BSI

Bundesamt für Sicherheit in der Informationstechnik

SPEZIFIKATION ZUR ENTWICKLUNG INTEROPERABLER VERFAHREN UND KOMPONENTEN NACH SIGG/SIGV

SIGNATUR-INTEROPERABILITÄTSSPEZIFIKATION SIGI

ABSCHNITT A3 ANWENDERINFRASTRUKTUR

STAND: 15.06.99
VERSION 4.0

Godesberger Allee 183, 53175 Bonn - Postfach 20 03 63, 53133 Bonn
Telefon: (0228) 9582 - 0, Telefax: (0228) 9582 - 400
Internet: www.bsi.bund.de

ABSCHNITT A3
ANWENDERINFRASTRUKTUR

Andreas Berger, Alfred Giessler, Petra Glöckner, Wolfgang Schneider
GMD – Forschungszentrum Informationstechnik GmbH
Institut für Telekooperationstechnik
Dolivostr. 15, 64293 Darmstadt

Michael Baum, Freier Mitarbeiter beim
BSI – Bundesamt für Sicherheit in der Informationstechnik, Referat VI3
Godesberger Allee 183, 53133 Bonn

INHALTSVERZEICHNIS

1 EINLEITUNG

In diesem Dokument wird die Schnittstelle der Anwenderinfrastruktur zum Anwender beschrieben. Die Schnittstellenbeschreibung ist hierbei beschränkt auf die Definition von eindeutigen Anzeigetexten der Signier- und Verifikationsprozesse, der Verzeichnisdienstauskünfte, der Zeitstempelverifikation, sowie der Felder von Signaturschlüssel- und Attributzertifikaten. Desweiteren wird in dieser Spezifikation von den möglichen technischen Realisierungen der Anwenderinfrastruktur in unterschiedlichen Ausprägungen abstrahiert.

Die Anwenderinfrastruktur wird konzeptionell als eine Menge von physikalischen und software-technischen Komponenten betrachtet, die zur Erbringung der Sicherheitsdienste "Signaturerzeugung" und "Verifikation von Signaturen" dienen. Anwender können hierbei sowohl in der Rolle als "Signierer" als auch "Verifizierer" auftreten. Aus der Sicht der Anwenderinfrastruktur sind für die Unterstützung der Signaturerzeugung und der Verifikation digitaler Signaturen sogenannte konzeptionelle Stellvertreterprozesse erforderlich. Über diese Stellvertreterprozesse läuft auch die Kopplung mit den anderen, in die Infrastruktur eingebundenen Instanzen wie Zertifizierungsstellen, Verzeichnisdienst, Zeitstempeldienst, Signaturkomponente und die Benutzer. Zur Veranschaulichung dieses Sachverhaltes mögen die beiden folgenden Szenarien der Signaturerzeugung und der Signaturverifikation dienen.

Ein Benutzer, in der Rolle als Signierer, muß beim Anstoß zur Signaturerstellung im allgemeinen Fall die Möglichkeit haben, einen bestimmten Signaturschlüssel auszuwählen mit dem Benutzernutzdaten, eigene Attributzertifikate, das zugehörige Signaturschlüsselzertifikat, Zeitstempel und Quittungsanforderungen zu signieren sind. Per Signaturgesetz wird dem Signierer eine aktive Rolle garantiert, da alle Aktivitäten nur durch dessen ausdrückliche Willenserklärung ablaufen dürfen. Die hierzu erforderliche Koordination und Kontrolle der Abläufe wie beispielsweise der Zugriff auf die Signierkomponente und der optionale Zugriff auf den Zeitstempeldienst zur Integration eines Zeitstempels in die zu signierenden Daten werden über den Stellvertreterprozeß für den Signaturvorgang abgewickelt.

Ein Benutzer, in der Rolle als Verifizierer, muß beim i.a. automatisch ablaufenden Verifikationsvorgang über die Verfikationsergebnisse und die verifizierten Daten informiert werden. Die für die Verifikation erforderliche Koordination und Kontrolle der Abläufe wie beispielsweise der Zugriff auf eine Verzeichnisdienststelle zur Überprüfung von Zertifikaten und Zertifikatspfaden wird über den Stellvertreterprozeß für den Verifikationsvorgang abgewickelt.

Desweiteren können Signaturerzeugungs- und Verifikationsprozesse auch überlappend benutzt werden. So können beispielsweise der Verifikationsprozeß zur Überprüfung der Gültigkeit eines eigenen Signaturschlüsselzertifikates während der Durchführung des Signaturerzeugungsprozesses oder der Signaturerzeugungsprozeß zum Signieren einer angeforderten Quittung während der Durchführung des Verifikationssprozesses beteiligt sein.

In Abbildung 1 werden die Architektur der SigI-Infrastruktur und der Zusammenhang mit den relevanten Teilen der SigI-Spezifikation (siehe Tabelle 2) veranschaulicht. Die Bedeu-

tung, der in der Abbildung 1 benutzten Symbole, ist in der Tabelle 1 erläutert. In der Grafik sind insbesondere die in der Infrastruktur eingebundenen Instanzen wie Zertifizierungsstellen, Zeitstempel- und Verzeichnisdienste, Signierkomponenten und Anwenderprozesse, sowie die Schnittstellen zwischen den beteiligten Instanzen und Teilnehmern und die Stellvertreterprozesse für die Signier- und Verifikationsvorgänge und deren Schnittstellen innerhalb der Anwenderprozesse dargestellt. Teilnehmer können in der Rolle als Signierer oder Verifizierer die Dienstleistungen der Infrastruktur in Anspruch nehmen.

Abbildung 1: Architektur der SigI-Anwenderinfrastruktur

Tabelle 2: Teile der SigI-Spezifikation

#	TITEL	INHALT
A1	Zertifikate	Zertifikatstypen, Zertifikatsformate
A2	Signatur	Signaturverfahren, Signaturumfang, Austauschformate
A3	Anwenderinfrastruktur: Schnittstelle zum Anwender	Sicherheitsereignisse und Anzeigetexte der Signier- und Verifikationsprozesse
A4	Zeitstempel: Schnittstelle zwischen Teilnehmer und Zeitstempeldienst	Kommunikationsabläufe, Anfrage- und Antwortformate, Fehlermeldungen, Sicherheitsverfahren
A5	Verzeichnisdienst: Schnittstelle zwischen Teilnehmer und Verzeichnisdienst	Sperrlistenformate, Mechanismen zur Verwaltung und zur Bereitstellung von Sperrlisten, Anfrage- und Antwortformate für Online-Verzeichnisdienste
A6	Gültigkeitsmodell für digitale Signaturen	Prüfschritte der Verifikation
B1	Anwenderinfrastruktur: Schnittstelle zur Zertifizierungsstelle	Schlüssel- und Zertifikatswechselfunktionen
B2	Signierkomponente	Schnittstelle der Anwenderinfrastruktur zur Signierkomponente, DIN-Signatur-Chipkarten
B5	Mehrfachsignaturen	Formate für Übersignaturen, parallele Signaturen

Die Grundlage für die Erstellung dieses Dokumentes sind das Signaturgesetz [SigG 97], die Signaturverordnung [SigV 97], der Maßnahmenkatalog [MKAT 98], sowie die SigI-Dokumente [A1 99], [A2 99], [A4 99], [A5 99] und [A6 99].

ANFORDERUNGEN AN DIE ANWENDERINFRASTRUKTUR, DIE SICH AUS DEM SIGNATURGESETZ UND DER SIGNATURVERORDNUNG ERGEBEN

Die Anwenderinfrastruktur muß technische Komponenten für die Signaturerzeugungs- und Verifikationsprozesse bereitstellen. Die Erzeugung einer digitalen Signatur darf nur auf Veranlassung des Anwenders von der Anwenderinfrastruktur, d.h. durch seine ausdrückliche Einwilligung hin durchgeführt werden. Der Anwender in der Rolle als Signierer muß hierbei wissen, welche Daten zu signieren sind und die Anwenderinfrastruktur muß den Bezug der erzeugten Signatur zu den zugehörigen Daten dem Anwender eindeutig darstellen. Die Verifikation einer digitalen Signatur muß dem Anwender in der Rolle als Verifizierer Informationen darüber liefern, ob eine überprüfte digitale Signatur korrekt ist, wer der Inhaber des zugehörigen Signaturschlüssels ist und welche Daten signiert wurden. Grundsätzlich können beim Signier- oder Verifikationsprozeß entweder die signierten Daten selbst oder ein eindeutiger Verweis auf die signierten Daten angezeigt werden.

[SigG 97, §14(2)] *Für die Darstellung zu signierender Daten sind technische Komponenten mit Sicherheitsvorkehrungen erforderlich, die die Erzeugung einer digitalen Signatur vorher eindeutig anzeigen und feststellen lassen, auf welche Daten sich die digitale Signatur bezieht. Für die Überprüfung signierter Daten sind technische Komponenten mit Sicherheitsvorkehrungen erforderlich, die feststellen lassen, ob die signierten Daten unverändert sind, auf welche Daten sich die digitale Signatur bezieht und welchem Signaturschlüssel-Inhaber die digitale Signatur zuzuordnen ist.*

[SigV 97, §16(3)] *Die zum Darstellen zu signierender Daten erforderlichen technischen Komponenten müssen so beschaffen sein, daß die signierende Person die Daten, auf die sich die Signatur erstrecken soll, eindeutig bestimmen kann, eine digitale Signatur nur auf ihre Veranlassung erfolgt und diese vorher eindeutig angezeigt wird. Die zum Prüfen signierter Daten erforderlichen technischen Komponenten müssen so beschaffen sein, daß die prüfende Person die Daten, auf die sich die digitale Signatur erstreckt, sowie den Signaturschlüssel-Inhaber eindeutig feststellen kann und die Korrektheit der digitalen Signatur zuverlässig geprüft und zutreffend angezeigt wird. Die technischen Komponenten zum Nachprüfen von Zertifikaten müssen eindeutig erkennen lassen, ob die geprüften Zertifikate im Verzeichnis der Zertifikate zu einem angegebenen Zeitpunkt vorhanden und nicht gesperrt waren. Die technischen Komponenten müssen nach Bedarf den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen. Werden technische Komponenten nach den Sätzen 1 bis 4 geschäftsmäßig Dritten zur Nutzung angeboten, so muß die eindeutige Interpretation der Daten sichergestellt sein und müssen die technischen Komponenten bei Benutzung automatisch auf ihre Echtheit überprüft werden. Sicherheitsrelevante Veränderungen an den technischen Komponenten müssen für den Nutzer erkennbar werden.*

ANFORDERUNGEN AN DIE ANWENDERINFRASTRUKTUR, DIE SICH AUS DEM MAßNAHMENKATALOG ERGEBEN

Im Maßnahmenkatalog werden die sich aus dem Signaturgesetz und der Signaturverordnung ergebenden Anforderungen weiter präzisiert und durch die folgenden Sicherheitsanforderungen zusammengefaßt [MKAT 98, A-SHIF 1-7]. Sicherheitsanforderungen und zugehörige Maßnahmen, die in Zusammenhang mit der Installation von Komponenten, der Authentisierung von Komponenten oder zwischen Anwender und Komponenten stehen, werden in diesem Dokument nicht behandelt und wie in [A6 99, 2.2.1] beschrieben als erfolgreich durchgeführt vorausgesetzt.

Die Anwenderinfrastruktur muß dem Signierer beim Signierprozeß die ausgewählten Daten anzeigen, auf die sich die zu erstellende Signatur beziehen wird [MKAT 98, A-SHIF 3].

Die Anwenderinfrastruktur darf den Signierprozeß erst dann starten, wenn der Signierer seine explizite Einwilligung zum Signieren der angezeigten Daten durch entsprechende manuelle Eingaben gegeben hat. [MKAT 98, A-SHIF 2].

[MKAT 98, A-SHIF 1] *Die Anwenderinfrastruktur muß die Daten, die dem Signierer dargestellt werden, zuverlässig, eindeutig und unfälschbar signieren.*

[MKAT 98, A-SHIF 2] *Die Anwenderinfrastruktur darf nur dann signieren, wenn der Signaturschlüssel-Inhaber dies ausdrücklich wünscht.*

[MKAT 98, A-SHIF 3] *Die Anwenderinfrastruktur darf nur genau die Daten signieren, die dem Signaturschlüssel-Inhaber dargestellt wurden und von ihm tatsächlich für die Signatur freigegeben werden.*

Die Anwenderinfrastruktur muß dem Verifizierer beim Verifikationsprozeß anzeigen, auf welche Daten sich die digitale Signatur bezieht, ob die Daten unverfälscht sind und welchem Signaturschlüssel-Inhaber die digitale Signatur zuzuordnen ist. Die Anwenderinfrastruktur muß die Ergebnisse der Überprüfung dem Verifizierer anzeigen. Bei erfolgreicher Verifikation müssen von der Anwenderinfrastruktur zusätzlich die durch [SigG 98,§7(1-3)] beschrie-

benen Zertifikatsfelder aus dem Signaturschlüsselzertifikat bzw. dem Attributzertifikat des Signierers extrahiert und dem Verifizierer angezeigt werden. [MKAT 98, A-SHIF 5].

[MKAT 98, A-SHIF 4] *Die Anwenderinfrastruktur muß die Daten, die dem Verifizierer dargestellt werden, zuverlässig, eindeutig und unverfälschbar verifizieren.*

[MKAT 98, A-SHIF 5] *Die Anwenderinfrastruktur muß dem Verifizierer das Ergebnis des Verifikationsprozesses eindeutig und manipulationssicher zur Verfügung stellen.*

Die Anwenderinfrastruktur kann während des Verifikationsprozesses im Zusammenhang mit der Überprüfung der Gültigkeit des Zertifikates des Signierers die Dienste des zugehörigen Verzeichnisdienstes [A5 99] in Anspruch nehmen [MKAT 98, A-SHIF 6].

Die Anwenderinfrastruktur kann während des Signierprozesses im Zusammenhang mit der Erzeugung von Zeitstempeln für eine geleistete Signatur die Dienste des zugehörigen Zeitstempeldienstes (siehe Dokument [A4 99]) in Anspruch nehmen [MKAT 98, A-SHIF 6].

[MKAT 98, A-SHIF 6] *Die Anwenderinfrastruktur muß die Rahmenbedingungen zur Abwicklung des Signiervorgangs zur Verfügung stellen. Dies beinhaltet Hilfsmaßnahmen:*

- *für die Abfrage und Auswertung der Zertifikatslisten des Verzeichnisdienstes*
- *für die Einholung eines Zeitstempels vom Zeitstempeldienst*
- *für die Änderung von Authentisierungsdaten der Signaturkomponente und der technischen Anwenderinfrastruktur*
- *für die Schlüsselgenerierung auf der Signaturkomponente*

[MKAT 98, A-SHIF 7] *Die Anwenderinfrastruktur muß bei geschäftsmäßiger Nutzung durch Dritte die technischen Komponenten automatisch auf ihre Echtheit überprüfen und technische Veränderungen dem Nutzer erkennbar machen.*

ANZEIGETEXTE

Die Menge der möglichen Anzeigetxte wird festgelegt durch die Menge der sicherheitsrelevanten Ereignisse, die während des Ablaufs der Signier- und Verifikationsprozesse auftreten können. Hierzu gehören auch Anzeigetexte, die sich auf Interaktionen der Signier- und Verifikationsprozesse mit den externen Komponenten und Instanzen wie Signierkomponente [B2 99, noch zu erstellen], Zeitstempel- [A4 99] und Verzeichnisdienst [A5 99] beziehen. Die vollständige Menge der sicherheitsrelevanten Ereignisse wird durch eine Verfeinerung der zuvor genannten groben Sicherheitsereignisse und Bedingungen insbesondere aus dem “Gültigkeitsmodell für digitale Signaturen” [A6 99] und dem “Signaturumfang und Signaturaustauschformat” [A2 99] abgeleitet.

Hinsichtlich der Verifikation von digitalen Signaturen werden drei Prüftiefen festgelegt, die vom Anwender für jeden einzelnen Verifikationsprozeß in Abhängigkeit von der Wichtigkeit und vom Vertrauen in den jeweiligen öffentlichen Schlüssel und die damit verbundene Bindung an den zugehörigen Schlüsselinhaber gewählt werden können. Jede Prüftiefe beruht auf einer bestimmten Prüfannahme, die das Maß an Vertrauen in die Zertifizierungsinfra-

struktur ausdrückt. Jeder einzelnen Prüftiefe ist ein definiertes Prüfziel zugeordnet, das durch eine zugehörige Menge von möglichen Prüfobjekten und Prüfschritten wie folgt festgelegt ist:

PRÜFTIEFE I

- Prüfannahme:

  Der Verifizierer hat Vertrauen in alle Zertifikate des Zertifizierungspfades des Signierers.

- Prüfziel:

  Die Prüftiefe I umfaßt ausschließlich die Überprüfung der mathematischen Korrektheit der Dokumentensignatur des Signierers und dient somit nur zur Anzeige der Sicherstellung der Integrität der signierten Daten. Die Prüftiefe I sollte nur in Einzelfällen verwendet werden, da sie keine Sicherstellung der Authentizität des Signierers liefert.

- Prüfobjekt:

  Dokumentensignatur

- Prüfschritt:

  Überprüfung der mathematischen Korrektheit der Dokumentensignatur mit Hilfe des öffentlichen Signaturschlüssels des Signierers

PRÜFTIEFE II

- Prüfannahme:

  Der Verifizierer hat Vertrauen in das Verzeichnisdienstzertifikat der Wurzelstelle, sowie in die Signatur des Verzeichnisdienstes der Wurzelstelle, nicht aber in die sonstigen Signaturen und Zertifikate des Zertifizierungspfades des Signierers, des Verzeichnisdienstes der Zertifizierungsstelle und der Zeitstempeldienste der Zertifizierungsstelle und der RegTP.

- Prüfziel:

  Die Prüftiefe II umfaßt den Prüfschritt der Prüftiefe I und beinhaltet darüber hinaus die Überprüfung der mathematischen Korrektheit der Signatur des Wurzelstellenzertifikats, aller Signaturen des gesamten Zertifizierungspfades des Signierers, der Signaturen der Verzeichnisdienste der Zertifizierungsstelle und des Zeitstempeldienstes der Zertifizierungsstelle und der RegTP, der Signaturen der zugehörigen Zeitstempeldienst- und Verzeichnisdienstzertifikate, sowie die Überprüfung, ob das Teilnehmerzertifikat vorhanden und nicht gesperrt ist. Die Prüftiefe II repräsentiert die Prüfschritte einer Standard-Verifikation und sollte im Normalfall benutzt werden.

- Zusätzliche Prüfobjekte:

  Signatur des Teilnehmerzertifikats, Signatur des Wurzelstellenzertifikats, Signatur des Verzeichnisdienstes der Zertifizierungsstelle, Signatur des Verzeichnisdienstzertifikats der Zertifizierungsstelle, Signatur des Zertifizierungsstellenzertifikats, Signatur des Zeitstempeldienstes, Signaturen der Zeitstempeldienstzertifikate der Zertifizierungsstelle und der RegTP, Teilnehmerzertifikat

- Zusätzliche Prüfschritte:

  Überprüfung der mathematischen Korrektheit des Wurzelstellenzertifikats mit Hilfe des öffentlichen Signaturschlüssels der Wurzelstelle, sofern das Zertifikat nicht in die signierte Anfrage an den Verzeichnisdienst der RegTP eingebunden ist oder in der Antwort desVerzeichnisdienstes enthalten ist

  Überprüfung der mathematischen Korrektheit der Signatur des Teilnehmerzertifikats mit Hilfe des öffentlichen Signaturschlüssels der Zertifizierungsstelle, sofern der Hashwert des Zertifikats nicht in eine signierte Anfrage an den entsprechenden Verzeichnisdienst eingebunden ist oder in einer zugehörigen Antwort des Verzeichnisdienstes enthalten ist

  Überprüfung der mathematischen Korrektheit der Signatur des Zertifizierungsstellenzertifikats mit Hilfe des öffentlichen Signaturschlüssels der Wurzelstelle, sofern der Hashwert des Zertifikats nicht in eine signierte Anfrage an den Verzeichnisdienst der RegTP eingebunden ist oder in einer zugehörigen Antwort des Verzeichnisdienstes enthalten ist

  Überprüfung der mathematischen Korrektheit der Signaturen von Zeitstempeldiensten mit Hilfe des entsprechenden öffentlichen Signaturschlüssels des Zeitstempeldienstes

  Überprüfung der mathematischen Korrektheit aller Signaturen von Zeitstempeldienstzertifikaten mit Hilfe des entsprechenden öffentlichen Signaturschlüssels, sofern der Hashwert des Zertifikats nicht in eine signierte Anfrage an den Verzeichnisdienst der RegTP eingebunden ist oder in einer zugehörigen Antwort des enthalten ist

  Überprüfung der mathematischen Korrektheit der Signaturen von Verzeichnisdiensten der zugehörigen Zertifizierungsstellen (ohne die der RegTP) mit Hilfe des entsprechenden öffentlichen Signaturschlüssels

  Überprüfung der mathematischen Korrektheit aller Signaturen von Verzeichnisdienstzertifikaten der zugehörigen Zertifizierungsstellen (ohne die der RegTP) mit Hilfe des entsprechenden öffentlichen Signaturschlüssels, sofern der Hashwert des Zertifikats nicht in eine signierte Anfrage an den Verzeichnisdienst der Zertifizierungsstelle eingebunden ist oder in einer zugehörigen Antwort des Verzeichnisdienstes enthalten ist

  Überprüfung, ob das Teilnehmerzertifikat vorhanden und nicht gesperrt ist

PRÜFTIEFE III

- Prüfannahme:

  Der Verifizierer hat kein Vertrauen.

- Prüftiefe:

  Die Prüftiefe III umfaßt die Prüfschritte der Prüftiefe II und beinhaltet darüber hinaus die Überprüfung der mathematischen Korrektheit der Signatur des Verzeichnisdienstes der RegTP, des Verzeichnisdienstzertifikats der RegTP, sowie die Überprüfungen, ob die Zertifikate der Zertifizierungsstelle, des Verzeichnisdienstes der Zertifizierungsstelle und der RegTP, des Zeitstempeldienstes der Zertifizierungsstelle und der RegTP, sowie das Wurzelstellenzertifikat vorhanden und nicht gesperrt sind. Die Prüftiefe III

repräsentiert die Prüfschritte einer vollständigen Verifikation und bietet das höchste Maß an Sicherheit. Sie sollte aber nur auf ausdrücklichen Wunsch des Verifizierers erfolgen.

- Zusätzliche Prüfobjekte:

  Signatur des Verzeichnisdienstes der RegTP, Signatur des Verzeichnisdienstzertifikats der RegTP, alle Zertifikate (Zertifizierungsstellenzertifikat, Zertifikat der RegTP, Verzeichnisdienstzertifikats der Zertifizierungsstelle und der RegTP, Zeitstempeldienst-zertifikate der Zertifizierungsstelle und der RegTP) außer dem Teilnehmerzertifikat (siehe Prüftiefe II)

- Zusätzliche Prüfschritte:

  Überprüfung der mathematischen Korrektheit der Signatur des Verzeichnisdienstes der RegTP mit Hilfe des öffentlichen Signaturschlüssels des Verzeichnisdienstes der RegTP.

  Überprüfung der mathematischen Korrektheit des Verzeichnisdienstzertifikats mit Hilfe des öffentlichen Signaturschlüssels der Wurzelstelle, sofern das Zertifikat nicht in die signierte Anfrage an den Verzeichnisdienst der RegTP eingebunden ist oder in der Antwort desVerzeichnisdienstes enthalten ist

  Überprüfung, ob alle Zertifikte (außer dem Teilnehmerzertifikat, siehe Prüftiefe II) vorhanden und nicht gesperrt sind.

Die Menge der möglichen Anzeigetexte der Anwenderinfrastruktur, die während der Durchführung der Signier- und Verifikationsprozesse zu verwenden sind, können grob in *informelle* und *prozedurale* Anzeigetexte, die eine Anwendereingabe erfordern, unterschieden werden. Die Anwenderinfrastruktur muß den Anwender zum einen über das Auftreten sicherheitsrelevanter Ereignisse während der Signier- und Verifikationsprozesse informieren, und zum anderen Interaktionsmöglichkeiten zur Verfügung stellen, um die Signier- und Verifikationsprozesse kontrollieren und steuern zu können.

MENGE ZU VISUALISIERENDER SICHERHEITSEREIGNISSE

Die Anwenderinfrastruktur muß das Eintreten der folgenden Sicherheitsereignisse bzw. der folgenden Bedingungen dem Anwender durch entsprechende informelle oder prozedurale Anzeigetexte visualisieren:

Management

- Laden aktueller Zertifizierungsrichtlinien
- Schlüsselwechsel des Teilnehmers, der Zertifizierungsstelle oder der RegTP
- Anzeige sicherheitstechnischer Veränderungen

Signierkomponente/Authentisierung

- Aufforderung zur Pin-Eingabe
- Bei Terminals für geschäftsmäßige Nutzung: Nach erfolgreich abgewickelter gegenseitigen Authentisierung Anzeige der kartenspezifischen Display-Info aus der Chipkarte [DIN SigG/V 98]

Signieren

- Notwendigkeit oder Möglichkeit zur Erzeugung einer Übersignatur
- Anzeige der zu signierenden Daten
- Explizite Einwilligung des Anwenders zum Starten der Signaturerstellung
- Auswahl möglicher Signaturschlüsselzertifikate
- Auswahl möglicher beizufügender Attributzertifikate
- Auswahl möglicher Signieralgorithmen
- Anzeige von Fehlermeldungen während des Signierprozesses

Verifikation

- Auswahl der Prüftiefe
- Angabe eines Verifikationszeitpunkts
- Anzeige der Ergebnisse und/oder Fehlermeldungen während des Verifikationsprozesses
- Anzeige der Daten und des Bezugs der digitalen Signatur zu diesen Daten
- Anzeige der Unverfälschtheit der signierten Daten
- Anzeige des Signaturschlüssel-Inhabers des Signierers
- Anzeige der in [SigG 98, §7(1)] beschriebenen und nach SigI [A1 98] obligatorischen Zertifikatsfelder des Signierers

Zeitstempel

- Hinzufügen eines Zeitstempels

Verzeichnisdienst

- Anzeige des Zustandes eines Zertifikates
- Anforderung eines Zertifikates

Voreinstellung

- Setzen, Ändern und Anzeige von Voreinstellungen

2 ANZEIGETEXTE

Anzeigetexte stellen eine Interpretation der komplexen Vorgänge während des Ablaufs der Signier- und Verifikationsprozesse durch die Anwenderinfrastruktur dar. Durch diese Interpretation soll der Anwender in die Lage versetzt werden, diese Vorgänge nachvollziehen zu können. Prozedurale Anzeigetexte bieten darüber hinaus dem Anwender die Möglichkeit zur Interaktion mit der Anwenderinfrastruktur, wodurch dieser durch seine Eingaben bestimmte Vorgänge wie beispielsweise den Start des Signierprozesses nach seinem Willen steuern kann.

Anzeigetexte sind ein wesentlicher Bestandteil der Oberfläche der Anwenderinfrastruktur. Über die technische Realisierung der Oberfläche werden in diesem Dokument keine Aussagen gemacht – sie ist Angelegenheit der Systementwickler. Aus Gründen der Benutzerfreundlichkeit und der Minimierung von erforderlichen Benutzereingaben wird jedoch die Realisierung eines Menüpunktes für Voreinstellungen empfohlen, der es den Benutzern ermöglicht, Voreinstellungen für die Signier- und Verifikationsprozesse festzulegen und diese dann wiederholt nutzen und ändern zu können.Im Rahmen der SigI-Spezifikation besteht ein Anzeigetext konzeptionell aus den Komponenten Titel, sowie Inhalts- und optionalen Eingabefeldern.

Der Titel liefert dem Anwender eine kompakte und präzise Information über ein eingetretenes Sicherheitsereignis. Die Anwenderinfrastruktur muß die in diesem Dokument definierten Titel verwenden. Editorische Änderungen des Wortlautes sind erlaubt, sofern hierdurch keine unterschiedlichen Interpretationsmöglichkeiten für den Anwender entstehen.

Das Inhaltsfeld dient zur Darstellung von Meldungen und Nutzinformationen wie z.B. zu signierende oder empfangene Daten, einzelne Zertifikatsfelder oder komplette Zertifikate und Verzeichnisdienstauskünfte, die dem Anwender in Abhängigkeit eines eingetretenen Sicherheitsereignisses anzuzeigen sind. Inhaltsfelder wie beispielsweise der Name eines Signaturschlüssel-Inhabers enthalten die betreffende Information für den Anwender, die mit einem definierten oder wählbaren Detaillierungsgrad dargestellt werden kann. Der Detaillierungsgrad der Anzeige legt hierbei die Ausprägung hinsichtlich des Umfangs und der Art der Informationsdarstellung fest, d.h. ob z.B. nur pauschale Anzeigen wie z.B.“die Nachricht ist signiert von <Name des Signierers>” oder ob “das zugehörige Zertifikat des Signierers lautet <Zertifikat>” oder “der verifizierte Zertifizierungspfad lautet <Zertifizierungspfad>” usw. ausgegeben werden soll. Mögliche Arten der Darstellung des Inhaltsfeldes sind beispielsweise interpretierte DER-Kodierungen, DER-Kodierungen, ASN.1-Wertedefinitionen oder kompletter Hexadezimalcode (siehe Beispiele in [A1 99, Anhang IV]). Die Anwenderinfrastruktur kann bis auf die folgenden Ausnahmen unterschiedliche Detaillierungsgrade für die Darstellung von Nutzinformationen verwenden und dem Anwender zur Verfügung stellen:

- Daten oder ein Verweis auf die Daten, die zu signieren sind, müssen dem Anwender vollständig und eindeutig angezeigt werden.

- Daten oder ein Verweis auf die Daten, die zu verifizieren sind, müssen dem Anwender vollständig und eindeutig angezeigt werden.

Für die Festlegung der Detaillierungsgrade werden folgende Empfehlungen vorgeschlagen:

DETAILLIERUNGSGRAD/UMFANG I

- Der Umfang der Informationsdarstellung ist beschränkt auf eine minimale Teilmenge der Komponenten einer Struktur { Signaturschlüsselzertifikat | Attributzertifikat | Antwort des Verzeichnisdienstes | Antwort des Zeitstempeldienstes | ... }

DETAILLIERUNGSGRAD/UMFANG II

- Der Umfang der Informationsdarstellung umfaßt alle Komponenten einer Struktur

DETAILLIERUNGSGRAD/ART I

- Die Art der Informationsdarstellung erfolgt durch eine Anzeige der interpretierten DER-Kodierung der Komponenten.

DETAILLIERUNGSGRAD/ART II

- Die Art der Informationsdarstellung erfolgt durch zusätzliche Anzeige des kompletten Hexadezimalcodes der Komponenten.

Der Detaillierungsgrad für die Darstellung von Nutzinformationen sollte vom Teilnehmer auch während der Durchführung der verschiedenen Teilprozesse änderbar sein, ohne daß der jeweilige Teilprozeß wie beispielsweise “Signieren” oder “Verifizieren” wiederholt werden muß, um die Ergebnisse in dem neuen Detaillierungsgrad darzustellen.

Das Eingabefeld ermöglicht die Auswahl, die Akzeptanz oder das Zurückweisen von angezeigten Feldern, die nach manueller Bestätigung des Anwenders von der Anwenderinfrastruktur zu verarbeiten sind. Darüberhinaus sind auch Felder möglich, in den der Anwender freie Eingaben vornehmen kann wie beispielsweise die Adresse einer zusätzlichen Vereichnisdienststelle. Das optionale Eingabefeld muß von der Anwenderinfrastruktur beim Eintreten von Sicherheitsereignissen verwendet werden, die eine explizite Anwendereingabe wie beispielsweise die Einwilligung zur Signaturerstellung erfordern.

In den folgenden Abschnitten werden die Anzeigetexte für den Signier- und den Verifikationsprozeß zusammengestellt, die Informationen enthalten über:

- das Eintreten von Sicherheitsereignissen,
- das Eintreten von Fehlersituationen,
- das Eintreten von Situationen, die eine Warnung erfordern,
- den Inhalt von Zertifikatsfeldern,
- mögliche Verzeichnisdienstauskünfte,
- mögliche Zeitstempeldienstauskünfte und
- mögliche Voreinstellungen.

In diesen Tabellen werden wesentliche Bestandteile der Anzeigetexte durch Fettschrift hervorgehoben. Die Beschreibung von Inhalts- und Eingabefelder erfolgt durch Normalschrift. Konkrete Zertifikatsfelder werden durch in spitze Klammern gesetzte ASN.1-Bezeichner der betreffenden Strukturen wie beispielsweise <subjectPublicKeyInfo> symbolisiert. Mengenklammern { } dienen zur Parametrisierung und kennzeichnen eine Zusammenfasung von Fehlersituationen und Anzeigetexten, wobei einzelne Fehlersituationen oder Anzeigetexte durch das Symbol | getrennt werden. Die Klassifikation von Anzeigetexten in informelle und prozedurale Anzeigetexte wird durch die Symbole I und P angezeigt.

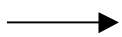
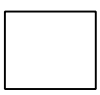
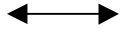
Die erste Spalte der folgenden Tabellen für Anzeigetexte enthält numerierte Kurzbezeichnungen der einzelnen Sicherheitsereignisse, Verzeichnisdienstauskünfte, Zeitstempeldienstauskünfte, Zertifikatsfelder, Fehler- oder Warnsituationen. Hierbei wird die folgende Namenskonvention für Kurzbezeichnungen gewählt:

Tabelle 3: Kurzbezeichnungen von Anzeigetexten

ABKÜRZUNG	BEDEUTUNG	ABKÜRZUNG	BEDEUTUNG
SI	Signaturerzeugung	VO	Voreinstellungen
ÜS	Übersignatur	ÄN	Änderungen
VE	Verifikation	ZI	Zertifikatsinhalte, Informationsinhalte
ZD	Zeitstempel	E	Anzeige eines normalen Ereignisses
VD	Verzeichnisdienst	F	Anzeige eines Fehlers
AM	Authentisierung/Management	W	Anzeige einer Warnung
AN	Anzeige von Voreinstellungen		

In der zweiten Spalte der folgenden Tabellen für Anzeigetexte werden die betreffenden Sicherheitsereignisse, Verzeichnisdienstauskünfte, Zeitstempeldienstauskünfte, Zertifikatsfelder, Fehler- oder Warnsituationen angegeben. Die zweite Spalte enthält im Falle von Fehlersituationen den betreffenden Prüfschritt und das zugehörige Prüfergebnis. Die dritte Spalte enthält den zugehörigen Anzeigetext und in der vierten Spalte wird der Typ des Anzeigetextes angezeigt. Die letzte Spalte enthält Veweise auf Einträge in anderen Tabellen und/oder auf Abschnitte in Dokumenten, aus denen das Sicherheitsereignis, die Fehlersituation oder Warnungen abgeleitet werden, bzw. in denen die Zertifikatsfelder bzw. Verzeichnisdienst- oder Zeitstempeldienstauskünfte beschrieben sind.

Tabelle 4: Bedeutung der grafischen Symbole

SYMBOL	BEDEUTUNG	SYMBOL	BEDEUTUNG
	Prozeß, Teilprozeß		Tabelle für Anzeigetexte
	Prozeßübergang		Verarbeitungsschritt, Auswahlschritt, Prüfschritt
	Rücksprung nach Prozeßbeendigung		
<...>	Kurzbezeichnung eines Anzeigetextes		Fehlerzustand

Um die Anzeigetexte, Fehlermeldungen und Warnungen im Rahmen der Spezifikation hinsichtlich Konsistenz und Vollständigkeit transparent zu machen, werden zur Visualisierung der komplexen Abläufe der Signaturerzeugung und Verifikation vereinfachte Ablaufdiagramme benutzt, in denen die in der Tabelle 4 dargestellten Symbole verwendet werden. Die graphisch dargestellten Abläufe sind allerdings nur als ein möglicher Vorschlag und nicht als eine obligatorische Implementationsvorgabe zu verstehen. Insbesondere können die dargestellten Abläufe und die damit verbundenen Prüfschritte auch in einer anderen Reihenfolge ablaufen. Die folgenden Abbildungen haben nur Beispielcharakter und enthalten nicht alle Vorgänge und Anzeigezeigetexte der zugehörigen Tabellen.

2.1 Authentisierung und Management

Bei der Durchführung von Managementaufgaben und bei Authentisierungsvorgängen sind von der Anwenderinfrastruktur die in den folgenden Tabellen zusammengefaßten Sicherheitsereignisse zu unterstützen. Für die Teilprozesse “Signieren/Übersignieren” und “Verifizieren” ist nach [SigV, §16 (3)] eine persönliche Authentizierung des Teilnehmers erforderlich. Der Vorgang der Authentisierung und der Prozeßauswahl ist in der Abbildung 2 dargestellt.

Tabelle 5: Anzeigetexte für die Authentisierung und das Management

#	SICHERHEITSEREIGNIS	ANZEIGETEXT	TYP	REFERENZ
AM-E-1	SigI-Anwendung ist gestartet	**Bitte legen Sie Ihre Chipkarte ein.**	P	[DIN SigG/V 98]
AM-E-2	Beenden der Sitzung	**Bitte entnehmen Sie Ihre Chipkarte.**	I	[DIN SigG/V 98]
AM-E-3	Erfolgreiche Authentisierung an E4-Terminal	**Die Authentisierung der Chipkarte und des Terminals wurde erfolgreich abgeschlossen. Sie befinden sich an einem signaturgesetzkonformen, geschäftsmäßig genutzten Terminal. Es wird Ihnen Ihre persönliche Benutzerinformation angezeigt.** Anzeige der kartenspezifischen **<Display-Info>** aus der Chipkarte	I	[DIN SigG/V 98]
AM-E-4	Erfolgreiche Authentifikation bei E4-Terminal, erfolgreiche Überprüfung der Chipkarte bei Nicht- E4-Terminal	**Welchen Prozeß möchten Sie auswählen?** Bereitstellung von Selektionskriterien zur Auswahl der folgenden Prozessese <Name der Prozesse/Menüpunkte>	P	
AM-E-5	Aufforderung zur Pin-Eingabe	**Wie lautet Ihre PIN?**	P	[DIN SigG/V 98]
AM-E-6	Erfolgreiche Authentisierung	**Die persönliche Authentisierung wurde erfolgreich abgeschlossen.**	I	[DIN SigG/V 98]

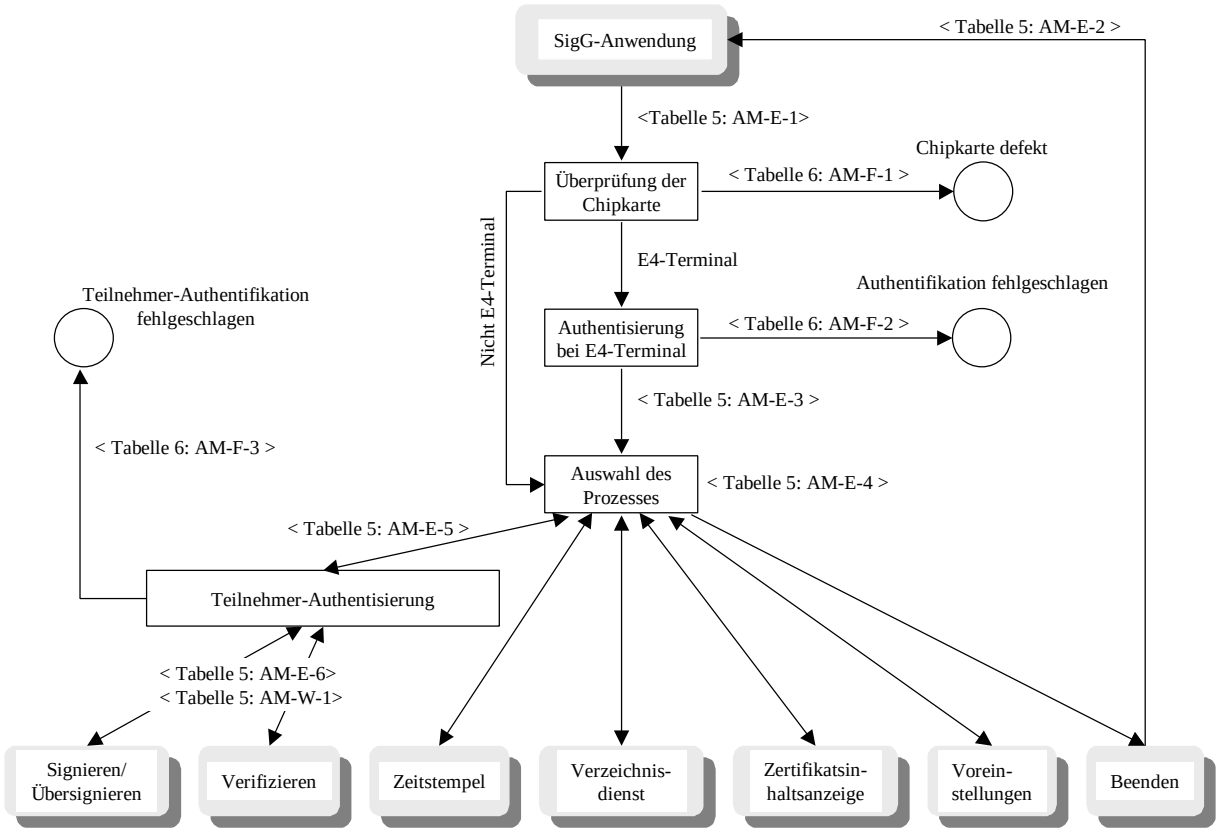
Fortsetzung von Tabelle 5

#	SICHERHEITSEREIGNIS	ANZEIGETEXT	TYP	REFERENZ
AM-E-7	Laden aktueller Zertifizierungsrichtlinien	**Sollen neue Zertifizierungsrichtlinien geladen werden?** Anzeige der neuen Zertifizierungsrichtlinien	P	
AM-E-8	Schlüsselwechsel { des | der } { Teilnehmers | Zertifizierungsstelle | RegTP}	**Soll { der | das } neue { Schlüssel | Signaturschlüsselzertifikat } geladen werden?** Anzeige des neuen { Schlüssels | Signaturschlüsselzertifikats }	P	
AM-E-9	Aufforderung zur Aktualisierung der Daten über die Eignung der Algorithmen	**Sollen die Daten über die Eignung der Algorithmen aktualisiert werden?** Eingabe { ja | nein }	P	

Tabelle 6: Anzeigetexte für Fehlermeldungen und Warnungen bei der Authentisierung und des Managements

#	SICHERHEITSEREIGNIS	ANZEIGETEXT	TYP	REFERENZ
AM-F-1	Defekt der Chipkarte	**Ihre Chipkarte ist defekt. Bitte informieren Sie Ihre Zertifizierungsstelle.**	P	[DIN SigG/V 98]
AM-F-2	Nicht-erfolgreiche Authentisierung von Karte und Terminal	**Die Authentisierung von Chipkarte und Terminal war nicht erfolgreich. Bitte informieren Sie Ihre Zertifizierungsstelle**	I	[DIN SigG/V 98]
AM-F-3	Nicht-erfolgreiche Authentisierung	**Die persönliche Authentisierung war nicht erfolgreich.**	I	[DIN SigG/V 98]
AM-W-1	Anzeige sicherheitstechnischer Veränderungen	**Es sind die folgenden sicherheitstechnischen Veränderungen aufgetreten:** Anzeige der sicherheitstechnischen Veränderungen	I	

Abbildung 2: Initialisierung und Prozeßauswahl



2.2 Voreinstellungen

Um die Prozesse der Signaturerzeugung und Verifikation zu vereinfachen, sollte der Benutzer die Möglichkeit haben, entsprechende Standardeinstellungen vorgeben und ändern zu können. Es wird empfohlen, daß von der Anwenderinfrastruktur die in der folgenden Tabelle zusammengefaßten Anzeigetexte für Voreinstellungen unterstützt werden.

HINWEISE:

In den Anzeigetexten müssen für den *Detaillierungsgrad/Umfang I* mindestens die folgenden Teilkomponenten angezeigt werden:

- Signaturschlüsselzertifikat: <*nameOrPseudonym*> (siehe [A1 99, 2.3.9.5]), <*issuer*> (siehe [A1 99, 2.3.4]), <*serialNumber*> (siehe [A1 99, 2.3.2])
- Signieralgorithmus: <*AlgorithmIdentifier*> (siehe [A2 99, 6])
- Signaturumfang (siehe [A2 99, 3-5]): Anzeige, ob Signaturschlüsselzertifikate und/oder Attributzertifikate in die Signatur miteinbezogen werden, Anzeige der folgenden optionalen Attribute für kryptographische Nachrichten: Signaturzeitpunkt <*SigningTime*>, Ort der Signaturerstellung <*Location*>, Quittungsanforderung <*ReceiptRequest*>, Name

des Dokumentes/Datei <*DocumentName*>, Typ des Dokumentes/Datei <*DocumentType*>, Speicherzeitpunkt <*StorageTime*> und Speichergröße/Dateigröße <*StorageSize*>

- Verzeichnisdienst (siehe [A5 99]): Anzeige, ob die Verifikation mit lokalen Sperrlisten und Zertifikaten oder mit aktuellen Sperrlisten und/oder Zustandsabfragen eines externen Verzeichnisdienstes durchgeführt werden soll.

Tabelle 7: Anzeigetexte für Voreinstellungen

#	SICHERHEITSEREIGNIS	ANZEIGETEXT	TYP	REFERENZ
VO-AN-1	Starten des Teilprozesses "Voreinstellungen"	**Anzeige der Voreinstellungen für die Signaturerstellung** Anzeige { des | der } voreingestellten { Signaturschlüsselzertifikats <Certificate> | Attributzertifikats <AttributCertificate> | Signieralgorithmus <AlgorithmIdentifier> | zu signierenden Attribute <SignedAttrs> } Anzeige, ob das Signaturschlüssel- und Attributzertifikat, in die Signatur eigebunden werden sollen. Anzeige, ob das Signaturschlüsselzertifikat verifiziert werden soll.	I	[A1 99, 2] [A1 99, 3.1] [A2 99, 4] [A2 99, 3]
VO-AN-2	Starten des Teilprozesses "Voreinstellungen"	**Anzeige der Voreinstellungen für die Verifikation** Anzeige der voreingestellten Prüftiefe Anzeige, ob eine Quittungsanforderung automatisch erstellt werden soll	I	
VO-AN-3	Starten des Teilprozesses "Voreinstellungen"	**Anzeige der Voreinstellungen für den Zeitstempeldienst** Anzeige der Addresse des Zeitstempeldienstes und des Namens der zugehörigen Zertifizierungsstelle	I	
VO-AN-4	Starten des Teilprozesses "Voreinstellungen"	**Anzeige der Voreinstellungen für den Verzeichnisdienst** Anzeige der Addresse und der Art des Verzeichnisdienstes und des Namens der zugehörigen Zertifizierungsstelle	I	
VO-AN-5	Starten des Teilprozesses "Voreinstellungen"	**Anzeige der Voreinstellungen für den Detaillierungsgrad der Anzeige von Zertifikatsinhalten** Anzeige, ob alle oder nur die minimal erforderliche Menge der Zertifikatsfelder angezeigt werden soll; Anzeige, ob Zertifikatsinhalte in interpretierter Form oder zusätzlich in Hexadezimalcode angezeigt werden sollen	I	

Fortsetzung von Tabelle 7

#	SICHERHEITSEREIGNIS	ANZEIGETEXT	TYP	REFERENZ
VO-ÄN-1	Starten des Teilprozesses "Voreinstellungen"	**Möchten Sie die { aktuellen | geänderten } Voreinstellungen übernehmen?** Eingabe { ja | nein } und Beenden der Voreinstellungen	P	
VO-ÄN-2	Starten des Teilprozesses "Voreinstellungen"	**Möchten Sie die Voreinstellungen ändern?** Anzeige der Änderungsmöglichkeiten und Eingabe { ja | nein }	P	
VO-SI-ÄN-1	Starten des Teilprozesses "Voreinstellungen"	**Welches Signaturschlüsselzertifikat soll als Voreinstellung für die Signaturerzeugung genutzt werden?** Bereitstellung von Selektionskriterien für die Auswahl **Soll das Zertifikat in die Signatur eingebunden werden?** Eingabe { ja | nein } **Hinweis: eine Einbindung ist erforderlich, wenn darin Beschränkungen oder Angaben Dritter enthalten sind, die für die signierten Daten von Bedeutung sind.** **Soll das Zertifikat verifiziert werden?** Eingabe { ja | nein }	P	
VO-SI-ÄN-2	Starten des Teilprozesses "Voreinstellungen"	**Welche Attributzertifikate sollen als Voreinstellung der Signatur beigefügt werden?** Bereitstellung von Selektionskriterien für die Auswahl, Eingabe { ja | nein } **Hinweis: eine Einbindung ist erforderlich, wenn darin Beschränkungen oder Angaben Dritter enthalten sind, die für die signierten Daten von Bedeutung sind.**	P	
VO-SI-ÄN-3	Starten des Teilprozesses "Voreinstellungen"	**Welcher Signieralgorithmus soll als Voreinstellung benutzt werden?** Bereitstellung von Selektionskriterien für die Auswahl, Eingabe { ja | nein }	P	[A2 99, 6]
VO-SI-ÄN-4	Starten des Teilprozesses "Voreinstellungen"	**Soll eine Quittungsanforderung erstellt werden?** Eingabe { ja | nein }	P	[A2 99, 5]

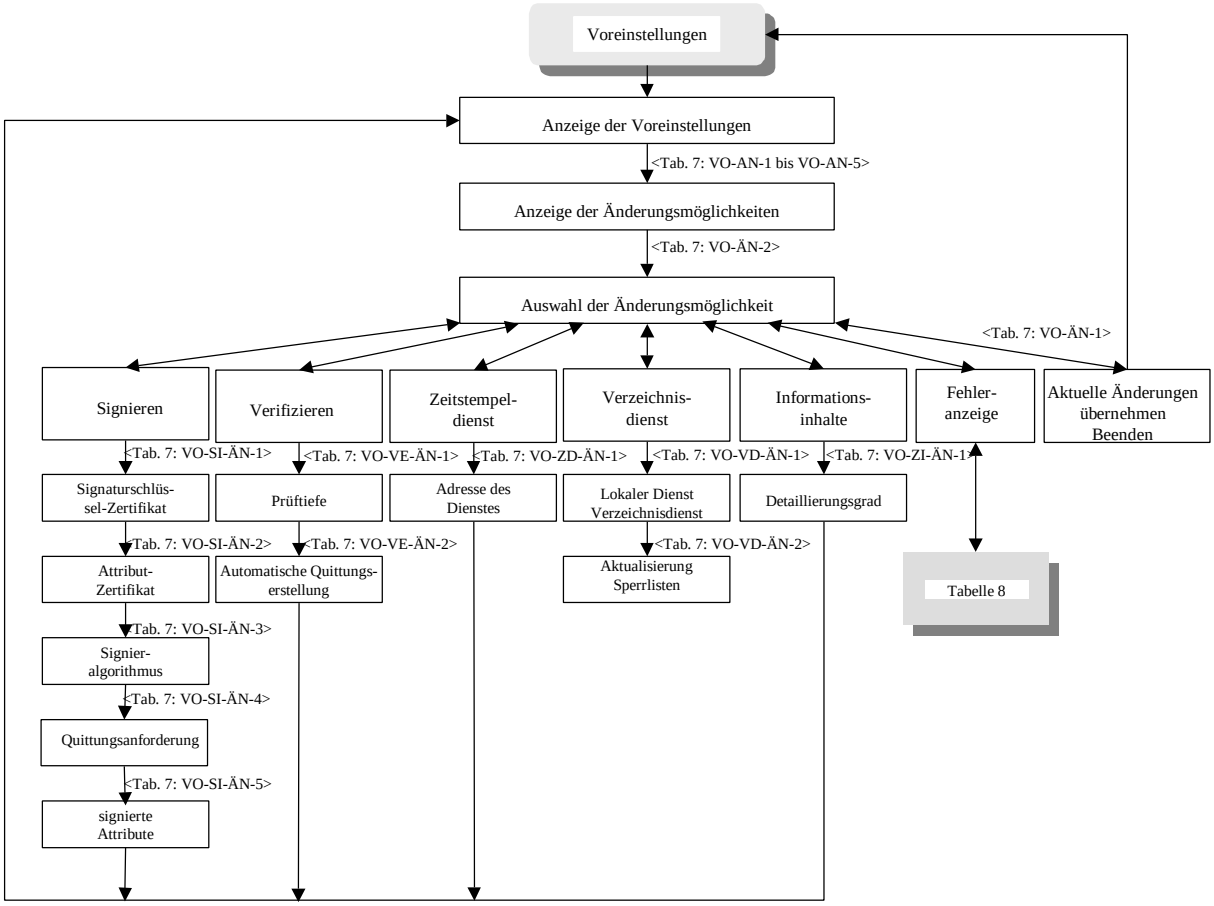
Fortsetzung von Tabelle 7

#	SICHERHEITSEREIGNIS	ANZEIGETEXT	TYP	REFERENZ
VO-SI-ÄN-5	Starten des Teilprozesses "Voreinstellungen"	**Welche sonstigen, optionalen Attribute sollen als Voreinstellung für { signierte | verschlüsselte } Nachrichten benutzt werden?** Bereitstellung von Selektionskriterien für die Auswahl der <*signedAttrs*>, Eingabe { ja | nein }	P	[A2 99, 5]
VO-VE-ÄN-1	Starten des Teilprozesses "Voreinstellungen"	**Welche Prüftiefe soll für die Verifikation benutzt werden?** **Hinweise:** **Prüftiefe I: Dokumentensignatur** **Prüftiefe II: Teilnehmerzertifikat, Attributzertifikate, Zeitstempel** **Prüftiefe III: vollständige Überprüfung** Eingabe { 1 | 2 | 3 }	P	
VO-VE-ÄN-2	Starten des Teilprozesses "Voreinstellungen"	**Soll automatisch eine Quittung erstellt werden, wenn eine solche vom Signierer verlangt wurde?** Eingabe { ja | nein }	P	[A2 99, 3]
VO-ZD-ÄN-1	Starten des Teilprozesses "Voreinstellungen"	**Welcher Zeitstempeldienst soll als Voreinstellung verwendet werden?** Bereitstellung von Selektionskriterien für die Auswahl	P	
VO-VD-ÄN-1	Starten des Teilprozesses "Voreinstellungen"	**Welcher Verzeichnisdienst soll als Voreinstellung verwendet werden?** Bereitstellung von Selektionskriterien für die Auswahl der Addresse und der Art des Verzeichnisdienstes	P	
VO-VD-ÄN-2	Starten des Teilprozesses "Voreinstellungen"	**Sollen die lokalen Sperrlisten aktualisiert werden?** Eingabe { ja | nein }	P	
VO-ZI-ÄN-1	Starten des Teilprozesses "Voreinstellungen"	**Welcher Detaillierungsgrad soll als Voreinstellung für die Anzeige von Informationsinhalten verwendet werden?** Bereitstellung von Selektionskriterien für die Auswahl des Detaillierungsgrades hinsichtlich des Umfangs und der Art der Informationsdarstellung Eingabe { 1 | 2 |... }	P	

Tabelle 8: Anzeigetexte für Fehlermeldungen und Warnungen bei Voreinstellungen

#	SICHERHEITSEREIGNIS	ANZEIGETEXT	TYP	REFERENZ
VO-SI-F-1	Signaturzeitpunkt außerhalb der Gültigkeitsdauer des Signaturschlüsselzertifikats	**Das Signaturschlüsselzertifikat ist { nicht mehr | noch nicht } gültig. Es kann daher nicht für die Signaturerstellung genutzt werden. Bitte wählen Sie eine anderes Signaturschlüsselzertifikat aus.**	I	
VO-SI-F-2	Signieralgorithmus nicht mehr geeignet für die Signaturerstellung	**Das Signaturschlüsselzertifikat sieht für die Signaturerstellung mathematische Verfahren vor, die nicht mehr als geeignet beurteilt werden. Bitte wählen Sie daher ein anderes Signaturschlüsselzertifikat aus.**	I	
VO-SI-F-3	Signaturzeitpunkt außerhalb der Gültigkeitsdauer des Attributzertifikats	**Das Attributzertifikat ist { nicht mehr | noch nicht } gültig. Es kann daher nicht mehr verwendet werden.**	I	
VO-SI-F-4	Signaturzeitpunkt außerhalb der Gültigkeitsdauer des Signaturschlüsselzertifikats	**Das Attributzertifikat verweist auf ein Signaturschlüsselzertifikat das { nicht mehr | noch nicht } gültig ist. Es kann daher nicht mehr verwendet werden.**	I	
VO-VD-F-1	Ablauf der lokal zur Verfügung stehenden Sperrlisten	**Die zur Verfügung stehenden lokalen Sperrlisten sind { abgelaufen | nicht aktuell genug }.**	I	

Abbildung 3: Anzeige und Ändern der Voreinstellungen



2.3 Signierprozeß

Die Eingabeinformation für den Signierprozeßprozeß umfaßt die Daten des Signierers, einen eventuellen Zeitstempel, eine eventuelle Quittungsanforderung und/oder weitere optionale Dokumentenaustauschformat-Attribute, eventuelle Attributzertifikate des Signierers, sowie das Signaturschlüsselzertifikat des Signierers, falls dieses Beschränkungen nach [SigG 97, §7(1)+(2)] und [SigV 97, §4(1) 4.] enthält.

Eine spezielle Form des Signierens ist das sog.“Übersignieren”, bei dem bereits signierte Informationen durch eine erneute Signatur mit einem anderen Signaturschlüssel signiert werden können. Das Übersignieren kann erforderlich werden, falls der Signieralgorithmus der “alten” Signatur als nicht mehr geeignet betrachtet wird.

Der Prozeß “Signieren/Übersignieren” kann im Regelfall mit den Standardeinstellungen des Prozesses “Voreinstellungen” durchgeführt werden. Darüberhinaus können alle für die Signaturerzeugung getroffenen Voreinstellung im Bedarfsfalle durch den Signierer (Verzweigen in den Prozeß “Voreinstellungen”) erneut geändert werden.

Zur Überprüfung der Gültigkeit des gewählten, eigenen Signaturschlüsselzertifikats kann der Signierprozeß in den Verifikationsprozeß verzweigen.

Beim Signieren bzw. Übersignieren sind Anzeigetexte für die in den folgenden Tabelle dargestellten Sicherheitsereignisse und Fehlersituationen zu unterstützen.

Tabelle 9: Anzeigetexte für Sicherheitsereignisse während des Signierprozesses

#	SICHERHEITSEREIGNIS	ANZEIGETEXT	TYP	REFERENZ
SI-E-1	Abweichungen von den Voreinstellungen	**Möchten Sie von den Voreinstellungen für die Signaturerzeugung abweichen?** Eingabe { ja | nein } Verzweigen in den Prozeß "Voreinstellung" bei der Antwort ja.	P	
SI-E-2	Selektion eines Signaturschlüsselzertifikats des Signierers	**Welches Signaturschlüsselzertifikat soll für die Signaturerstellung benutzt werden?** Bereitstellung von Selektionskriterien für die Auswahl eines Signaturschlüsselzertifikates des Signierers, falls dieser mehrere Signaturschlüsselzertifikate besitzt **<Certificate>** **Soll das Signaturschlüsselzertifikat in die Signatur eingebunden werden?** Eingabe { ja | nein } **Hinweis: Eine Einbindung ist erforderlich, wenn darin Beschränkungen oder Angaben Dritter enthalten sind, die für die signierten Daten von Bedeutung sind.**	P	[A1 99, 2]
SI-E-3	Selektion von Attributzertifikaten des Signierers	**Welche Attributzertifikate sollen beigefügt werden?** Bereitstellung von Selektionskriterien für die Auswahl von Attributzertifikaten des Signierers, falls dieser eines oder mehrereAttributzertifikate besitzt, die mitsigniert werden sollen **<AttributeCertificate>** **Hinweis: Eine Einbindung ist erforderlich, wenn darin Beschränkungen oder Angaben Dritter enthalten sind, die für die signierten Daten von Bedeutung sind.**	P	[A1 99, 3.1]
SI-E-4	Verifikation der eigenen Zertifikate des Signierers	**Soll {Ihr eigenes Signaturschlüsselzertifikat | Ihre eigenen Attributzertifikate }verifiziert werden?** Eingabe { ja | nein } Verzweigen in den Prozeß "Verifizieren" bei der Antwort ja.	P	

Fortsetzung von Tabelle 9

#	SICHERHEITSEREIGNIS	ANZEIGETEXT	TYP	REFERENZ
SI-E-5	Selektion des Signieralgorithmus	**Welcher Signieralgorithmus soll verwendet werden?** Bereitstellung von Selektionskriterien zur Auswahl von Signieralgorithmen	P	[A2 99, 6]
SI-E-6	Selektion der zu signierenden Daten	**Welche Daten sollen signiert werden?** Bereitstellung von Selektionskriterien zur Auswahl der zu signierenden Daten **Welches Datentyp haben die Daten?** Bereitstellung von Selektionskriterien zur Auswahl des Datentyps <**type**> **Sollen die Daten angezeigt werden?** Eingabe {ja | nein }	P	[A2 99, Anhang A]
SI-E-7	Automatisch generierte Daten	**Es liegen Daten vor, die automatisch generiert wurden.** Anzeige des Grundes für die automatische Erzeugung der Daten	I	[A2 99, 3]
SI-E-8	Anzeige der zu signierenden Informationen, bestehend aus Daten, Dokumentenaustausch format-Attributen, Attributzertifikaten und des Signaturschlüsselzertifikats	**Von Ihnen wurden die folgenden zu signierenden Daten und Attributzertifikate, sowie das folgende Signaturschlüsselzertifikat ausgewählt:** Anzeige der zu signierenden Daten mit dem Datentyp <**type**> Anzeige der Dokumentenaustauschformat-Attribute <**signedAttrs**>, Attributzertifikate **<AttributeCertificate>**, sowie des Signaturschlüsselzertifikats **<Certificate>**	I	[SigG 97, §14(2)] [A2 99, Anhang A] [A2 99, 4] [A1 99, 3.1., 2]
SI-E-9	Einwilligung zur Signaturerstellung	**Sollen die Ihnen angezeigten Daten und Attributzertifikate mit dem von Ihnen ausgewählten Signaturschlüssel signiert werden?** Bereitstellung von Eingabefeldern, in denen der Signierer seine Einwilligung oder seine Ablehnung zum Signieren der angezeigten Daten und Attributzertifikate **<AttributeCertificate>** mit dem angezeigten Signaturschlüssel **<subjectPublicKeyInfo>** geben kann	P	[SigV 97, §16(3)] [A1 99, 3.1] [A1 99, 2.3.7]
SI-E-10	Erfolgreicher Signiervorgang	**Die Daten wurden mit einer aus technischer Sicht signaturgesetzkonformen digitalen Signatur versehen. Hierdurch sind Manipulationsfreiheit und nachweisbare Urheberschaft mindest bis zum Ablauf <Ablauf-Eignungszeitraum der Algorithmen> sichergestellt.**		

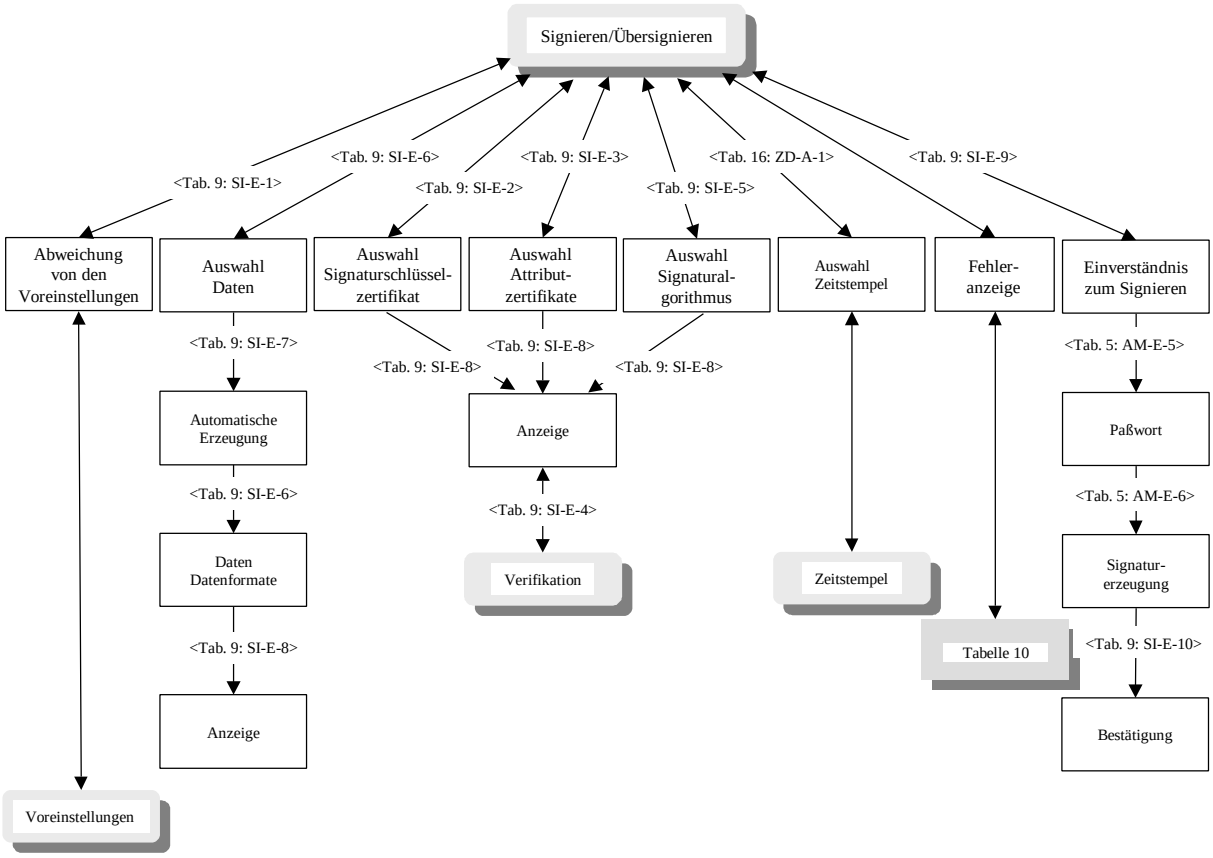
Fortsetzung von Tabelle 9

#	SICHERHEITSEREIGNIS	ANZEIGETEXT	TYP	REFERENZ
SI-E-10	Erfolgreicher Signiervorgang	**Hinweis:** **Soll die Gültigkeit der Signatur über diesen Zeitraum hinaus gewährleistet sein, so muß vorher eine weitere digitale Signatur mit Zeitstempel (Übersignatur) angebracht werden.** **Für den Fall einer nachfolgenden Sperrung Ihres Zertifikates kann das Anbringen eines Zeitstempels sinnvoll sein. So kann der Nachweis geführt werden, daß die Signatur vor der Sperrung erstellt wurde.**	I	

Tabelle 10: Anzeigetexte für Fehlermeldungen während des Signierprozesses

#	FEHLERSITUATION	ANZEIGETEXT	TYP	REFERENZ
SI-F-1	Gültigkeitsdauer des { Signaturschlüsselzertifikats | Attributzertifikats }:	**Das** {**Signaturschlüsselzertifikat | Attributzertifikat**} **ist zum Signierzeitpunkt { abgelaufen | noch nicht gültig }.** Anzeige des Endes der Gültigkeitsdauer **<notAfter | notAfterTime >** oder	I	
	zum Signierzeitpunkt abgelaufen oder noch nicht gültig	Anzeige des Beginns der Gültigkeitsdauer **<notBefore | notBeforeTime >**		[A1 99, 2.3.5, 3.7]
SI-F-2	Fehlerhafter Signiervorgang	**Die Daten, Datei, Signierkomponente, Signierschlüssel sind nicht verfügbar oder defekt. Die Daten konnten nicht signiert werden.**	I	

Abbildung 4: Signierprozeß



2.4 Verifizierprozeß

Die Eingabeinformation für den Verifikationsprozeß umfaßt die Daten des Signierers, eventuelle Attributzertifikate des Signierers, einen eventuellen Zeitstempel, eine eventuelle Quittungsanforderung, das Signaturschlüsselzertifikat des Signierers, falls dieses Beschränkungen nach [SigG 97,§7(1)+(2)] enthält, sowie die zu verifizierende Signatur unter alle genannten Einzelinformationen.

Der Prozeß “Verifizieren” kann im Regelfall mit den Standardeinstellungen des Prozesses “Voreinstellungen” durchgeführt werden. Darüberhinaus können alle für die Verifikation getroffenen Voreinstellung im Bedarfsfalle durch den Verifizierer (Verzweigen in den Prozeß “Voreinstellungen”) erneut geändert werden.

Zur Erstellung einer Quittung und eines Zeitstempels kann der Verifizierprozeß in die Prozesse “Signieren/Übersignieren” und “Zeitstempel” verzweigen.

Zur Beschaffung erforderlicher Zertifikate und zur Abfrage von deren Zuständen kann der Verifizierprozeß in den Prozeß “Verzeichnisdienst” verzweigen. Die Verifikation digitaler Signaturen und Zertifikate erfolgt hinsichtlich eines bestimmten Prüfzeitpunktes, den der Verifizierer vorgeben kann oder der durch einen Zeitstempel <*tstTime*> (siehe [A4 99, 6.2.1])

vorgeben sein kann. Die betreffenden Zertifikate müssen zum Prüfzeitpunkt beim Verzeichnisdienst vorhanden gewesen sein und dürfen nicht gesperrt gewesen sein. Falls ein Prüfzeitpunkt nicht explizit vorgegeben ist, so wird die aktuelle Zeit als Prüfzeitpunkt genommen. In dem Verifikationsprozeß werden im Zusammenhang mit dem Prüfzeitpunkt die Antworten des Verzeichnisdienstes (siehe [A5 99, 2.2.2]) ausgewertet und dem Benutzer angezeigt. Mögliche Antworten des Verzeichnisdienstes sind:

- Das Zertifikat ist zum <Prüfzeitpunkt> nicht im Verzeichnisdienst vorhanden.
- Das am <*dateOfCertGen*> erstellte Zertifikat ist seit <*certInDirSince*> im Verzeichnisdienst vorhanden und nicht gesperrt.
- Das am <*dateOfCertGen*> erstellte Zertifikat ist seit <*certInDirSince*> im Verzeichnisdienst vorhanden und seit <*revocationTime*> gesperrt.

Beim Verifizieren sind Anzeigetexte für die in den folgenden Tabelle dargestellten Sicherheitsereignisse und Fehlersituationen zu unterstützen.

Tabelle 11: Anzeigetexte für Sicherheitsereignisse während des Verifikationsprozesses

#	SICHERHEITSEREIGNIS	ANZEIGETEXT	TYP	REFERENZ
VE-E-1	Abweichungen von den Voreinstellungen	**Möchten Sie von den Voreinstellungen für die Verifikation abweichen?** Eingabe { ja | nein } Verzweigen in den Prozeß "Voreinstellung" bei der Antwort ja.	P	
VE-E-2	Auswahl des Dokumentes	**Welche Daten sollen auf das Vorliegen einer digitalen Signatur überprüft werden?** Bereitstellung der Selektionskriterein zur Auswahl des zu überprüfenden Dokumentes.	P	
VE-E-3	Anzeige der signierten Daten und Attributzertifikate, sowie des Signaturschlüsselzertifikates	**Es wurden die folgenden signierten Daten, Attributzertifikate und das Signaturschlüsselzertifikat } empfangen:** Anzeige der empfangenen Daten mit dem Datenformat <**type**> und Attributzertifikate <**AttributeCertificate**> und des Signaturschlüsselzertifikates <**Certificate**>	I	[SigV 97,§16(3)] [SigV 97, §4(1)] [A2 99, Anhang A] [A1 99, 3.1] [A1 99, 2]
VE-E-4	Anzeige des Namens bzw. Pseudonyms des Signierers	**{ Der gesetzliche Name | Das Pseudonym } des Signierers lautet:** Anzeige des gesetzlichen Namens bzw. des Pseudonyms des Signierers <**subjectAltName**> **Sollen Ihnen die signierten Daten angezeigt werden?** Eingabe { ja | nein }	P	[SigG 97,§14(2)] [A1 99, 2.3.9.5]

Fortsetzung von Tabelle 11

#	SICHERHEITSEREIGNIS	ANZEIGETEXT	TYP	REFERENZ
VE-E-5	Anzeige einer Übersignatur Anzeige eines Zeitstempels	**Die Signatur stellt eine Übersignatur dar. Die Daten wurden vom Signierer am <signing-Time> übersigniert.** **Die Signatur weist einen integren Zeitstempel vom <tstTime > auf. Es erfolgt eine auf diesen Zeitpunkt bezogene Verifikation - eine spätere erfolgte Sperrung des Zertifikats hat keine Auswirkung auf die Gültigkeit der Signatur.**	P	[A2 99, 5.2] [A5 99, 2.2]
VE-E-6	Aufforderung zur Eingabe eines Prüfzeitpunktes	**Auf welchen Prüfzeitpunkt soll sich die Überprüfung beziehen?** **Hinweis: Das Zertifikat muß zum Zeitpunkt der Signaturerstellung bei der ausstellenden Zertifizierungsstelle vorhanden gewesen sein und darf zu diesem Zeitpunkt nicht gesperrt gewesen sein. Ist der Zeitpunkt der Signaturerstellung unbekannt, so genügt es, wenn diese Anforderungen zu einem späteren Zeitpunkt gegeben sind.**	P	[A6 99, 5.2.2]
VE-E-7	Anzeige des Prüfzeitpunktes	**Die Signatur wurde zum <Prüfzeitpunkt> verifiziert.**	I	[A5 99, 2.2]
VE-E-8	Anzeige der mathematischen Korrektheit der signierten Daten und Attributzertifikate, sowie des Signaturschlüsselzertifikates	**Die empfangenen Daten, Attributzertifikate und das Signaturschlüsselzertifikat sind mathematisch korrekt, d.h. sie wurden nicht manipuliert.**	I	[SigG 97,§14(2)]
VE-E-9	Anzeige der erfolgreichen Verifikation mit Visualisierung der überprüften Zertifikate	**Alle durchgeführten Prüfschritte waren erfolgreich. Bei der Verifikation wurden die folgenden Zertifikate {des | der } {Signierers | Zertifizierungsstelle | RegTP | Verzeichnisdienstes | Zeitstempeldienstes } überprüft:** Anzeige der durchgeführten Prüfschritte und überprüften Zertifikate. **Hinweis:** **Soll die Gültigkeit der Signatur über diesen Zeitraum hinaus gewährleistet sein, so muß vorher eine weitere digitale Signatur mit Zeitstempel (Übersignatur) angebracht werden.** **Für den Fall einer nachfolgenden Sperrung Ihres Zertifikates kann das Anbringen eines Zeitstempels sinnvoll sein. So kann der Nachweis geführt werden, daß die Signatur vor der Sperrung erstellt wurde.**		

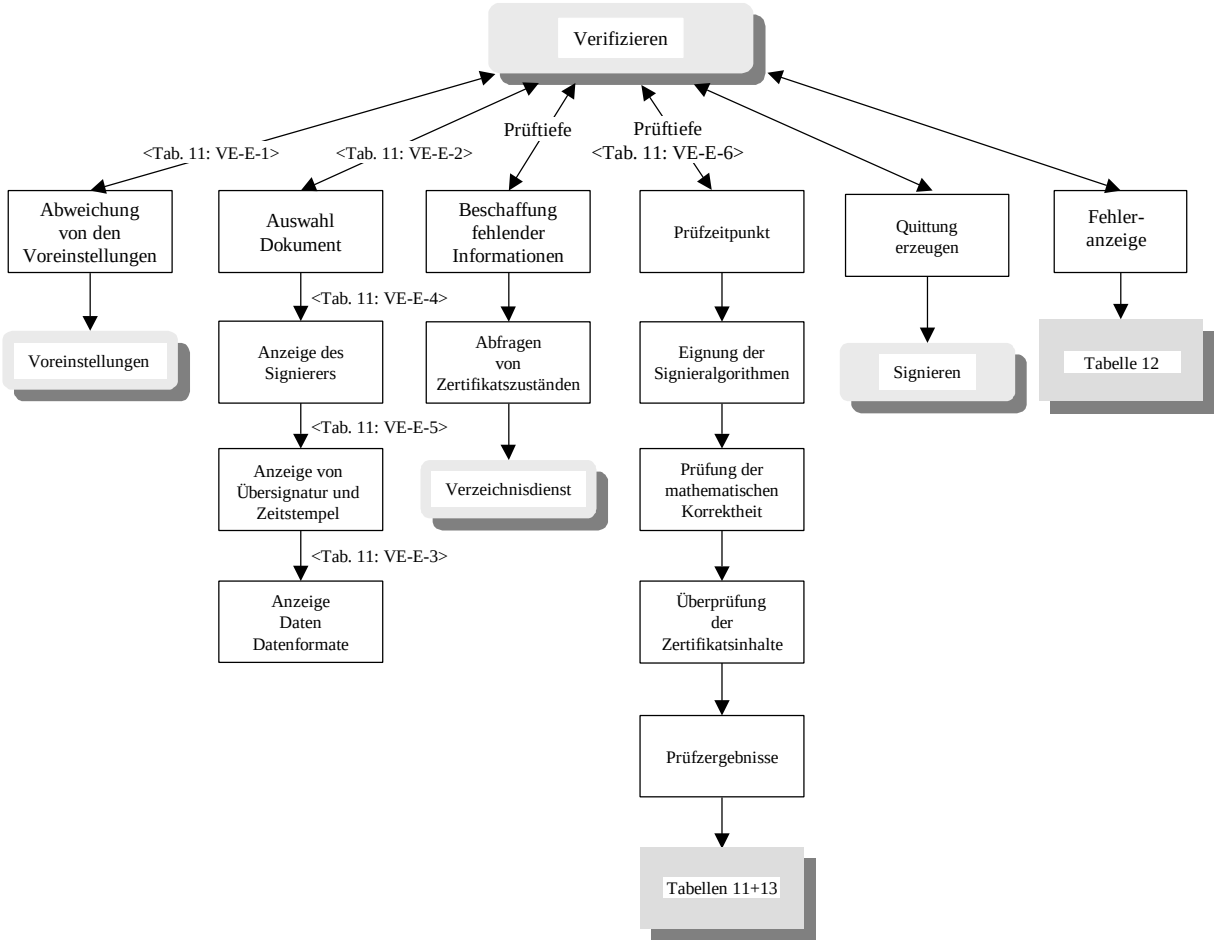
Tabelle 12: Anzeigetexte für Fehlermeldungen und Warnungen während des Verifikationsprozesses

#	FEHLERSITUATION	ANZEIGETEXT	TYP	REFERENZ
VE-F-1	Fehlgeschlagene Prüfschritte	**Die Verifikation konnte nicht erfolgreich durchgeführt werden**. Anzeige der Gründe für das Scheitern der Verifikation	I	
VE-F-2	Nicht signierte Daten	**Die ausgewählten Daten sind nicht digital signiert.**	I	
VE-F-3	Nicht verfügbare Zertifikate	**Das { Signaturschlüsselzertifikat | Attributzertifikat} { des | der } {Signierers | Zertifizierungsstelle | RegTP | Verzeichnisdienstes | Zeitstempeldienstes } ist nicht im Verzeichnisdienst vorhanden.**	I	
VE-F-4	Gültigkeitsdauer des Zertifikates: Zum Prüfzeitpunkt abgelaufen oder noch nicht gültig.	**Das { Signaturschlüsselzertifikat | Attributzertifikat} { des | der } { Signierers | Zertifizierungsstelle | RegTP | Verzeichnisdienstes | Zeitstempeldienstes } ist zum <Prüfzeitpunkt> abgelaufen oder noch nicht gültig** Anzeige des Endes der Gültigkeitsdauer **<notAfter | notAfterTime>** oder Anzeige des Beginns der Gültigkeitsdauer **<notBefore | notBeforeTime>**	I	[A5 99,2.2] [A1 99, 2.3.5]
VE-F-5	Überprüfung der Signatur: nicht erfolgreich	**Die Signatur unter { den | der | dem } { Benutzerdaten | Sperrinformation | Zeitstempel-information | Zertifikat des Signierers | Zertifikat der Zertifizierungsstelle | Zertifikat der RegTP | Zertifikat des Verzeichnisdiensts | Zertifikat des Zeitstempeldiensts } ist mathematisch nicht korrekt; evtl. wurden die unterschriebenen Daten manipuliert.**	I	
VE-F-6	Zertifikatserweiterungen : Unbekannte kritische Erweiterung	**Das Signaturschlüsselzertifikat { des |der } { Signierers | Zertifizierungsstelle | RegTP | Verzeichnisdienstes | Zeitstempeldienstes } enthält folgende unbekannte und als critical markierte Erweiterungen:** Anzeige der betreffenden Erweiterung <**Extension**>	I	[A1 99, 2.3.9]
VE-F-7	Zertifikatserweiterungen : Unbekannte Sicherheitsrichtlinien	**Das Signaturschlüsselzertifikat { des | der} { Signierers | Zertifizierungsstelle | RegTP | Verzeichnisdienstes | Zeitstempeldienstes } enthält folgende unbekannten Bezeichner für Sicherheitsrichtlinien:** Anzeige der betreffenden Bezeichners für Sicherheitsrichtlinien: <**policyIdentifier**>	I	[A1 99, 2.3.9.4]
VE-F-8	Schlüsselnutzungsberechtigung :	**Der Schlüssel darf nicht zum Signieren von { Benutzerdaten | Zertifikaten | Sperrlisten } sondern nur für die folgenden Zwecke benutzt werden:**	I	

Fortsetzung von Tabelle 12

#	FEHLERSITUATION	ANZEIGETEXT	TYP	REFERENZ
VE-F-8	Erforderliche Bits nicht gesetzt	Anzeige der gesetzten Nutzungsbits des Signaturschlüsselzertifikat { des | der } { Signierers | Zertifizierungsstelle | RegTP | Verzeichnisdienstes | Zeitstempeldienstes }: <**KeyUsage**>	I	[A1 99, 2.3.9.2]
VE-F-9	Erweiterte Schlüsselnutzungsberechtigung :	**Der Zertifikatsinhaber des { Verzeichnisdienstes | Zeitstempeldienstes } darf keine { Verzeichnisdienstauskünfte | Zeitstempelinformationen } ausstellen:**	I	
	Erforderliche Bits nicht gesetzt	Anzeige der anwendungsabhängigen Verwendungszwecke im Signaturschlüsselzertifikat des/der { Verzeichnisdienstes | Zeittempeldienstes }: <**extKeyUsage** >		[A1 99, 2.3.9.3]
VE-F-10	Berechtigung für das Erstellen von Zertifikaten : nicht vorhanden	**Der Inhaber des Zertifizierungsstellen-Zertifikats darf keine Zertifikate ausstellen:** Anzeige der Berechtigung für das Erstellen von Zertifikaten: <**basicConstraints**>	I	[A1 99, 2.3.9.1]
VE-F-11	Überprüfung des Zertifizierungspfades:	**Die Überprüfung der mathematischen Korrektheit des Zertifizierungspfades des { Signaturschlüsselzertifikats | Attributzertifikats** } { **des | der } { Signierers | Zertifizierungsstelle | Verzeichnisdienstes | Zeitstempeldienstes } endet bei einem unbekannten Schlüssel der RegTP.**	I	
	Unbekannter Schlüssel der RegTP	Anzeige des unbekannten öffentlichen Schlüssels **<subjectPublicKey>** der RegTP		[A1 99, 2.3.7]
VE-F-12	Überprüfung der Eignung des Signieralgorithmus: Ungültig oder zum Prüfzeitpunkt nicht mehr geeignet	**Der verwendete Signieralgorithmus der Signatur unter { den | der | dem }{ Benutzerdaten | Sperrinformation | Zeitstempelinformation | Zertifikat des Signierers | Zertifikat der Zertifizierungsstelle | Zertifikat der RegTP | Zertifikat des Verzeichnisdiensts | Zertifikat des Zeitstempeldienstes** }**ist ungültig oder nicht mehr geeignet.** Anzeige des ungeeigneten Signieralgorithmus	I	
VE-W-1	Überprüfung der Eignungsdauer des Signieralgorithmus : Zum Prüfzeitpunkt nur noch begrenzt gültig	**Der verwendete Signieralgorithmus der Signatur unter { den | der | dem }{ Benutzerdaten | Sperrinformation | Zeitstempelinformation | Zertifikat des Signierers | Zertifikat der Zertifizierungsstelle | Zertifikat der RegTP | Zertifikat des Verzeichnisdiensts | Zertifikat des Zeitstempeldienstes** }**ist mindestens bis zum <date> geeignet.** **Wird die Eignungsdauer nicht verlängert, so ist vor ihrem Ablauf ein Übersignieren der signierten Daten erforderlich.** Anzeige des Endes der Eignungsdauer des verwendeten Signieralgorithmus **Soll eine Übersignatur erzeugt werden?**	I	

Abbildung 5: Verifikationsprozeß



2.5 Zertifikatsfelder

Beim Signieren und Verifizieren sind von der Anwenderinfrastruktur die in der folgenden Tabelle zusammengefaßten Anzeigetexte für Signaturschlüssel- und Attribut-Zertifikatsfelder [SigG 97, §7(1)] zu unterstützen.

Tabelle 13: Anzeigetexte für Zertifikatsfelder

#	ZERTIFIKATSFELD	ANZEIGETEXT	TYP	REFERENZ
ZI-1	Name bzw. Pseudonym des Signierers	**{ Der gesetzliche Name | Das Pseudonym } des Signierers lautet:** Anzeige des { gesetzlichen Namens | Pseudonyms } des { Signaturschlüsselzertifikats | Attributzertifikats } des Signierers <**subjectAltName**>	I	[SigG 97, §7(1)] [A1 99, 2.3.9.5]
ZI-2	Verweis auf Signaturschlüsselzertifikat im Attributzertifikat	**Das Attributzertifikat enthält folgenden Verweis auf das korrespondierende Signaturschlüsselzertifikat:** Anzeige des Inhaberfeldes <**subject**> des Attributzertifikats des Signierers.	I	[SigG 97, §7(1)] [A1 99, 3.3]
ZI-3	Öffentlicher Signaturschlüssels des Signierers	**Folgender öffentlicher Signaturschlüssel ist dem Zertifikatsinhaber zugeordnet:** Anzeige des öffentlichen Signaturschlüssels <**subjectPublicKeyInfo**>	I	[SigG 97, §7(1)] [A1 998, 2.3.7]
ZI-4	Signaturalgorithmus der Zertifizierungsstelle	**Das { Signaturschlüsselzertifikat | Attributzertifikat } des Signierers ist mit dem folgenden Algorithmus von der zugehörigen Zertifizierungsstelle signiert worden:** Anzeige des benutzten Algorithmus der Zertifizierungsstelle <**signatureAlgorithm**>	I	[SigG 97, §7(1)] [A1 99, 2.1, 3.5]
ZI-5	Seriennummer	**Die laufende Nummer des { Signaturschlüsselzertifikats | Attributzertifikats } des Signierers lautet:** Anzeige der Seriennummer des { Signaturschlüsselzertifikats | Attributzertifikats } des Signierers <**serialNumber**>	I	[SigG 97, §7(1)] [A1 99, 2.3.2, 3.6]
ZI-6	Gültigkeitsdauer	**Die Gültigkeitsdauer des { Signaturschlüsselzertifikats | Attributzertifikats } des Signierers ist durch die folgenden zwei Zeitpunkte begrenzt:** Anzeige des Beginns und des Endes der Gültigkeitsdauer des { Signaturschlüsselzertifikats | Attributzertifikats } des Signierers <**validity** | **attrCertValidityPeriod**>	I	[SigG 97, §7(1)] [A1 99, 2.3.5, 3.7]
ZI-7	Name der Zertifizierungsstelle	**Der technische Name der Zertifizierungsstelle, die das { Signaturschlüsselzertifikat | Attributzertifikat } des Signierers ausgestellt hat, lautet:** Anzeige des technischen Namens der Zertifizierungsstelle die das Signaturschlüsselzertifikat des Signierers ausgestellt hat <**issuer**>	I	[SigG 97, §7(1)] [A1 99, 2.3.4, 3.4]

Fortsetzung von Tabelle 13

#	ZERTIFIKATSFELD	ANZEIGETEXT	TYP	REFERENZ
ZI-8	Unterscheidung von Zertifizierungsstellen- und Endbenutzer-Zertifikaten	**Der Zertifikatsinhaber des { Signaturschlüsselzertifikats | Attributzertifikats } {darf | darf nicht} als Zertifizierungsinstanz auftreten** Anzeige der cA-Komponente im <**basicConstraints**> Erweiterungsfeld.	I	[A1 99, 2.3.9.1]
ZI-9	Verwendungszweck des Signaturschlüssels	**Der Signaturschlüssel darf zu folgenden Zwecken benutzt werden:** Anzeige der gesetzten Nutzungsbits im <**keyUsage**> Erweiterungsfeld.	I	[A1 99, 2.3.9.2]
ZI-10	Anwendungsabhängige Verwendungszwecke des Signaturschlüssels	**Der Signaturschlüssel darf für folgende Anwendungen benutzt werden:** Anzeige der Objektbezeichner im <**extKeyUsage**> Erweiterungsfeld	I	[A1 99, 2.3.9.3]
ZI-11	Zertifizierungsrichtlinien	**Das { Signaturschlüsselzertifikat | Attributzertifikat } enthält folgende Bezeichner für Sicherheitsrichtlinien:** Anzeige der Objektbezeichner im <**certificatePolicies**> Erweiterungsfeld	I	[A1 99, 2.3.9.4]
ZI-12	Alternative Namen von Zertifikatsinhabern	**Das { Signaturschlüsselzertifikat | Attributzertifikat } enthält folgende alternative Namen des Zertifikatsinhabers:** Anzeige der Namen im <**subjectAltName**> Erweiterungsfeld	I	[A1 99, 2.3.9.5]
ZI-13	Alternative Namen von Zertifizierungsstellen	**Das { Signaturschlüsselzertifikat | Attributzertifikat } enthält folgende alternative Namen der Zertifizierungsstelle:** Anzeige der Namen im **<issuerAltName>** Erweiterungsfeld	I	[A1 99, 2.3.9.6]
ZI-14	Identifizierung der Signaturschlüssel von Zertifizierungsstellen	**Das { Signaturschlüsselzertifikat | Attributzertifikat } enthält folgenden Signaturschlüssel-Identifikator der Zertifizierungsstelle:** Anzeige des Signaturschlüssel-Identifikators der Zertifizierungsstelle <**authorityKeyIdentifier**>	I	[A1 99, 2.3.9.7]
ZI-15	Identifizierung des öffentlichen Teilnehmerschlüssels	**Das { Signaturschlüsselzertifikat | Attributzertifikat } enthält folgenden Signaturschlüssel-Identifikator des Zertifikatsinhabers:** Anzeige des Signaturschlüssel-Identifikators des Zertifikatsinhabers **<subjectKeyIdentifier>**	I	[A1 99, 2.3.9.8]

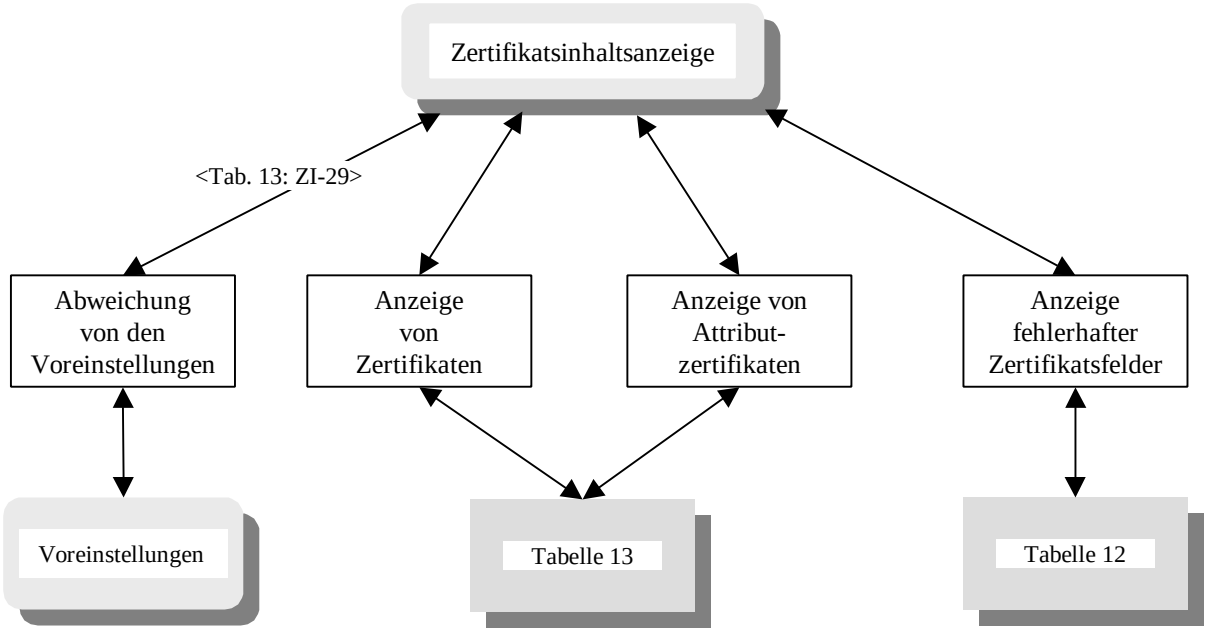
Fortsetzung von Tabelle 13

#	ZERTIFIKATSFELD	ANZEIGETEXT	TYP	REFERENZ
ZI-16	Beschaffung von Sperrlisten	**Das { Signaturschlüsselzertifikat | Attributzertifikat } enthält folgende Informationen zur Beschaffung von Sperrlisten:** Anzeige der Informationen der **<cRLDistributionPoints>** Erweiterung	I	[A1 99, 2.3.9.9]
ZI-17	Anerkennung fremder Zertifizierungsrichtlinien	**Das { Signaturschlüsselzertifikat | Attributzertifikat } enthält folgende anerkannte fremde Zertifizierungsrichtlinien:** Anzeige der Objektbezeichnerpaare im <**policyMappings**> Erweiterungsfeld	I	[A1 99, 2.3.9.10]
ZI-18	Verzeichnisattribute für Zertifikatsinhaber	**Das { Signaturschlüsselzertifikat | Attributzertifikat } enthält folgende Verzeichnisattributwerte des Zertifikatsinhabers:** Anzeige der Attribute im <**subjectDirectoryAttributes**> Erweiterungsfeld	I	[A1 99, 2.3.9.11]
ZI-19	Informationen zur Zertifizierungsstelle	**Das { Signaturschlüsselzertifikat | Attributzertifikat } enthält folgende Zugriffs-Informationen über die Zertifizierungsstelle:** Anzeige der Informationen im <**AuthorityInfoAccess**> Erweiterungsfeld	I	[A1 99, 2.3.9.15.1]
ZI-20	Beschränkungsinformation	**Das Signaturschlüsselzertifikat des Signierers { enthält | enthält keine } Beschränkungen der Nutzung des Signaturschlüssels.** Anzeige der Beschränkungsinformation <**liabilityLimitationFlag**>	I	[SigG 97, §7(1)] [A1 99, 2.3.9.15.2]
ZI-21	Vertretungsmacht	**Das { Signaturschlüsselzertifikat | Attributzertifikat } des Signierers enthält folgende Angaben zur Vertretungsmacht für eine dritte Person:** Anzeige der Vetretungsmacht <**procuration | atProcuration>**	I	[SigG 97, §7(2)] [A1 99, 2.3.9.15.4, 3.9.1]
ZI-22	Berufsrechtliche Zulassungsinformation	**Das { Signaturschlüsselzertifikat | Attributzertifikat } des Signierers enthält folgende Angaben zu einer berufsrechtlichen Zulassung:** Anzeige der berufsrechtlichen Zulassung < **admission | atAdmission >**	I	[SigG 97, §7(2)] [A1 99, 2.3.9.15.5, 3.9.1]

Fortsetzung von Tabelle 13

#	ZERTIFIKATSFELD	ANZEIGETEXT	TYP	REFERENZ
ZI-23	Erstellungsdatum des Zertifikates	**Das { Signaturschlüsselzertifikat | Attributzertifikat } des Signierers enthält das folgende Erstellungsdatum des Zertifikates:** Anzeige des Erstellungsdatums des Signaturschlüsselzertifikates des Signierers <**dateOfCertGen**>	I	[SigG 97, §7(2)] [A1 99, 2.3.9.15.3]
ZI-24	Monetäre Beschränkung	**Das { Signaturschlüsselzertifikat | Attributzertifikat } des Signierers enthält folgende Angaben zu einer monetären Beschränkung:** Anzeige der monetären Beschränkung < **monetaryLimit** | **atMonetaryLimit >**	I	[SigG 97, §7(1)] [A1 99, 2.3.9.15.6, 3.9.3]
ZI-25	Angaben zur Volljährigkeit	**Das { Signaturschlüsselzertifikat | Attributzertifikat } des Signierers enthält folgende Angaben zur Volljährigkeit des Signierers:** Anzeige der Volljährigkeitsinformation <**declarationOfMajority** | **atDeclarationOfMajority**>	I	[SigG 97, §7(3)] [A1 99, 2.3.9.15.7, 3.9.4]
ZI-26	Angaben zur Chipkarten-seriennummer	**Das { Signaturschlüsselzertifikat | Attributzertifikat } des Signierers enthält folgende Angaben zur Seriennummer im Chipkartenbereich:** Anzeige der Seriennummer <**iCCSN**>	I	[SigG 97, §7(3)] [A1 99, 2.3.9.15.8]
ZI-27	Angaben zur Chipkarten-Referenzierung öffentlicher Schlüssel	**Das { Signaturschlüsselzertifikat | Attributzertifikat } des Signierers enthält folgende Angaben zur Referenzierung öffentlicher Schlüssel im Chipkartenbereich:** Anzeige der Referenzierungsinformation <**pkReference**>	I	[SigG 97, §7(3)] [A1 99, 2.3.9.15.9]
ZI-28	Sonstige Beschränkung	**Das { Signaturschlüsselzertifikat | Attributzertifikat } des Signierers enthält folgende Angaben zu sonstigen Beschränkungen:** Anzeige der sonstigen Beschränkungsinformation <**restriction** | **atRestriction**>}	I	[SigG 97, §7(2)] [A1 99, 2.3.9.15.10, 3.9.5]
ZI-29	Starten der "Zertifikats-inhaltsanzeige"	**Möchten Sie die Voreinstellung für den Teilprozeß "Zertifikatsinhaltsanzeige" ändern?** Eingabe { ja | nein}	P	

Abbildung 6: Zertifikatsinhaltsanzeige



2.6 Verzeichnisdienstauskünfte

Beim Signieren und Verifizieren sind von der Anwenderinfrastruktur die in den folgenden Tabellen zusammengefaßten Anzeigetexte für Verzeichnisdienstauskünfte zu unterstützen

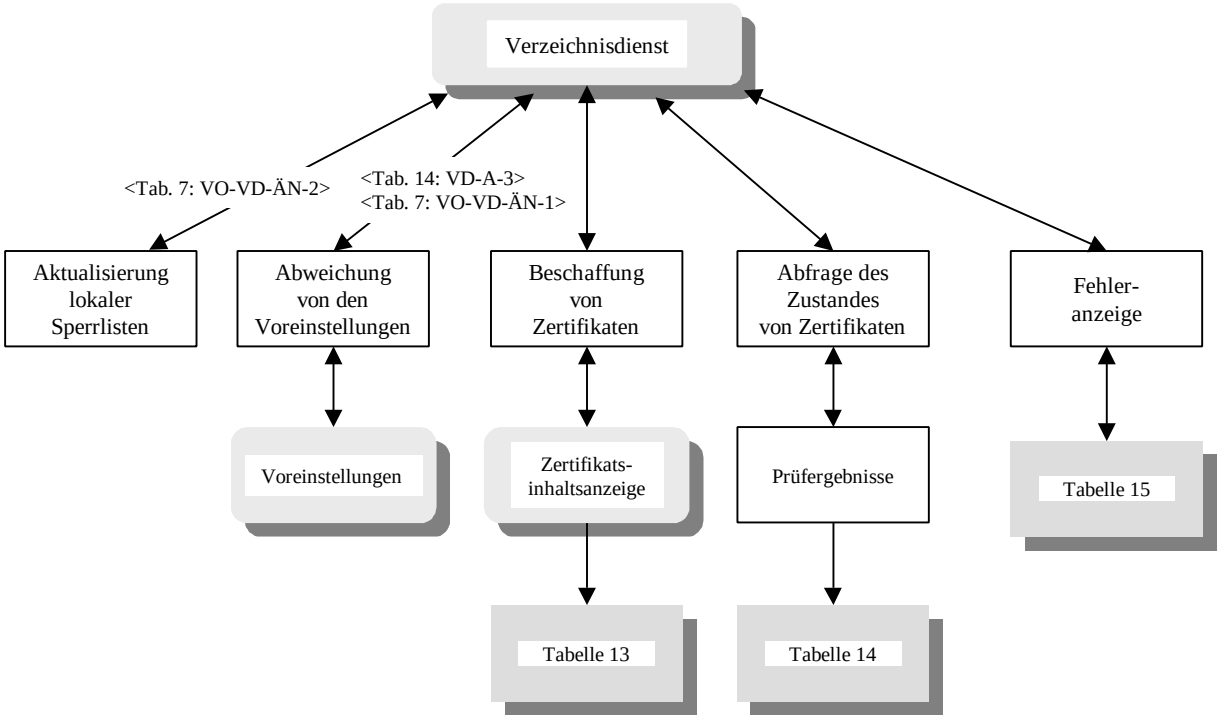
Tabelle 14: Anzeigetexte für Verzeichnisdienstauskünfte

#	VERZEICHNIS-DIENSTAUSKUNFT	ANZEIGETEXT	TYP	REFERENZ
VD-A-1	Zertifikat vorhanden seit und nicht gesperrt	**Das { Signaturschlüsselzertifikat | Attributzertifikat } <certID> ist seit < certInDirSince> im Verzeichnis vorhanden und nicht gesperrt.**	I	[A5 99, 3.2.2]
VD-A-2	Zertifikat vorhanden seit, aber nicht abrufbar	**Das { Signaturschlüsselzertifikat | Attributzertifikat } <certID> ist seit < certInDirSince > im Verzeichnis vorhanden, aber nicht abrufbar.**	I	[A5 99, 3.2.2]
VD-A-3	Starten des Teilprozesses“ Verzeichnisdienst”	**Möchten Sie die Voreinstellung für den Teilprozeß “Verzeichnisdienst” ändern?** Eingabe { ja | nein}	P	

Tabelle 15: Anzeigetexte für Fehlermeldungen bei Verzeichnisdienstauskünften

#	VERZEICHNIS-DIENSTAUSKUNFT	ANZEIGETEXT	TYP	REFERENZ
VD-F-1	Nicht-Verfügbarkeit	**Der Verzeichnisdienst der { Zertifizierungsstelle | RegTP }ist temporär nicht verfügbar.**	I	[A5 99, 3.2.2]
VD-F-2	Zertifikat vorhanden seit und gesperrt seit	**Das { Signaturschlüsselzertifikat | Attributzertifikat } <certID>** { **des | der } { Signierers | Zertifizierungsstelle | Verzeichnisdienstes | Zeitstempeldienstes }** i**st seit < certInDirSince> im Verzeichnis vorhanden und seit <revocationTime> aus dem Sperrgrund <revocationReason> gesperrt.**	I	[A5 99, 3.2.2]
VD-F-3	Zertifikat nicht vorhanden	**Das { Signaturschlüsselzertifikat | Attributzertifikat } <certID> ist zum Zeitpunkt <Prüfzeitpunkt> dem Verzeichnisdienst nicht bekannt.**	I	[A5 99, 3.2.2]
VD-F-4	Sperrinformation nicht verfügbar	**Sperrinformation über das { Signaturschlüsselzertifikat | Attributzertifikat** } { **des | der } { Signierers | Zertifizierungsstelle | Verzeichnisdienstes | Zeitstempeldienstes } ist nicht verfügbar, da entweder keine Antwort des Verzeichnisdienstes, kein Abruf von CRLs möglich und keine lokal gespeicherte Sperrliste vorhanden ist.**	I	[A5 99, 3.2.2]
VD-F-5	Sperrinformation veraltet	**Sperrinformation über das { Signaturschlüsselzertifikat | Attributzertifikat** } {**des | der } { Signierers | Zertifizierungsstelle | Verzeichnisdienstes | Zeitstempeldienstes } ist veraltet.** Anzeige des Zeitpunktes **<nextUpdate>**, ab dem die Antwort des Verzeichnisdienstes ungültig ist oder Anzeige des planmäßigen Ausstellungszeitpunkts der nächsten CRL **<nextUpdate>**	I	[A5 99, 3.2.2]
VD-F-6	Fehlerhaftes Format in der Anfrage	**Die Verzeichnisdienst-Anfrage enthält ein fehlerhaftes Format.**	I	[A5 99, 3.2.2]
VD-F-7	Interner Fehler	**Beim Verzeichnisdienst trat ein interner Fehler auf.**	I	[A5 99, 3.2.2]

Abbildung 7: Verzeichnisdienst



2.7 Zeitstempeldienstauskünfte

Beim Signieren und Verifizieren sind von der Anwenderinfrastruktur die in den folgenden Tabellen zusammengefaßten Anzeigetexte für Zeitstempeldienstauskünfte zu unterstützen

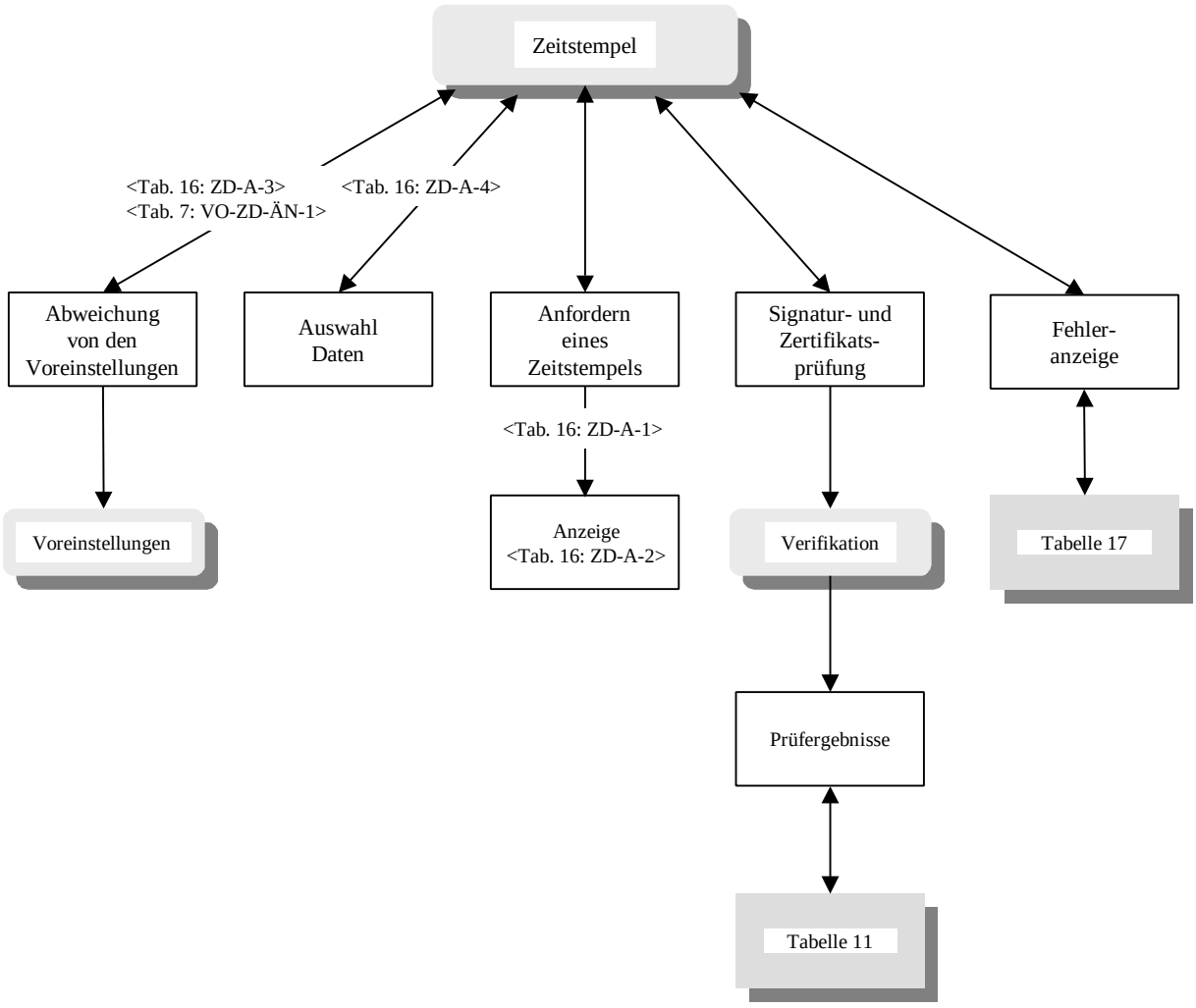
Tabelle 16: Anzeigetexte für Zeitstempeldienstauskünfte

#	ZEITSTEMPEL-DIENSTAUSKUNFT	ANZEIGETEXT	TYP	REFERENZ
ZD-A-1	Anforderung eines Zeitstempels	**Soll zu den ausgewählten Daten ein Zeitstempel eingeholt werden?** Eingabe { ja | nein }	P	[A4 99]
ZD-A-2	Anzeige des Zeitstempels	**Die ausgewählten Daten sind mit folgendem Zeitstempel versehen: <tstTime>**	I	[A4 99, 6.2.1]
ZD-A-3	Starten des Teilprozesses“Zeitstempel”	**Möchten Sie die Voreinstellung für den Teilprozeß “Zeitstempel” ändern?** Eingabe { ja | nein}	P	
ZD-A-4	Auswahl von Daten	**Welche Daten sollen mit einem Zeitstempel versehen werden?** Auswahl der Daten	P	

Tabelle 17: Anzeigetexte für Fehlermeldungen bei Zeitstempeldienstauskünften

#	ZEITSTEMPEL-DIENSTAUSKUNFT	ANZEIGETEXT	TYP	REFERENZ
ZD-F-1	Zeitstempel-anforderung:	**Der von Ihnen angeforderte Zeitstempel konnte nicht erzeugt werden.**	I	
	nicht durchführbar	Anzeige des Grundes **<TimeStampFailureInfo>**		[A4 99, 4]

Abbildung 8: Zeitstempeldienst



LITERATUR

[A1 99] BSI: *Signatur-Interoperabilitätsspezifikation SigI, Abschnitt A1 Zertifikate,* 1999

[A2 99] BSI: *Signatur-Interoperabilitätsspezifikation SigI, Abschnitt A2 Signatur,* 1999

[A4 99] BSI: *Signatur-Interoperabilitätsspezifikation SigI, Abschnitt A4 Zeitstempeldienst,* 1999

[A5 99] BSI: *Signatur-Interoperabilitätsspezifikation SigI, Abschnitt A5 Verzeichnisdienst,* 1999

[A6 99] BSI: *Signatur-Interoperabilitätsspezifikation SigI, Abschnitt A6 Gültigkeitsmodell für digitale Signaturen,* 1999

[DIN SigG/V 98] DIN NI-17.4: *Spezifikation der Schnittstelle zu Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV, Version 1.0,* Dezember 1998

[MKAT 98] *Regulierungsbehörde für Telekommunikation und Post: Maßnahmenkatalog nach §16 der Verordnung zur digitalen Signatur (Signaturverordnung – SigV), Version 1.0*, März 1998

[SigG 97] BRD: *Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG), Artikel 3, Gesetz zur digitalen Signatur (Signaturgesetz - SigG),* Juli 1997

[SigV 97] BRD: *Verordnung zur digitalen Signatur (Signaturverordnung - SigV*), Juli 1997