



bremen
online services

bos-Prüfprotokoll mit Zertifikatsanzeige

**bremen online services
GmbH & Co. KG**

Stand: 21.10.2009

Der Verification Interpreter Version 2.1.2 verwendet den Certificate Interpreter 1.8.3
© 2009 bremen online services Entwicklungs- und Betriebsgesellschaft mbH & Co. KG

Inhaltsverzeichnis

1	Rechtliche Informationen und weitere Hinweise	5
2	Einleitung	6
3	Bereich „Zusammenfassung“	8
3.1	Bereich „Zusammenfassung“ für OSCI-Nachrichten	8
3.1.1	Überschrift	8
3.1.2	Feld „Betreff“	9
3.1.3	Feld „Nachrichtenkennzeichen“	9
3.1.4	Feld „Absender“	9
3.1.5	Feld „Empfänger“	9
3.1.6	Feld „Eingang auf dem Server“	10
3.1.7	Feld „Gesamtprüfergebnis“	10
3.2	Bereich „Zusammenfassung“ alle anderen Signaturformate	12
3.2.1	Feld „Gesamtprüfergebnis“	12
3.2.2	Felder "Signaturdatei" und „Signierte Datei“	12
3.2.3	Zeile „Autoren“	13
3.2.4	Hinweistexte	13
3.3	Bereich „Nachrichtenstruktur“ - nur bei OSCI-Nachrichten -	16
3.3.1	Zeile „Inhaltsdatencontainer“	16
3.3.2	Zeile „Autoren“	16
3.3.3	Hinweistexte	17
3.3.4	Zeilen „Inhaltsdaten und Anhänge“	17
3.4	Bereich „Signaturen“	17
3.4.1	Spalte „Name“	18
3.4.1.1	Zeile „S“ (Signierzeitpunkt)	18
3.4.1.2	Zeile „P“ (Zeitpunkt der Durchführung der Prüfung)	19
3.4.2	Spalte „Inhaltsdatensignatur“	19
3.4.2.1	Spalte „H“ (Hash-Algorithmus)	19
3.4.2.2	Name des Algorithmus	19
3.4.2.3	Spalte „C“ (Chiffrieralgorithmus)	20
3.4.3	Spalte „Q“ (qualifiziertes Zertifikat)	20
3.4.4	Spalte „INT“ (Integrität)	20
3.4.5	Spalte „ID“ (Identität)	20
3.4.6	Spalte „G“ (Gesamtergebnis)	21
3.4.7	Attributzertifikat	22
4	Bereich „Zertifikate und Ergebnisse der Zertifikatsprüfung“	23
4.1	Angaben zum „Zertifikat für den Signaturschlüssel des Autors“	23
4.1.1	Feld „Inhaber“	23
4.1.2	Feld „Herausgeber“	23
4.1.3	Feld „Gültig bis“	24
4.1.4	Feld „Signaturniveau“	24
4.1.5	Link „Details“	24
4.1.6	Feld „Gesamtprüfergebnis“	24
4.1.7	Feld „Online-Prüfung“ - nur bei OSCI-Nachrichten	25
4.1.8	Feld „Online-Prüfung“ - alle anderen Signaturformate	26
4.1.9	Feld „Prüfung der Zertifikatskette“ - nicht bei OSCI-Nachrichten	26
4.1.10	Feld „Mathematische Signaturprüfung“	27
4.1.11	Feld „Gültigkeit zum Zeitpunkt der Prüfung“	27
4.1.12	Feld „Qualifiziertes Zertifikat“	27
4.1.13	Feld „Signierzeitpunkt“	27

4.1.14	Feld „Prüfzeitpunkt“ (nicht bei OSCI-Nachrichten)	28
4.1.15	Feld Prüfmethode	28
4.2	Nachprüfung	29
5	Detailansicht der Zertifikate	30
5.1	Zusammenfassung der wichtigsten Zertifikatsinhalte	31
5.1.1	Anzeige des Inhabers des Zertifikats (QZ, FZ, VZ)	32
5.1.2	Anzeige des Herausgebers des Zertifikats (QZ, FZ, QAZ, VZ)	32
5.1.3	Anzeige der Zertifikatsgültigkeit (QZ, FZ, QAZ, VZ)	32
5.1.4	Anzeige des Signaturniveaus (QZ)	32
5.1.5	Anzeige des Inhabers des Basiszertifikats bei Attributzertifikaten (QAZ)	33
5.1.6	Eintrag „Beschränkende Attribute (Common PKI)“ (QZ)	33
5.1.7	Link „Details“	33
5.2	Beschränkende Zertifikatsinhalte (Attribute) gemäß SigG / Common PKI	33
5.2.1	Erweiterung „Attributzertifikat“ (QZ)	33
5.2.2	Erweiterung „Monetäre Beschränkung“ (QZ, QAZ)	34
5.2.3	Erweiterung „Vertretungsmacht“ (QZ, QAZ)	34
5.2.4	Erweiterung „bestätigte/r Beruf/sausübung“ (QZ, QAZ)	35
5.2.5	Erweiterung „altersabhängige Einschränkung“ (QZ, QAZ)	36
5.2.6	Erweiterung „Einschränkung“ (QZ, QAZ)	36
5.2.7	Erweiterung „Zusatzinformationen“ (QZ, QAZ)	37
5.3	Detaildarstellung der Zertifikatsinhalte	37
5.3.1	Feld „Herausgeber“ (QZ, QAZ, FZ, VZ)	37
5.3.2	Bereich „Allgemeines“ (QZ, QAZ, FZ, VZ)	38
5.3.2.1	Feld „Typ“ (QZ, QAZ, FZ, VZ)	38
5.3.2.2	Feld „Version“ (QZ, QAZ, FZ, VZ)	38
5.3.2.3	Feld „Seriennummer“ (QZ, QAZ, FZ, VZ)	38
5.3.2.4	Feld „Gültigkeit ab“ (QZ, QAZ, FZ, VZ)	39
5.3.2.5	Feld „Gültigkeit bis“ (QZ, QAZ, FZ, VZ)	39
5.3.2.6	Feld „Inhaber“ (QZ, FZ, VZ, QAZ)	39
5.3.3	Bereich „öffentlicher Schlüssel des Signaturinhabers“ (QZ, FZ, VZ)	40
5.3.3.1	Feld „Algorithmus“ (QZ, FZ, VZ)	40
5.3.3.2	Feld „Schlüssellänge“ (QZ, VZ)	41
5.3.3.3	Feld „Modulus“ (QZ, VZ)	41
5.3.3.4	Feld „Exponent“ (QZ, VZ)	41
5.3.4	Feld „UID des Herausgebers“ (QZ, FZ, VZ, QAZ)	41
5.3.5	Feld „UID des Inhabers“ (QZ, FZ, VZ)	41
5.3.6	Erweiterung „Ausstellerschlüssel-ID“ (QZ, FZ, QAZ, VZ)	41
5.3.7	Erweiterung „Inhaberschlüssel-ID“	42
5.3.8	Erweiterung „Schlüsselverwendung“ (QZ, FZ, VZ)	42
5.3.8.1	Digitale Signatur (FZ)	42
5.3.8.2	Nichtabstreitbar (QZ)	42
5.3.8.3	Schlüsselverschlüsselung (VZ)	43
5.3.8.4	Datenverschlüsselung (VZ)	43
5.3.8.5	Schlüsselvereinbarung	43
5.3.8.6	Zertifikatsignatur/CRL-Signatur	43
5.3.9	Erweiterung „Private Key Validity Usage Period“ (FZ, VZ)	43
5.3.10	Erweiterung „Zertifizierungsrichtlinien“ (QZ, QAZ, FZ, VZ)	43
5.3.11	Erweiterung „Richtlinienzuordnungen“	44
5.3.12	Erweiterung „Alternativer Name des Inhabers“ (QZ, FZ, VZ)	44
5.3.13	Erweiterung „Alternativer Name des Ausstellers“ (QZ, FZ, VZ)	44
5.3.14	Erweiterung „Verzeichnisattribute des Inhabers“ (QZ, QAZ, FZ, VZ)	44
5.3.15	Erweiterung „Allgemeine Einschränkungen“	45
5.3.16	Erweiterung „Beschränkung des Namensraums“	45
5.3.17	Erweiterung „Richtlinienbeschränkungen“	45

5.3.18	Erweiterung „Erweiterte Schlüsselverwendung“	45
5.3.19	Erweiterung „Distributionspunkt für CRL“ (QZ, QAZ, FZ, VZ)	45
5.3.20	Erweiterung „Zugangsinformationen des Ausstellers“ (QZ, FZ, QAZ, VZ)	46
5.3.21	Erweiterung „BiometricData“	46
5.3.22	Erweiterung „Angaben zum qualifizierten Zertifikat“ (QZ, QAZ)	46
5.3.22.1	Statement „Konform mit EU-Direktive 1999/93/EC“	47
5.3.22.2	Statement „Monetäre Beschränkung“	47
5.3.22.3	Statement „Aufbewahrung externer Identifikationsdokumente“	47
5.3.22.4	Statement „Privater Schlüssel auf SmartCard gemäß EU- Direktive 1999/93/EC Anhang 3“	47
5.3.23	Erweiterung „Keine OCSP-Prüfung“	47
5.3.24	Erweiterung „Seriennummer der Chipkarte“ (QZ).....	48
5.3.25	Bereich „Signatur des Herausgebers“	48
5.3.25.1	Feld „Signaturalgorithmus des Herausgebers“ (QZ, QAZ, FZ, VZ)	48
5.3.25.2	Feld „Signatur des Herausgebers“ (QZ, QAZ, FZ, VZ).....	48
5.3.26	Anzeige des Fingerabdrucks über das Zertifikat (QZ, QAZ, FZ, VZ).....	48
6	Bereich "Übertragungssicherheit"	49
6.1	Feld "Autoren"	49
6.2	Feld "Mathematische Signaturprüfung"	49
7	Verzeichnis der Abbildungen und Tabellen	50

1 Rechtliche Informationen und weitere Hinweise

Obwohl diese Produktdokumentation nach bestem Wissen und mit größter Sorgfalt erstellt wurde, können Fehler und Ungenauigkeiten nicht vollständig ausgeschlossen werden. Eine juristische Verantwortung oder Haftung für eventuell verbliebene fehlerhafte Angaben und deren Folgen wird nicht übernommen. Die in dieser Produktdokumentation enthaltenen Angaben spiegeln den aktuellen Entwicklungsstand wider und können ohne Ankündigung geändert werden. Künftige Auflagen können zusätzliche Informationen enthalten. Technische und typografische Fehler werden in künftigen Auflagen korrigiert.

Diese Produktinformation sowie sämtliche urheberrechtsfähigen Materialien, die mit dem Produkt vertrieben werden, sind urheberrechtlich geschützt. Alle Rechte sind der bremen online services Entwicklungs- und Betriebsgesellschaft mbH & Co. KG, Bremen, (bos KG) vorbehalten. Alle urheberrechtsfähigen Materialien dürfen ohne vorherige Einwilligung der bos KG weder ganz noch teilweise kopiert oder auf sonstige Art und Weise reproduziert werden. Für rechtmäßige Nutzer des Produkts gilt diese Einwilligung im Rahmen der vertraglichen Vereinbarungen als erteilt. Jegliche Kopien dieser Produktinformation bzw. von Teilen daraus müssen den gleichen Hinweis auf das Urheberrecht enthalten wie das Original.

Governikus ist eingetragene Marke der bremen online services Entwicklungs- und Betriebsgesellschaft mbH & Co. KG, Bremen.

Sofern in dem vorliegenden Dokument für Personen ausschließlich die männliche Form benutzt wird, geschieht dies nur aus Gründen der besseren Lesbarkeit und hat keinen diskriminierenden Hintergrund.

2 Einleitung

In der EU-Direktive zur elektronischen Signatur werden im Anhang IV Empfehlungen für die sichere Signaturprüfung beschrieben. Während des Signaturprüfungsvorgangs ist demnach u. a. mit hinreichender Sicherheit zu gewährleisten, dass

- die zur Überprüfung der Signatur verwendeten Daten den Daten entsprechen, die dem Überprüfer angezeigt werden,
- die Signatur zuverlässig überprüft wird und das Ergebnis dieser Überprüfung korrekt angezeigt wird,
- die Echtheit und die Gültigkeit des zum Zeitpunkt der Überprüfung der Signatur verlangten Zertifikats zuverlässig überprüft werden,
- das Ergebnis der Überprüfung sowie die Identität des Unterzeichners korrekt angezeigt werden und
- die Verwendung eines Pseudonyms eindeutig angegeben wird.

Diese Anforderungen wurden auch in das Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) übernommen und in der "Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten - Arbeitsgrundlage für Entwickler/Hersteller und Prüf-/Bestätigungsstellen" – herausgegeben von der Bundesnetzagentur in Kapitel 2.2 präzisiert. So muss die Signaturanwendungskomponente (SAK) u. a. gewährleisten, dass

- erkennbar wird, auf welche Daten sich die Signatur bezieht,
- erkennbar wird, ob die Daten unverändert sind,
- erkennbar wird, welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist,
- erkennbar wird, welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attributzertifikate aufweisen,
- erkennbar wird, ob die nachgeprüften, qualifizierten Zertifikate im jeweiligen Zertifikatsverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren,
- die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird.

Das Governikus-Prüfmodul „Verification Interpreter“ als Teil einer SAK erfüllt diese Anforderungen für die folgenden Datenformate:

- OSCI -Nachrichten,
- PKCS#7 (in den Formaten "detached" und "enveloped"),
- S/MIME,
- PDF mit eingebetteten PKCS#7-Signaturen (PDF-Inline) und
- TSP.

Das bos-Prüfmodul analysiert diese Formate auf ihre Struktur hin, prüft vorhandene Signaturen hinsichtlich ihrer Integrität und prüft ggf. auch die Identität des Signierenden. Die resultierenden Informationen beinhalten nicht nur Signatur(prüfungs)informationen, sondern spiegeln auch die Struktur der Daten wider. Alle Ergebnisse werden im bos-Prüfprotokoll als HTML-Seite dargestellt.

Die Anzeige der Prüfergebnisse im bos-Prüfprotokoll gliedert sich in mehrere Hauptbereiche: Die folgende Kurzbeschreibung aller Bereiche ist jeweils um eine direkte Referenz auf das entsprechende Kapitel ergänzt, in dem ausführlich die einzelnen Einträge erläutert werden:

1. Im Bereich „Zusammenfassung“ wird das kumulierte Gesamtergebnis aller Prüfungen als Ampelstatus angezeigt. Bei OSCI-Nachrichten darüber hinaus weitere Informationen, wie bspw. Betreff, Nachrichtenkennzeichen und Informationen zum Sender und Empfänger (Kapitel 3.1). Bei allen anderen Signaturformaten wird in diesem Bereich u. a. der Name der signierten Datei und der Name des Autors, d.h. der signierenden Person angezeigt (Kapitel 3.2).
2. Den Bereich „Nachrichtenstruktur“ gibt es **nur** bei der Anzeige der Prüfergebnisse für **OSCI-Nachrichten**. Diese können eine wesentlich komplexere Nachrichtenstruktur aufweisen als die anderen unterstützten Signaturformate, bspw. sind ineinander geschachtelte Nachrichten-Container mit mehreren Dateien, die ggf. von verschiedenen Autoren signiert wurden, bei OSCI-Nachrichten möglich. Im Bereich „Nachrichtenstruktur“ wird daher für OSCI-Nachrichten dargestellt, auf welche Inhaltsdaten sich welche elektronischen Signaturen beziehen und welchem Signaturschlüsselinhaber die elektronische Signatur zuzuordnen ist (Kapitel 3.3).
3. Im Bereich „Signaturen“ werden das Ergebnis der mathematischen Signaturprüfung (Integrität) und die Einzelergebnisse der Zertifikatsprüfung, d.h. die Prüfung der Integrität der Inhaltsdaten und der Identität des Autors tabellarisch zusammengefasst, Bei einer qualifizierten elektronischen Signatur (QES) wird auch die Eignung der für die QES verwendeten Algorithmen angezeigt. Sollten mehrere elektronische Signaturen vorhanden sein, werden die Prüfergebnisse separat für jeden Autor angezeigt. Sollte ein Autor ein Attributzertifikat beigefügt haben, werden auch dessen Prüfergebnisse separat ausgewiesen und dem Signaturzertifikat zugeordnet (Kapitel 3.4).
4. Im Bereich „Zertifikate und Ergebnisse der Zertifikatsprüfungen“ werden die Ergebnisse der Zertifikatsprüfung (Signatur des Signaturzertifikats, Gültigkeitsdauer, Widerrufsstatus und Zertifikatspfad) und die wichtigsten Informationen aus dem Zertifikat (Inhaber, Herausgeber, Gültigkeit, etc.) angezeigt (Kapitel 4).
5. Im Bereich „Detailansicht der Zertifikate“ werden alle wesentlichen Zertifikatsinhalte der geprüften Signaturzertifikate (und Attributzertifikate) und ggf. nicht geprüfter weiterer Zertifikate angezeigt (Kapitel 5).
6. Im Bereich „Übertragungssicherheit“ wird im Fehlerfall angezeigt, dass eine sichere Kommunikation zwischen Client und dem Verifikationsserver mit OCSP/CRL-Relay bei der Online-Zertifikatsprüfung nicht gewährleistet werden konnte (Kapitel 6).

3 Bereich „Zusammenfassung“

In diesem Kapitel wird der Bereich „Zusammenfassung“ ausführlich vorgestellt. Aufgrund der Unterschiede zwischen der Anzeige für OSCI-Nachrichten und den anderen Signaturformaten wird im Kapitel 3.1 der Bereich „Zusammenfassung“ für OSCI-Nachrichten in einem eigenen Kapitel behandelt. Im Kapitel 3.2 wird dann dieser Bereich des bos-Prüfprotokolls für alle anderen Signaturformate vorgestellt.

3.1 Bereich „Zusammenfassung“ für OSCI-Nachrichten

Das bos-Prüfmodul analysiert und zeigt die Signatur(prüfungs)informationen sowie die Struktur der Daten für folgende OSCI-Nachrichtentypen an:

- empfangende asynchrone OSCI-Nachrichten,
- ausgewählte synchrone Nachrichtentypen:
 - Abwicklungsantwort (Response_To_Mediate_Delivery),
 - Abwicklungsauftrag (Request_To_Mediate_Delivery),
 - Bearbeitungsauftrag (Process_Delivery),
 - Weiterleitungsantwort (Response_To_Forward_Delivery),
 - Annahmearauftrag (Accept_Delivery),

Die Beschreibung zum Bereich „Zusammenfassung“ für OSCI-Nachrichten erfolgt im Folgenden chronologisch.

3.1.1 Überschrift

Die Überschrift „Prüfprotokoll“ wird immer um den Zeitpunkt der Durchführung der Prüfung in der Form TT.MM.JJJJ hh:mm:ss ergänzt.

Prüfprotokoll vom 16.09.2009 13:45:02

Zusammenfassung

Betreff Testnachricht
Nachrichtenkennzeichen govbei_12507703206837832192355548795398
Absender Jan Pelz
Empfänger Jan Pelz
Eingang auf dem Server 20.08.2009 14:12:07 (lokale Serverzeit)
(Ende des Empfangsvorgangs)
Gesamtprüfergebnis **Sämtliche durchgeführten Prüfungen lieferten ein positives Ergebnis.**
(Signaturen und Signaturzertifikate)

Abbildung 1: Prüfprotokoll – Ausschnitt asynchrone OSCI-Nachricht

Prüfprotokoll vom 21.09.2009 11:10:27

für eine OSCI-Nachricht des Typs "Bearbeitungsauftrag"

Zusammenfassung

Betreff	east_request
Nachrichtenkennzeichen	dpma_test_11682599889686167082807018459951
Absender	htabrizi
Empfänger	test_recipient-1_cypher
Eingang auf dem Server (Ende des Empfangsvorgangs)	08.01.2007 13:40:01 (kryptographischer Zeitstempel von test_crypto-timestamp_signature)
Gesamtprüfresultat (Signaturen und Signaturzertifikate)	! Mindestens eine der Prüfungen lieferte kein eindeutiges Ergebnis.

Abbildung 2: Prüfprotokoll – Ausschnitt synchrone OSCI-Nachricht

Bei einer synchronen OSCI-Nachricht wird unterhalb der Überschrift zusätzlich der Nachrichtentyp angegeben.

3.1.2 Feld „Betreff“

Dieses Feld beschreibt den ausgewählten Nachrichtentyp der Nachricht der Autorin oder des Autors bzw. der sendenden Person bei OSCI-Nachrichten.

3.1.3 Feld „Nachrichtenkennzeichen“

Das „Nachrichtenkennzeichen“ wird vom OSCI-Manager vergeben und dient auch im Nachhinein zur eindeutigen Bezugnahme auf die betreffende Nachricht. Jedes Nachrichtenkennzeichen ist eindeutig, da es nur einmal vergeben wird.

3.1.4 Feld „Absender“

Dieses Feld gibt die absendende Person der Nachricht laut Verschlüsselungszertifikat an. Es ist der Name des Zertifikatseigentümers [subject commonName], in der Regel Nachname und Vorname des Zertifikatsinhabers oder auch ein Pseudonym. Alle vorhandenen Informationen zum Inhaber des Zertifikats sind dem Bereich Detailansicht der Zertifikate des bos-Prüfprotokolls zu entnehmen.

Ist kein InspectionReport und damit ggf. kein Absender vorhanden, wird die Meldung „Die Nachricht enthält keinen Absender“ ausgegeben:

Absender	x Die Nachricht enthält keinen Absender.
Empfänger	x Die Nachricht enthält keinen Empfänger.

Abbildung 3: Meldung, wenn kein Absender/Empfänger vorhanden ist

3.1.5 Feld „Empfänger“

Dieses Feld stellt die Empfängerin bzw. den Empfänger der Nachricht laut Verschlüsselungszertifikat dar. Es ist der Name des Zertifikatseigentümers [subject commonName]. In der Regel ist dies Nachname und Vorname des Zertifikatsinhabers oder auch ein Pseudonym. Alle vorhandenen Informationen zum Inhaber des Zertifikats sind dem Bereich Detailansicht der Zertifikate des bos-Prüfprotokolls zu entnehmen.

Ist kein InspectionReport und damit ggf. kein Empfänger vorhanden, wird die Meldung „Die Nachricht enthält keinen Empfänger“ ausgegeben:

3.1.6 Feld „Eingang auf dem Server“

„Eingang auf dem Server“ bezeichnet den Zeitpunkt, zu dem der Empfang der Nachricht auf dem Server abgeschlossen wurde. Bei Nachrichten an eine Behörde, die eine bestimmte Fristenanforderung gestellt hat, kann hierüber der fristgerechte Eingang kontrolliert werden. Aus dem Eintrag geht hervor, ob es sich um die Serverzeit des OSCI-Managers oder den Zeitstempel eines entsprechend akkreditierten Dienstleisters handelt.

Ist kein InspectionReport und damit ggf. kein Eingangszeitpunkt vorhanden, wird die Meldung ausgegeben „Die Nachricht enthält kein Datum des Eingangs auf dem Server“.

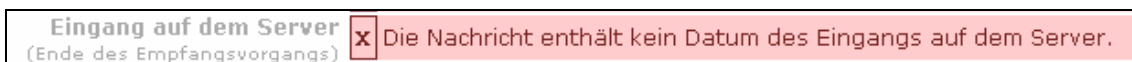





Abbildung 4: Meldung, wenn kein Eingangszeitpunkt angegeben ist

3.1.7 Feld „Gesamtprüfergebnis“

In diesem Feld wird der Gesamtstatus aller durchgeführten Signaturprüfungen (Integrität der Inhaltsdaten und Identität des Autors/der Autoren) angezeigt und als Ampelstatus visualisiert.

Die folgenden Status sind möglich:

- a)  Grün mit Haken: Alle durchgeführten Prüfungen lieferten ein positives Ergebnis
- b)  Gelb mit Ausrufungszeichen: Mindestens eine der Prüfungen lieferte kein eindeutiges Ergebnis.
- c)  Rot mit Kreuz: Mindestens eine der durchgeführten Prüfungen lieferte ein negatives Ergebnis


Erläuterung zu a) Sämtliche durchgeführten Prüfungen lieferten ein positives Ergebnis

Die elektronische Signatur mit dem zugeordneten Signaturzertifikat wurde mit positivem Ergebnis überprüft.

Damit ist

- die Unverfälschtheit (Integrität der signierten Inhaltsdaten, der Nachricht, des Dokuments) sichergestellt und
- der Unterzeichner sicher identifiziert und seine Authentizität bestätigt.


Bei einer qualifizierten elektronischen Signatur (QES) wurde auch die Eignung der Algorithmen (Inhaltsdaten, Signaturzertifikat) gemäß aktuellem Algorithmenkatalog der Bundesnetzagentur festgestellt.

	<p>Hinweis: Gesamtprüfergebnis „Grün“</p> <p>Das Gesamtprüfergebnis mit dem Status „Grün“ ist eine Momentaufnahme zum Zeitpunkt der Durchführung der Prüfung. Eine Nachprüfung der Signatur nach einigen Jahren kann gerade bei fortgeschrittenen Signaturzertifikaten dazu führen, dass das Zertifikat nicht mehr online gegen das ausstellende Trustcenter prüfbar ist, weil das Trustcenter einen entsprechenden Dienst eingestellt hat.</p> <p>Im Kontext der qualifizierten elektronischen Signatur (QES)</p>
---	---

	kann bei einer „Nachprüfung“ der Status auf „Gelb“ wechseln, weil z. B. zum Zeitpunkt der Durchführung der „Nachprüfung“ dann der zur Signatur der Inhaltsdaten verwendete Algorithmus gemäß dem dann geltenden Algorithmenkatalog der Bundesnetzagentur nicht mehr für eine QES als geeignet einzustufen ist.
--	--

Erläuterung zu b) Mindestens eine der Prüfungen lieferte kein eindeutiges Ergebnis.


Der Prüfstatus der Signaturprüfung ist aus Empfängersicht nicht eindeutig. Die Ursache sollte in jedem Fall durch den Empfänger genauer analysiert werden.

	<p>Hinweis: Gesamtprüfergebnis „Gelb“</p> <p>Häufig kommt dieses Prüfergebnis dadurch zustande, dass eine Online-Zertifikatsprüfung nicht durchgeführt werden konnte, weil das Trustcenter nicht erreichbar war. In diesem Fall ist in der Tabelle „Signaturen“ in der Spalte ID (für Identität) der Status „Gelb“ (mit Ausrufezeichen). Im Bereich "Ergebnisse der Zertifikatsprüfung" hat das Prüfergebnis für die Onlineprüfung des Zertifikats den Status „Gelb“. Sollten alle anderen Signaturprüfergebnisse in der Tabelle „Signaturen“ den Status „Grün“ aufweisen, ist eine „Nachprüfung“ des Sperrstatus des Signaturzertifikats sinnvoll. Der Gesamtstatus kann dann auf „Rot“ oder „Grün“ wechseln.</p> <p>Der Status „Gelb“ kann aber auch endgültig sein, wenn z. B. das Signaturzertifikat nicht konform zum Standard x509V3 ist und daher nicht ausgewertet werden kann. In diesem Fall kann bspw. der Gültigkeitszeitraum des Signaturzertifikats nicht ausgelesen werden.</p> <p>Im Kontext der qualifizierten elektronischen Signatur (QES) kann der Status „Gelb“ auch dadurch zustande kommen, das zum Zeitpunkt der Durchführung der Prüfung ein zur Signatur der Inhaltsdaten oder des Signaturzertifikats verwendeter Algorithmus gemäß aktuellem Algorithmenkatalog der Bundesnetzagentur nicht mehr für eine QES als geeignet einzustufen ist. Das Ergebnis ist in diesem Fall nicht veränderbar. Mögliche Konsequenzen beschreibt die Bundesnetzagentur (BNetzA) in der FAQ 28 (http://www.bundesnetzagentur.de, dort den Bereich QES und anschließend FAQ auswählen).</p>
---	---

Erläuterung zu c) Mindestens eine der durchgeführten Prüfungen lieferte ein negatives Ergebnis

Mindestens eine Prüfung hatte abschließend ein negatives Ergebnis. Damit ist entweder die Unverfälschtheit der Inhaltsdaten (Integrität der Daten) nicht sichergestellt oder es konnte die signierende Person abschließend nicht sicher identifiziert werden.

Bei einer qualifizierten elektronischen Signatur (QES, ermittelt über das qualifizierte Zertifikat) wird auch die Eignung der Algorithmen (Inhaltsdaten, Signaturzertifikat) gemäß aktuellem Algorithmenkatalog der Bundesnetzagentur überprüft. War die Eignung zum Signaturzeitpunkt nicht gegeben, ist keine QES zustande gekommen und das Gesamtprüfergebnis ist „Rot“.

	<p>Hinweis: Gesamtprüfergebnis „Rot“</p> <p>Das Gesamtprüfergebnis mit dem Status „Rot“ ist endgültig, da z. B. das Signaturzertifikat zum Signaturzeitpunkt gesperrt war oder bei einer QES ein Algorithmus zum Signaturzeitpunkt nicht mehr für eine QES geeignet war.</p>
---	---

Der Gesamtstatus kann sich auch auf mehrere Signaturen beziehen. In diesem Fall handelt es sich um ein kumulatives Gesamtergebnis, d.h. eine „Gelbprüfung“ oder eine „Rotprüfung“ führt zum Gesamtstatus „Gelb“ oder „Rot“. Welche Inhaltsdaten von wem signiert wurden, wird in der Tabelle „Nachrichtenstruktur“ dargestellt. Informationen zu dieser Tabelle entnehmen Sie bitte dem Kapitel 3.3 dieser Dokumentation.

3.2 Bereich „Zusammenfassung“ alle anderen Signaturformate

Zusammenfassung	
<p>Gesamtprüfergebnis (Signaturen und Signaturzertifikate)</p> <p>Signaturdatei signer200_P7-det_Qgrün.doc.p7s</p> <p>Signierte Datei signer200_P7-det_Qgrün.doc</p> <p>Autoren</p>	<p><input checked="" type="checkbox"/> Sämtliche durchgeführten Prüfungen lieferten ein positives Ergebnis.</p> <p><input checked="" type="checkbox"/> Jan Wilhelm Pelz Qualifizierte elektronische Signatur</p>

Abbildung 5: Bereich Zusammenfassung (PKCS#7, detached)

3.2.1 Feld „Gesamtprüfergebnis“

In diesem Feld wird der Gesamtstatus aller durchgeführten Signaturprüfungen (Integrität der Inhaltsdaten und Identität des Autors/der Autoren) angezeigt und als Ampelstatus visualisiert. Die folgenden Status sind möglich:

- a) Grün mit Haken:
Alle durchgeführten Prüfungen lieferten ein positives Ergebnis
- b) Gelb mit Ausrufungszeichen:
Mindestens eine der Prüfungen lieferte kein eindeutiges Ergebnis.
- c) Rot mit Kreuz:
Mindestens eine der durchgeführten Prüfungen lieferte ein negatives Ergebnis

Weitere Informationen zum Ampelstatus entnehmen Sie bitte den ausführlichen Erläuterungen im Kapitel 2.

3.2.2 Felder "Signaturdatei" und „Signierte Datei“

Bei PKCS#7-, PDF- und S/MIME-Signaturen wird im Bereich „Zusammenfassung“ nach dem Gesamtprüfergebnis die Zuordnung der Signatur zum signierten Dokument vorgenommen.

PKCS#7

Das PKCS#7-Signaturformat erlaubt es, Dokumente sowohl losgelöst (detached) als auch zusammen (enveloped) mit dem Originaldokument zu signieren.

Im Falle einer detached PKCS#7-Signatur wird eine separate Datei mit der Signatur erzeugt. Angezeigt wird im Prüfprotokoll die signierte Datei und die Signaturdatei (im Beispiel auf

Abbildung 5 die signierte Datei `signer2000_P7_det_Qgrün.doc` und die Signaturdatei `signer2000_P7_det_Qgrün.doc.p7s`).

Bei einer enveloped PKCS#7-Signatur liegt im Ergebnis nur eine Datei vor, diese besteht aus Signatur und Dokument. Dieses wird im bos-Prüfprotokoll dadurch gekennzeichnet, dass der Name der signierten Datei und der Name der Signaturdatei identisch sind (siehe Abbildung 6).

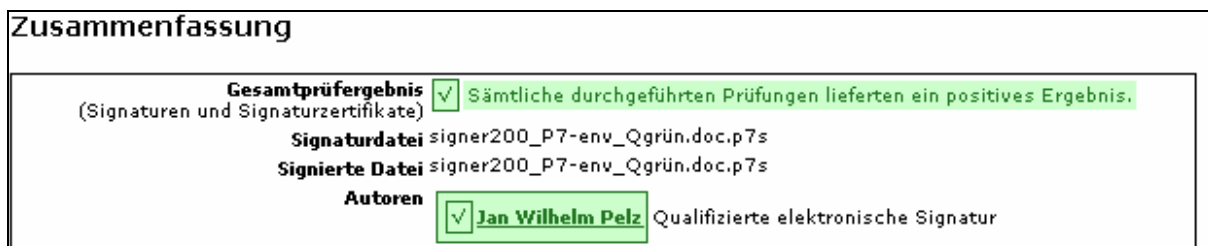


Abbildung 6: Bereich Zusammenfassung (PKCS#7, enveloped)

S/MIME

S/MIME ist ein Standard für die Verschlüsselung und Signatur von MIME-gekapselten E-Mails (Endung häufig `.eml`). Technisch entspricht die S/MIME einer PKCS#7-Datei im "detached" Format. Daher wird die Anzeige für PKCS#7 verwendet.

PDF-Signatur

Signierte PDF-Dokumente sind PDF-Dateien im so genannten PDF-Inline-Format mit eingebetteten PKCS#7-Signaturen (vergleichbar mit PKCS#7, enveloped). Daher wird die Anzeige für PKCS#7, enveloped verwendet.

3.2.3 Zeile „Autoren“

Das Feld „Autoren“ zeigt an, welche Person die signierte Datei signiert hat. Bei dem Namen handelt es sich um den „CommonName“ des Inhabers aus dem zugeordneten Signaturzertifikat. Dabei wird der Status der signierten Datei in der bekannten Ampelform angezeigt sowie das Signaturniveau. Im Status „Gelb“ bzw. „Rot“ wird zusätzlich auch noch ein Hinweistext gegeben, der eine Ursache für den Status beschreibt.

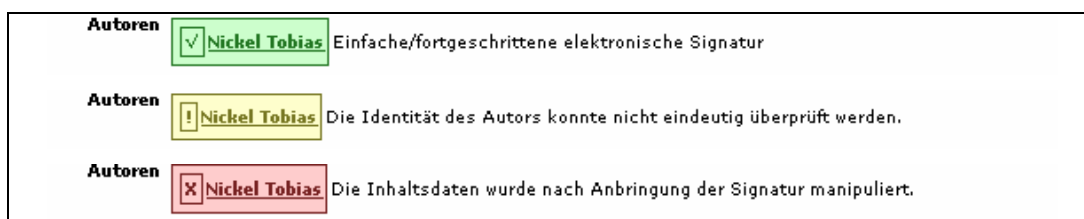



Abbildung 7:Feld Autoren: Ampelstatus

3.2.4 Hinweistexte


Neben den Informationen zu den Autoren wird das autorenspezifische Ergebnis der Signaturprüfung angezeigt. Dieses fasst das Ergebnis der mathematischen Signaturprüfung (= Integritätsprüfung) für den benannten Autor und das Ergebnis der Zertifikatsprüfung (= Identitätsprüfung) zusammen. Bei einer qualifizierten elektronischen Signatur wird in diesem Zusammenhang auch die Eignung der verwendeten Algorithmen geprüft.

	<p>Hinweis: Hintergrund Integrität</p> <p>Bevor ein elektronisches Dokument signiert wird, wird mit der so genannten Hash-Funktion ein Hashwert (häufig auch digitaler Fingerabdruck genannt) des Dokuments erzeugt. Dieser ist ein kurzer Extrakt des Dokuments mit fester Länge. Aus dem Extrakt kann die ursprüngliche Datei nicht rekonstruiert werden. Zudem ist es ausgeschlossen, dass eine zweite Datei anderen Inhalts erzeugt werden kann, die denselben Hashwert liefert.</p> <p>Der so genannte Original-Hashwert wird an das Dokument "angehängt", aus dem er berechnet wurde. Bei der Integritätsprüfung beim Empfänger werden Hashwert und Dokument wieder getrennt und erneut der Hashwert über das Dokument berechnet. Stimmen der Original- und der neue berechnete Hashwert überein, so wurde das Dokument nicht verändert, die Integrität ist gegeben. Wurde das Dokument manipuliert, stimmen die Hashwerte nicht mehr überein. Die Integrität des Dokuments ist nicht mehr gegeben.</p>
---	--

a) Status „Grüner Kasten mit Haken“

Beim Status „Grün“ wird angezeigt, welches Signaturniveau festgestellt werden konnte:


- Einfache/fortgeschrittene elektronische Signatur
- Qualifizierte elektronische Signatur

	<p>Hinweis: Signatur anbringen und prüfen</p> <p>Mit einem mathematischen Verfahren auf der Basis des privaten Signaturschlüssels wird der Hashwert verschlüsselt. Dieser Signaturschlüssel ist geheim. Der korrespondierende öffentliche Signaturprüfschlüssel wird zur Entschlüsselung des Hashwerts verwendet. Der Signaturprüfschlüssel befindet sich im Signaturzertifikat.</p>
---	---

b) Status „Gelber Kasten mit Ausrufezeichen“


Beim Status „Gelb“ können folgende ergänzende Informationen angezeigt werden:

- Die Integrität der Signatur konnte nicht geprüft werden, da der Algorithmus nicht implementiert ist.
- Die Identität des Autors konnte nicht eindeutig überprüft werden.
- Das Attributzertifikat gehört nicht zum Signaturzertifikat.

	<p>Hinweis: Signaturzertifikat</p> <p>Das Signaturzertifikat bescheinigt die Identität einer signierenden Person. Bei einem qualifizierten elektronischen Signaturzertifikat werden die Angaben zur Person dem Personalausweis entnommen.</p> <p>Um das Signaturzertifikat vor Manipulationen zu schützen, wird es vom ausstellenden Trustcenter signiert. Auch die Identität des Ausstellers des Signaturzertifikats - und damit die Vertrauenswürdigkeit des Ausstellers des Signaturzertifikats - wird durch ein so genanntes CA-Zertifikat bestätigt. Auch dieses CA-Zertifikat ist vor Manipulation geschützt, bei einer qualifizierten elektronischen Signatur mit Anbieterakkreditierung bspw. wird dieses Zertifikat durch die Bundesnetzagentur ausgestellt und signiert.</p>
---	---

Nur bei QES:

- Qualifizierte elektronische Signatur (QES). Jedoch wurde für die Signatur der Inhaltsdaten ein Hash-Algorithmus verwendet, der zum Zeitpunkt der Durchführung der Prüfung gemäß aktuellem Algorithmenkatalog nicht mehr für eine QES geeignet war.
- Qualifizierte elektronische Signatur (QES). Jedoch wurde für die Signatur der Inhaltsdaten ein Chiffrieralgorithmus verwendet, der zum Zeitpunkt der Durchführung der Prüfung gemäß aktuellem Algorithmenkatalog nicht mehr für eine QES geeignet war.
- Qualifizierte elektronische Signatur (QES). Jedoch wurde für die Signatur des Signaturzertifikats ein Hash-Algorithmus verwendet, der zum Zeitpunkt der Durchführung der Prüfung gemäß aktuellem Algorithmenkatalog nicht mehr für eine QES geeignet war.
- Qualifizierte elektronische Signatur (QES). Jedoch wurde für die Signatur des Signaturzertifikats ein Chiffrieralgorithmus verwendet, der zum Zeitpunkt der Durchführung der Prüfung gemäß aktuellem Algorithmenkatalog nicht mehr für eine QES geeignet war.

	<p>Prüfung der verwendeten Algorithmen bei qualifizierten elektronischen Signaturen</p> <p>Wenn eine qualifizierte elektronische Signatur auf einem Algorithmus oder Parameter beruht, der als nicht mehr geeignet und damit als nicht mehr hinreichend sicher eingestuft ist, muss dieses zutreffend im bos-Prüfprotokoll angezeigt werden. Grundlage der Eignungsprüfung ist die aktuelle Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA).</p> <p>Dabei sind zwei Fälle zu unterscheiden:</p> <ol style="list-style-type: none"> 1. Bereits erzeugte elektronische Signaturen bleiben auch dann noch qualifiziert, wenn der zugrunde liegende Algorithmus nach der Signatur seine Eignung verloren hat. Sie büßen jedoch graduell und sukzessive ihren Beweiswert ein. 2. Signaturen, die nach dem Schwachwerden des zugrunde liegenden Algorithmus erzeugt wurden, sind von vornherein nicht qualifiziert, da bei der Erzeugung der Signatur nicht mehr sichergestellt ist, dass der Signaturschlüssel-Inhaber die alleinige Kontrolle über die Mittel zur Erzeugung der Signatur hat.
---	---

c) Status  „Roter Kasten mit Kreuz“

Beim Status „Rot“ werden folgende ergänzende Informationen angezeigt:

- Die Inhaltsdaten wurden nach Anbringung der Signatur manipuliert.
- Das Signaturzertifikat war zum Signierzeitpunkt gesperrt oder abgelaufen.

Nur bei QES:

- Keine qualifizierte elektronische Signatur (QES). Für die Signatur der Inhaltsdaten wurde ein Hash-Algorithmus verwendet, der zum Signierzeitpunkt gemäß aktuellem Algorithmenkatalog nicht mehr für eine QES geeignet war.
- Keine qualifizierte elektronische Signatur (QES). Für die Signatur der Inhaltsdaten wurde ein Chiffrieralgorithmus verwendet, der zum Signierzeitpunkt gemäß aktuellem Algorithmenkatalog nicht mehr für eine QES geeignet war.

- Keine qualifizierte elektronische Signatur (QES). Für die Signatur des Signaturzertifikats wurde ein Hash-Algorithmus verwendet, der zum Signierzeitpunkt gemäß aktuellem Algorithmenkatalog nicht mehr für eine QES geeignet war.
- Keine qualifizierte elektronische Signatur (QES). Für die Signatur des Signaturzertifikats wurde ein Chiffrieralgorithmus verwendet, der zum Signierzeitpunkt gemäß aktuellem Algorithmenkatalog nicht mehr für eine QES geeignet war.

3.3 Bereich „Nachrichtenstruktur“ - nur bei OSCI-Nachrichten -

Im Bereich „Nachrichtenstruktur“ wird zunächst textlich angezeigt, ob die Nachricht entschlüsselt werden konnte und ob sich im entschlüsselten Teil elektronische Signaturen befinden. Folgende Meldungen können ausgegeben werden:

- Die Nachricht wurde vollständig dechiffriert.
- Die Nachricht enthält chiffrierte Inhaltsdatencontainer. **Hinweis:** In diesem Fall können keine Aussagen über die verschlüsselten Inhalte gemacht werden.
- Im dechiffrierten Teil der Nachricht befindet sich keine Signatur.
- Im dechiffrierten Teil der Nachricht befindet sich mindestens eine Signatur.

Nachrichtenstruktur

Die Nachricht wurde vollständig dechiffriert. Im dechiffrierten Teil der Nachricht befindet sich mindestens eine Signatur.

Inhaltsdatencontainer: project_coco (signiert)

Autoren ✓ Jan Wilhelm Pelz Qualifizierte elektronische Signatur

✓ Jan Wilhelm Pelz Qualifizierte elektronische Signatur

Inhaltsdaten [nachricht.xml](#), [nachricht.xml](#), [visitenkarte.xml](#), [visitenkarte.xml](#), [herstellerinformation.xml](#)

Anhänge [Testdokument.doc](#)

Inhaltsdatencontainer: govello_coco (unsigniert)

Autoren

Inhaltsdaten [additional infos](#), [local timestamps](#)

Anhänge

Abbildung 8: Bereich Nachrichtenstruktur bei einer OSCI-Nachricht mit zwei Signaturen

Ist mindestens eine elektronische Signatur im dechiffrierten Teil vorhanden, werden (getrennt für jeden Inhaltsdatencontainer, in dem sich mindestens eine elektronische Signatur befindet) die Zuordnung der Signaturen zu den signierten Inhalten und die Ergebnisse der Identität- und Integritätsprüfung für jeden Autor angezeigt, der die Inhaltsdatencontainer signiert hat.

Dadurch ist genau festgehalten, welche Daten von wem signiert wurden und wie der Status der signaturspezifischen Integritäts- und Identitätsprüfungen (Online-Prüfung) ist.

3.3.1 Zeile „Inhaltsdatencontainer“

Angezeigt wird der Name des Inhaltsdatencontainers und ob dieser Container signiert wurde (signiert/unsigniert).

3.3.2 Zeile „Autoren“

Die Anzeige in der Zeile „Autoren“ bei OSCI-Nachrichten ist identisch zu der Anzeige der Autoren bei allen anderen Signaturformaten. Lesen Sie hierzu bitte das Kapitel 3.2.3.

3.3.3 Hinweistexte

Die Hinweistexte zur Anzeige in der Zeile Autoren bei OSCI-Nachrichten ist identisch zu den Hinweistexten bei Anzeige der Autoren bei allen anderen Signaturformaten. Lesen Sie hierzu bitte das Kapitel 3.2.4.

3.3.4 Zeilen „Inhaltsdaten und Anhänge“

Angezeigt werden die Namen der signierten oder nicht signierten Inhaltsdaten und ggf. die vorhandenen Anhänge.

3.4 Bereich „Signaturen“

Signaturen													
A	Zugehöriges Attributzzertifikat				C	Chiffrieralgorithmus							
G	Gesamtergebnis				H	Hashalgorithmus							
INT	Integritätsprüfung				Q	Qualifiziertes Zertifikat							
ID	Identitätsprüfung				P	Zeitpunkt der Durchführung der Prüfung							
S	Signierzeitpunkt												
Name	Inhaltsdatensignatur				Zertifikatssignatur				Q	INT	ID	G	
	S	H	C		H	C							
Jan Wilhelm Pelz	S	✓		✓	✓		✓			✓	✓	✓	✓
	P	✓	RIPEMD160	✓	RSA-2048	SHA1	✓	RSA-2048	✓	✓	✓	✓	✓

Abbildung 9: Bereich „Signaturen“ für eine QES

Im Bereich „Signaturen“ wird für jeden Autor das Ergebnis der mathematischen Signaturprüfung (= Integritätsprüfung, Spalte „INT“) und das Ergebnis der Zertifikatsprüfung (= Identitätsprüfung, Spalte „ID“) sowie in der letzten Spalte das Gesamtergebnis (Spalte „G“) zusammengefasst

Bei einer qualifizierten elektronischen Signatur wird in diesem Zusammenhang auch die Eignung der verwendeten Algorithmen geprüft (Spaltenbereiche „Inhaltsdatensignatur“ und „Zertifikatssignatur“). Dabei wird die Eignung der verwendeten Algorithmen konform zur FAQ 28 der Bundesnetzagentur geprüft

- zum Zeitpunkt der Signaturerstellung und
- zum Zeitpunkt der Durchführung der Prüfung.

Wurde bereits bei der Signaturerstellung ein zu diesem Zeitpunkt nicht mehr geeigneter Algorithmus verwendet, so wurde, gemäß FAQ 28 der Bundesnetzagentur (BNetzA), keine gültige QES erzeugt.

Ist der verwendete Algorithmus zum Zeitpunkt der Durchführung der Prüfung schwach, hat die vorliegende QES laut FAQ 28 möglicherweise einen sukzessive eingeschränkten Beweiswert. Bei diesen Prüfungen ist jeweils zu differenzieren zwischen den für die Inhaltsdatensignatur und Zertifikatssignatur verwendeten Algorithmen.

Aus den einzelnen Prüfergebnissen wird im Bereich „Signaturen“ ein Gesamtergebnis für Inhaltsdaten- und Zertifikatssignatur zum Signaturzeitpunkt und zum Zeitpunkt der Durchführung der Prüfung ermittelt, das in das Gesamtprüfergebnis der qualifizierten elektronischen Signatur eines Autors einfließt. Für die verwendeten Algorithmen wird das jeweilige Ablaufdatum in einem gesonderten Bereich dargestellt.

Zusätzlich werden im Prüfprotokoll auch ausführliche Informationen zum Prüfergebnis der Eignung der Algorithmen angezeigt. Da im besonderen Fall auch keine QES erzeugt wurde,

wird grundsätzlich eine Aussage darüber getroffen, ob eine QES vorliegt, und wenn nein, weshalb nicht.

Es ergibt sich somit folgende zusammenfassende Darstellung der Prüfergebnisse:

Eignung aller Algorithmen der Inhalts- und Zertifikatssignatur zum		Status bezüglich der Eignung der Algorithmen	Gesamtprüfergebnis der Autozensignatur ¹
Signaturzeitpunkt?	Zeitpunkt der Durchführung der Prüfung?		
Ja	Ja	Grün	Gültige QES
Ja	Nein	Gelb	Gültige QES mit einschränkendem Hinweis
Nein	Nein	Rot	Keine QES

¹ alle anderen Prüfungen wurden mit einem positiven Ergebnis durchgeführt.

Tabelle 1: Ermittlung des Gesamtprüfergebnisses abhängig von der Eignung der verwendeten Algorithmen


Im Folgenden wird die komplexe Struktur des Bereichs „Signatur“ spaltenweise von links nach rechts erläutert. Der Aufbau ist für alle Signaturformate identisch.


3.4.1 Spalte „Name“

Angeigt wird in der Spalte „Name“ für jeden Autor (= signierende Person) dessen Name. Dieses ist der Name des Inhabers (*subject*) des der Signatur eindeutig zugeordneten Signaturzertifikats [*subject commonName*]. In der Regel ist dies Nachname und Vorname oder auch ein Pseudonym. Durch einen Klick auf den Namen gelangen Sie direkt zu der Detailansicht der Prüfergebnisse des Signaturzertifikats des Autors (siehe Kapitel 4).

3.4.1.1 Zeile „S“ (Signierzeitpunkt)

In der Zeile „S“ wird angegeben, inwieweit die verwendeten Algorithmen (Hash-Algorithmus „H“ und Chiffrieralgorithmus „C“) für die Inhaltsdatensignatur und Zertifikatssignatur (nur für das Signaturzertifikat des Autors) zum Zeitpunkt der Signaturanbringung (Signierzeitpunkt „S“) geeignet waren. Die Anzeige existiert nur bei einer intendierten QES.

Ein  grüner Kasten mit Haken bedeutet: Algorithmus war zum Signierzeitpunkt für eine QES geeignet.


Ein  roter Kasten mit Kreuz signalisiert, dass der Algorithmus zum Zeitpunkt der Anbringung gemäß aktuellem Algorithmenkatalog nicht mehr für eine QES geeignet war. Die Anzeigen gelten sowohl für eine Inhaltsdaten- als auch eine Zertifikatssignatur. Signaturen, die nach dem Schwachwerden des zugrunde liegenden Algorithmus erzeugt wurden, sind von vornherein nicht qualifiziert, da bei der Erzeugung der Signatur nicht mehr sichergestellt ist, dass der Signaturschlüssel-Inhaber die alleinige Kontrolle über die Mittel zur Erzeugung der Signatur hat.


Das Prüfergebnis „Rot“ führt immer auch zu dem Gesamtergebnis für den Autor „Rot“ (Spalte „G“).

Der Signaturzeitpunkt wird im Bereich "Zertifikate und Ergebnisse der Zertifikatsprüfung" angegeben (siehe Kapitel 4.1.13 und 4.1.14).

3.4.1.2 Zeile „P“ (Zeitpunkt der Durchführung der Prüfung)

In der Zeile „P“ wird angegeben, inwieweit die verwendeten Algorithmen (Hash-Algorithmus „H“ und Chiffrieralgorithmus „C“) für die Inhaltsdatensignatur und Zertifikatssignatur (nur für das Signaturzertifikat des Autors) zum Zeitpunkt der Durchführung der Prüfung geeignet waren.

Ein  grüner Kasten mit Haken bedeutet, dass der Algorithmus zum Zeitpunkt der Durchführung der Prüfung für eine QES geeignet war.

Das Prüfergebnis  gelber Kasten mit Ausrufezeichen bedeutet, dass der Algorithmus erst zum Zeitpunkt der Durchführung der Prüfung als nicht mehr für eine QES als geeignet anzusehen ist, während er zum Signierzeitpunkt noch für eine QES geeignet war. Bereits erzeugte elektronische Signaturen bleiben auch dann noch qualifiziert, wenn der zugrunde liegende Algorithmus nach der Signatur seine Eignung verloren hat. Sie büßen jedoch graduell und sukzessive ihren Beweiswert ein. Deshalb dieser Warnhinweis, der sich auf das Gesamtergebnis „G“ für den Autor auswirkt. Wurde bereits die Eignung des Algorithmus zum Signierzeitpunkt verneint, wird für den Zeitpunkt der Durchführung der Prüfung auch der gelbe Kasten mit Ausrufezeichen angezeigt.

Hinweis: Der Zeitpunkt der Durchführung der Prüfung steht in der Überschrift des Prüfprotokolls.

3.4.2 Spalte „Inhaltsdatensignatur“

Die „Inhaltsdatensignatur“ bezeichnet die Daten, die durch einen Autor signiert wurden. In Abgrenzung zur Zertifikatssignatur durch den Zertifizierungsdiensteanbieter (ZDA) oder das Trustcenter. Die Unterscheidung zwischen beiden Signaturen ist notwendig, da dieselben Algorithmen, je nachdem ob sie zur Inhaltsdatensignatur oder zur Zertifikatssignatur verwendet wurden, unterschiedliche Ablaufdaten hinsichtlich ihrer Eignung für eine qualifizierte elektronische Signatur haben können.

3.4.2.1 Spalte „H“ (Hash-Algorithmus)

In der Spalte „H“ wird die Eignung des Hash-Algorithmus für die Inhaltsdaten- oder Zertifikatssignatur zum Signierzeitpunkt („S“) oder zum Zeitpunkt der Durchführung der Prüfung angezeigt.

Alle geprüften Algorithmen werden am Ende des Prüfprotokolls tabellarisch zusammengefasst aufgeführt. Angezeigt werden der Name des Algorithmus, der Verwendungszweck (z. B. Hash-Algorithmus für eine Zertifikatssignatur) und das Datum des Ablaufs der Eignung gemäß verwendetem, aktuellem Algorithmenkatalog der Bundesnetzagentur (BNetzA).

Algorithmusname	Verwendungszweck	Gültig bis
RSA-2048	Chiffrieralgorithmus für Zertifikatssignaturen	31.12.2015
RSA-1536	Chiffrieralgorithmus für Inhaltsdatensignaturen	31.12.2009
SHA1	Hashalgorithmus für Zertifikatssignaturen	31.12.2010
RIPEMD160	Hashalgorithmus für Inhaltsdatensignaturen	31.12.2010

Abbildung 10: Anzeige der verwendeten Algorithmen mit Datum des Ablaufs der Eignung


3.4.2.2 Name des Algorithmus


In den Spalten zwischen der Spalte „H“ und „C“ wird der Name des Hash-Algorithmus oder des Chiffrieralgorithmus für die Inhaltsdaten- oder Zertifikatssignatur angezeigt. Kann der Name eines Algorithmus nicht angezeigt werden, wird nur dessen OID angezeigt.

3.4.2.3 Spalte „C“ (Chiffrieralgorithmus)

In der Spalte „C“ wird die Eignung des Chiffrieralgorithmus für die Inhaltsdaten- oder Zertifikatssignatur zum Signierzeitpunkt („S“) oder zum Zeitpunkt der Durchführung der Prüfung angezeigt.

3.4.3 Spalte „Q“ (qualifiziertes Zertifikat)

Ein  grüner Kasten mit Haken bedeutet, dass das Signaturzertifikat, das der elektronischen Signatur zugeordnet ist, als qualifiziert gemäß Signaturgesetz anzusehen ist. Die Information zur Qualität des Zertifikats und damit der erzeugten qualifizierten elektronischen Signatur wurde der Konfiguration der Zertifizierungsdiensteanbieter/Trustcenter des OCSP/CRL-Relays entnommen.

Ein  grauer Kasten mit Kreuz bedeutet, dass das der elektronischen Signatur zugeordnete Signaturzertifikat nicht als qualifiziert gemäß Signaturgesetz anzusehen ist.







Signaturen								
A	Zugehöriges Attributzertifikat		C	Chiffrieralgorithmus				
G	Gesamtergebnis		H	Hashalgorithmus				
INT	Integritätsprüfung		Q	Qualifiziertes Zertifikat				
Name	Inhaltsdatensignatur		Zertifikatssignatur		Q	INT	ID	G
	H	C	H	C				
Nickel Tobias	SHA256	RSA-2048	SHA256	RSA-2048				


Abbildung 11: Bereich „Signaturen“ für eine fortgeschrittene oder einfache Signatur mit manipulierter Integrität der Inhaltsdaten

3.4.4 Spalte „INT“ (Integrität)

In der Spalte "INT" wird angezeigt, ob die jeweilige, autoren spezifische Signatur über den Hashwert mathematisch korrekt ist und der Hashwert-Vergleich erfolgreich durchgeführt werden konnte.


Der Status  grüner Kasten mit Haken bedeutet, dass der Original- und der neu berechnete Hashwert überein stimmen. Der signierte Inhalt wurde nicht verändert, die Integrität ist gegeben.


Ein  roter Kasten mit Kreuz kennzeichnet einen manipulierten, signierten Inhalt, weil die beiden Hashwerte nicht überein stimmen. Die Integrität des Inhalts ist nicht gegeben.


Das Prüfergebnis  gelber Kasten mit Ausrufezeichen zeigt an, dass die Integrität der Signatur nicht geprüft werden konnte, da der Algorithmus nicht implementiert ist.


3.4.5 Spalte „ID“ (Identität)

In dieser Spalte wird angezeigt, ob die Identität der unterzeichnenden Person auf der Basis ihres Signaturzertifikats erfolgreich festzustellen war. Es wird das Gesamtergebnis zum jeweiligen Signaturzertifikat aus dem Bereich „Zertifikate und Ergebnisse der Zertifikatsprüfung“ des bos-Prüfprotokolls übernommen.

Ein  grüner Kasten mit Haken signalisiert, dass die Identität des Autors eindeutig festgestellt werden konnte. Alle im Kontext der Zertifikatsprüfung durchgeführten Einzelprüfungen lieferten ein positives Ergebnis.

Ein  gelber Kasten mit Ausrufezeichen zeigt an, dass die Identität des Autors nicht eindeutig festgestellt werden konnte. Mindestens eine der im Kontext der Zertifikatsprüfung durchgeführten Einzelprüfungen konnte nicht durchgeführt werden. Welche Einzelprüfung(en) nicht durchgeführt werden konnte(n), wird im Bereich „Zertifikate und Ergebnisse der Zertifikatsprüfung“ angezeigt.


	<p>Hinweis: Status „Gelb“</p> <p>Häufig kommt dieses Ergebnis dadurch zustande, dass die Onlineprüfung des Signaturzertifikats gegen den Verzeichnisdienst des ausstellenden Trustcenters nicht durchgeführt werden konnte, weil das Trustcenter temporär nicht erreichbar war. Hier sollte eine Nachprüfung des Signaturzertifikats erfolgen.</p>
---	---


Ein  roter Kasten mit Kreuz bedeutet, dass die Identität des Autors endgültig nicht zweifelsfrei festgestellt werden konnte. Mindestens eine der im Kontext der Zertifikatsprüfung durchgeführten Einzelprüfungen lieferte abschließend ein negatives Ergebnis. Welche Einzelprüfung(en) nicht durchgeführt werden konnte(n), wird im Bereich „Zertifikate und Ergebnisse der Zertifikatsprüfung“ angezeigt).


Das angezeigte kumulierte Ergebnis der Identitätsprüfung berücksichtigt auch das Prüfergebnis einer Nachprüfung eines Zertifikats, sollte im Status „Gelb“ initial mindestens eine Prüfung nicht durchgeführt werden können. Detaillierte Informationen zur automatischen Nachprüfung entnehmen sie bitte Kapitel 4.2.

3.4.6 Spalte „G“ (Gesamtergebnis)


In der Spalte „G“ werden die Einzelprüfungen zur Eignung der eingesetzten Algorithmen (nur bei QES) und die Ergebnisse der Integritäts- und kumulierten Identitätsprüfung zu einem autorenspezifischen Gesamtergebnis zusammengefasst.

Ein  grüner Kasten mit Haken signalisiert, dass alle durchgeführten Einzelprüfungen zum Zeitpunkt der Durchführung der Prüfung ein positives Ergebnis lieferten. Bei einer QES wurde auch die Eignung der verwendeten Algorithmen zum Signierzeitpunkt und zum Zeitpunkt der Durchführung der Prüfung positiv geprüft.

	<p>Hinweis: Status „Grün“ bei einer QES nicht mehr endgültig</p> <p>Bei der Prüfung einer QES ist ein positives Gesamtprüfergebnis nicht mehr final: Die Anforderungen der FAQ 28 der Bundesnetzagentur führen dazu, dass sich ein Gesamtprüfergebnis, bezogen auf eine qualifizierte elektronische Signatur, zu unterschiedlichen Zeitpunkten der Prüfungsdurchführung von „Grün“ auf „Gelb“ ändern kann, wenn mindestens ein Algorithmus zwischenzeitlich als schwach einzustufen ist. Bislang war der Status „Grün“ nachträglich nicht veränderbar.</p>
---	---

Ein  gelber Kasten mit Ausrufezeichen zeigt an, dass mindestens eine der durchgeführten Einzelprüfungen nicht durchgeführt werden konnte. Einige, mögliche Ursachen sind:

- Die Integrität der Signatur konnte nicht geprüft werden, da der Algorithmus nicht implementiert ist.
- Die Identität des Autors konnte nicht eindeutig festgestellt werden, weil das Trustcenter temporär nicht erreichbar war.
- Bei einer QES: mindestens ein Algorithmus ist zum Zeitpunkt der Durchführung der Prüfung nicht mehr für eine QES geeignet



Ein  roter Kasten mit Kreuz bedeutet, dass mindestens eine der durchgeführten Einzelprüfungen abschließend ein negatives Ergebnis lieferte.

3.4.7 Attributzertifikat

Ist zu einem Signaturzertifikat ein Attributzertifikat vorhanden, wird das Attributzertifikat eingerückt und vorläufig mit einem A: gekennzeichnet. Angezeigt wird der `commonName` des Attributzertifikats. Dieses ist in der Regel der Organisationsname des Herausgebers des Basiszertifikats, [`issuer organization`] aus dem qualifizierten Signaturzertifikat und manchmal die Seriennummer des Basiszertifikats [`baseCertificateID`].

Name	Inhaltsdatensignatur				Zertifikatssignatur			Q	INT	ID	G	
	H	C	H	C	H	C						
<u>Dominik Gassen</u>	S											
	P		SHA1		RSA-1024		SHA1		RSA-1024			
A: <u>BUNDESNOTARKAMMER</u>	S											
	P				SHA1		RSA-1024					

Abbildung 12: Bereich „Signaturen“ - Anzeige der Prüfergebnisse zum Attributzertifikat

In Abänderung zur Standardbedeutung der Spalte „INT“, kennzeichnet ein  grüner Kasten mit Haken, dass eine eindeutige Zuordnung zum Signaturzertifikat/Basiszertifikat gemäß Spezifikation Common PKI möglich war. Ein  gelber Kasten mit Ausrufezeichen signalisiert, dass eine Zuordnung zum Signaturzertifikat/Basiszertifikat gescheitert ist.

Die einzelnen Prüfergebnisse zur Eignung der verwendeten Algorithmen zur Zertifikatssignatur und zur Identitätsprüfung des Attributzertifikats fließen in das Gesamtergebnis des zugeordneten Signaturzertifikats ein. Da mit dem Attributzertifikat keine Inhaltsdaten geprüft werden können (es gibt kein zugeordnetes RSA-Schlüsselpaar) sind im Bereich Inhaltsdatensignatur keine Prüfergebnisse eingetragen.

4 Bereich „Zertifikate und Ergebnisse der Zertifikatsprüfung“

Im Bereich „Zertifikate und Ergebnisse der Zertifikatsprüfung“ des bos-Prüfprotokolls werden detailliert die Ergebnisse der Prüfung des Signaturzertifikats, ggf. auch mehrerer Signaturzertifikate, dargestellt. Damit zugeordnet werden kann, zu welchem Zertifikat die Prüfergebnisse gehören, werden für jedes geprüfte Zertifikat zunächst der Name des Inhabers, der Herausgeber, das Signaturniveau und der Zeitraum der Gültigkeit angegeben. Anschließend werden das Gesamtprüfergebnis und darauf folgend die Einzelprüfergebnisse sowie technische Informationen zum Signaturzertifikat angezeigt.

4.1 Angaben zum „Zertifikat für den Signaturschlüssel des Autors“

Dieser Bereich im bos-Prüfprotokoll ist für jeden Autor in zwei Bereiche unterteilt. Der obere Bereich enthält die Angaben aus dem Zertifikat, der untere Bereich stellt die durchgeführten Prüfungen in grafisch aufbereiteter Form dar.

Zertifikat für den Signaturschlüssel des Autors	
Inhaber	Dr. Jan Pelz
Herausgeber	Deutscher Sparkassen Verlag GmbH
Gültig bis	31.12.2009 00:59:59
Signaturniveau	Qualifiziert
Details	
! Mindestens eine der Prüfungen konnte nicht durchgeführt werden. ⁴	

Abbildung 13: Zusammenfassende Angaben zum Zertifikat (oberer Bereich)

4.1.1 Feld „Inhaber“

In diesem Feld wird der Name des Zertifikatseigentümers [`subject commonName`] angezeigt. In der Regel ist dies Nachname und Vorname des Zertifikatsinhabers oder auch ein Pseudonym. Alle vorhandenen Informationen zum Inhaber des Zertifikats sind dem Bereich „Detailansicht der Zertifikate des Prüfprotokolls“ zu entnehmen. Sollte es sich um ein deutsches, qualifiziertes elektronisches Zertifikat (QES) handeln, ist der `commonName` der im Personalausweis angegebene Vor- und Nachname [`givenName, surName`]. Durch die Angabe „:PN“ hinter dem Namen bei qualifizierten Signaturzertifikaten, lässt sich erkennen, dass nicht der Name (bei einer QES gem. Personalausweis) angezeigt wird, sondern ein Pseudonym.

4.1.2 Feld „Herausgeber“


Dieses Feld zeigt nur den Namen [`issuer organization`] des herausgebenden Zertifizierungsdiensteanbieters bzw. Trustcenters an. Dieses ist bei der QES nach Common PKI der aus dem CA-Zertifikat des Trustcenters übernommene Name des Inhabers des CA-Zertifikats. Da auch diese Zertifikate qualifizierte Signaturzertifikate sind und auf eine natürliche Person ausgestellt werden müssen, wird hier in der Regel ein Pseudonym verwendet („:PN“ hinter dem `commonName`). Alle vorhandenen Informationen zum Aussteller des Zertifikats sind dem Bereich „Detailansicht der Zertifikate des Prüfprotokolls“ zu entnehmen.

4.1.3 Feld „Gültig bis“

In diesem Feld wird das Datum, bis zu dem das Zertifikat gültig ist, in der Form Tag.Monat.Jahr Stunde:Minute: Sekunde (tt.mm.jjjj hh:mm:ss) angezeigt.

4.1.4 Feld „Signaturniveau“

Dieses Feld zeigt an, ob es sich um ein fortgeschrittenes, qualifiziertes oder qualifiziertes Signaturzertifikat mit Anbieterakkreditierung nach deutschem Signaturgesetz (SigG) handelt. Die Information wird dem Zertifikat entnommen.

	<p>Hinweis: Qualifiziertes Signaturzertifikat</p> <p>Ein Signaturzertifikat ist eine elektronische Bescheinigung, mit der ein Signaturprüf Schlüssel einer Person zugeordnet und die Identität dieser Person bestätigt wird (§ 2 Nr. 6 Signaturgesetz [SigG]). Ein Signaturprüf Schlüssel ist der in der Form elektronischer Daten vorliegende öffentliche kryptografische Schlüssel, mit dem sich eine elektronische Signatur überprüfen lässt (§ 2 Nr. 5 SigG).</p>
---	--

4.1.5 Link „Details“

Durch einen Klick auf diesen Link gelangen Sie direkt zur Detailansicht für dieses Zertifikat.






	<p>Sämtliche durchgeführten Prüfungen lieferten ein positives Ergebnis.⁴</p>
	Online-Prüfung
	Mathematische Signaturprüfung
	Gültigkeit zum Zeitpunkt der Prüfung


Abbildung 14: Gesamt- und Einzelprüfergebnisse (OSCI) (unterer Bereich)


4.1.6 Feld „Gesamtprüfergebnis“

Das oberste Feld im unteren Bereich der Angaben zum „Zertifikat für den Signaturschlüssel des Autors“ kumuliert die Ergebnisse der durchgeführten Einzelprüfungen (siehe Hinweis „Prüfung eines qualifizierten Signaturzertifikats durch die Prüfkomponente OCSP/CRL-Relay“ in diesem Kapitel) zu einem Gesamtprüfergebnis.

Das mögliche Gesamtergebnis ist identisch mit den Ergebnissen aus dem Kapitel 3.4.5 (Bereich „Signaturen“, Spalte „ID“ [Identität]):

Ein  grüner Kasten mit Haken signalisiert, dass die Identität des Autors eindeutig festgestellt werden konnte. Alle im Kontext der Zertifikatsprüfung durchgeführten Einzelprüfungen lieferten ein positives Ergebnis.


Ein  gelber Kasten mit Ausrufezeichen zeigt an dass die Identität des Autors nicht eindeutig festgestellt werden konnte. Mindestens eine im Kontext der Zertifikatsprüfung durchgeführte Einzelprüfungen konnte nicht durchgeführt werden. Welche Einzelprüfung(en) nicht durchgeführt werden konnte(n), wird in den folgenden Kapiteln erläutert.

Ein  roter Kasten mit Kreuz bedeutet, dass die Identität des Autors endgültig nicht zweifelsfrei festgestellt werden konnte. Mindestens eine im Kontext der Zertifikatsprüfung durchgeführten Einzelprüfungen lieferte abschließend ein negatives Ergebnis. Welche Einzelprüfung(en) nicht durchgeführt werden konnte(n), wird in den folgenden Kapiteln erläutert.

Folgende, ergänzende Fehlermeldungen informieren über den Grund der Negativprüfung als Erläuterung der Einzelprüfergebnisse:


- Mindestens ein Zertifikat der Zertifikatskette wurde manipuliert.
- Zertifikat war zum Zeitpunkt der Prüfung außerhalb des Gültigkeitszeitraums.
- Zertifikat war zum Zeitpunkt der Prüfung zurückgewiesen.

Das angezeigte kumulierte Ergebnis der Identitätsprüfung berücksichtigt auch das Prüfergebnis der Nachprüfung eines Zertifikats, sollte im Status „gelb“ initial mindestens eine Prüfung nicht durchgeführt werden können. Detaillierte Informationen zur automatischen Nachprüfung entnehmen sie bitte Kapitel 4.2.

	<p>Hinweis: Prüfung eines qualifizierten Signaturzertifikats (stark vereinfacht) durch die Prüfkomponente OCSP/CRL-Relay</p> <ol style="list-style-type: none"> 1. Zertifikatsqualität für das Signaturzertifikat aus bos-Konfiguration ermitteln 2. Herstellung der direkten Signaturzertifikatskette (über korrespondierende Common-Name und Key-Identifizier, CA- und Root-Zertifikat aus bos-Konfiguration) 3. Prüfung der Signaturen aller Zertifikate der Kette 4. Gültigkeit aller Zertifikate <ol style="list-style-type: none"> a) Signaturzertifikat: übergebener Prüfzeitpunkt innerhalb des Gültigkeitszeitraums b) CA-Zertifikat: Erstellungszeitpunkt des EE-Zertifikats c) Root-Zertifikat: Erstellungszeitpunkt des CA-Zertifikats 5. Sperrstatus aller Zertifikate (Online-Abfragen gegen OCSP-Dienste (bekannt u. nicht gesperrt)) <ol style="list-style-type: none"> a) Signaturzertifikat: übergebener Prüfzeitpunkt b) CA-Zertifikat: übergebener Prüfzeitpunkt, hilfsweise Erstellungszeitpunkt des EE-Zertifikats c) Root-Zertifikat: übergebener Prüfzeitpunkt, hilfsweise Erstellungszeitpunkt des CA-Zertifikats 6. mathematische Signaturprüfung der signierten Prüfantwort (OCSP-Response) 7. Herstellung der Kette (OCSP-Signer-Zertifikat und Root) für das Signaturzertifikat der Prüfantwort 8. mathematische Signaturprüfung über die Zertifikate der Kette OCSP-Signer-Zertifikat und Root-Zertifikat) 9. Gültigkeit der Zertifikate der Prüfantwort <ol style="list-style-type: none"> a) OCSP-Signer-Zertifikats: Liegt der Signaturzeitpunkt der Antwort innerhalb des Gültigkeitszeitraums des OCSP-Signer-Zertifikats. b) Root-Zertifikat: Liegt der Erstellungszeitpunkt des OCSP-Signer-Zertifikats innerhalb des Gültigkeitszeitraums des Root-Zertifikats 10. Sperrstatus aller Zertifikate der „technischen“ Kette (Online-Abfragen gegen OCSP-Dienst der ZDA, neue Prüfantwort wird wieder überprüft (6 bis 9), Abbruch, wenn das Zertifikat bereits geprüft wurde. <p>Schlägt einer dieser Schritte endgültig fehl, ist das Signaturzertifikat endgültig als ungültig zu betrachten.</p>
---	--


4.1.7 Feld „Online-Prüfung“ - nur bei OSCI-Nachrichten


Dieses Feld zeigt an, ob die durchgeführte Online-Prüfung erfolgreich war.

Ein  grüner Kasten mit Haken signalisiert, dass die Onlineprüfung des Zertifikats erfolgreich war:

- Dem herausgebenden Trustcenter ist das Nutzerzertifikat bekannt und es ist gültig (nicht möglich bei einer reinen Negativprüfung über CRL-Listen).


- Die Antwort des Trustcenters war mathematisch korrekt signiert und die Identität des antwortenden Trustcenters konnte bestätigt werden.
- Die Verbindung zum Verzeichnisdienst des Trustcenters, der das Nutzerzertifikat ausgestellt hat, konnte hergestellt werden.
- Die Prüfung der Zertifikatskette war erfolgreich. Alle Zertifikate oberhalb des zu prüfenden Signaturzertifikats waren zum Zeitpunkt der Zertifikatssignatur gültig und nicht gesperrt.

Ein  gelber Kasten mit Ausrufezeichen zeigt an, dass mindestens einer der oben benannten Prüfschritte nicht durchgeführt werden konnte. Der Status der Onlineprüfung ist daher nicht eindeutig.


Ein  roter Kasten mit Kreuz bedeutet, dass mindestens einer der oben benannten Prüfschritte endgültig gescheitert ist.


4.1.8 Feld „Online-Prüfung“ - alle anderen Signaturformate

Dieses Feld zeigt an, ob die durchgeführte Online Prüfung erfolgreich war.

Ein  grüner Kasten mit Haken signalisiert, dass die Onlineprüfung des Zertifikats erfolgreich war:


- Die Verbindung zum Verzeichnisdienst des Trustcenters, der das Nutzerzertifikat ausgestellt hat, konnte hergestellt werden.
- Dem herausgebenden Trustcenter ist das Nutzerzertifikat bekannt und es ist gültig (nicht möglich bei einer reinen Negativprüfung über CRL-Listen).

Ein  gelber Kasten mit Ausrufezeichen zeigt an, dass mindestens einer der oben benannten Prüfschritte nicht durchgeführt werden konnte. Der Status der Onlineprüfung ist daher nicht eindeutig.


Ein  roter Kasten mit Kreuz bedeutet, dass mindestens einer der oben benannten Prüfschritte endgültig gescheitert ist.


4.1.9 Feld „Prüfung der Zertifikatskette“ - nicht bei OSCI-Nachrichten

Die in diesem Kapitel beschriebene „Prüfung der Zertifikatskette“ wird auch bei OSCI-Nachrichten immer durchgeführt. Gemäß OSCI-Spezifikation wird im bos-Prüfprotokoll für eine OSCI-Nachricht das Ergebnis jedoch nicht gesondert ausgewiesen, sondern fließt in das Ergebnis der Online-Prüfung mit ein.

Ein  grüner Kasten mit Haken signalisiert, dass die Prüfung der Zertifikatskette erfolgreich war:

- Die Prüfung der Zertifikatskette war erfolgreich. Alle Zertifikate oberhalb des zu prüfenden Signaturzertifikats waren zum Zeitpunkt der Zertifikatssignatur gültig und nicht gesperrt.
- Die Antwort des Trustcenters war mathematisch korrekt signiert und die Identität des antwortenden Trustcenters konnte bestätigt werden.

Ein  gelber Kasten mit Ausrufezeichen zeigt an, dass mindestens einer der oben benannten Prüfschritte bei der die Prüfung der Zertifikatskette nicht durchgeführt werden konnte.

Ein  roter Kasten mit Kreuz bedeutet, dass mindestens einer der oben benannten Prüfschritte endgültig gescheitert ist.

4.1.10 Feld „Mathematische Signaturprüfung“

<input checked="" type="checkbox"/>	Mathematische Signaturprüfung
<input checked="" type="checkbox"/>	Gültigkeit zum Zeitpunkt der Prüfung
	Qualifiziertes Zertifikat: ja
	Länge RSA-Modulus: 1024 Bit
	Signierzeitpunkt ¹ : 22.02.2006 15:58:22
	Prüfzeitpunkt ² : 22.02.2006 15:58:22
	Prüfmethode ³ : OCSP

Abbildung 15: Einzelprüfergebnisse und Informationen zum Zertifikat

Das Feld „Mathematische Signaturprüfung“ zeigt an, ob die Signaturen über die Zertifikate der Zertifikatskette korrekt sind.

Ein grüner Kasten mit Haken signalisiert, dass die mathematische Signaturprüfung fehlerfrei durchgeführt werden konnte.

Ein roter Kasten mit Kreuz bedeutet, dass die Prüfung fehlgeschlagen ist.

4.1.11 Feld „Gültigkeit zum Zeitpunkt der Prüfung“

Das Feld „Gültigkeit zum Zeitpunkt der Prüfung“ zeigt an, ob der Signaturzeitpunkt innerhalb des Gültigkeitszeitraums des Signaturzertifikats lag.

Ein grüner Kasten mit Haken signalisiert, dass der Signaturzeitpunkt der Inhaltsdaten/des Dokuments innerhalb des Gültigkeitszeitraums des Signaturzertifikats lag.

Ein gelber Kasten mit Ausrufezeichen zeigt an, dass die Prüfung nicht durchgeführt werden konnte, weil z. B. der Gültigkeitszeitraum des Zertifikats nicht aus dem Zertifikat ausgelesen werden konnte.

Ein roter Kasten mit Kreuz bedeutet, dass die Prüfung fehlgeschlagen ist. Der Signaturzeitpunkt der Inhaltsdaten/des Dokuments lag außerhalb des Gültigkeitszeitraums des Signaturzertifikats.

4.1.12 Feld „Qualifiziertes Zertifikat“

Dieses Feld gibt an, ob es sich um ein qualifiziertes Signaturzertifikat nach Deutschen Signaturgesetz (SigG) handelt. Die Information zur Qualität des Zertifikats und damit der erzeugten qualifizierten elektronischen Signatur wurde der Konfiguration der Zertifizierungsdiensteanbieter/Trustcenter des OCSP/CRL-Relays entnommen.

Mögliche Werte in diesem Feld sind: „ja“, „nicht feststellbar“ oder „nein“.

4.1.13 Feld „Signierzeitpunkt“

Dieses Feld stellt den Zeitpunkt der Signaturanbringung (Signaturzeitpunkt) in der Form Tag.Monat.Jahr Stunde:Minute:Sekunde (tt.mm.jjjj hh:mm:ss) dar.

Konnte der Signierzeitpunkt nicht ermittelt werden, wird „k. A.“ für „keine Angabe“ angezeigt. Bitte beachten Sie in diesem Zusammenhang: Ist kein Signierzeitpunkt angegeben, ist nicht feststellbar, ob der Signaturzeitpunkt innerhalb des Gültigkeitszeitraums des Signaturzertifikats lag. Das heißt, das Ergebnis der Gültigkeitsprüfung zum Signierzeitpunkt weist den Status „Gelb“ auf (siehe Kapitel 4.1.11.).

4.1.14 Feld „Prüfzeitpunkt“ (nicht bei OSCI-Nachrichten)

Dieses Feld stellt den Zeitpunkt der Gültigkeitsprüfung (Prüfzeitpunkt) in der Form Tag.Monat.Jahr Stunde:Minute: Sekunde (tt.mm.jjjj hh:mm:ss) dar.


4.1.15 Feld Prüfmethode

Dieses Feld zeigt an, nach welcher Prüfmethode die durchgeführte Statusprüfung gegen den Verzeichnisdienst des ZDA/Trustcenters durchgeführt wurde.

Drei verschiedene Prüfmethoden werden unterstützt:


OCSP

Bei der OCSP-Prüfung nach Common PKI meldet das Trustcenter den Status des Zertifikats („gültig und nicht gesperrt“, „unbekannt“ oder „gesperrt“) zurück. Den Status „gesperrt“ erhält ein Zertifikat bspw. dann, wenn der Inhaber seine Signaturkarte (wegen Verlust o. ä.) hat sperren lassen.

	<p>Hinweis: OCSP</p> <p>Das OCSP-Protokoll ist in RFC 2560 näher spezifiziert. Es sieht vor, dass dem OCSP-Responder eine CertificateID übergeben wird, die aus der Seriennummer des User-Zertifikats und Teilen des Aussteller-Zertifikats gebildet wurde. Diese CertificateID wird dann an den OCSP-Responder gesendet. Dieser antwortet dann mit dem Status des Zertifikats. Bei ungültigen Zertifikaten werden zusätzlich der Sperrgrund und der Sperrzeitpunkt durch den Server eingetragen.</p> <p>Die Übergabe eines Zeitpunkts, zu dem geprüft werden soll, ist bei OCSP nicht möglich. Da aber bei einer erfolgten Sperrung des Zertifikats der Sperrzeitpunkt angegeben wird, ist es möglich, den Status eines Zertifikats zu einem bestimmten Zeitpunkt zu ermitteln.</p> <p>Grundsätzlich sind zwei Arten von OCSP-Respondern zu unterscheiden:</p> <ul style="list-style-type: none"> • Responder mit Positiv-Prüfung: Neben dem Sperrstaus wird zusätzlich geprüft, ob das Zertifikat überhaupt von der ZDA ausgestellt wurde. Dieses sind so genannte OCSP-Responder nach Common-PKI-SigG-Profil, die von allen deutschen ZDA, die mindestens qualifizierte Zertifikate herausgeben, eingesetzt werden. • Responder ohne positiv Prüfung: Es wird nur der reine Sperrstatus des Zertifikats geprüft. <p>Die Antworten eines OCSP-Responders werden signiert, damit sichergestellt ist, dass die Antwort auf dem Weg nicht verändert worden ist.</p>
---	---

CRL

Bei der CRL-Prüfung wird geprüft, ob sich das Zertifikat in der aktuellen Sperrliste des Herausgebers befindet. In der Sperrliste wird ein Zertifikat bspw. dann geführt, wenn der Inhaber seine Signaturkarte hat sperren lassen.

	<p>Hinweis: CRL</p> <p>In der Certificate Revocation List (CRL) sind nur die gesperrten Zertifikate der jeweiligen CAs enthalten. Zusätzlich sind in der Regel ein Sperrgrund sowie ein Sperrzeitpunkt enthalten. Dies ermöglicht die</p>
---	--

	Prüfung des Status eines Zertifikats zu einem bestimmten Zeitpunkt in der Vergangenheit. Die CRLs enthalten normalerweise ein Ablaufdatum, zu dem von der CA eine neue CRL erzeugt wird (bekannte Ausnahme: Bundesnetzagentur, hier wird kein Ablaufdatum eingetragen). Außerdem erzeugen die meisten CAs sofort nach Sperrung eines Zertifikats eine neue CRL.
--	---

LDAP

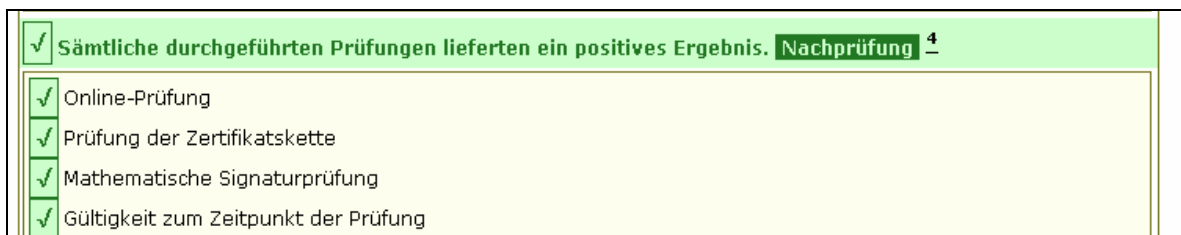
Bei der LDAP-Prüfung wird geprüft, ob das Zertifikat beim Herausgeber bekannt ist.

4.2 Nachprüfung

Sollte der Status einer Zertifikatsprüfung nicht eindeutig sein (Gelb-Prüfung), ist dies häufig durch eine temporäre Nichterreichbarkeit des Trustcenters bedingt. Das Governikus-Prüfmodul „Verification Interpreter“ ermöglicht in diesem Fall eine (automatische) Nachverifikation des betroffenen Zertifikats.

Nur wenn sich auf Basis der Ergebnisse der Nachprüfung der Gelb-Status auf „Grün“ oder „Rot“ verändert, wird bei der Anzeige der Prüfergebnisse das Prüfergebnis der Nachprüfung an das Ergebnis der initialen Zertifikatsprüfung angehängt. Das Ergebnis der Nachprüfung ist durch den invers unterlegten Zusatz „Nachprüfung“ zu erkennen (siehe Abbildung 16). Angezeigt werden das kumulierte Prüfergebnis und nachfolgend die Einzelprüfergebnisse sowie Informationen zum Zertifikat wie in Kapitel 4.1.6 ff. beschrieben.

Wichtig: Das Ergebnis einer angezeigten Nachprüfung hat Auswirkungen auf das angezeigte Gesamtergebnis im Bereich „Signaturen“ und alle anderen zusammenfassenden Prüfergebnisse.




✓ Sämtliche durchgeführten Prüfungen lieferten ein positives Ergebnis. Nachprüfung 4
✓ Online-Prüfung
✓ Prüfung der Zertifikatskette
✓ Mathematische Signaturprüfung
✓ Gültigkeit zum Zeitpunkt der Prüfung


Abbildung 16: Prüfergebnisse einer Nachprüfung

5 Detailansicht der Zertifikate

Zertifikate besitzen eine komplexe Struktur, die für eine bessere Anzeige und Lesbarkeit in eine sinnvolle Reihenfolge gebracht werden. Dieses geschieht auch im bos-Prüfprotokoll. Die technischen Feldbezeichnungen, die Namen von Zertifikatserweiterungen und Attribute werden dabei für den Leser in verständliche Namen ‚übersetzt‘. Dieses gilt auch für zugeordnete Inhalte, Werte und IDs, die, wenn sie codiert sind, aufgelöst werden (siehe Infobox „Interpretation von Zertifikatsinhalten“).

	<p>Beispiel: Interpretation von Zertifikatsinhalten</p> <p>In der Erweiterung <code>QcStatement</code> gibt es eine Statement-ID <code>id-Etsi-qcs-Qccompliance</code> (OID 0.4.0.1862.1.1). Dieses bedeutet, dass es sich um ein Zertifikat handelt, das in Übereinstimmung mit der in nationales Recht umgesetzten EU-Richtlinie zur elektronischen Signatur herausgegeben wurde. Dies ist der Indikator dafür, dass es sich um ein qualifiziertes Signaturzertifikat gemäß deutschem Signaturgesetz handelt. Bei der Anzeige eines Zertifikats wird der Wert „<code>id-Etsi-qcs-QcCompliance</code>“ im <code>qcStatement</code> aufgelöst zu „Qualifizierte elektronische Signatur“.</p>
---	---

Angezeigt werden in der Detailansicht der Zertifikate mindestens alle vorgeschriebenen und optionalen Inhalte von Nutzerzertifikaten nach der deutschen Common-PKI-Spezifikation Version 2.0. Die Spezifikation beschreibt ein Profil über international verbreitete und anerkannte Standards für elektronische Signaturen, Verschlüsselung und Public-Key-Infrastrukturen. Im Januar 2009 ist die Spezifikation gemeinsam von T7 und TeleTrust verabschiedet worden. Sowohl Signatur-Anwendungsanbieter als auch Trustcenter-Betreiber waren an der Erarbeitung der Spezifikation beteiligt. Die Common-PKI-Spezifikation referenziert die gängigen internationalen Standards (z. B. RFC 5280, 3039, Etsi QC, CPN) so, dass davon auszugehen ist, dass Zertifikate in der Regel vollständig interpretiert werden können. Nur im seltenen Einzelfall wird es vorkommen, dass ein technischer Feldname (bzw. dessen OID) oder ein Wert nicht aufgelöst werden kann. Angezeigt werden dann zumindest die OID und der Wert.


	<p>Hinweis: OID</p> <p>OIDs [Object-Identifizier] sind weltweit eindeutige Bezeichner, die benutzt werden, um ein Informationsobjekt (Knoten) in einem hierarchisch zugewiesenen Namensraum, der durch den ASN.1-Standard definiert ist, eindeutig zu identifizieren. Jeder Knoten ist durch eine Folge von Nummern eindeutig gekennzeichnet, die seine Position beginnend an der Wurzel des Baumes angibt. Neue Knoten zur eigenen Verwendung können bei den entsprechenden Autoritäten des übergeordneten Knotens beantragt werden. Die Regeln für die Vergabe und Registrierung von OIDs sind festgelegt in den Normen ISO/IEC 9834 und DIN 66334.</p>
---	--

Bitte beachten Sie in diesem Zusammenhang, dass ein Zertifikat in der Regel nicht alle in dieser Dokumentation beschriebenen Inhalte enthält. Angezeigt werden kann nur das, was vorhanden ist.

Zunächst wird im Kapitel 5.1 die zusammenfassende Darstellung der wichtigsten Zertifikatsinhalte erläutert. Anschließend folgen im Kapitel 5.2 die in qualifizierten Signaturzertifikaten (QZ) und in qualifizierten Attributzertifikaten (QAZ) möglichen Erweiterungen, die die Wirksamkeit einer qualifizierten elektronischen Signatur einschränken, erweitern oder präzisieren. Abschließend werden im Kapitel 5.3 alle (soweit bekannt) in Nutzerzertifikaten (bedingt) vor-

geschriebenen und optionalen Einträge gemäß Common-PKI-Spezifikation und den relevanten RFCs erläutert. Die einzelnen Erläuterungen sind wie folgt aufgebaut:

- Angezeigter Name;
- Zertifikatstyp: wahlweise qualifiziertes Signaturzertifikat (QZ), fortgeschrittenes Signaturzertifikat (FZ), qualifiziertes Attributzertifikat (QAZ), Verschlüsselungszertifikat (VZ) in runden Klammern;
- Technischer Eintrag im Zertifikat in eckigen Klammern (damit wird das Auffinden detaillierter Informationen in den referenzierten Standards erleichtert);
- Ggf. Beschreibung des Inhalts (Wertebereich).

	<p>Hinweis: Zertifikatstypen</p> <p>Die einzelnen Zertifikatstypen lassen sich am Verwendungszweck des im Zertifikat enthaltenen öffentlichen Schlüssels (<code>keyusage</code>) und an der verwendeten X509-Zertifikatsversion festmachen:</p> <p>Signaturzertifikate besitzen die Zertifikatsversion X509v3. Mit der Keyusage „contentCommitment“ (vormals „nonRepudiation“) werden sie (genauer der darin enthaltene öffentliche Signaturprüfchlüssel) für die Prüfung der qualifizierten Signatur oder der qualifizierten Signatur mit Anbieterakkreditierung nach Deutschem Signaturgesetz verwendet. Mit der Keyusage "digitalSignature" werden sie für die fortgeschrittene Signatur verwendet. Häufig werden diese Zertifikate auch zur Authentifizierung genutzt.</p> <p>Qualifizierte Attributzertifikate (mit der Zertifikatsversion X509v1) sind immer einem Signaturzertifikat (als Basiszertifikat) zugeordnet. Attributzertifikate selbst besitzen, gemäß ihrer Zertifikatsstruktur, keinen öffentlichen Schlüssel und daher auch keine Keyusage.</p> <p>Verschlüsselungszertifikate sind Zertifikate, die nicht durch das Signaturgesetz geregelt sind. Sie besitzen ebenfalls die Zertifikatsversion X509v3 jedoch mit der Keyusage "keyEncipherment" und/oder "dataEncipherment". Häufig besitzen fortgeschrittene Signaturzertifikate auch diese Keyusages und sind daher auch für die Daten- bzw. Schlüsselverschlüsselung zu verwenden.</p> <p>Allen genannten Zertifikatstypen gemein sind viele der im Folgenden beschriebenen Zertifikatsinhalte. Bestimmte Angaben sind aber spezifisch für bestimmte Zertifikatstypen vorgesehen. Dieses wird zur besseren Orientierung in diesem Dokument jeweils in Klammern nach dem Namen des Eintrags kenntlich gemacht (QZ, FZ, QAZ, VZ).</p>
---	--

5.1 Zusammenfassung der wichtigsten Zertifikatsinhalte

Die zusammenfassende Darstellung der wichtigsten Zertifikatsinhalte gliedert sich in Informationen zum Inhaber und Herausgeber (Trustcenter, Zertifizierungsdiensteanbieter) des Zertifikats, zur Gültigkeit und zum Signaturniveau. Außerdem wird bei einem qualifizierten Signaturzertifikat angezeigt, ob mindestens eine Beschränkung existiert, die die Nutzung des qualifizierten Signaturzertifikats einschränkt.

Zertifikat für den Signaturschlüssel des Autors	
Inhaber	Jan Wilhelm Pelz
Herausgeber	CA DP Com 7:PN
Gültig bis	31.12.2009 22:59:59
Signaturniveau	Qualifiziert
	Beschränkende Attribute (CommonPKI)

Abbildung 17: Zusammenfassung Signaturzertifikat

5.1.1 Anzeige des Inhabers des Zertifikats (QZ, FZ, VZ)

Angezeigt wird der Name des Zertifikatseigentümers [`subject commonName`]. Dieses sind in der Regel Nachname und Vorname des Zertifikatsinhabers oder auch ein Pseudonym. Alle vorhandenen Informationen zu Inhaberin oder Inhaber des Zertifikats sind dem Detail- eintrag zu entnehmen (siehe Kapitel 5.3.2.6).

QZ: Sollte es sich um ein qualifiziertes Zertifikat handeln, ist der `commonName` der im Personalausweis angegebene Vor- und Nachname [`givenName, surName`]. Durch die Angabe ":PN" hinter dem Namen bei qualifizierten Signaturzertifikaten lässt sich erkennen, dass nicht der Name angezeigt wird, sondern ein Pseudonym.

5.1.2 Anzeige des Herausgebers des Zertifikats (QZ, FZ, QAZ, VZ)

Angezeigt wird nur der Name des herausgebenden Zertifizierungsdiensteanbieters bzw. Trustcenters [`issuer OrganizationName`]. Dieses ist bei QZ nach Common-PKI-SigG-Profil der aus dem CA-Zertifikat des Trustcenters übernommene `commonName` des Inhabers des CA-Zertifikats. Da auch diese Zertifikate - sollte ein qualifiziertes Signaturzertifikat angezeigt werden - qualifizierte Signaturzertifikate sind und auf eine natürliche Person ausgestellt werden müssen, wird hier in der Regel ein Pseudonym verwendet in der Form: Name des Trustcenters mit dem Zusatz :PN. Alle vorhandenen Informationen zum Aussteller des Zertifikats sind dem Detail- eintrag zu entnehmen (siehe Kapitel 5.3.1).

5.1.3 Anzeige der Zertifikatsgültigkeit (QZ, FZ, QAZ, VZ)

Angezeigt wird das Datum, bis zu dem das Zertifikat gültig ist in der Form `Tag.Monat.Jahr Stunde:Minute: Sekunde (tt.mm.jjjj hh:mm.ss)`. [QZ, FZ, VZ: `Validity notAfter`; QAZ: `attrCertValidityPeriod notAfterTime`]. Ist ein Zertifikat (zum Prüfzeit- punkt) abgelaufen, wird das Datum in rot angezeigt.

5.1.4 Anzeige des Signaturniveaus (QZ)

Angezeigt wird das Signaturniveau, soweit es sich bei qualifizierten Zertifikaten aus dem Zertifikat ermitteln lässt. Das Signaturniveau wird wie folgt bezeichnet:

- **Qualifiziert:** In der Zertifikatserweiterung „Angaben zum qualifizierten Zertifikat“ [`qcStatement`] ist die Statement-ID mit dem Wert „`id-Etsi-qcs-Qccompliance`“ gesetzt.
- **Qualifiziert mit Anbieterakkreditierung:** In der Zertifikatserweiterung „Zertifizierungsrichtlinien“ [`certificatePolicies`] ist die Statement-ID mit dem Wert „`id-commonpki-cp-accredited`“, gesetzt.


Genauere Erläuterungen zu den beiden Erweiterungen finden sich in den Kapiteln 5.3.10 und 5.3.22.

5.1.5 Anzeige des Inhabers des Basiszertifikats bei Attributzertifikaten (QAZ)

Bei Attributzertifikaten wird das zugehörige Basiszertifikat referenziert. Angezeigt werden der Organisationsname des Herausgebers des Basiszertifikats [`issuer organization`] aus dem qualifizierten Signaturzertifikat und die Seriennummer des Basiszertifikats [`base-CertificateID`].

5.1.6 Eintrag „Beschränkende Attribute (Common PKI)“ (QZ)

Sollte der Eintrag „Beschränkende Attribute (Common PKI)“ angezeigt werden, existiert im Zertifikat mindestens ein Attribut, das den Zweck/die Nutzung des qualifizierten Signaturzertifikats beschränkt, erweitert oder präzisiert. Genauere Informationen zu diesen beschränkenden Attributen sind dem folgenden Kapitel 5.2 zu entnehmen.

	<p>Hinweis: Kritikalitäts-Flag</p> <p>Alle Zertifikatserweiterungen [<code>extensions</code>] besitzen ein so genanntes Kritikalitäts-Flag, das signalisiert, ob eine Erweiterung als kritisch einzuschätzen ist. Angezeigt wird dieses Flag immer nach dem Namen der Erweiterung in folgender Form: kritisch: „ja“ oder „nein“. Wenn dieses Flag gesetzt ist, muss die Erweiterung berücksichtigt werden.</p>
---	---

5.1.7 Link „Details“

Durch einen Klick auf diesen Link gelangen Sie direkt zur Detailansicht für dieses Zertifikat.

5.2 Beschränkende Zertifikatsinhalte (Attribute) gemäß SigG / Common PKI

Die Common-PKI-Spezifikation beschreibt im SigG-Profil eine Reihe von Zertifikatserweiterungen (oder Attributen), die die Verwendung eines qualifizierten Signaturzertifikats beschränken, erweitern oder präzisieren. Damit werden u. a. die speziellen Anforderungen umgesetzt, die sich aus dem deutschen Signaturgesetz für qualifizierte Zertifikate ergeben. Diese Erweiterungen (Attribute) können sich im qualifizierten Signaturzertifikat (Hauptzertifikat) oder in einem korrespondierenden, gesonderten qualifizierten Attributzertifikat (QAZ) befinden. Folgende Zertifikatserweiterungen (Attribute) werden in der Spezifikation beschrieben:

- Monetäre Beschränkung (Kapitel 5.2.2),
- Vertretungsmacht (Kapitel 5.2.3),
- Bestätigte/r Beruf/sausübung (Kapitel 5.2.4),
- Altersabhängige Einschränkung (Kapitel 5.2.5),
- Eine allgemeine Einschränkung (Kapitel 5.2.6) und die
- Zusatzinformation (Kapitel 5.2.7).


Diese Erweiterungen werden in den jeweils benannten Kapiteln ausführlich erläutert.

5.2.1 Erweiterung „Attributzertifikat“ (QZ)

Die Erweiterung „Attributzertifikat“ [`extension LiabilityLimitationFlag`] kann die Werte „vorhanden“ oder „nicht vorhanden“ besitzen. Der Wert „vorhanden“ (BOOLEAN (true)) zeigt an, dass ein Attributzertifikat zu dem qualifizierten Signaturzertifikat existiert, durch das die Verwendung des Signaturzertifikats beschränkt, erweitert oder präzisiert wird.

Erweiterung	Attributzertifikat (0.2.262.1.10.12.0)
Kritisch	Nein
	vorhanden (BOOLEAN[true])

Abbildung 18: Erweiterung „Attributzertifikat“ vorhanden

	<p>Achtung: Der Wert „nicht vorhanden“ oder die nicht vorhandene Erweiterung „Attributzertifikat“ darf nicht zu der Annahme verleiten, es würde kein Attributzertifikat existieren. Einige Zertifizierungsdiensteanbieter stellen Attributzertifikate nämlich auch nachträglich aus, so dass diese Information dann im Signaturzertifikat nicht vorhanden sein kann.</p>
---	---

5.2.2 Erweiterung „Monetäre Beschränkung“ (QZ, QAZ)

Die Erweiterung „monetäre Beschränkung“ schränkt den finanziellen Verfügungsrahmen des Zertifikatsinhabers ein und besitzt folgende Form: „Zahlenwert Währung“ Die Währung wird gemäß ISO4217CurrencyCode interpretiert. [extension QcStatement.id-etsi-qcs-QcLimitValue].

Diese Erweiterung sollte gemäß Common-PKI-SigG-Profil als nicht kritisch markiert werden. Sie ersetzt die Erweiterung/das Attribut¹ id-commonpki-at-MonetaryLimit, die seit 31.12.2003 nicht mehr verwendet werden soll.

5.2.3 Erweiterung „Vertretungsmacht“ (QZ, QAZ)

Die Erweiterung „Vertretungsmacht“ [procuration] wird verwendet, wenn ein Zertifikatsinhaber für eine andere Person Unterschriften leisten darf. In der Regel hat die Einschränkung folgenden Aufbau:

- Vertretung gemäß Landesrecht von [country],
- Art der Vertretung [substitution]
- Vertretene Person [signingFor].

Angezeigt werden alle im Zertifikat vorhandenen Einträge zu dieser Erweiterung, wie z. B. der Name und die Anschrift.

¹ Im QAZ handelt es sich technisch gesehen bei allen Beschränkungen um Erweiterungen [extensions] oder um Attribute [attributes]. Die Syntax ist jeweils identisch.

Erweiterung	Vertretungsmacht (1.3.36.8.3.2)
Kritisch	Nein
Vertretung gemäß Landesrecht von	DE
Art der Vertretung	Prokura
Vertretene Person	
Familiename	Mustermann
Rufname	Franz
Organisation	Musterfirma
Organisationseinheit	Vorstand
Ort	Berlin
Land	DE
Anschrift	Musterstrasse 5 12345 Berlin


Abbildung 19: Erweiterung „Vertretungsmacht“

Die Erweiterung muss gemäß Common-PKI-SigG-Profil angezeigt werden. Sie sollte allerdings nicht als kritisch markiert sein.

5.2.4 Erweiterung „bestätigte/r Beruf/sausübung“ (QZ, QAZ)

Die Erweiterung „bestätigte/r Beruf/sausübung“ [admission] wird verwendet, um einen Beruf oder eine Berufsausübung zu bestätigen. Damit verbunden ist häufig auch die Berechtigung, bestimmte Aufgaben erledigen zu dürfen. In der Regel hat die Erweiterung folgenden Aufbau:

Anzeigt wird zunächst der Betätigungseintrag. Das ist der Name der bestätigenden Institution [admissionAuthority] oder der Institution, die die bestätigenden Register führt [namingAuthority].

	<p>Hinweis: NamingAuthority und Berufsbezeichnung</p> <p>Als <code>namingAuthority</code> wird eine Institution bezeichnet, die auf der Basis nationalen Rechts Register führt, in denen „offizielle“ Titel hinterlegt sind (z. B. Ärztekammern). Bei einer durch diese Institution bestätigten Berufsbezeichnung kann davon ausgegangen werden, dass die Berufsbezeichnung zu Recht geführt und die im konkreten Fall ausgeübte Funktion zu Recht ausgeübt wird. Die Festlegung der verwendeten Berufsattribute basiert auf den einschlägigen Vorschriften des §7 Abs. 2 SigG.</p> <p>Der Name kann als Text [<code>namingauthorityText</code>] (Name, Land, Name des Registers) und/oder als Nummer (ObjectIdentifier) [<code>namingauthorityID</code>] angegeben werden, wenn diese bei www.teletrust.de und/oder als URL [<code>namingauthorityUrl</code>] geführt wird.</p> <p>Die Berufsbezeichnung kann als Text [<code>professionItems</code>] und bei von TeleTrust geführten NamingAuthorities, die Berufsbezeichnungen festgelegt haben, als OID [<code>professionOIDs</code>] geführt werden. Zusätzlich kann noch die Registernummer im Titelregister [<code>registrationNumber</code>] angegeben sein.</p>
---	---

Angezeigt werden alle vorhandenen Inhaber-Attribute (siehe Kapitel 5.3.2.6.) wie z. B. Name [`commonName`], Organisation [`organizationName`], Organisationseinheit [`organizatio-`

nalUnitName], Ort [localityName], Land [countryName] und die Postanschrift [postalAddress].

Es folgt die Anzeige des Berufs [professionInfo] im Feld Berufseintrag und bei registrierenden Institutionen, soweit vorhanden, die Registernummer [registrationNumber].

Erweiterung	Bestätigte(r) Beruf(sausübung) (1.3.36.8.3.3)
Kritisch	Nein
Bestätigungseintrag	
Bestätigende Institution	
Familienname	###not set###
Rufname	###not set###
Organisation	Hanseatische Rechtsanwaltskammer Bremen
Ort	Bremen
Land	DE
Anschrift	Knochenhauersraße 36-37 28195 Bremen
Berufsinformation	
Berufseintrag	Rechtsanwältin
Registernummer	2504

Abbildung 20: Erweiterung „bestätigte/r Beruf/sausübung (einer namingAuthority)“

Die Erweiterung muss gemäß Common-PKI-SigG-Profil angezeigt werden. Sie sollte allerdings nicht als kritisch markiert sein.

5.2.5 Erweiterung „altersabhängige Einschränkung“ (QZ, QAZ)

In der Erweiterung „altersabhängige Einschränkung“ [declarationOfMajority] werden vom Alter des Zertifikatsinhabers abhängige Einschränkungen vorgenommen. Angezeigt werden kann das Mindestalter (nicht jünger als (in Jahren) [notYoungerThan]) und ob der Zertifikatsinhaber volljährig ist. Angegeben wird dann (Volljährigkeit: ja/nein [fullage-Country]) sowie das Land, nach dessen Recht die Volljährigkeit festgestellt wurde oder das Geburtsdatum [dateOfBirth]. In der Zertifikatsanzeige wird dabei der ISO-Code des Landes interpretiert, auf das sich die Volljährigkeit bezieht.

Die Erweiterung muss gemäß Common-PKI-SigG-Profil angezeigt werden. Sie sollte allerdings nicht als kritisch markiert sein.

5.2.6 Erweiterung „Einschränkung“ (QZ, QAZ)

Die Erweiterung „Einschränkung“ (QZ, QAZ) [restriction] kann nur eine Einschränkung in Textform enthalten (maximale Länge 1024 Zeichen).

Die Erweiterung muss gemäß Common-PKI-SigG-Profil angezeigt werden. Sie sollte allerdings nicht als kritisch markiert sein.

<p>Erweiterung Zusatzinformationen (1.3.36.8.3.15)</p> <p>Kritisch Nein</p> <p>Dies ist die Extension AdditionalInformation. Sie kann bis zu 2048 Zeichen Freitext enthalten.</p> <p>Erweiterung Einschränkung (1.3.36.8.3.8)</p> <p>Kritisch Nein</p> <p>Dies ist die Extension Restriction. Sie kann bis zu 1024 Zeichen enthalten.</p>

Abbildung 21: Erweiterungen „Einschränkung“ und „Zusatzinformationen“

5.2.7 Erweiterung „Zusatzinformationen“ (QZ, QAZ)

Die Erweiterung „Zusatzinformationen“ [additionalInformation] dient der Angabe von nicht einschränkenden Zusatzinformationen in Textform (maximale Länge 2048 Zeichen), die ansonsten nicht im Zertifikat untergebracht werden können.

Die Erweiterung muss gemäß Common-PKI-SigG-Profil angezeigt werden. Sie sollte allerdings nicht als kritisch markiert sein.

5.3 Detaildarstellung der Zertifikatsinhalte

Im folgenden Kapitel werden alle typischerweise im Signaturzertifikat vorhandenen Einträge in chronologischer Reihenfolge beschrieben, die dem Standard RFC 5280 folgen. Bitte beachten Sie, dass nicht alle Inhalte in jedem Zertifikat tatsächlich vorhanden sind und auch die tatsächliche Reihenfolge im Zertifikat im Vergleich zur folgenden Auflistung variieren kann.

5.3.1 Feld „Herausgeber“ (QZ, QAZ, FZ, VZ)

Anzeigt werden alle im Zertifikat vorhandenen Informationen (Attribute) des Feldes „Herausgeber“ [issuer name].

Nach Common-PKI-SigG-Profil gibt es nur die Pflichtattribute „Land“ [countryName] und „Organisation“ [organizationName], die angegeben werden müssen. Das Attribut „Organisation“ soll dem Namen der Organisation entsprechen, die das Trustcenter operativ führt. Im Attribut „Name“ steht bei QZ nach Common-PKI-SigG-Profil der aus dem CA-Zertifikat übernommene Name [commonName] des Inhabers des CA-Zertifikats. Qualifizierte CA-Zertifikate müssen auf eine natürliche Person ausgestellt werden, verwenden aber in der Regel ein Pseudonym in der Form: Name mit dem Zusatz :PN.

Nach RFC 5280 und RFC 3739 sind die folgenden Attribute möglich:

- Name [commonName],
- Familienname (Nachname) [surName],
- Rufname (Vorname) [givenName],
- Titel [title],
- Initialen [initials]
- Generationskennzeichen [generationQualifier]
- Organisation [organizationName],
- Organisationseinheit [organizationalUnitName],
- Ort [localityName],

- Bundesland [stateOrProvidenceName],
- Land (c) [countryName],
- Namensunterscheider [distinguishedNamequalifier],
- Domainname [domainComponent],
- Pseudonym [pseudonym].
- Seriennummer [serialNumber].

Herausgeber	
Land	DE
Organisation	Deutsche Post Com GmbH
Organisationseinheit	Signtrust
Name	CA DP Com 7:PN

Abbildung 22: Feld „Herausgeber“

Nach Common-PKI-SigG-Profil gibt es nur die beiden Pflichtattribute „Land“ [countryName] und „Organisation“ [organizationName], die angegeben werden müssen. Das Attribut „Organisation“ soll dem Namen der Organisation entsprechen, die das Trustcenter operativ führt. Im Attribut „Name“ steht bei QZ nach Common-PKI-SigG-Profil der aus dem CA-Zertifikat übernommene Name [commonName] des Inhabers des CA-Zertifikats. Qualifizierte CA-Zertifikate müssen auf eine natürliche Person ausgestellt werden, verwenden aber in der Regel ein Pseudonym in der Form: Name mit dem Zusatz :PN.

5.3.2 Bereich „Allgemeines“ (QZ, QAZ, FZ, VZ)

Im Bereich „Allgemeines“ werden technische Informationen zum Zertifikat und die Zertifikatsgültigkeit zusammengefasst.

Allgemeines	
Typ	X.509
Version	3
Gültig ab	06.12.2006 15:09:34
Gültig bis	06.03.2008 15:09:34
Seriennummer	52704
	cd e0

Abbildung 23: Bereich „Allgemeines“

5.3.2.1 Feld „Typ“ (QZ, QAZ, FZ, VZ)

Angezeigt wird die Version des Zertifikats (immer X.509).

5.3.2.2 Feld „Version“ (QZ, QAZ, FZ, VZ)

Signatur-, Verschlüsselungs- und Authentifizierungszertifikate sind gekennzeichnet durch die Version 3 [QZ, FZ, VZ: version]; Attributzertifikate sind an der Version 1 zu erkennen [QAZ: version.AttCertVersion].

5.3.2.3 Feld „Seriennummer“ (QZ, QAZ, FZ, VZ)

Angezeigt wird die Seriennummer des Zertifikats [certificateSerialNumber], auch hexadezimal.

5.3.2.4 Feld „Gültigkeit ab“ (QZ, QAZ, FZ, VZ)

Angezeigt wird das Datum, ab dem das Zertifikat gültig ist, in der Form Tag.Monat.Jahr Stunde:Minute: Sekunde (tt.mm.jjjj hh:mm.ss). [QZ, FZ, VZ: validity notBefore; QAZ: attrCertValidityPeriod notBeforeTime].

5.3.2.5 Feld „Gültigkeit bis“ (QZ, QAZ, FZ, VZ)

Angezeigt wird das Datum, bis zu dem das Zertifikat gültig ist in der Form Tag.Monat.Jahr Stunde:Minute: Sekunde (tt.mm.jjjj hh:mm.ss). [QZ, FZ, VZ: validity notAfter; QAZ: attrCertValidityPeriod notAfterTime].

5.3.2.6 Feld „Inhaber“ (QZ, FZ, VZ, QAZ)“

Angezeigt werden alle im Zertifikat vorhandenen Informationen (Attribute) zum Inhaber des Zertifikats aus dem Feld „Inhaber“ [subject name].

Der Name [commonName] ist gemäß Common-PKI-SigG-Profil das einzige Pflichtattribut, das angegeben werden muss, ggf. mit dem Suffix :PN bei Pseudonymen.

Beispiel: Peter Pelikan:PN.

Inhaber	
Name	Maxi Musterfrau
Titel	Dr.
Familiennamen	Musterfrau
Rufname	Maxi
Organisation	Musterfirma
Organisationseinheit	Vertrieb
Ort	Berlin
Land	DE
Anschrift	Mustergasse 1 12345 Berlin

Abbildung 24: Bereich „Inhaber“

Folgende Attribute können gemäß RFC 5280 und RFC 3039 zusätzlich verwendet werden::

- Name [commonName],
- Familienname (Nachname) [surName],
- Rufname (Vorname) [givenName],
- Titel [title],
- Initialen [initials],
- Generationskennzeichen [generationQualifier],
- Geburtstag [dateOfBirth],
- Geburtsort [placeOfBirth],
- Geschlecht [Gender],
- Geburtsland [countryOfCitizenship],
- Aufenthaltsland [countryOfResidence],

- Geburtsname [nameAtBirth],
- Organisation [organizationName],
- Organisationseinheit [organizationalUnitName],
- Geschäftsfeld [businessCategory],
- Ort [localityName],
- Bundesland [stateOrProvidenceName],
- Land (c) [countryName],
- Namensunterscheider [distinguishedNamequalifier],
- Domainname [domainComponent],
- Straße [streetAddress],
- Postleitzahl [postalCode],
- Postanschrift [postalAddress],
- E-Mailadresse [emailAddress],
- Pseudonym [pseudonym],
- Seriennummer [serialNumber].

Bei einem Attributzertifikat wird hier das zugehörige Basiszertifikat referenziert [subject]. Angezeigt werden in der Regel Attribute, die die ausstellenden Trustcenter angeben. Im Feld Name [commonName] wird der Name des Herausgebers des zugehörigen Basiszertifikats (Signaturzertifikat) und die Seriennummer dieses Zertifikats, bezeichnet als „Seriennummer des Herausgebers“ [baseCertificateID] angegeben.

Inhaber	
Land	DE
Organisation	Deutsche Post Com GmbH
Organisationseinheit	Signtrust
Name	CA DP Com 5:PN
Seriennummer des Herausgebers	64867

Abbildung 25: Bereich „Inhaber“ bei Attributzertifikaten

5.3.3 Bereich „öffentlicher Schlüssel des Signaturinhabers“ (QZ, FZ, VZ)

Angezeigt wird in diesem Bereich der öffentliche Schlüssel des Zertifikatsinhabers [Feld subjectPublicKeyInfo], die Schlüssellänge und der Name des verwendeten Algorithmus.

5.3.3.1 Feld „Algorithmus“ (QZ, FZ, VZ)

Angezeigt wird die Bezeichnung für die angegebene OID des Algorithmus des öffentlichen Schlüssels des Inhabers [algorithmIdentifier] (z. B. SHA1withRSA).

Öffentlicher Schlüssel	
Algorithmus	SHA1withRSA (1.2.840.113549.1.1.1)
Schlüssellänge	2048 Bit
Modulus	97 72 56 c6 25 d9 54 f3 98 b9 98 a4 f4 b9 65 30 8c ad d0 c3 23 ef f3 ae ec 48 58 67 07 f5 cf 57 8f a2 e4 d5 58 b0 59 dc d3 6f c2 ce 8f 08 7d 46 5e 7b 19 ce 5f 9f 8e 98 a8 9e d8 b7 44 31 bc 96 d5 ca 97 71 78 c5 59 9b e9 18 dc fa cd b9 60 a5 a1 a9 a5 f3 59 a5 0f c9 c2 ff 4c ad 93 d2 8e e3 c1 01 63 82 b6 b7 bc db 2d 99 33 94 12 22 28 56 53 36 f8 f1 e6 21 fc f6 2a da ff 81 f8 64 c0 cc c9 6e 47 cb fd b1 a8 94 45 e1 b7 12 28 68 b3 25 90 e3 13 13 d4 58 e8 27 19 66 c3 e9 3e 33 d5 5e f4 bc 51 72 d4 6a 16 00 7a d8 cd 14 c7 66 8e be 01 44 2b d0 40 b0 6b c6 49 cf 1b 0b e9 1a ef be a4 24 6c a3 ad 16 29 18 e3 91 38 b1 2a 74 3e ec 29 ef 64 7c f2 2c 68 c4 e2 df 7f 62 d8 2a fb aa 78 45 24 56 1f 47 51 15 e6 ff 89 83 7c 5d e4 49 35 ba 5a d5 69 8b 03 e5 61 45 35 45 14 55 2c 55
Exponent	00 01

Abbildung 26: Bereich „öffentlicher Schlüssel“

5.3.3.2 Feld „Schlüssellänge“ (QZ, VZ)

Angezeigt wird die Schlüssellänge des Modulus des öffentlichen Schlüssels, berechnet aus dem im Feld `subjectPublicKey` angegebenen Modulus. Mögliche Werte sind alle Längen des Modulus des RSA-Schlüssels.

5.3.3.3 Feld „Modulus“ (QZ, VZ)


Angezeigt wird der Modulus des öffentlichen Schlüssels des Zertifikatsinhabers [`subjectPublicKeyInfo.subjectPublicKey`].

5.3.3.4 Feld „Exponent“ (QZ, VZ)

Angezeigt wird der Exponent des öffentlichen Schlüssels des Zertifikatsinhabers [`subjectPublicKeyInfo.subjectPublicKey`].

5.3.4 Feld „UID des Herausgebers“ (QZ, FZ, VZ, QAZ)

Angezeigt wird ein (eindeutiges) Identifikationskennzeichen für den Herausgeber des Zertifikats als Zeichenkette [`issuerUniqueID`].


	<p>Hinweis: UID des Herausgebers/Inhabers bei QZ</p> <p>Rein formal verbietet Common PKI das Ausstellen von Zertifikaten mit <code>issuerUniqueID/subjectUniqueIDs</code>, da sie für die eindeutige Konstruktion der Verifikationsketten bei der Prüfung von Zertifikaten nicht geeignet sind. Vielmehr wird eine Kettenbildung über den <code>issuer.DName/subject.DName</code>, hilfsweise über die Erweiterung <code>SubjectKeyIdentifier</code> (CA-Zertifikat) bzw. <code>AuthorityKeyIdentifier</code> (Nutzerzertifikat [EE-Zertifikat]) durchgeführt.</p>
---	---

5.3.5 Feld „UID des Inhabers“ (QZ, FZ, VZ)

Angezeigt wird ein (eindeutiges) Identifikationskennzeichen für den Inhaber des Zertifikats als Zeichenkette [`subjectUniqueID`] siehe auch obigen Hinweis zur UID des Herausgebers/Inhabers bei QZ.

5.3.6 Erweiterung „Ausstellerschlüssel-ID“ (QZ, FZ, QAZ, VZ)

Angezeigt wird eine eindeutige Zeichenkette, die die eindeutige Identifizierung des öffentlichen Schlüssels des Herausgeberzertifikats erlaubt [`AuthorityKeyIdentifier`].

	<p>Hinweis: Aussteller- und Inhaberschlüssel-ID bei QZ</p> <p>Die Ausstellerschlüssel-ID ist eine Erweiterung gemäß X509, beschrieben in RFC 5280. Sie sollte nicht als kritisch markiert sein. Die Angabe kann mit einer eindeutigen Schlüssel-ID (z. B. Hash) erfolgen oder einer Kombination aus einer Seriennummer und dem DName [subject DName] des CA-Zertifikats des Herausgebers. Die Ausstellerschlüssel-ID in User-Zertifikaten wird zur Zertifikatsprüfung für die eindeutige Konstruktion der Verifikationskette genutzt, sollte über den Herausgebernamen [isuser DName] eine eindeutige Zuordnung zu einem CA-Zertifikat nicht möglich sein (weil z. B. mehrere CA-Zertifikate denselben Herausgebernamen verwenden). Die Inhaberschlüssel-ID [subjectKeyIdentifier] aus dem CA-Zertifikat und die Ausstellerschlüssel-ID [authorityKeyIdentifier] aus dem User-Zertifikat müssen gem. Common-PKI-SigG-Profil identisch sein.</p>
---	--

5.3.7 Erweiterung „Inhaberschlüssel-ID“

Diese Erweiterung findet sich nur in CA-Zertifikaten, die nicht selbst signiert sind [(subject)KeyIdentifier].

5.3.8 Erweiterung „Schlüsselverwendung“ (QZ, FZ, VZ)

In dieser Erweiterung wird der Zweck, für den der öffentliche Schlüssel des Zertifikats verwendet werden darf [keyUsage], angezeigt. Diese Erweiterung hat eine herausragende Bedeutung und muss nach Common-PKI-Spezifikation als kritisch markiert sein. In den folgenden Unterkapiteln werden die möglichen Verwendungszwecke von Nutzerzertifikaten (EE-Zertifikaten) erläutert.

Erweiterungen	
Erweiterung	Schlüsselverwendung (2.5.29.15)
Kritisch	Ja
	01000000
	nichtabstreitbar

Abbildung 27: Erweiterung „Schlüsselverwendung“ hier: „nichtabstreitbar“

5.3.8.1 Digitale Signatur (FZ)

Die Schlüsselverwendung „Digitale Signatur“ [digitalSignature] bezeichnet den öffentliche Schlüssel, der für digitale Signaturen verwendet werden soll und nicht den Zweck der Nichtabstreitbarkeit erfüllen sollen (siehe auch den folgenden Verwendungszweck). Sie wird häufig im Bereich der fortgeschrittenen elektronischen Signatur nach Signaturgesetz verwendet und für Zertifikate für die Authentifizierung.

5.3.8.2 Nichtabstreitbar (QZ)

Die Schlüsselverwendung „Nichtabstreitbarkeit“ [nonRepudiation bzw. contentCommitment] ist gesetzt, wenn der Schlüssel für digitale Signaturen eines Nichtabstreitbarkeits-service verwendet werden soll, wie zum Beispiel für qualifizierte elektronische Signaturen nach Deutschem Signaturgesetz, die bis auf einige spezielle, gesetzlich festgelegte Ausnahmen eine Rechtswirkung wie eine eigenhändige Unterschrift entfalten.



Achtung: Nach Common-PKI-SigG-Profil darf bei qualifizierten Zertifikaten nur der Verwendungszweck nonRepudiation (contentCommitment) verwendet werden.

5.3.8.3 Schlüsselverschlüsselung (VZ)

Die Schlüsselverwendung „Schlüsselverschlüsselung“ [keyEncipherment] ist gesetzt, wenn der Schlüssel für die Verschlüsselung von anderen Schlüsseln oder Sicherheitsinformationen verwendet werden soll.

5.3.8.4 Datenverschlüsselung (VZ)

Die Schlüsselverwendung „Datenverschlüsselung“ [dataEncipherment] ist gesetzt, wenn der Schlüssel zur Verschlüsselung von Benutzerdaten [und nicht anderen Schlüsseln] verwendet werden soll.

5.3.8.5 Schlüsselvereinbarung

Die Schlüsselverwendungen „Schlüsselvereinbarung“ [keyAgreement], „nur Verschlüsselung“ [encipherOnly], nur „Entschlüsselung“ [decipherOnly] werden gesetzt, wenn der Diffie-Hellman-Algorithmus für die Schlüsselvereinbarung verwendet werden soll. „Nur Verschlüsselung“ und „Nur Entschlüsselung“ sind nur zusammen mit Schlüsselvereinbarung nach Diffie Hellman sinnvoll.

5.3.8.6 Zertifikatsignatur/CRL-Signatur

Die Schlüsselverwendung „Zertifikatsignatur“ [keycertSign] und „CRL-Signatur“ [CRLSign]: Diese werden gemäß RFC 5280 nur bei CA-Zertifikaten verwendet, wenn der Schlüssel für die Verifikation von Signaturen auf Zertifikaten verwendet wird, bzw. wenn der Schlüssel für die Verifikation von Signaturen auf CRLs verwendet wird.

5.3.9 Erweiterung „Private Key Validity Usage Period“ (FZ, VZ)

Die Erweiterung „Private Key Usage Period“ [privateKey(Validity)UsagePeriod] ermöglicht es, dem privaten Schlüssel eine andere Gültigkeitsperiode als dem Zertifikat zuzuweisen. Sie besteht aus einer Sequenz von 2 Datumsangaben.

Diese Erweiterung gemäß RFC 5280 wird im Bereich qualifizierter Zertifikate nicht verwendet.

5.3.10 Erweiterung „Zertifizierungsrichtlinien“ (QZ, QAZ, FZ, VZ)

In der Erweiterung „Zertifizierungsrichtlinien“ [certificatePolicies] sind die Bedingungen festgelegt, unter denen das Zertifikat herausgegeben wurde und unter denen es verwendet werden darf. Sie enthält eine Liste von Zertifikatsrichtlinien, jeweils mit OID und Name, z. B. auch die URL, die auf das Certification Practice Statement (CPS) verweist. Dieses Dokument erläutert die Vorgehensweise des Trustcenters bei der Ausgabe von Zertifikaten und beschreibt vorhandene Sicherheitsmaßstäbe.

Eine besondere Bedeutung hat in diesem Zusammenhang eine OID [id-commonpki-cp-accredited], die besagt, dass eine Zertifizierungsrichtlinie vorliegt, in der beschrieben ist, dass es sich um ein Zertifikat handelt, das den Anforderungen an ein qualifiziertes Zertifikat mit Anbieterakkreditierung nach Signaturgesetz (SigG) genügt.

Die Erweiterung sollte gemäß Common-PKI-SigG-Profil nicht als kritisch markiert sein.

5.3.11 Erweiterung „Richtlinienzuordnungen“

Die Erweiterung „Richtlinienzuordnungen“ [`policyMappings`] findet nur bei CA-Zertifikaten Anwendung.

5.3.12 Erweiterung „Alternativer Name des Inhabers“ (QZ, FZ, VZ)

Die Erweiterung „Alternativer Name des Inhabers“ [`subjectAlternativeName`] besteht aus einer Liste von alternativen (technischen) Namen für den Inhaber des Zertifikats. Diese Namen können RFC 822-Namen, DNS-Namen, X.400 Adressen, EDI-Namen, URIs oder IP-Adressen sein, im Grunde ist jedes strukturierte Namensschema verwendbar.

Häufig wird hier nur die E-Mail-Adresse des Zertifikatsinhabers als RFC 822-Name eingetragen (z. B. `myuser@example.com`).

Diese Erweiterung sollte gemäß Common-PKI-Spezifikation nicht als kritisch markiert sein. Gemäß PKIX-Standard muss diese Erweiterung allerdings als kritisch markiert werden, wenn das Subject-Feld im Zertifikat leer ist.

5.3.13 Erweiterung „Alternativer Name des Ausstellers“ (QZ, FZ, VZ)

Die Erweiterung „Alternativer Name des Ausstellers“ [`issuerAlternativeName`] besteht aus einer Liste von alternativen (technischen) Namen für den Aussteller des Zertifikats. Diese Namen können RFC 822-Namen, DNS-Namen, X.400 Adressen, EDI-Namen, URIs oder IP-Adressen sein, im Grunde ist jedes strukturierte Namensschema verwendbar. Nach Common-PKI-Spezifikation sollte hier u. a. die LDAP-URL angegeben sein, über die das Zertifikat herunter geladen werden kann.

Diese Erweiterung sollte gemäß Common PKI nicht als kritisch markiert sein.

5.3.14 Erweiterung „Verzeichnisattribute des Inhabers“ (QZ, QAZ, FZ, VZ)

Die Erweiterung „Verzeichnisattribute des Inhabers“ [`subjectDirectoryAttributes`] ist dafür gedacht, zusätzliche Informationen (Attribute) über den Inhaber bereitzustellen. Folgende Attribute können gemäß RFC 5280 verwendet werden:

- Name [`commonName`],
- Nachname [`surName`],
- Vorname [`givenName`],
- Titel [`title`],
- Postanschrift [`postalAddress`],
- Geburtstag [`dateOfBirth`],
- Geburtsort [`placeOfBirth`],
- Geschlecht [`Gender`],
- Geburtsland [`countryOfCitizenship`],
- Aufenthaltsland [`countryOfResidence`] und
- Geburtsname [`nameAtBirth`].

Diese Erweiterung sollte gemäß Common-PKI-Spezifikation nicht als kritisch markiert sein. Qualifizierte Trustcenter können diese Extension für rechtlich zugelassene Identifikationsda-

ten verwenden. Diese Informationen können in Attributzertifikaten als Attribut verwendet werden.

5.3.15 Erweiterung „Allgemeine Einschränkungen“

Die Erweiterung „Allgemeine Einschränkungen“ [`basicConstraints`] findet sich nur bei CA-Zertifikaten. Dadurch lassen sich CA-Zertifikate identifizieren. Außerdem wird dort angegeben, wie tief der unter dem CA-Zertifikat liegende Zertifizierungspfad sein darf.

5.3.16 Erweiterung „Beschränkung des Namensraums“

Die Erweiterung „Beschränkung des Namensraums“ [`nameConstraints`] findet sich nur bei CA-Zertifikaten. Sie definiert erlaubte Namen in untergeordneten Zertifikaten.

5.3.17 Erweiterung „Richtlinienbeschränkungen“

Die Erweiterung „Richtlinienbeschränkungen“ [`policyConstraints`] findet sich nur in CA-Zertifikaten. Sie legt fest, dass dem CA-Zertifikat folgende Zertifikate im Zertifizierungspfad Policy-Identifizier (OIDs) zu definieren haben und/oder verbietet das Policy Mapping in untergeordneten Zertifikaten.

5.3.18 Erweiterung „Erweiterte Schlüsselverwendung“

Die Erweiterung „Erweiterte Schlüsselverwendung“ [`extendedKeyUsage`] kann zusätzlich die Verwendungsmöglichkeiten des öffentlichen Schlüssels des Zertifikats einschränken oder erweitern. Nach PKIX-Standard werden folgende standardisierte Möglichkeiten verwendet:

- TLS Web Server authentication,
- TLS Web Client authentication,
- Code-Signing, EmailProtection,
- Zeitstempeldienst [`timeStamping`] und
- OCSP-Responder-Signatur [`OCSP-Signing`].

Zeitstempeldienstzertifikate müssen nach RFC 3161 den Verwendungszweck „Zeitstempeldienst“ besitzen. Zusätzlich zu dieser erweiterten Schlüsselverwendung darf gemäß Common-PKI-SigG-Profil bei qualifizierten Zeitstempelzertifikaten noch die Schlüsselverwendung „`nonRepudiation`“ verwendet werden (siehe Kapitel 5.3.8.2). Die Common-PKI-Spezifikation verlangt, dass die Erweiterung „`ExtendedKeyUsage`“ bei dieser erweiterten Schlüsselverwendung als kritisch markiert werden muss.

OCSP-Responder-Zertifikate müssen nach RFC 2560 Eintrag eine „OCSP-Responder-Signatur“ besitzen.

5.3.19 Erweiterung „Distributionspunkt für CRL“ (QZ, QAZ, FZ, VZ)

Die Erweiterung „Distributionspunkt für CRL“ [`CRLDistributionPoint`] liefert Informationen darüber, wie Sperrinformationen zu dem Zertifikat bezogen werden können.

Angegeben werden, zumindest bei qualifizierten Zertifikaten, die LDAP-URL [Feld `fullName`] und – soweit vorhanden - die alternative HTTP-URL der Zertifikatssperrliste sowie der Herausgeber der Zertifikatssperrliste [`cRLIssuer`]. Nach Common-PKI-Spezifikation müssen konforme CAs die CRL über eine LDAP-URL bereitstellen.

Erweiterung	Distributionspunkt für CRL (2.5.29.31)
Kritisch	Nein
	ldap://pkldap.tttc.de:389/o=Deutsche Telekom AG,c=de http://www.tttc.de/telesec/servlet/download_crl
Herausgeber der Zertifikatssperrliste	
Land	DE
Organisation	Deutsche Telekom AG
Organisationseinheit	T-TeleSec Test
Namenstrenner	1
Name	T-TeleSec Test DIR 8:PN

Abbildung 28: Erweiterung „Distributionspunkt für CRL“

Diese Erweiterung sollte gemäß Common-PKI-Spezifikation nicht als kritisch markiert sein.

In der Regel wird in der Erweiterung auch angegeben, wer der Herausgeber der Sperrliste ist. Dieses sind in der Regel die wichtigsten Attribute aus dem Feld „Inhaber“ [subject] des Zertifikats, von dem die Sperrliste signiert worden ist:

- Land [countryName],
- Organisation [organizationName],
- Organisationseinheit [organizationalUnitName],
- Name [commonName].

5.3.20 Erweiterung „Zugangsdaten des Ausstellers“ (QZ, FZ, QAZ, VZ)

Die Erweiterung „Zugangsdaten des Ausstellers“ [authorityInformationAccess] definiert, wie weitere Informationen und Services der ausstellenden CA genutzt werden können.

Bei qualifizierten Signaturzertifikaten enthält diese Erweiterung im Feld „Zugangsart“ [accessMethod] den Wert „OCSP oder einfache OCSP-Antwort“ [OID id-ad-ocsp] und die URL, unter der der OCSP-Responder für die Zertifikatsprüfung angesprochen werden kann [accessLocation].

Erweiterung	Zugangsdaten des Ausstellers (1.3.6.1.5.5.7.1.1)
Kritisch	Nein
Zugangsart	Einfache OCSP-Antwort http://www.tttc.de/ocspr

Abbildung 29: Erweiterung „Zugangsdaten des Ausstellers“

Für den Fall, dass ein Trust Center einen OCSP-Service anbietet, muss diese Erweiterung nach Common-PKI-Spezifikation angegeben werden.

5.3.21 Erweiterung „BiometricData“

Erweiterung für gehashte, biometrische Informationen, wie z.B. die Angabe des Hash-Algorithmus, mit dem das biometrische Datenimage gehasht wurde.

5.3.22 Erweiterung „Angaben zum qualifizierten Zertifikat“ (QZ, QAZ)

In der Erweiterung „Angaben zum qualifizierten Zertifikat“ [qcStatement] werden so genannte qualifizierte Zertifikatsstatements aufgelistet. Diese Erweiterung sollte gemäß Com-

mon-PKI-Spezifikation nicht als kritisch markiert sein. Folgende Statements können aufgenommen werden.

5.3.22.1 Statement „Konform mit EU-Direktive 1999/93/EC“

Das Statement „Konform mit EU-Direktive 1999/93/EC“ [id-etsi-qcs-QcCompliance] ist ein Indikator dafür, dass es sich um ein qualifiziertes Zertifikat, herausgegeben von einem Zertifizierungsdiensteanbieter, handelt, der sich konform zur in nationales Recht umgesetzten EU-Direktive 1999/93/EC verhält. Bei einem deutschen Zertifizierungsdiensteanbieter, der qualifizierte Signaturzertifikate erstellt, ist dieses das Deutsche Signaturgesetz. Der Nachweis selbst wird über eine Certificate Policy erbracht, die konform zu ETSI TS 101 456 v1.1.1 ist.

<p>Erweiterung Angaben zum qualifizierten Zertifikat (1.3.6.1.5.5.7.1.3)</p> <p>Kritisch Nein</p> <p>Konform mit EU-Direktive 1999/93/EC</p> <p>Externe Identifikationsdokumente werden 30 Jahre bei der CA aufbewahrt.</p> <p>Privater Schlüssel auf SmartCard gemäß EU-Direktive 1999/93/EC Anhang 3</p>
--

Abbildung 30: Erweiterung „Angaben zum qualifizierten Zertifikat“

5.3.22.2 Statement „Monetäre Beschränkung“

Das Statement „Monetäre Beschränkung“ [id-etsi-qcs-QcLimitValue] schränkt den finanziellen Verfügungsrahmen des Zertifikatsinhabers ein. Es besitzt folgende Form: Zahlenwert Währung. Siehe auch die ausführliche Beschreibung in Kapitel 5.2.2.

5.3.22.3 Statement „Aufbewahrung externer Identifikationsdokumente“

Das „Statement Aufbewahrung externer Identifikationsdokumente“ [id-etsi-qcs-QcRetentionPeriod] zeigt an, wie viele Jahre externe Identifikationsdokumente (z. B. Kopie des Personalausweises und die Postident-Bescheinigung) beim Zertifizierungsdiensteanbieter nach Ablauf der Zertifikatsgültigkeit aufbewahrt werden. Dadurch ist es möglich, für den genannten Zeitraum im Streitfall die physische Person zu identifizieren.

5.3.22.4 Statement „Privater Schlüssel auf SmartCard gemäß EU-Direktive 1999/93/EC Anhang 3“

Das Statement "Privater Schlüssel auf SmartCard gemäß EU-Direktive 1999/93/EC Anhang 3" [id-etsi-qcs-QcSSCD] wird gesetzt, wenn es sich bei der verwendeten Smartcard um eine sichere Signaturerstellungseinheit (SSEE) handelt. Eine Smartcard wird dann zur SSEE, wenn sie von einer unabhängigen Bestätigungsstelle (z. B. TÜV-IT) geprüft wurde. Diese bestätigt, dass die SSEE für den Einsatz mit Signaturanwendungskomponenten zur Erzeugung qualifizierter elektronischer Signaturen nach deutschem Signaturgesetz (SigG) geeignet ist. Nachdem die zuständige Aufsichtsbehörde, die Bundesnetzagentur (BNetzA), die Bestätigung veröffentlicht hat, können ZDA diese SSEE personalisieren.

5.3.23 Erweiterung „Keine OCSP-Prüfung“

Die Erweiterung „keine OCSP-Prüfung“ wird nur bei OCSP-Responder-Zertifikaten verwendet („private Extension“ gemäß RFC 2560),

5.3.24 Erweiterung „Seriennummer der Chipkarte“ (QZ)

Die Erweiterung „Seriennummer der Chipkarte“ zeigt die Seriennummer der Signaturkarte an, auf der der zum öffentlichen Schlüssel korrespondierende private Schlüssel abgespeichert werden kann [ICSSN] (Common-PKI-SigG-Profil „private Extension“).

5.3.25 Bereich „Signatur des Herausgebers“

Angezeigt wird hier zuerst der Bezeichner (OID) des Signaturalgorithmus, der von dem Herausgeber und Aussteller (Zertifizierungsdiensteanbieter) zur Signatur des Zertifikats verwendet wurde und die Signatur des Zertifikats, erzeugt durch den Zertifizierungsdiensteanbieter.

Signatur des Herausgebers	
Signaturalgorithmus	SHA1withRSA (1.2.840.113549.1.1.5)
Signatur	52 bd af e8 ce 9f 64 23 b4 0c 2e 77 8e 85 4e 08 dc 53 75 f9 ef 9e 9b 0c fd 56 d9 47 af b9 0d 0e 8f af 1c 72 f2 61 6b 0c 56 23 f7 ef 8b 14 0d fa a6 5c 02 ce 8f 2c a9 bd bc c2 8f 25 06 8b c8 98 57 1e c7 70 c3 36 53 3a 87 2c 27 67 29 4f 3d 39 0a 33 bc a9 aa f3 60 f6 fd 1d 64 eb 0c ab 58 81 8b 13 8f b6 ec cf f2 83 b3 10 48 aa a4 aa 8a 93 57 34 35 12 e6 74 e3 c4 6d 24 34 75 60 44 80 2e 90 d5 a9 b5 a1 29 5c 5c e0 34 30 fa c5 28 2d 5e 3e 2e 17 53 9e 96 52 9a db 4b 89 38 cc 5b 5d 34 23 98 2b 51 0d ba 81 b4 9f f2 15 27 e5 44 68 50 9b 4b 20 23 36 2a 80 79 a2 95 1f a7 4d 75 f0 70 d8 54 be 2d 3c ae fb 5c a3 50 f7 28 c6 82 6a 44 a8 0e f6 3b 72 1d 79 71 28 13 4c ec 84 92 17 49 d2 3d 6c 58 54 07 98 f7 55 b5 bb 1f 3a 2e 8d a9 d8 2c 43 f8 2e 6e 43 4c 45 32 01 ca 27 7f 92 5b
Fingerabdruck	
SHA-1	90 1a 33 9b b0 80 9a 6e 2a 22 b9 c3 f2 1a 37 3d b5 f0 89 ee
MD5	8d 09 6c 0a ae 91 5d af 48 16 57 a6 b6 d7 3a 01

Abbildung 31: Bereich „Signatur des Herausgebers“

5.3.25.1 Feld „Signaturalgorithmus des Herausgebers“ (QZ, QAZ, FZ, VZ)

Angezeigt wird der vom Zertifizierungsdiensteanbieter (Trust Center) verwendete Algorithmus zur Signatur des Zertifikats [signatureAlgorithm].

5.3.25.2 Feld „Signatur des Herausgebers“ (QZ, QAZ, FZ, VZ)

Angezeigt wird die Signatur des Herausgebers (Zertifizierungsdiensteanbieter) [signatureValue] hexadezimal.

5.3.26 Anzeige des Fingerabdrucks über das Zertifikat (QZ, QAZ, FZ, VZ)

Der Fingerabdruck (Fingerprint) ist der durch die bos-Zertifikatsanzeige berechnete Hashwert einer, auf das Zertifikat mit öffentlichen Schlüssel des Inhabers angewendeten Hash-Funktion.

6 Bereich "Übertragungssicherheit"

Der Bereich "Übertragungssicherheit" wird bei Nachprüfungen von Zertifikaten und bei der Online-Prüfung von PKCS#7, PDF und S/MIME-Dateien im Fehlerfall am Anfang des Prüfprotokolls angezeigt.

Zertifikate signierter PKCS#7-, PDF-Dokumente und S/MIMEs werden clientseitig online verifiziert. Die Online-Verifikation erfolgt über verschiedene Serverinstanzen (u. a. den Verifikationsserver und das OCSP/CRL-Relay von Governikus). Serverantworten, wie auch die Antwortnachricht zur Übermittlung eines Prüfergebnisses werden vom Server signiert. Durch eine Überprüfung der Signatur kann die Client-Anwendung die Echtheit der übermittelten Antwort feststellen. Für diese Antwortüberprüfung benötigt das Programm das vom Server verwendete Zertifikat.



Abbildung 32: Übertragungssicherheit (PKCS#7 und PDF)

6.1 Feld "Autoren"

Das Feld "Autoren" zeigt den "CommonName" des hinterlegten Zertifikats des Verifikationsservers bzw. des OCSP/CRL-Relays an, das die Antwort signiert hat. Der Name ist als Link hinterlegt und führt zur Detailansicht "Zertifikat des Verifikationsservers" im Bereich "Zertifikate und Ergebnisse der Zertifikatsprüfung" im bos-Prüfprotokoll.

6.2 Feld "Mathematische Signaturprüfung"

Dieses Feld zeigt an, ob die Signatur der Antwortnachricht des Servers lokal verifiziert werden konnte.

Das Feld "mathematische Signaturprüfung" zeigt an, ob die Signaturen über die Zertifikate der Zertifikatskette korrekt sind.

Ein grüner Kasten mit Haken signalisiert, dass die mathematische Signaturprüfung erfolgreich war.

Ein roter Kasten mit Kreuz bedeutet, dass die Prüfung fehlgeschlagen ist.

7 Verzeichnis der Abbildungen und Tabellen

Abbildung 1: Prüfprotokoll – Ausschnitt asynchrone OSCI-Nachricht	8
Abbildung 2: Prüfprotokoll – Ausschnitt synchrone OSCI-Nachricht	9
Abbildung 3: Meldung, wenn kein Absender/Empfänger vorhanden ist	9
Abbildung 4: Meldung, wenn kein Eingangszeitpunkt angegeben ist	10
Abbildung 5: Bereich Zusammenfassung (PKCS#7, detached)	12
Abbildung 6: Bereich Zusammenfassung (PKCS#7, enveloped)	13
Abbildung 7: Feld Autoren: Ampelstatus	13
Abbildung 8: Bereich Nachrichtenstruktur bei einer OSCI-Nachricht mit zwei Signaturen	16
Abbildung 9: Bereich „Signaturen“ für eine QES	17
Abbildung 10: Anzeige der verwendeten Algorithmen mit Datum des Ablaufs der Eignung	19
Abbildung 11: Bereich „Signaturen“ für eine fortgeschrittene oder einfache Signatur mit manipulierter Integrität der Inhaltsdaten	20
Abbildung 12: Bereich „Signaturen“ - Anzeige der Prüfergebnisse zum Attributzertifikat	22
Abbildung 13: Zusammenfassende Angaben zum Zertifikat (oberer Bereich)	23
Abbildung 14: Gesamt- und Einzelprüfergebnisse (OSCI) (unterer Bereich)	24
Abbildung 15: Einzelprüfergebnisse und Informationen zum Zertifikat	27
Abbildung 16: Prüfergebnisse einer Nachprüfung	29
Abbildung 17: Zusammenfassung Signaturzertifikat	32
Abbildung 18: Erweiterung „Attributzertifikat“ vorhanden	34
Abbildung 19: Erweiterung „Vertretungsmacht“	35
Abbildung 20: Erweiterung „bestätigte/r Beruf/sausübung (einer namingAuthority)“	36
Abbildung 21: Erweiterungen „Einschränkung“ und „Zusatzinformationen“	37
Abbildung 22: Feld „Herausgeber“	38
Abbildung 23: Bereich „Allgemeines“	38
Abbildung 24: Bereich „Inhaber“	39
Abbildung 25: Bereich „Inhaber“ bei Attributzertifikaten	40
Abbildung 26: Bereich „öffentlicher Schlüssel“	41
Abbildung 27: Erweiterung „Schlüsselverwendung“ hier: „nichtabstreitbar“	42
Abbildung 28: Erweiterung „Distributionspunkt für CRL“	46
Abbildung 29: Erweiterung „Zugangsinformationen des Ausstellers“	46
Abbildung 30: Erweiterung „Angaben zum qualifizierten Zertifikat“	47
Abbildung 31: Bereich „Signatur des Herausgebers“	48
Abbildung 32: Übertragungssicherheit (PKCS#7 und PDF)	49

Tabelle 1: Ermittlung des Gesamtprüfergebnisses abhängig von der Eignung der
verwendeten Algorithmen 18