierungsstellen

Die Vertrauenswürdigkeit von Zertifikaten wird durch die Bildung von Zertifikatsketten geprüft, die auf vertrauenswürdigen „Wurzelzertifizierungsstellen“ enden. Diese müssen beim Prüfenden lokal vorgehalten werden. Die besondere Problematik bei der Veröffentlichung von Zertifikaten von Wurzelzertifizierungsstellen (oder deren öffentliche Schlüssel) ist die Notwendigkeit der gegen Verfälschung und Austausch gesicherten Übertragung an den Endteilnehmer sowie die gesicherte Speicherung und Benutzung dieser Zertifikate (oder der öffentlichen Schlüssel) in den Prüfanwendungen des Endteilnehmers.

Vorgaben:

Vorgaben sind noch festzulegen.

Konvergenzziele:

- Im Signaturlbündnis wird ein Rollout-Verfahren festgelegt, mit dem die Zertifikate (oder öffentlichen Schlüssel) aller zu diesem Zeitpunkt produktiven Wurzelzertifizierungsstellen an die Endteilnehmer verteilt werden, z. B. bei der Übergabe der Chipkarte und der Prüfkomponente an den Karteninhaber. Existierende Spezifikationen und Modelle wie Cross-Zertifizierung, gemeinsame Wurzelzertifizierungsstellen sowie Bridge-CA-Konzepte werden auf ihre Verwendbarkeit zur Vereinfachung und Sicherung der Verteilungsverfahren geprüft.
- Für die gesicherte Speicherung von Wurzelzertifikaten (oder der öffentlichen Schlüssel) in den Prüfanwendungen der Endteilnehmer sind zwei Fälle zu unterscheiden: im ersten

Fall besitzt der Bürger eine Chipkarte, im zweiten Fall nicht. Das Signaturlbündnis konzentriert sich auf den ersten Fall und wird Modelle entwickeln, die die Chipkarte als sicheren Speicher für Wurzelzertifikate (oder öffentliche Schlüssel) nutzen.

3.2.2.6 Gültigkeitsmodell

Das für die Prüfung verwendete Gültigkeitsmodell entscheidet, ob ein Zertifikat akzeptiert wird oder nicht. Zur Zeit sind zwei unterschiedliche Gültigkeitsmodelle markt- und anwendungsrelevant. Anwendungen unterstützen in der Regel nur eins der beiden Modelle.

Vorgabe:

- Für allgemeine PKI-Anwendungen wird das Gültigkeitsmodell nach ISIS-MTT, Teil 5 verwendet (Schalenmodell gemäß PKIX).

3.3 Organisatorische Anforderungen

3.3.1 Registrierung und Identifikation des Schlüsselinhabers

In vielen Fällen kann der Kartenherausgeber die für die Personalisierung erforderlichen Kunden- oder Mitarbeiterdaten aus vorhandenen Datenbeständen extrahieren. Lediglich für qualifizierte Zertifikate ist eine persönliche Erst-Registrierung unter Vorlage eines Ausweisdokuments erforderlich. Nach § 5 SigG können eine Vertretungsmacht oder berufsbezogene oder sonstige Angaben in ein qualifiziertes Zertifikat aufgenommen werden..

Vorgaben:

Die Vorgaben sind noch festzulegen.

Konvergenzziele:

- Das Signaturlbündnis wird ein einheitliches Namenskonzept entwickeln. Dabei sollen die Namensregeln und -formate berücksichtigt werden, die für die PKI-1-Verwaltung entwickelt wurden.
- Für die Ausstellung von allgemeinen Zertifikaten können Registrierungsdaten verwendet werden, die auf einer persönlichen Erst-Identifikation und einem anschließenden kontinuierlichen Vertragsverhältnis basieren (Beispiel: Identifikationen nach § 154 AO oder Arbeitsverträge). Es wird eine Liste konkreter Anforderungen an die persönliche Erst-Registrierung, die Pflege der Datenbestände und das Vertragsverhältnis festgelegt.
- Einzelfragen, die sich diesbezüglich aus der Umsetzung der gesetzlichen Anforderungen ergeben, werden im Bündnis diskutiert und hierzu Lösungsvorschläge erarbeitet.

3.3.2 Ausgabe von Chipkarte und PIN

Die **Ausgabe von Chipkarte und PIN** muss ein ausreichendes Sicherheitsniveau gewährleisten.

Vorgaben:

Sind noch festzulegen.

Konvergenzziele:

- Für Chipkarten sind folgende Übergabeverfahren ausreichend:
 - eine vom Schlüsselinhaber bestätigte persönliche Übergabe von Chipkarte und PIN-Brief,
 - ein getrennter Versand von Chipkarte und PIN-Brief (entsprechend ec- oder Kreditkarten).
- Einzelfragen, die sich aus der Umsetzung der gesetzlichen Anforderungen ergeben, werden im Bündnis diskutiert und hierzu Lösungsvorschläge erarbeitet.

3.3.3 Sperrung

Für die Sperrung von Zertifikaten muss vor allem bekannt sein, welche Zertifikate gesperrt werden sollen, wer zur Sperrung berechtigt ist und wo der Sperrantrag einzureichen ist.

Vorgaben:

- Der Sperrdienst wird vom jeweiligen Kartenherausgeber angeboten.
- Neben dem Karteninhaber müssen weitere Instanzen (einschließlich des Kartenherausgebers) eine Sperrung verlangen können.
- Für allgemeine PKI-Anwendungen muss die Verfügbarkeit des Sperrdienstes innerhalb normaler Bürozeiten sichergestellt sein. Die Reaktionszeit darf einen Arbeitstag nicht überschreiten.

Konvergenzziel:

- Die Reaktionszeit und Verfügbarkeit des Sperrdienstes für allgemeine Zertifikate wird gemäß den Anforderungen der Anwendungen ggf. verbessert.

4 Abkürzungen

AO	Abgabenordnung
API	Application Programming Interface (Programmierschnittstelle)
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority (Zertifikatserzeugende Stelle)
CMC	Certificate Management Messages over CMS (Standard für die Kommunikation der Verwaltungsfunktionen eines PKI-Systems)
CMS	Cryptographic Message Syntax (Spezifikation für verschlüsselte und signierte Nachrichten)
CRL	Certificate Revocation List (Sperrliste für Zertifikate)
CSP	Certification Service Provider (Zertifizierungsdienstanbieter)
CT-API	CardTerminal - Application-Programming-Interface (Schnittstellenbeschreibung für die Ansteuerung von Chipkarten und Lesern)
DIN	Deutsches Institut für Normung
HTTP	Hypertext Transfer Protocol (Spezifikation zum Abruf von Web-Seiten)
IETF	Internet Engineering Task Force (Standardisierungsgruppe der Internet society für das Internet)
ISIS	Industrial Signature Interoperability Standard (Standardisierung der „T7“-Gruppe von Trustcenter-Betreibern)
ISIS-MTT	Gemeinsame Standardisierung der "T7" Gruppe von Trustcenter-Betreibern und dem MTTv2-Standard des TeleTrusT Deutschland e.V.
ISO	International Standardisation Organisation (Normungsgremium)
ITU	International Telecommunication Union (Normungsgremium)
LDAP	Lightweight Directory Access Protocol (Spezifikation für die Kommunikation mit Verzeichnisdiensten)
MTT	MailTrusT (Spezifikation für gesicherte Ende-zu-Ende Kommunikation herausgegeben vom TeleTrusT Deutschland e.V.)
NIST	National Institute for Standards and Technology (Behörde der amerikanischen Regierung für Standardisierung)
OCF	Open Card Framework (Java-basierte API und Treiberarchitektur für die Ansteuerung von Smartcards durch Java-Programme)
OCSP	Online Certificate Status Protocol (Spezifikation für die Abfrage von Statusinformation zu Zertifikaten)
OSCI	Online Services Computer Interface (Spezifikation für sichere Transaktionen im Bereich der öffentlichen Verwaltung)
PC/SC	Personal Computer / Smartcard (Spezifikation zur Ansteuerung von Chipkarten durch Personal Computer)
PIN	Personal Identification Number (Schutzmechanismus für Chipkarten)

PKCS	Public Key Cryptography Standards (Standard-Serie von RSA Security zu Public Key Verfahren)
PKI	Public Key Infrastructure
PKI-1	PKI-Verwaltung der Bundesbehörden
PSE	Personal Secure Environment (Allgemeine Bezeichnung für Medien zur sicheren Ablage von geheimen Schlüsseln)
PKIX	Public Key Infrastructure (X.509) (Normungsgruppe)
PUK	PIN Unblocking Key (Rücksetzcode für PINs auf Chipkarten)
RegTP	Regulierungsbehörde für Telekommunikation und Post
RFC	Request For Comments, Standardschriftenreihe der IETF
SAGA	Standards und Architekturen für E-Government-Anwendungen
SigBü	Signaturbündnis
SigG	Signaturgesetz
SigV	Signaturverordnung
S/MIME	Secure Multipurpose Internet Mail Extensions (Spezifikation für Verschlüsselung und Signatur von E-Mail)
SSL/TLS	Secure Socket Layer / Transport Layer Security (Spezifikation für die Verschlüsselung und Authentifizierung von Online-Verbindungen über das Internet)
StDÜV	Steuerdaten-Übermittlungsverordnung
TSP	Timestamping Protocol (Spezifikation eines Abfrageprotokolls für Zeitstempel)
X.509	Standard für Zertifikate und Zertifikatsmanagement
XML	Extended Markup Language (Spezifikation für die Gestaltung von strukturierten Daten)
ZKA	Zentraler Kreditausschuss

5 Referenzen

- [ALGO] Empfehlung des BSI zu geeigneten Kryptoalgorithmen für die kommenden sechs Jahre gemäß § 17 Abs. 1 SigG in Verbindung mit § 17 Abs. 2 SigV, 05.07.2001
- [CEN-G1] Security Requirements for Signature Creation Systems, CEN/ISSS WS/E-Sign N 141, Draft CWA, Version 3.9, 12.03.2001
- [CEN-G2] Procedures for electronic signature verification, CEN/ISSS/E-Sign N 140, Draft CWA, Version 1.0.5, 13.03.2001
- [CT-API] Deutsche Telekom, GMD, RWTÜV, TeleTrust Deutschland, CT-API 1.1 – Application independent Card-Terminal Application Programming Interface for ICC applications, 1995
- [D21] Initi@tive D21 - D21 Arbeitsgruppe 5: Sicherheit und Vertrauen im Internet - Projektgruppe Smartcards (2002): Mehr Sicherheit, Mobilität und Effizienz durch den Einsatz von Chipkarten, Version 1.0 vom 26.06.2002; <http://www.initiated21.de>
- [DINSIG1] DIN V66291-1: 1999, Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV, Teil 1: Anwendungsschnittstelle, Ausgabe: 2000-04
- [DINSIG2] DIN V66291-2: 2000, Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV, Teil 2: Personalisierungs-Prozesse, Ausgabe: 2003-01
- [DINSIG3] DIN V66291-3: 2002, Chipcards with digital signature application/function according to SigG and SigV, Part 3: Commands for Personalisation, Final Draft, September 2002
- [DINSIG4] DIN V66291-4: 2000, Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV, Teil 4: Grundlegende Sicherheitsdienste, Ausgabe: 2002-04
- [ETSI] Electronic signature formats, ETSI TS 101 733, V1.2.2, 12.2000
- [EU-SIG] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen
- [ISIS] Industrial Signature Interoperability Specification ISIS, Version 1.2, 03.12.1999
- [ISIS-MTT] ISIS-MTT Specification, Common ISIS-MTT Specification for PKI Applications, Version 1.0.2, 19.07.2002
- [ISIS-MTT-T] ISIS-MTT Test Specification, Version 1.0, 01.02.2002

- [ISO 7816-1] ISO 7816 - 1, Identification cards - Integrated circuit(s) cards with contacts, Part 1: Physical characteristics, 1987
- [ISO 7816-2] ISO 7816 - 2, Identification cards - Integrated circuit(s) cards with contacts, Part 2: Dimensions and location of the contacts, 1988
- [ISO 7816-3] ISO 7816 - 3, Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols, 1997
- [ISO 7816-4] ISO/IEC 7816-4: 1995, Identification cards - Integrated circuit(s) cards with contacts, Part 4: Interindustry commands for inter-change, IS 1995, FCD December 2002
- [ISO 7816-5] ISO 7816 - 5, Identification cards - Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers, 1994
- [ISO 7816-6] ISO 7816 - 6, Identification cards - Integrated circuit(s) cards with contacts, Part 6: Inter-industry data elements, 1996
- [ISO 7816-8] ISO/IEC 7816-8: IS 1998, Identification cards - Integrated circuit(s) cards with contacts, Part 8: Security related interindustry commands , IS 1999, FCD August 2002
- [ISO 7816-9] ISO 7816 - 9, Identification cards - Integrated circuit(s) cards with contacts, Part 9: Additional interindustry commands and security attributes, FDIS 2000
- [ISO 7816-15] ISO/IEC 7816-15: 2002, Identification cards - Integrated circuit(s) cards with contacts, Part 15: Cryptographic information application, FDIS 2002, December 2002
- [KT-SIGK] Schnittstellenspezifikation für die ZKA-Chipkarte, Konzept für die Unterstützung der Signatur-Anwendung der ZKA-Chipkarte durch das Internet-Kundenterminal, Version 1.0, 15.02.2002
- [OSCIv1.2] Online Service Computer Interface, Spezifikation Transport, Version 1.2 Draft, Mai 2002
- [PCSC] PC/SC Workgroup, PC/SC Specifications 1.0, erhältlich via <http://www.pcscworkgroup.com>
- [PKCS11] RSA Laboratories, PKCS #11: Cryptographic Token Interface Standard, Version 2.1, 1999
- [PKCS15] RSA Laboratories PKCS #15 v1.0: Cryptographic Token Information Format Standard, 1999
- [RFC 2045] N. Fried, N. Borenstein: Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies

- [RFC 2046] N. Fried, N. Borenstein: Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types
- [RFC 2630] R. Housley: Cryptographic Message Syntax
- [RFC 2633] B. Ramsdell: S/MIME Version 3 Message Specification; June 1999
- [RFC 2797] M. Myers, X. Liu, J. Weinstein: Certificate Management Messages over CMS, <draft-ietf-pkix-rfc2797-bis-01.txt>; July 2001
- [SECCOS] Schnittstellenspezifikation für die ZKA-Chipkarte, Secure Chip Card Operating System (SECCOS), Version 5.0, 5.06.2001
- [SigG] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16. Mai 2001, Bundesgesetzblatt Jahrgang 2001 Teil I Seite 676 ff.
- [SigV] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. November 2001, Bundesgesetzblatt Jahrgang 2001 Teil I Seite 3074 ff.
- [SOAP] D. Box, D. Ehnebuske, G. Kakivaya, A. Layman, N. Mendelsohn, H. Nielsen, S. Thattai: Simple Object Access Protocol (SOAP) 1.1. W3C Note 08 May 2000. Online verfügbar unter <http://www.w3.org/TR/2000/NOTE-SOAP-20000508>
- [TT-OIC] TeleTrusT Deutschland, German Office Identity Card (Elektronischer Dienstausweis), Version 1.0, 2000, http://www.sit.fhg.de/german/SICA/si-ca_links/OIC_10fv.pdf
- [X.509] ITU-T X.509: Information Technology - Open Systems Interconnection – The Directory: Authentication Framework, 1997
- [XML] Extensible Markup Language (XML) 1.0 (Second Edition). W3C Recommendation 6, October 2000. Online verfügbar unter <http://www.w3.org/TR/2000/REC-xml-20001006>
- [XDSIG] Mark Bartel, John Boyer, Barb Fox, Brian LaMacchia, Ed Simon: XML-Signature Syntax and Processing. W3C Recommendation 12 February 2002. Online verfügbar unter <http://www.w3.org/TR/2002/REC-xmlsig-core-20020212>
- [XENC] Takeshi Imamura, Blair Dillaway, Ed Simon: XML Encryption Syntax and Processing. W3C Candidate Recommendation 04 March 2002. Online verfügbar unter <http://www.w3.org/TR/2002/CR-xmlenc-core-20020304>
- [ZKASIG10] Schnittstellenspezifikation für die ZKA-Chipkarte, Signatur-Anwendung, Version 1.0, 14.09.2001



[ZKA-PS] Konzept zu Personalisierung von ZKA Chipkarten (insbesondere Signaturkarten) des deutschen Kreditgewerbes mit dem Betriebssystem SECCOS, Version 1.0, 13.07.2001