Governikus KG

Anwenderhandbuch

Governikus Prüfprotokoll

Verification Interpreter Version 3_6_1_3

Dokumentenversion 1.0

13. März 2015

© 2015 Governikus GmbH & Co. KG

Dokumentversion Release-Nummer_Dokumentversionsnr.

Änderungsnachweise

Version	Freigabedatum	Autor	Kapitel	Änderungen
1.0	13.03.2015	JP	1 und 2	Version hochgezählt

Inhaltsverzeichnis

1 Einleitung 7

2 Rechtlicher und technischer Hintergrund 9
2.1 Signaturprüfung 9
2.2 Signaturniveaus in der EU und Deutschland 9
2.2.1 Fortgeschrittene elektronische Signatur (EU und Deutschland) 10
2.2.2 Fortgeschrittene elektronische Signatur mit qualifiziertem Zertifikat (EU) 10
2.2.3 Qualifizierte elektronische Signatur (EU) 10
2.2.4 Qualifizierte elektronische Signatur mit Anbieterakkreditierung (EU) 11
2.2.5 Qualifizierte elektronische Signatur (D) 11
2.2.6 Qualifizierte elektronische Signatur mit Anbieterakkreditierung (D) 12
2.3 Ablauf der Signaturprüfung 12
2.3.1 Unterstützte Signaturformate und Signaturalgorithmen 12
2.3.2 Zertifikatsprüfung durch das OCSP/CRL-Relay 13
2.3.3 Anzeige der Prüfergebnisse 13
2.3.4 Einhaltung der gesetzlichen Anforderungen 13

3 Bereich 1: Zusammenfassung und Struktur 14
3.1 OSCI-Nachrichten (OSCI 1.2) 15
3.1.1 Zeile Name der OSCI-Nachricht 15
3.1.2 Kontextinformationen zur OSCI-Nachricht 15
3.1.3 Zeile "Name des Inhaltsdaten-Containers" 16
3.1.4 Zeile "Autor, Prüfergebnis und Erläuterung" 17
3.1.5 Zeile "Inhaltsdaten" 20
3.1.6 Zeile "Anhänge" 20
3.2 PKCS#7-Signaturen 21
3.2.1 Zeile "Dateiname" 21
3.2.2 Zeile "Signaturform" 21
3.2.3 Zeile "Inhaltsdaten" (nur Signatur ohne Dokumenteninhalt) 22
3.2.4 Zeile "Autor, Prüfergebnis und Erläuterung" 22
3.3 PDF-Inline-Signaturen und PAdES 26
3.3.1 Zeile "Dateiname" 27
3.3.2 Zeile "PDF-Revision" 27
3.3.3 Zeile "PAdES-Profilierung" (nur PAdES) 27
3.3.4 Zeile "Hinweis" 27
3.3.5 Zeile "Autor, Prüfergebnis und Erläuterung" 29
3.3.6 Anzeige der Prüfergebnisse von PDF-Portfolios" 32
3.4 Signaturzertifikate (Einzelprüfung) 34
3.4.1 Bereich 1: Zusammenfassung und Struktur 34
3.4.2 Bereich 2: Zertifikatsprüfungen 37
3.5 Gesamtprüfergebnis 41
3.5.1 Fachliches Gesamtprüfergebnis bei PDF-Dokumenten 42

4 Bereich 2: "Signaturprüfungen" 43
4.1 Kumuliertes Prüfergebnis und Informationen zur Signatur 44
4.1.1 Zeile "Prüfergebnis, Signaturformat und Dateiname/Container" 44
4.1.2 Zeile "Autor" 46
4.1.3 Zeile "Aussteller des Zertifikats" 46
4.1.4 Zeile Ort der Signatur (nur bei *AdES-Dokumenten) 46
4.1.5 Zeile "Signaturgrund" (nur bei *AdES-Dokumenten) 47
4.1.6 Zeile "Signaturrichtlinie" (nur bei *AdES-Dokumenten) 47
4.1.7 Zeile "Signaturniveau" 47
4.1.8 Zeile "Signierzeitpunkt" 49
4.1.9 Zeile "Durchführung der Prüfung" 49

4.1.10 Zeile "Aussteller des Attributzertifikats" (nur bei Attributzertifikaten) 49
4.2 Signaturprüfung der Inhaltsdaten 50
4.2.1 Zeile "Mathematische Signaturprüfung der Inhaltsdaten" 50
4.2.2 Zeile "Eignung des verwendeten Signaturalgorithmus" 51
4.3 Prüfung des Zertifikats 56
4.3.1 Zeile "Prüfung des Zertifikats 56
4.3.2 Zeile "Vertrauenswürdigkeit des Trustcenters" 56
4.3.3 Zeile "Mathematische Signaturprüfung der Zertifikatskette" 57
4.3.4 Zeile "Gültigkeitsintervall des geprüften Zertifikats" 58
4.3.5 Zeile "Sperrstatus des geprüften Zertifikats" 58
4.3.6 Zeile "Eignung des verwendeten Signaturalgorithmus" 60
4.3.7 Link "Technische Informationen zur Prüfung" 64
4.3.8 Zeile "Erläuterungen" 65
4.4 Zusätzliche Prüfung eines Attributzertifikats 67
4.4.1 Zeile "Aussteller des Attributzertifikats" (nur bei Attributzertifikaten) 68
4.4.2 Zeile "Zuordnung des Attributzertifikats zum Signaturzertifikat" 68
4.5 Teil 3: Nachprüfung eines Zertifikats bei OSCI-Nachrichten 69

5 Bereich 3: Zertifikate 70
5.1 Anzeige von Zertifikatsinhalten im Prüfprotokoll 71
5.2 Inhaber eines Zertifikats 72
5.2.1 Qualifiziertes Zertifikat gemäß CommonPKI SigG-Profil 73
5.2.2 Qualifiziertes Attributzertifikat gemäß CommonPKI SigG-Profil 73
5.3 Aussteller eines Zertifikats 73
5.3.1 Qualifiziertes Signaturzertifikat gemäß Common PKI-Profil 74
5.4 Allgemeine Informationen 74
5.4.1 Zeilen "Typ" und "Version" 74
5.4.2 Zeile "Algorithmus" 75
5.4.3 Zeilen "gültig ab" und "gültig bis" (Gültigkeitszeitraum) 75
5.4.4 Zeile "Seriennummer" 75
5.5 Öffentlicher Schlüssel aus dem Zertifikat 75
5.5.1 RSA-Schlüssel 75
5.5.2 ECDSA-Schlüssel 76
5.6 Signatur des Ausstellers im Zertifikat 77
5.6.1 Zeile "Signaturalgorithmus" 77
5.6.2 Zeile "Signatur" 77
5.7 Fingerabdruck des Zertifikats 78
5.7.1 Zeilen "UID des Ausstellers" und "UID des Inhabers" 78
5.8 Allgemeine Zertifikatserweiterungen 78
5.8.1 Erweiterungen "Aussteller- und Inhaberschlüssel-ID" 79
5.8.2 Erweiterung "Schlüsselverwendung" 80
5.8.3 Erweiterung "Zertifizierungsrichtlinien" 82
5.8.4 Erweiterung "Richtlinienzuordnungen" 83
5.8.5 Erweiterung "Alternativer Name des Inhabers" 83
5.8.6 Erweiterung "Alternativer Name des Ausstellers" 84
5.8.7 Erweiterung "Verzeichnisattribute des Inhabers" 84
5.8.8 Erweiterung "Allgemeine Einschränkungen" 85
5.8.9 Erweiterung "Beschränkung des Namensraums" 85
5.8.10 Erweiterung "Richtlinienbeschränkungen" 85
5.8.11 Erweiterung "Erweiterte Schlüsselverwendung" 86
5.8.12 Erweiterung "Distributionspunkt für CRL" 86
5.8.13 Erweiterung "Unterdrückung jeder Policy" 88
5.8.14 Erweiterung "neueste CRL" 88
5.8.15 Erweiterung Zugangsinformationen des Ausstellers 88
5.8.16 Erweiterung Zugangsinformationen des Inhabers 89

5.8.17 Erweiterung "BiometricData" 89
5.8.18 Erweiterung "Angaben zum qualifizierten Zertifikat" 89
5.8.19 Erweiterung "keine OCSP-Prüfung" 91
5.8.20 Erweiterung "Attributzertifikat" 91
5.8.21 Erweiterung "Datum Zertifikatserzeugung" 91
5.8.22 Erweiterung "Seriennummer der Chipkarte" 91
5.9 Inhaberattribute nach Common PKI SigG-Profil 92
5.9.1 Attribut "Vertretungsmacht" 92
5.9.2 Attribut "bestätigter Beruf" 94
5.9.3 Attribut "monetäre Beschränkung" 95
5.9.4 Attribut "altersabhängige Einschränkung" 95
5.9.5 Attribut "Einschränkung" 96
5.9.6 Attribut "Zusatzinformationen" 96

6 Bereich 4: Technische Informationen 97
6.1 Informationen zum Trustcenter 97
6.1.1 Zeile "Zuordnung der technischen Informationen zum Zertifikat" 97
6.1.2 Zeile "Staat in dem der ZDA ansässig ist" 97
6.1.3 Zeile "Art der Überwachung" des Trustcenters 98
6.1.4 Zeile "Zertifikatsniveau gemäß Zertifizierungsrichtlinie des TC" 99
6.2 Zertifikatsprüfung und Prüfinstanz 102
6.2.1 Zeile "Gültigkeitsmodell der Zertifikatsprüfung" 102
6.2.2 Zeile "Art der Statusprüfung" 103
6.2.3 Zeile "Prüfinstanz" 103
6.2.4 Zeile "Konfiguration der Prüfinstanz" 104
6.2.5 Zeile "Policy der Prüfinstanz" 104
6.2.6 Zeile "Vertrauenswürdige Liste der ZDA" 104
6.2.7 Zeile "XKMS-Verarbeitung" 104
6.2.8 Zeile "interner Fehler" 105

7 Bereich "Übertragungsinformation" 107
7.1 Zeile "Prüfinstanz und Prüfergebnis mit Erläuterung" 107
7.1.1 Spalten "Name der Prüfinstanz" mit Prüfergebnis und Erläuterung 107
7.1.2 Spalte "Name der Prüfinstanz" 109
7.1.3 Zeile "Fehler" 109

8 Verzeichnis der Abbildungen und Tabellen 110

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 orthografische 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 Governikus GmbH & Co. KG, im folgenden Governikus KG, vorbehalten. Alle urheberrechtsfähigen Materialien dürfen ohne vorherige Einwilligung der Governikus 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 eine eingetragene Marke der Governikus KG, Bremen. Andere in diesem Produkt aufgeführte Produkt- und/ oder Firmennamen sind möglicherweise Marken weiterer Eigentümer, deren Rechte ebenfalls zu wahren sind.

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

1 Einleitung

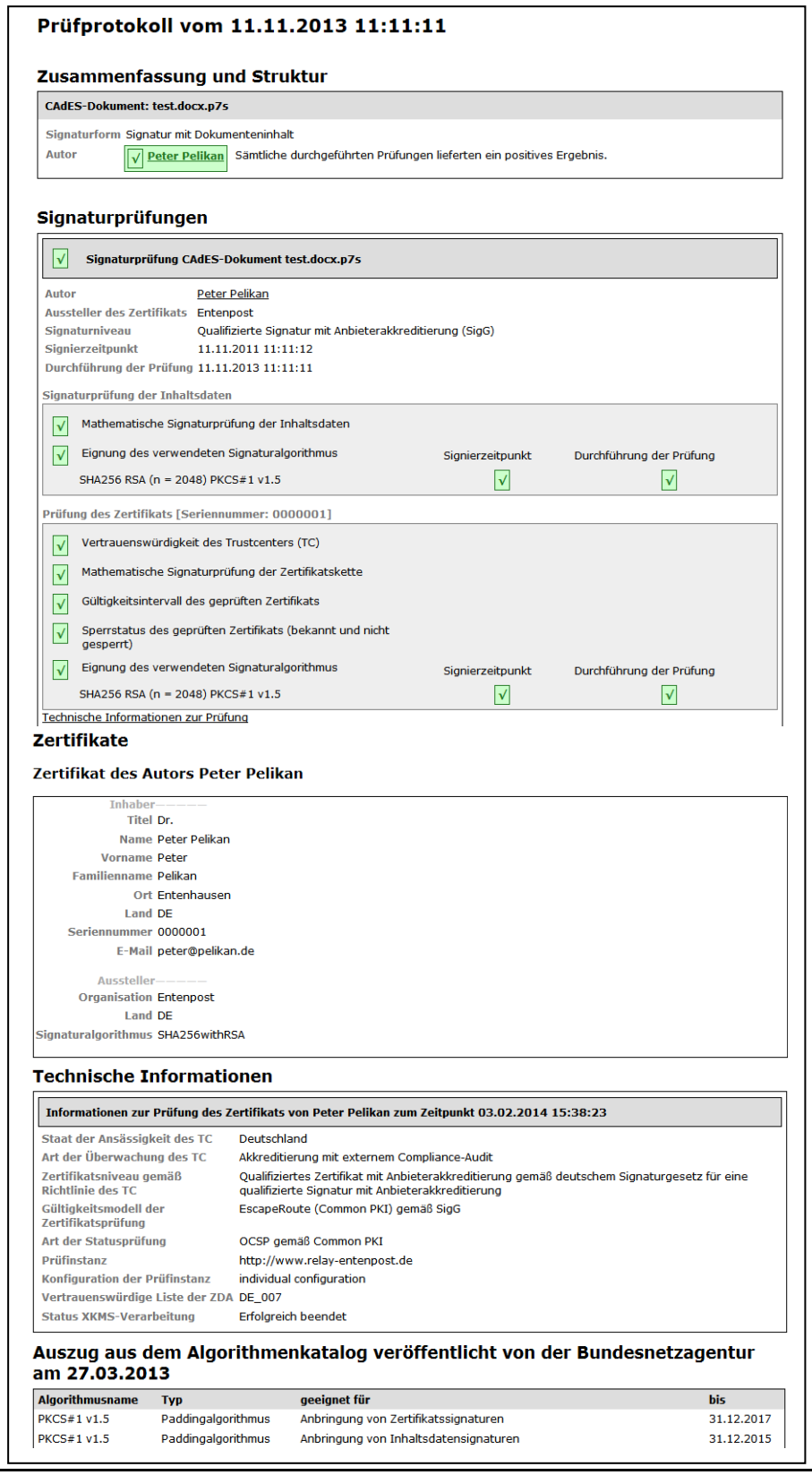
Dieses Anwenderhandbuch erläutert das Governikus Prüfprotokoll (zukünftig Prüfprotokoll), das die Ergebnisse der Prüfung einer elektronischen Signatur anzeigt. Das Prüfprotokoll gliedert sich in vier Hauptbereiche:

Bereich 1:
Zusammenfassung und Struktur
(siehe Kapitel 3)

Bereich 2:
Signaturprüfungen
(siehe Kapitel 4)

Bereich 3:
Zertifikate
(siehe Kapitel 5)

Bereich 4:
Technische Informationen
(siehe Kapitel 6)



Prüfprotokoll vom 11.11.2013 11:11:11

Zusammenfassung und Struktur

CAdES-Dokument: test.docx.p7s

Signaturform Signatur mit Dokumenteninhalt

Autor √ Peter Pelikan Sämtliche durchgeführten Prüfungen lieferten ein positives Ergebnis.

Signaturprüfungen

√ Signaturprüfung CAdES-Dokument test.docx.p7s

Autor	Peter Pelikan
Aussteller des Zertifikats	Entenpost
Signaturniveau	Qualifizierte Signatur mit Anbieterakkreditierung (SigG)
Signierzeitpunkt	11.11.2011 11:11:12
Durchführung der Prüfung	11.11.2013 11:11:11

Signaturprüfung der Inhaltsdaten

√ Mathematische Signaturprüfung der Inhaltsdaten

√ Eignung des verwendeten Signaturalgorithmus — Signierzeitpunkt — Durchführung der Prüfung

SHA256 RSA (n = 2048) PKCS#1 v1.5 — √ — √

Prüfung des Zertifikats [Seriennummer: 0000001]

√ Vertrauenswürdigkeit des Trustcenters (TC)

√ Mathematische Signaturprüfung der Zertifikatskette

√ Gültigkeitsintervall des geprüften Zertifikats

√ Sperrstatus des geprüften Zertifikats (bekannt und nicht gesperrt)

√ Eignung des verwendeten Signaturalgorithmus — Signierzeitpunkt — Durchführung der Prüfung

SHA256 RSA (n = 2048) PKCS#1 v1.5 — √ — √

Technische Informationen zur Prüfung

Zertifikate

Zertifikat des Autors Peter Pelikan

Inhaber

Titel	Dr.
Name	Peter Pelikan
Vorname	Peter
Familienname	Pelikan
Ort	Entenhausen
Land	DE
Seriennummer	0000001
E-Mail	peter@pelikan.de

Aussteller

Organisation	Entenpost
Land	DE
Signaturalgorithmus	SHA256withRSA

Technische Informationen

Informationen zur Prüfung des Zertifikats von Peter Pelikan zum Zeitpunkt 03.02.2014 15:38:23

Staat der Ansässigkeit des TC	Deutschland
Art der Überwachung des TC	Akkreditierung mit externem Compliance-Audit
Zertifikatsniveau gemäß Richtlinie des TC	Qualifiziertes Zertifikat mit Anbieterakkreditierung gemäß deutschem Signaturgesetz für eine qualifizierte Signatur mit Anbieterakkreditierung
Gültigkeitsmodell der Zertifikatsprüfung	EscapeRoute (Common PKI) gemäß SigG
Art der Statusprüfung	OCSP gemäß Common PKI
Prüfinstanz	http://www.relay-entenpost.de
Konfiguration der Prüfinstanz	individual configuration
Vertrauenswürdige Liste der ZDA	DE_007
Status XKMS-Verarbeitung	Erfolgreich beendet

Auszug aus dem Algorithmenkatalog veröffentlicht von der Bundesnetzagentur am 27.03.2013

Algorithmusname	Typ	geeignet für	bis
PKCS#1 v1.5	Paddingalgorithmus	Anbringung von Zertifikatssignaturen	31.12.2017
PKCS#1 v1.5	Paddingalgorithmus	Anbringung von Inhaltsdatensignaturen	31.12.2015

Abbildung 1: Aufbau Prüfprotokoll

Im ersten Bereich "Zusammenfassung und Struktur" des Prüfprotokolls wird das Prüfergebnis in Ampelform zusammengefasst. Wurden mehrere Signaturen geprüft, werden sie grafisch in ihrer Zuordnung zum signierten Inhalt angezeigt. Der Bereich "Zusammenfassung und Struktur" des Prüfprotokolls wird ausführlich im Kapitel 3 beschrieben.

Im zweiten Bereich "Signaturprüfungen" werden Kontextinformationen zur geprüften Signatur und die einzelnen Prüfergebnisse angezeigt. Der Bereich gliedert sich für jede geprüfte Signatur in drei Teile:

- Im ersten Teil werden Kontextinformationen zur Signatur und zum Signierenden, wie der Name des Signierenden, der Aussteller des Signaturzertifikats, das Signaturniveau und der Signierzeitpunkt, angezeigt.
- Im zweiten Teil folgt das Ergebnis der mathematischen Signaturprüfung.
- Im dritten Teil wird das Ergebnis der Zertifikatsprüfung angezeigt. Dazu gehört die Vertrauenswürdigkeit des Trustcenters, die mathematische Prüfung der Zertifikatssignaturen, der Sperrstatus des geprüften Zertifikats und dessen Gültigkeitszeitraum.

Die Darstellung wird ggf. für jede Signaturprüfung wiederholt. Der Bereich "Signaturprüfungen" wird ausführlich im Kapitel 4 beschrieben.

Im dritten Bereich "Zertifikate" des Prüfprotokolls wird der Inhalt des geprüften Signaturzertifikats angezeigt. Die Darstellung wird ggf. für jedes Zertifikat wiederholt. Der Bereich "Zertifikate" des Prüfprotokolls wird ausführlich in Kapitel 5 dieser Anwenderdokumentation beschrieben.

Im vierten Bereich folgen abschließend technische Informationen zur durchgeführten Prüfung. Diese helfen dabei, die Qualität der Signatur und des Zertifikats genauer beurteilen zu können. Der Bereich "technische Informationen" des Prüfprotokolls wird ausführlich in Kapitel 6 dieser Anwenderdokumentation beschrieben.

In dem Fall, dass eine sichere Kommunikation zwischen dem Client und dem Server, der die Zertifikatsprüfung durchführt, nicht sichergestellt werden konnte, wird am Anfang des Prüfprotokolls eine Fehlermeldung ausgegeben. Erläuterungen hierzu finden sich im Kapitel 7.

Aufbau und Inhalt des Prüfprotokolls ergeben sich wesentlich aus den rechtlichen Anforderungen an die Prüfung qualifizierter Signaturen und die Anzeige der Prüfergebnisse. In Kapitel 2.1 werden diese rechtlichen Anforderungen, soweit sie sich aus dem deutschen Signaturgesetz und der deutschen Signaturverordnung ergeben, beschrieben. Ein Überblick über die verschiedenen Signaturniveaus gemäß der EU-Signaturrichtlinie und dem deutschen Signaturgesetz folgt in Kapitel 2.2. Das Kapitel 2.3 informiert schließlich kurz über den Ablauf einer Signaturprüfung.

2 Rechtlicher und technischer Hintergrund

Der Aufbau des Prüfprotokolls ergibt sich aus den rechtlichen Anforderungen an die Prüfung qualifizierter Signaturen und die Anzeige der Prüfergebnisse und notwendiger Kontextinformationen. Im diesem Kapitel werden deshalb die rechtlichen Anforderungen an die Signaturprüfung und die Anzeige der Prüfergebnisse, soweit sie sich aus dem deutschen Signaturgesetz (SigG) ergeben, skizziert. In diesem Zusammenhang werden auch die gesetzlich definierten Signaturniveaus vorgestellt, die in der Praxis relevant sind.

2.1 Signaturprüfung

Grundlage für die Signaturprüfung und die Anzeige der Prüfergebnisse bei qualifizierten elektronischen Signaturen ist die Richtlinie 1999/93/EG des europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (EU-Signaturrichtlinie). Im Anhang IV dieser Richtlinie wird beschrieben, dass für eine sichere Signaturprüfung folgende Anforderungen zu gewährleisten sind:

- Die Signatur muss zuverlässig überprüft und das Ergebnis dieser Überprüfung korrekt angezeigt werden.
- Die Echtheit und die Gültigkeit des zum Zeitpunkt der Überprüfung der Signatur verlangten Zertifikats müssen zuverlässig überprüft werden.
- Das Ergebnis der Überprüfung sowie die Identität des Unterzeichners müssen korrekt angezeigt werden.

Die EU-Signaturrichtlinie verpflichtet die Mitgliedstaaten, die erforderlichen Rechts- und Verwaltungsvorschriften zu erlassen, um dieser Richtlinie nachzukommen. Dieser Verpflichtung ist der deutsche Gesetzgeber durch das Signaturgesetz (SigG) und die Verordnung zur elektronischen Signatur (SigV) nachgekommen.

Im SigG (§ 17) werden ergänzend zur EU-Signaturrichtlinie weitere Anforderungen an eine Signaturanwendungskomponente (SAK) für die Überprüfung von qualifizierten Signaturen gestellt. Die SAK muss auch feststellen,

- auf welche Daten sich die Signatur bezieht und ob die signierten Daten unverändert sind,
- welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist und
- welche Inhalte das qualifizierte Zertifikat aufweist und zu welchem Ergebnis die Nachprüfung von Zertifikaten geführt hat.

Zusätzlich wird in der SigV (§ 15) auch eine hohe Qualität der Prüfung und Anzeige gefordert: Die Korrektheit der Signatur muss zuverlässig geprüft und zutreffend angezeigt werden. Es muss eindeutig erkennbar sein, ob die geprüften qualifizierten Zertifikate im jeweiligen Zertifikatsverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.

2.2 Signaturniveaus in der EU und Deutschland

In der EU-Signaturrichtlinie werden mehrere Signaturniveaus definiert oder können daraus abgeleitet werden. Diese werden im Folgenden beschrieben.

2.2.1 Fortgeschrittene elektronische Signatur (EU und Deutschland)

Eine fortgeschrittene elektronische Signatur bezeichnet eine elektronische Signatur, die gemäß Artikel 2, Absatz 2 der EU-Signaturrichtlinie die folgenden Anforderungen erfüllt:

- Die fortgeschrittene elektronische Signatur ist ausschließlich dem Unterzeichner zugeordnet und ermöglicht die Identifizierung des Unterzeichners.
- Die fortgeschrittene elektronische Signatur wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann.
- Die fortgeschrittene elektronische Signatur ist so mit den Daten, auf die sie sich bezieht, verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Die Definition entspricht weitestgehend auch der Formulierung im deutschen Signaturgesetz.

2.2.2 Fortgeschrittene elektronische Signatur mit qualifiziertem Zertifikat (EU)

Wird eine fortgeschrittene elektronische Signatur von einem qualifizierten Zertifikat unterstützt, bezeichnet die EU-Signaturrichtlinie diese Signatur als fortgeschrittene elektronische Signatur mit qualifiziertem Zertifikat (siehe Artikel 2, Absatz 10). An das Zertifikat werden folgende besondere Anforderungen gestellt (siehe Anhang I und II):

- Es muss von einem Zertifizierungsdiensteanbieter bereitgestellt werden, der besondere Anforderungen bezüglich seiner Qualifikation und Überwachung zu erfüllen hat (siehe Anhang II).
- Das qualifizierte Zertifikat muss außerdem folgende Angaben enthalten:
  - Angabe, dass das Zertifikat als qualifiziertes Zertifikat ausgestellt wird;
  - Angabe des Zertifizierungsdiensteanbieters und des Staates, in dem er niedergelassen ist;
  - Name des Unterzeichners oder ein Pseudonym, das als solches zu identifizieren ist;
  - Platz für ein spezifisches Attribut des Unterzeichners, das gegebenenfalls je nach Bestimmungszweck des Zertifikats aufgenommen wird;
  - Signaturprüfdaten, die den vom Unterzeichner kontrollierten Signaturerstellungsdaten entsprechen;
  - Angaben zu Beginn und Ende der Gültigkeitsdauer des Zertifikats;
  - Identitätscode des Zertifikats;
  - die fortgeschrittene elektronische Signatur des ausstellenden Zertifizierungsdiensteanbieters;
  - gegebenenfalls Beschränkungen des Geltungsbereichs des Zertifikats und
  - gegebenenfalls Begrenzungen des Wertes der Transaktionen, für die das Zertifikat verwendet werden kann.

Das deutsche Signaturgesetz kennt eine fortgeschrittene elektronische Signatur, unterstützt von einem qualifizierten Zertifikat, nicht.

2.2.3 Qualifizierte elektronische Signatur (EU)

Die qualifizierte elektronische Signatur ist in der EU-Signaturrichtlinie zwar explizit als Begriff nicht definiert, kann aber über Artikel 5 "Rechtswirkung elektronischer Signaturen" abgeleitet werden. Dort steht: "(1) Die Mitgliedstaaten tragen dafür Sorge, dass fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen und die von einer siche-

ren Signaturerstellungseinheit erstellt werden, a) die rechtlichen Anforderungen an eine Unterschrift in Bezug auf in elektronischer Form vorliegende Daten in gleicher Weise erfüllen wie handschriftliche Unterschriften in Bezug auf Daten, die auf Papier vorliegen, und b) in Gerichtsverfahren als Beweismittel zugelassen sind".

Die Anforderungen an eine sichere Signaturerstellungseinheit (Signaturkarte) werden in der EU-Signaturrichtlinie in Anhang III definiert. Das Signaturniveau "qualifizierte elektronische Signatur" ist in der EU-Signaturrichtlinie nicht explizit als Begriff definiert worden.

2.2.4 Qualifizierte elektronische Signatur mit Anbieterakkreditierung (EU)

Die freiwillige Akkreditierung bezeichnet nach Artikel 2 der EU-Signaturrichtlinie eine Erlaubnis, mit der die Rechte und Pflichten für die Erbringung von Zertifizierungsdiensten festgelegt werden und die auf Antrag des betreffenden Zertifizierungsdiensteanbieters von der öffentlichen oder privaten Stelle, die für die Festlegung dieser Rechte und Pflichten sowie für die Überwachung ihrer Einhaltung zuständig ist, erteilt wird, wenn der Zertifizierungsdiensteanbieter die sich aus der Erlaubnis ergebenden Rechte nicht ausüben darf, bevor er den Bescheid der Stelle erhalten hat.

In Grund 11 der Präambel der EU-Signaturrichtlinie wird ausgeführt, dass durch eine freiwillige Akkreditierung das Niveau der erbrachten Dienste gesteigert werden soll, um das auf dem sich entwickelnden Markt geforderte Maß an Vertrauen, Sicherheit und Qualität zu erreichen. Das Signaturniveau "qualifizierte elektronische Signatur mit Anbieterakkreditierung" ist in der EU-Signaturrichtlinie nicht explizit als Begriff definiert worden.

2.2.5 Qualifizierte elektronische Signatur (D)

Konform zur EU-Signaturrichtlinie sind gemäß den Begriffsbestimmungen des § 2 SigG qualifizierte elektronische Signaturen elektronische Signaturen, die

- ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
- die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
- mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann,
- mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann,
- auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen,
- mit einer sicheren Signaturerstellungseinheit erzeugt werden.

Qualifizierte Zertifikate sind dabei elektronische Bescheinigungen für natürliche Personen, die von Zertifizierungsdiensteanbietern ausgestellt werden, die mindestens die Anforderungen nach den §§ 4 bis 14 oder § 23 des SigG und der sich darauf beziehenden Vorschriften der Rechtsverordnung nach § 24 erfüllen. In diesen Paragrafen werden die qualitativen Anforderungen an die ZDA definiert und das Anzeigeverfahren bei der Bundesnetzagentur beschrieben. Das Signaturniveau "qualifizierte elektronische Signatur" ist im deutschen Signaturgesetz explizit als Begriff definiert worden.

Die Anforderungen an eine sichere Signaturerstellungseinheit erfüllen nach dem Stand der Technik in Deutschland zurzeit nur entsprechend SigG-bestätigte Signaturkarten.

2.2.6 Qualifizierte elektronische Signatur mit Anbieterakkreditierung (D)

Konform zur EU-Signaturrichtlinie gibt es auch in Deutschland die Möglichkeit der freiwilligen Akkreditierung von ZDA. Die "freiwillige Akkreditierung" ist ein Verfahren zur Erteilung einer Erlaubnis für den Betrieb eines Zertifizierungsdienstes, mit der besondere Rechte und Pflichten verbunden sind. Die Akkreditierung wird erteilt, wenn der ZDA nachweist, dass die Vorschriften nach dem SigG und der SigV erfüllt sind. Akkreditierte ZDA erhalten dann ein Gütezeichen der Bundesnetzagentur als Nachweis der umfassend geprüften technischen und administrativen Sicherheit. Das Signaturniveau "qualifizierte elektronische Signatur mit Anbieterakkreditierung" ist im deutschen Signaturgesetz nicht explizit als Begriff definiert worden.

2.3 Ablauf der Signaturprüfung

Für die Prüfung elektronischer Signaturen und die Anzeige des Prüfergebnisses in Clientanwendungen der Governikus KG sind in der Regel zwei Komponenten verantwortlich. Die mathematische Signaturprüfung und die Anzeige des Prüfergebnisses erfolgt durch das in den Clients integrierte Kryptomodul "Verification Interpreter". Die Zertifikatsprüfung wird durch dieses Modul beim "OCSP/CRL-Relay" angefordert. Diese zentrale Serverkomponente ist Bestandteil der Governikus Service Components.

2.3.1 Unterstützte Signaturformate und Signaturalgorithmen

Signierte Dokumente liegen in unterschiedlichen Signaturformaten vor. Das Modul "Verification Interpreter" unterstützt folgende Signaturformate:

- **Asynchrone OSCI-Nachrichten** mit Laufzettel gemäß OSCI 1.2-Spezifikation und ausgewählte **synchrone Nachrichtentypen** (Abwicklungsantwort, Abwicklungsauftrag, Bearbeitungsauftrag, Weiterleitungsantwort, Annahmeauftrag),
- **PKCS#7-Signaturen** der Version 1.5 (RFC 2315) sowie **CMS-Signaturen** (Cryptographic Message Syntax) gemäß RFC 2630, 3211, 3369, 3852, 5126 (alle basierend auf PKCS #7),
- **PDF-Dokumente mit eingebetteten PDF-Signaturen**. Unterstützt werden PDF-Dokumente (ab PDF 1.3) mit PDF-Signaturen gemäß folgender Spezifikationen oder Profilierungen:
  - PAdES BES (PAdES Part 2) und PAdES EPES (PAdES Part 3). PAdES (PDF Advanced Electronic Signatures) ist ein Standard gemäß ETSI TS 102 778 in der Profilierung gemäß Beschluss der EU-Kommission vom 25. Februar 2011 über Mindestanforderungen für die grenzüberschreitende Verarbeitung von Dokumenten im Kontext der europäischen Dienstleistungsrichtlinie (RL 2006/123/EG) basierend auf PDF-Signaturen wie in ISO 32 000 spezifiziert. PAdES BES ist die Grundform.
  - Bestimmte Alt-Signaturen (Legacy-Formate) nach ISO 32000. Dadurch wird sichergestellt, dass auch bestehende PDF-Signaturen weiterhin geprüft werden können.

Der Verification Interpreter unterstützt technisch folgende Signaturalgorithmen:

- MD2, MD5, RIPEMD-160, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512withRSA. Es wird eine RSA-Schlüssellänge bis 2048 Bit unterstützt in Verbindung mit den Signaturschemata PKCS#1 Version 1.5 und Version 2.1 (PSS).
- SHA-1, SHA-224, SHA-256withDSA
- SHA-1, SHA-224, SHA-256, SHA-384, SHA-512withECDSA. Es werden ECDSA-

Signaturen gemäß ANSI 9.62 und ISO Standard 14888-3 (international) und BSI TR 03111 (CVC national) unterstützt. Bei XML-Signaturen gemäß OSCI 1.2 und 2.0 Spezifikation wird spezifikationsbedingt nur der CVC-Modus unterstützt.

Bei einer qualifizierten elektronischen Signatur (erzeugt mit einer Signaturkarte eines deutschen ZDA) wird durch den Verification Interpreter auch die Eignung des verwendeten Signaturalgorithmus zum Signaturzeitpunkt und zum Zeitpunkt der Durchführung der Prüfung ermittelt.

2.3.2 Zertifikatsprüfung durch das OCSP/CRL-Relay

Die Zertifikatsprüfung erfolgt durch das "OCSP/CRL-Relay". Dieser Server ist Bestandteil der Governikus Service Components. Das Modul Verification Interpreter stellt eine Prüfanfrage (XKMS-Request) an das OCSP/CRL-Relay, das folgende Prüfungen durchführt:

- Bildung des Vertrauenspfades bis zum Rootzertifikat (Issuer Trust)
- mathematische Prüfung der Signaturen der Zertifikate (Signature)
- Prüfung, ob der Signaturzeitpunkt innerhalb des Gültigkeitsintervalls des Zertifikats liegt (Validity Interval)
- Ermittlung des Sperrstatus des geprüften Zertifikats (Revocation Status)

Die Prüfantwort (XKMS-Response) wird vom OCSP/CRL-Relay an den Verification Interpreter zurückgesendet. Die Interpretation dieser Prüfergebnisse obliegt dabei dem Verification Interpreter.

2.3.3 Anzeige der Prüfergebnisse

Das gesamte Prüfergebnis (mathematische Signaturprüfung und Zertifikatsprüfung) kann durch den Verification Interpreter als HTML-Ansicht, als PDF oder als XML bereitgestellt werden. Anwendungen können die Anzeigeformate einschränken.

2.3.4 Einhaltung der gesetzlichen Anforderungen

Qualifizierte elektronische Signaturen, erzeugt mit einer Signaturkarte eines deutschen ZDA (basierend auf einer SigG-bestätigten sicheren Signaturerstellungseinheit), werden durch den Verification Interpreter konform zu den Anforderungen des deutschen Signaturgesetzes geprüft. Dieses gilt auch für die Prüfung qualifizierter elektronischer Zertifikate durch das OCSP/CRL-Relay und die Anzeige der Prüfergebnisse durch den Verification Interpreter.

3 Bereich 1: Zusammenfassung und Struktur

Im ersten Bereich des Prüfprotokolls "Zusammenfassung und Struktur" wird die Struktur der signierten Nachricht bezogen auf die Signatur und das Signaturprüfergebnis angezeigt. Jeder Signatur werden der Name des Signierenden (Autor) und das Prüfergebnis in Ampelform zugeordnet. Wurden mehrere Signaturen geprüft, werden diese grafisch in ihrer Zuordnung zum signierten Inhalt angezeigt.

Grundsätzlich hat die Anzeige im Bereich "Zusammenfassung und Struktur" immer folgenden Aufbau:

- In der ersten Zeile wird grau unterlegt immer das Dokumentenformat angezeigt. In der nächsten Zeile folgen ggf. formatspezifische Kontextinformationen.
- In der Zeile "Autor" wird immer der Name des Autors (Name des Signierenden) und das Prüfergebnis der dem Autor zugeordneten Einzelsignatur in Ampelform (grün, gelb, rot) sowie eine Erläuterung zum Prüfergebnis angezeigt. Es folgen ggf. weitere formatspezifische Kontextinformationen.

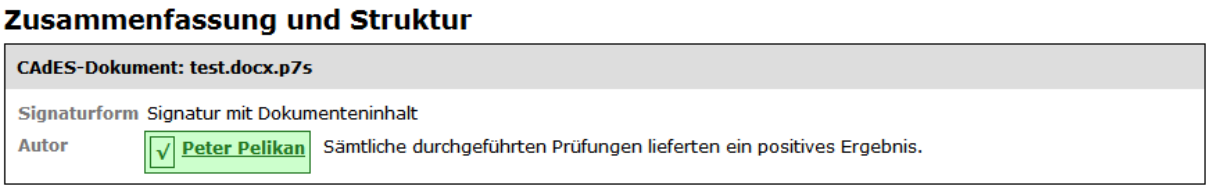


Abbildung 2: Grundaufbau Bereich 1 "Zusammenfassung und Struktur"

Der Grundaufbau ist für alle unterstützten Signaturformate identisch, allerdings unterscheiden sich die unterstützten Signaturformate hinsichtlich ihrer Komplexität und der angezeigten formatspezifischen Kontextinformationen. Die unterstützten Signaturformate werden daher in den folgenden Unterkapiteln getrennt dargestellt.

3.1 OSCI-Nachrichten (OSCI 1.2)

OSCI-Nachrichten können eine komplexe Nachrichtenstruktur besitzen, wie z.B. mehrere signierte, ineinander geschachtelte Datencontainer mit signierten Anhängen. Die Strukturanzeige im Prüfprotokoll entspricht dabei der OSCI-Nachrichtenstruktur. Im Bereich 1 "Zusammenfassung und Struktur" ist das Prüfprotokoll für OSCI-Nachrichten wie folgt aufgebaut:

3.1.1 Zeile Name der OSCI-Nachricht

In der ersten Zeile wird grau unterlegt hinter der Bezeichnung des Signaturformats

- OSCI-Nachricht

und dahinter der Name der OSCI-Nachricht angezeigt.

Abbildung 3: Zusammenfassung und Struktur bei einer signierten OSCI-Nachricht (1.2)

3.1.2 Kontextinformationen zur OSCI-Nachricht

Eine gesendete und empfangene OSCI-Nachricht enthält immer Kontextinformationen, wie ein Betreff und ein Nachrichtenkennzeichen. Außerdem enthält sie Informationen zum Absender und zum Empfänger sowie das Eingangsdatum auf dem Server. In den folgenden Unterkapiteln werden diese Kontextinformationen und die Anzeige der Nachrichtstruktur einer OSCI-Nachricht erläutert.

3.1.2.1 Zeile "Betreff"

In der Zeile "Betreff" wird der ausgewählte Nachrichtentyp der OSCI-Nachricht angezeigt.

3.1.2.2 Zeile "Nachrichtenkennzeichen"

In der Zeile "Nachrichtenkennzeichen" wird das Nachrichtenkennzeichen der OSCI-Nachricht angezeigt. Das Nachrichtenkennzeichen selbst 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.

3.1.2.3 Zeile "Absender"

In der Zeile "Absender" wird der Name des Absenders der OSCI-Nachricht angezeigt. Dieses ist der Name des Zertifikatsinhabers [Feld `subject`, Attribut `commonName`], in der Regel Nachname und Vorname des Zertifikatsinhabers oder auch ein Pseudonym. Ist kein Inspection Report und damit ggf. kein Absender vorhanden, wird die Meldung "k. A." für "keine Angabe" ausgegeben.

3.1.2.4 Zeile "Empfänger"

In der Zeile "Empfänger" wird der Name des Empfängers der OSCI-Nachricht angezeigt. Dieses ist der Name des Zertifikatsinhabers [Feld `subject`, Attribut `commonName`]. Ist kein Inspection Report und damit ggf. kein Empfänger vorhanden, wird die Meldung "k. A." für "keine Angabe" ausgegeben.

3.1.2.5 Zeile "Eingang auf dem Server"

In der Zeile "Eingang auf dem Server" wird der Zeitpunkt angegeben, 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. Die Zeit wird angezeigt in der Form `TT.MM.JJJJ hh:mm:ss` mit der Erläuterung in Klammern "lokale Serverzeit".

Ist kein Laufzettel und damit ggf. kein Eingangszeitpunkt vorhanden, wird die Meldung "k. A." für "keine Angabe" ausgegeben. Bei einer OSCI-Nachricht wird der "Eingang auf dem Server" hilfsweise als Signierzeitpunkt verwendet. Der fehlende Eingangszeitpunkt führt in diesem Fall zum Status "rot" im kumulierten Prüfergebnis der Signaturprüfung.

3.1.3 Zeile "Name des Inhaltsdaten-Containers"

In der ersten Zeile wird grau unterlegt hinter der Bezeichnung "Inhaltsdatencontainer" der Name des Containers angezeigt. Ist der Datencontainer verschlüsselt, können keine Aussagen über den Inhalt gemacht werden. In diesem Fall ist die Zeile vollständig hell ausgegraut und es wird der Hinweis angezeigt "Inhaltsdaten chiffriert".

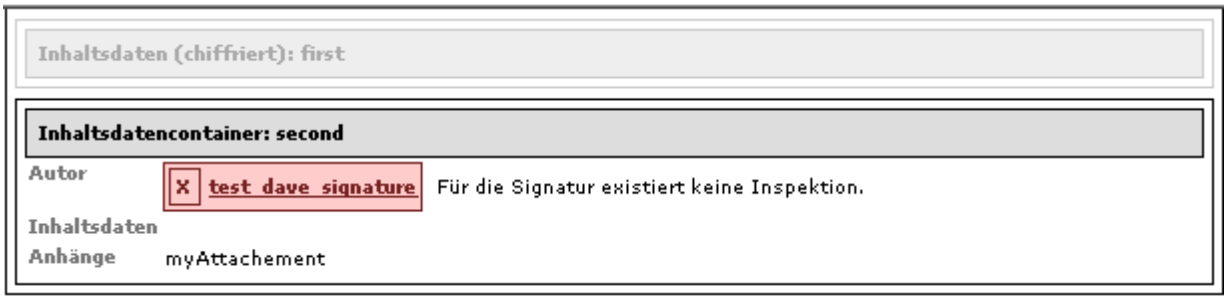


Abbildung 4: nicht gesendete OSCI-Nachricht mit verschlüsseltem Inhaltsdatencontainer

3.1.4 Zeile "Autor, Prüfergebnis und Erläuterung"

In der Zeile "Autor mit kumuliertem Prüfergebnis und Erläuterung" wird von links nach rechts zunächst das kumulierte Prüfergebnis mit dem Namen des Autors in einem farbig unterlegten Kasten und anschließend eine Erläuterung zum Prüfergebnis angezeigt.

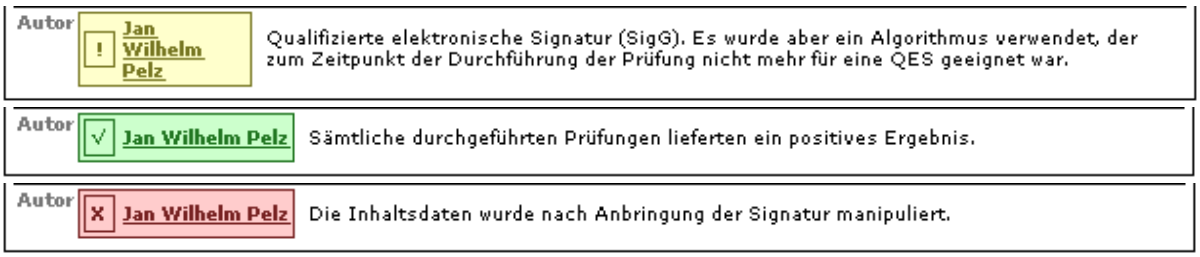


Abbildung 5: kumulierte Prüfergebnisse im Bereich 1 "Zusammenfassung und Struktur"

3.1.4.1 Spalte "Autor" mit kumuliertem Prüfergebnis

In der Spalte "Autor" werden rechts neben der Feldbezeichnung "Autor" das kumulierte Prüfergebnis bezogen auf eine Signatur und der Name des Autors (der signierenden Person) in einem farbig unterlegten Kasten angezeigt. Folgende Status sind möglich:

- √ Grüner Kasten mit Haken
- ! Gelber Kasten mit Ausrufungszeichen
- X Roter Kasten mit Kreuz

Erläuterungen zu √ Grüner Kasten mit Haken:

Alle durchgeführten Einzelprüfungen besitzen den Status „grün“. Die elektronische Signatur und das zugeordnete Signaturzertifikat wurden mit positivem Ergebnis überprüft. Bei einer qualifizierten Signatur (erstellt mit einer Signaturkarte eines deutschen ZDAs) gehört dazu auch die Prüfung der Eignung der verwendeten Signaturalgorithmen (Inhaltsdatensignatur, Zertifikatssignatur) gemäß aktuellem Algorithmenkatalog der Bundesnetzagentur zum Signierzeitpunkt und zum Zeitpunkt der Durchführung der Prüfung. Damit ist die Unverfälschtheit (Integrität der signierten Inhaltsdaten, der Nachricht, des Dokuments) sichergestellt, der Signierende sicher identifiziert und seine Authentizität bestätigt.

Dieses kumulierte Prüfergebnis ist immer nur eine Momentaufnahme zum Zeitpunkt der Durchführung der Prüfung. Bei einer „Nachprüfung“ (z.B. nach einigen Jahren) kann der Status auch auf "gelb" wechseln, weil das Trustcenter keine Sperrinformationen zum Signatur-

zertifikat mehr bereitstellt oder weil der bei einer qualifizierten Signatur verwendete Signaturalgorithmus nicht mehr für die Prüfung einer qualifizierten Signatur geeignet ist.

Erläuterungen zu Gelber Kasten mit Ausrufungszeichen:

Mindestens eine der Einzelprüfungen besitzt den Status "gelb" und damit kein eindeutiges Ergebnis. Einzelprüfungen mit dem finalen Status „rot“ gibt es nicht.

Der Status der Signaturprüfung ist aus Empfängersicht unbestimmt. Die Ursache sollte in jedem Fall genauer analysiert werden. Häufig kommt dieses Prüfergebnis nämlich dadurch zustande, dass der Sperrstatus des Zertifikats nicht ermittelt werden konnte, weil z.B. der OCSP-Responder des Trustcenters temporär nicht erreichbar war. Im Teil "Prüfung des Zertifikats" hat die Einzelprüfung „Sperrstatus des Zertifikats“ in diesem Fall den Status "gelb". Eine "Nachprüfung" des Signaturzertifikats ist dann sinnvoll.

Der Status "gelb" kann aber auch endgültig sein, weil z. B. der Signierzeitpunkt nicht ermittelt werden konnte (In diesem Fall kann dann auch der Sperrstatus des Zertifikats nicht ermittelt werden) oder weil der bei einer qualifizierten Signatur verwendete Signaturalgorithmus nicht mehr für die Prüfung einer qualifizierten Signatur (Inhaltsdatensignatur, Zertifikatssignatur) geeignet ist. Bereits erzeugte qualifizierte elektronische Signaturen bleiben zwar auch dann noch qualifiziert, wenn der zugrundeliegende Signaturalgorithmus nach der Signaturerzeugung seine Eignung verloren hat, sie büßen jedoch graduell und sukzessive ihren Beweiswert ein. In der Spalte Erläuterungen wird in diesem Fall immer der folgende Warnhinweis ausgegeben:

- Qualifizierte elektronische Signatur (SigG). Es wurde aber ein Algorithmus verwendet, der zum Zeitpunkt der Durchführung der Prüfung nicht mehr für eine qualifizierte Signatur geeignet war.

Der Status "gelb" wird bei einer qualifizierten Signatur auch dann angezeigt, wenn die Eignung des verwendeten Signaturalgorithmus nicht ermittelt werden konnte. In der Spalte Erläuterungen wird in diesem Fall immer der folgende Warnhinweis ausgegeben:

- Die Eignung eines Algorithmus konnte nicht ermittelt werden.

Erläuterungen zu Roter Kasten mit Kreuz:

Mindestens eine der Einzelprüfungen besitzt den Status „rot“, d.h. war abschließend nicht erfolgreich. Damit ist entweder die Unverfälschtheit der Inhaltsdaten (Integrität der Daten) nicht sichergestellt oder es konnte die signierende Person abschließend nicht sicher identifiziert werden.

Der Status „rot“ wird bei einer qualifizierten Signatur auch dann angezeigt, wenn der verwendete Signaturalgorithmus bereits zum Signierzeitpunkt nicht mehr für eine qualifizierte Signatur geeignet war. Signaturen, die nach dem Schwachwerden des zugrundeliegenden Signaturalgorithmus erzeugt wurden, sind von vornherein keine qualifizierten Signaturen. Schon bei der Erzeugung der Signatur konnte nämlich nicht mehr sichergestellt werden, dass der Signaturschlüssel-Inhaber die alleinige Kontrolle über die Mittel zur Erzeugung der Signatur hatte. In der Spalte Erläuterungen in diesem Fall wird immer die folgende Meldung ausgegeben:

- Fortgeschrittene Signatur und keine qualifizierte Signatur (SigG). Es wurde ein Algorithmus verwendet, der zum Signierzeitpunkt nicht mehr für eine qualifizierte Signatur geeignet war.

Das kumulierte Prüfergebnis mit dem Status "rot" ist in der Regel final. Nur bei temporär gesperrten Zertifikaten (im europäischen Ausland möglich) ist ein Statuswechsel möglich.

3.1.4.2 Name des Autors

In der Spalte "Autor" werden rechts neben der Feldbezeichnung "Autor" das kumulierte Prüfergebnis und der Name des Autors (der signierenden Person) in einem farbig unterlegten Kasten angezeigt. Der Name des Autors ist das Attribut "Name des Zertifikatseigentümers" aus dem Feld "Inhaber" [`subject`] des Signaturzertifikats. Das Attribut "Name" [`CommonName`] besteht in der Regel aus dem Vor- und Nachnamen des Zertifikatsinhabers, kann aber auch ein Pseudonym enthalten.

3.1.4.3 Spalte "Erläuterungen"

In der letzten Spalte rechts wird das Prüfergebnis erläutert.

Erläuterungen bei Prüfergebnis Grüner Kasten mit Haken

Es ist nur eine Meldung möglich:

- Sämtliche durchgeführten Prüfungen lieferten ein positives Ergebnis.

Erläuterungen bei Prüfergebnis Gelber Kasten mit Ausrufungszeichen:

Folgende Meldungen aus dem Bereich der Einzelprüfergebnisse sind möglich, die zu einem Gelbstatus des kumulierten Prüfergebnisses führen:

- Es liegt kein Signierzeitpunkt vor.
- Die Integrität der Signatur konnte nicht geprüft werden, da das Signaturzertifikat nicht vorhanden ist.
- Die Integrität der Signatur konnte nicht geprüft werden, da keine Inhaltsdaten vorliegen.
- Die Integrität der Signatur konnte nicht geprüft werden, da der Algorithmus nicht implementiert ist.
- Der Sperrstatus des Zertifikats konnte nicht ermitteln werden.
- Die Vertrauenswürdigkeit des Trustcenters konnte nicht ermittelt werden.
- Die Gültigkeit des Zertifikats konnte nicht überprüft werden.
- Die Signaturen der Zertifikatskette konnten nicht überprüft werden.
- Qualifizierte elektronische Signatur (SigG). Es wurde aber ein Algorithmus verwendet, der zum Zeitpunkt der Durchführung der Prüfung nicht mehr für eine qualifizierte Signatur geeignet war (nur bei einer qualifizierten Signatur, die mit einer Signaturkarte eines deutschen ZDAs erstellt wurde).
- Die Eignung eines Algorithmus konnte nicht ermittelt werden (nur bei einer qualifizierten Signatur, die mit einer Signaturkarte eines deutschen ZDAs erstellt wurde).

Erläuterungen bei Prüfergebnis Roter Kasten mit Kreuz:

Folgende Meldungen aus dem Bereich der Einzelprüfergebnisse sind möglich, die zu einem Rotstatus des kumulierten Prüfergebnisses führen:

- Die Inhaltsdaten wurden nach Anbringung der Signatur manipuliert.
- Die Signatur der OSCI-Nachricht ist inkorrekt.
- Das Attributzertifikat gehört nicht zum Signaturzertifikat.

- Das Zertifikat war zum Signierzeitpunkt gesperrt oder abgelaufen.
- Das Zertifikat ist gesperrt.
- Das Trustcenter ist nicht vertrauenswürdig.
- Das Zertifikat ist nicht gültig.
- Die Zertifikatskette ist nicht gültig.
- Fortgeschrittene Signatur und keine qualifizierte Signatur (SigG). Es wurde ein Algorithmus verwendet, der zum Signierzeitpunkt nicht mehr für eine qualifizierte Signatur geeignet war. (nur bei einer qualifizierten Signatur, die mit einer Signaturkarte eines deutschen ZDAs erstellt wurde)

3.1.5 Zeile "Inhaltsdaten"

Angezeigt werden hinter dem Eintrag "Inhaltsdaten" die Dateinamen der Inhaltsdaten.

3.1.6 Zeile "Anhänge"

Angezeigt werden hinter dem Eintrag "Anhänge" die Dateinamen der Anhänge.

3.2 PKCS#7-Signaturen

Unterstützt werden PKCS#7-Signaturen der Version 1.5 (RFC 2315) sowie CMS-Signaturen (Cryptographic Message Syntax) gemäß RFC 2630, 3211, 3369, 3852, 5126, alle basierend auf PKCS #7.

Im Bereich 1 "Zusammenfassung und Struktur" ist das Prüfprotokoll für PKCS#7-Signaturen wie folgt aufgebaut:

3.2.1 Zeile "Dateiname"

In der ersten Zeile wird grau unterlegt hinter der Bezeichnung des Signaturformats

- PKCS#7-Dokument

und dahinter der Name der Datei angezeigt, die die Signatur enthält.

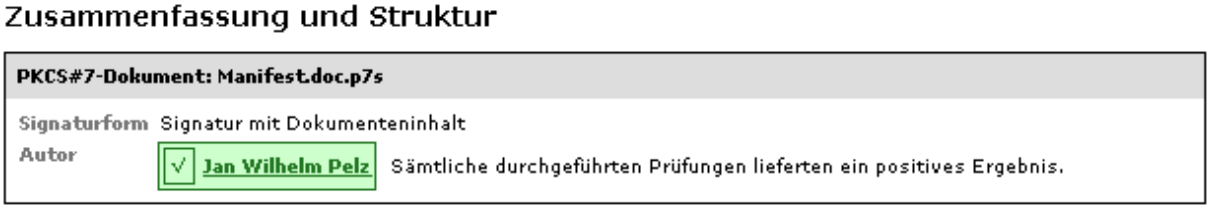


Abbildung 6: Bereich 1 "Zusammenfassung und Struktur" bei CMS/PKCS#7-Dokumenten

Kann ein Dokument nicht verarbeitet werden, wird folgende Meldung angezeigt: "Nicht interpretierte Datei: [`Dateiname`]" (siehe Abbildung 7).

Abbildung 7: Anzeige einer nicht interpretierten Datei

3.2.2 Zeile "Signaturform"

Das PKCS#7-Signaturformat erlaubt es, Dokumente sowohl losgelöst (detached) als auch zusammen (enveloped) mit dem Originaldokument zu signieren. Bei einer enveloped PKCS#7-Signatur liegt im Ergebnis nur eine Datei vor; diese besteht aus Signatur und Dokument. Bei einer detached PKCS#7-Signatur wird eine separate Datei mit der Signatur erzeugt.

Angezeigt wird im Prüfprotokoll hinter der Bezeichnung "Signaturform", ob die Signatur losgelöst (detached) oder zusammen (enveloped) mit dem Originaldokument vorliegt:

- Signatur ohne Dokumenteninhalt
- Signatur mit Dokumenteninhalt

Erläuterungen zur Signaturform:

Bei der Signatur ohne Dokumenteninhalt handelt es sich um eine detached Signatur. Die Signatur liegt in einer separaten Datei vor, in der Regel mit dem Dateinamen des Originaldokuments und häufig der Endung p7s (Governikus Signer), seltener auch mit den Endungen p7, pk7, pkcs7 oder cms. Der Name des Originaldokuments wird in der Zeile "Inhaltsdaten" angegeben. Bei der Signatur mit Dokumenteninhalt handelt es sich um eine enveloped Signatur. Die Signatur befindet sich im Originaldokument häufig mit der Endung p7s (Governikus Signer), seltener mit den Endungen p7m, p7, pk7, pkcs7 oder cms.

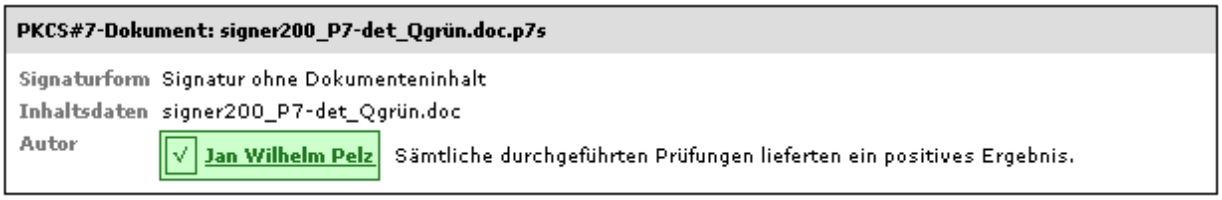


Abbildung 8: PKCS#7-Signatur ohne Dokumenteninhalt

3.2.3 Zeile "Inhaltsdaten" (nur Signatur ohne Dokumenteninhalt)

Hinter der Bezeichnung "Inhaltsdaten" wird bei der Signaturform ohne Dokumenteninhalt der Name des Originaldokuments mit dem Dokumenteninhalt angegeben, auf den sich die Signatur bezieht. Ist das Feld leer, konnte das Originaldokument nicht gefunden werden. In diesem Fall kann die mathematische Signaturprüfung nicht vollständig durchgeführt werden, da der Hashwert über das Originaldokument nicht berechnet werden konnte. Dieses führt immer zu einem Signaturstatus "gelb" und zur Fehlermeldung "Die Integrität der Signatur konnte nicht geprüft werden, da keine Inhaltsdaten vorliegen".

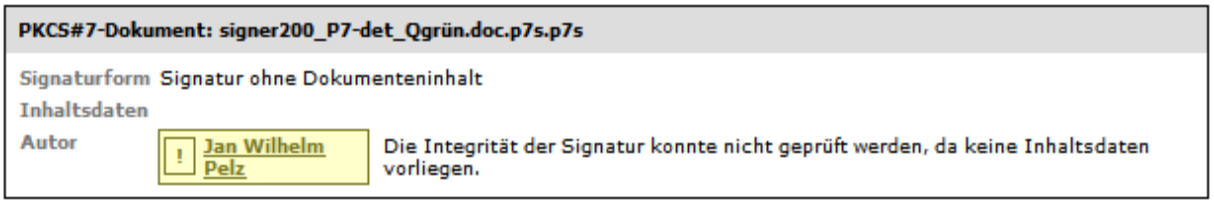


Abbildung 9: PKCS#7-Signatur ohne Dokumenteninhalt und ohne Originaldokument

3.2.4 Zeile "Autor, Prüfergebnis und Erläuterung"

In dieser Zeile wird von links nach rechts zunächst das kumulierte Prüfergebnis mit dem Namen des Autors in einem farbig unterlegten Kasten und anschließend eine Erläuterung zum Prüfergebnis angezeigt.

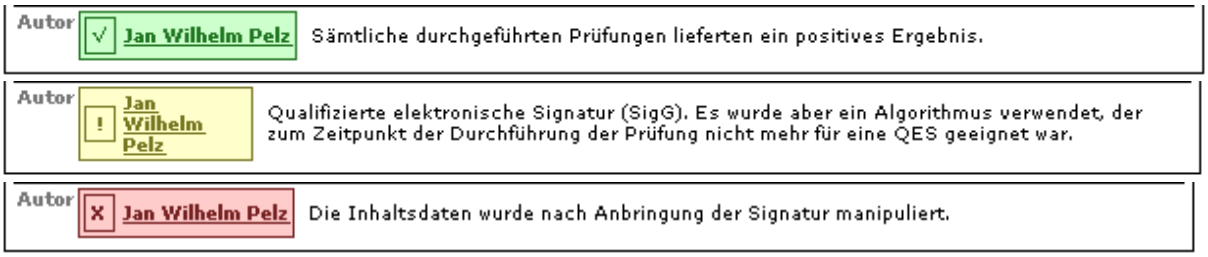


Abbildung 10: kumulierte Prüfergebnisse im Bereich 1 "Zusammenfassung und Struktur"

3.2.4.1 Spalte "Autor" mit kumuliertem Prüfergebnis

In der Spalte "Autor" werden rechts neben der Feldbezeichnung "Autor" das kumulierte Prüfergebnis bezogen auf eine Signatur und der Name des Autors (der signierenden Person) in einem farbig unterlegten Kasten angezeigt. Folgende Status sind möglich:

- √ Grüner Kasten mit Haken
- ! Gelber Kasten mit Ausrufungszeichen
- X Roter Kasten mit Kreuz

Erläuterungen zu √ Grüner Kasten mit Haken:

Alle durchgeführten Einzelprüfungen besitzen den Status „grün“. Die elektronische Signatur und das zugeordnete Signaturzertifikat wurden mit positivem Ergebnis überprüft. Bei einer qualifizierten Signatur (erstellt mit einer Signaturkarte eines deutschen ZDAs) gehört dazu auch die Prüfung der Eignung der verwendeten Signaturalgorithmen (Inhaltsdatensignatur, Zertifikatssignatur) gemäß aktuellem Algorithmenkatalog der Bundesnetzagentur zum Signierzeitpunkt und zum Zeitpunkt der Durchführung der Prüfung. Damit ist die Unverfälschtheit (Integrität der signierten Inhaltsdaten, der Nachricht, des Dokuments) sichergestellt, der Signierende sicher identifiziert und seine Authentizität bestätigt.

Dieses kumulierte Prüfergebnis ist immer nur eine Momentaufnahme zum Zeitpunkt der Durchführung der Prüfung. Bei einer „Nachprüfung“ (z.B. nach einigen Jahren) kann der Status auch auf "gelb" wechseln, weil das Trustcenter keine Sperrinformationen zum Signaturzertifikat mehr bereitstellt oder weil der bei einer qualifizierten Signatur verwendete Signaturalgorithmus nicht mehr für die Prüfung einer qualifizierten Signatur geeignet ist.

Erläuterungen zu ! Gelber Kasten mit Ausrufungszeichen:

Mindestens eine der Einzelprüfungen besitzt den Status "gelb" und damit kein eindeutiges Ergebnis. Einzelprüfungen mit dem finalen Status „rot“ gibt es nicht.

Der Status der Signaturprüfung ist aus Empfängersicht unbestimmt. Die Ursache sollte in jedem Fall genauer analysiert werden. Häufig kommt dieses Prüfergebnis nämlich dadurch zustande, dass der Sperrstatus des Zertifikats nicht ermittelt werden konnte, weil z.B. der OCSP-Responder des Trustcenters temporär nicht erreichbar war. Im Teil "Prüfung des Zertifikats" hat die Einzelprüfung „Sperrstatus des Zertifikats“ in diesem Fall den Status "gelb". Eine "Nachprüfung" des Signaturzertifikats ist dann sinnvoll.

Der Status "gelb" kann aber auch endgültig sein, weil z. B. der Signierzeitpunkt nicht ermittelt werden konnte (In diesem Fall kann dann auch der Sperrstatus des Zertifikats nicht ermittelt werden) oder weil der bei einer qualifizierten Signatur verwendete Signaturalgorithmus nicht mehr für die Prüfung einer qualifizierten Signatur (Inhaltsdatensignatur, Zertifikatssignatur) geeignet ist. Bereits erzeugte qualifizierte elektronische Signaturen bleiben zwar auch dann

noch qualifiziert, wenn der zugrunde liegende Signaturalgorithmus nach der Signaturerzeugung seine Eignung verloren hat, sie büßen jedoch graduell und sukzessive ihren Beweiswert ein. In der Spalte Erläuterungen wird in diesem Fall immer der folgende Warnhinweis ausgegeben:

- Qualifizierte elektronische Signatur (SigG). Es wurde aber ein Algorithmus verwendet, der zum Zeitpunkt der Durchführung der Prüfung nicht mehr für eine qualifizierte Signatur geeignet war.

Der Status "gelb" wird bei einer qualifizierten Signatur auch dann angezeigt, wenn die Eignung des verwendeten Signaturalgorithmus nicht ermittelt werden konnte. In der Spalte Erläuterungen wird in diesem Fall immer der folgende Warnhinweis ausgegeben:

- Die Eignung eines Algorithmus konnte nicht ermittelt werden.

Erläuterungen zu Roter Kasten mit Kreuz:

Mindestens eine der Einzelprüfungen besitzt den Status „rot“, d.h. war abschließend nicht erfolgreich. Damit ist entweder die Unverfälschtheit der Inhaltsdaten (Integrität der Daten) nicht sichergestellt oder es konnte die signierende Person abschließend nicht sicher identifiziert werden.

Der Status „rot“ wird bei einer qualifizierten Signatur auch dann angezeigt, wenn der verwendete Signaturalgorithmus bereits zum Signierzeitpunkt nicht mehr für eine qualifizierte Signatur geeignet war. Signaturen, die nach dem Schwachwerden des zugrundeliegenden Signaturalgorithmus erzeugt wurden, sind von vornherein keine qualifizierten Signaturen. Schon bei der Erzeugung der Signatur konnte nämlich nicht mehr sichergestellt werden, dass der Signaturschlüssel-Inhaber die alleinige Kontrolle über die Mittel zur Erzeugung der Signatur hatte. In der Spalte Erläuterungen wird in diesem Fall wird immer die folgende Meldung ausgegeben:

- Fortgeschrittene Signatur und keine qualifizierte Signatur (SigG). Es wurde ein Algorithmus verwendet, der zum Signierzeitpunkt nicht mehr für eine qualifizierte Signatur geeignet war.

Das kumulierte Prüfergebnis mit dem Status "rot" ist in der Regel final. Nur bei temporär gesperrten Zertifikaten (im europäischen Ausland möglich) ist ein Statuswechsel möglich.

3.2.4.2 Name des Autors

In der Spalte "Autor" werden rechts neben der Feldbezeichnung "Autor" das kumulierte Prüfergebnis und der Name des Autors (der signierenden Person) in einem farbig unterlegten Kasten angezeigt. Der Name des Autors ist das Attribut "Name des Zertifikatseigentümers" aus dem Feld Inhaber [`subject`] des Signaturzertifikats. Das Attribut "Name" [`CommonName`] besteht in der Regel aus dem Vor- und Nachnamen des Zertifikatsinhabers, kann aber auch ein Pseudonym enthalten.

3.2.4.3 Spalte "Erläuterungen"

In der letzten Spalte rechts wird das Prüfergebnis erläutert.

Erläuterungen bei Prüfergebnis Grüner Kasten mit Haken

Es ist nur eine Meldung möglich:

- Sämtliche durchgeführten Prüfungen lieferten ein positives Ergebnis.

Erläuterungen bei Prüfergebnis Gelber Kasten mit Ausrufungszeichen:

Folgende Meldungen aus dem Bereich der Einzelprüfergebnisse sind möglich, die zu einem Gelbstatus des kumulierten Prüfergebnisses führen:

- Es liegt kein Signierzeitpunkt vor.
- Die Integrität der Signatur konnte nicht geprüft werden, da das Signaturzertifikat nicht vorhanden ist.
- Die Integrität der Signatur konnte nicht geprüft werden, da keine Inhaltsdaten vorliegen.
- Die Integrität der Signatur konnte nicht geprüft werden, da der Algorithmus nicht implementiert ist.
- Der Sperrstatus des Zertifikats konnte nicht ermittelt werden.
- Die Vertrauenswürdigkeit des Trustcenters konnte nicht ermittelt werden.
- Die Gültigkeit des Zertifikats konnte nicht überprüft werden.
- Die Signaturen der Zertifikatskette konnten nicht überprüft werden.
- Qualifizierte elektronische Signatur (SigG). Es wurde aber ein Algorithmus verwendet, der zum Zeitpunkt der Durchführung der Prüfung nicht mehr für eine qualifizierte Signatur geeignet war (nur bei einer qualifizierten Signatur, die mit einer Signaturkarte eines deutschen ZDAs erstellt wurde).
- Die Eignung eines Algorithmus konnte nicht ermittelt werden (nur bei einer qualifizierten Signatur, die mit einer Signaturkarte eines deutschen ZDAs erstellt wurde).

Erläuterungen bei Prüfergebnis Roter Kasten mit Kreuz:

Folgende Meldungen aus dem Bereich der Einzelprüfergebnisse sind möglich, die zu einem Rotstatus des kumulierten Prüfergebnisses führen:

- Die Inhaltsdaten wurden nach Anbringung der Signatur manipuliert.
- Die Signatur der OSCI-Nachricht ist inkorrekt.
- Das Attributzertifikat gehört nicht zum Signaturzertifikat.
- Das Zertifikat war zum Signierzeitpunkt gesperrt oder abgelaufen.
- Das Zertifikat ist gesperrt.
- Das Trustcenter ist nicht vertrauenswürdig.
- Das Zertifikat ist nicht gültig.
- Die Zertifikatskette ist nicht gültig.
- Fortgeschrittene Signatur und keine qualifizierte Signatur (SigG). Es wurde ein Algorithmus verwendet, der zum Signierzeitpunkt nicht mehr für eine qualifizierte Signatur geeignet war. (nur bei einer qualifizierten Signatur, die mit einer Signaturkarte eines deutschen ZDAs erstellt wurde)

3.3 PDF-Inline-Signaturen und PAdES

PDF-Dokumente mit Signaturen sind PDF-Dokumente mit eingebetteten Signaturen. Unterstützt werden PDF-Dokumente (ab PDF 1.3) mit PDF-Signaturen gemäß folgender Spezifikationen oder Profilierungen:

- PAdES BES (PAdES Part 2) und PAdES EPES (PAdES Part 3). PAdES (PDF Advanced Electronic Signatures) ist ein Standard gemäß ETSI TS 102 778 basierend auf PDF-Signaturen, wie in ISO 32 000 spezifiziert. PAdES BES ist die Grundform.
- Bestimmte Alt-Signaturen (Legacy-Formate) nach ISO 32000. Dadurch wird sichergestellt, dass auch bestehende PDF-Signaturen weiterhin geprüft werden können.

Das PDF-Dateiformat unterstützt die inkrementelle Dokumentenaktualisierung. Jedes Mal, wenn das Dokument ergänzt/verändert wird, wird eine neue Revision des Dokuments erstellt. Eine Signatur ist dabei immer einer sogenannten Revision zugeordnet, die vorangegangene Revisionen mit und ohne Signatur umfassen kann. Enthält ein PDF-Dokument mehrere Signaturen, sind sie ineinander geschachtelt (Zwiebelsignaturen). Im Prüfprotokoll werden für jede signierte Revision das Prüfergebnis und ein Gesamtstatus über alle geprüften Signaturen angezeigt. Die grafische Anzeige im Prüfprotokoll spiegelt diese Zwiebelstruktur der Signaturen wider:

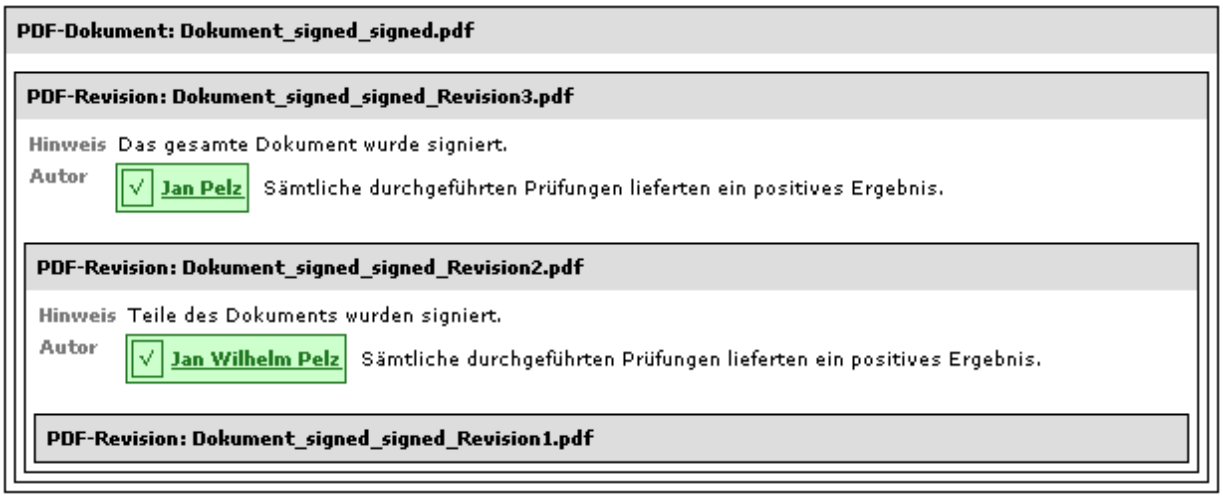


Abbildung 11: Bereich 1 "Zusammenfassung und Struktur bei einem PDF-Dokument mit zwei Signaturen"

Im Beispiel enthält das PDF-Dokument zwei Signaturen, wobei die äußere Signatur (Dokument_signed_signed_Revision3.pdf) auch die andere Signatur (Dokument_signed_ signed_Revision2.pdf) umschließt. Die signierten Revisionen eines PDFs lassen sich im Adobe Reader im Fenster "Unterschrifteneigenschaften", Reiter "Dokument" über den Button "unterschriebene Version anzeigen" anzeigen.

Im Bereich 1 "Zusammenfassung und Struktur" ist das Prüfprotokoll für PDF/PAdES-Dokumente wie folgt aufgebaut:

3.3.1 Zeile "Dateiname"

In der ersten Zeile wird grau unterlegt hinter der Bezeichnung des Signaturformats "PDF-Dokument" oder "PAdES-Dokument" der Name der PDF-Datei angezeigt, die mindestens eine Signatur (signierte Revision) enthält.

3.3.2 Zeile "PDF-Revision"

In der Zeile werden grau unterlegt hinter der Bezeichnung "PDF-Revision" der Name des Dokuments und die Revisionsnummer angezeigt.

3.3.3 Zeile "PAdES-Profilierung" (nur PAdES)

In der Zeile wird der Name der PAdES-Profilierung angezeigt. Folgende PAdES-Profilierungen werden unterstützt und angezeigt:

- PAdES basic (Part 2)
- PAdES erweitert (Part 3)

3.3.4 Zeile "Hinweis"

3.3.4.1 Hinweise mit informativem Charakter

Folgende Hinweise können bei einem PDF-Dokument angezeigt werden, die nur einen informativen Charakter haben und das Ergebnis der Signaturprüfung nicht beeinflussen:

- Das gesamte Dokument wurde signiert.
- Teile des Dokuments wurden signiert.
- Die Signatur ist nicht standardkonform.
- Das PDF-Dokument ist mit einem Passwortschutz versehen und konnte nicht geöffnet werden.

Erläuterungen zu den Hinweisen:

- Das gesamte Dokument wurde signiert.

Die Signatur umfasst den gesamten Dokumenteninhalt. Nach der Signaturanbringung wurden keine weiteren Revisionen, zum Beispiel durch eine Annotation, erzeugt.

- Teile des Dokuments wurden signiert.

Die Signatur umfasst nicht das gesamte Dokument. Nach der Signaturanbringung wurde mindestens eine weitere Revision, zum Beispiel durch eine Annotation, erzeugt, die nicht mit signiert wurde. Es ist zu empfehlen, sich davon zu überzeugen, dass die nicht signierte Revision keine Inhalte enthält, die z.B. den signierten Text "verfälschend" überlagern. Die Revisionen eines PDFs lassen sich z.B. im Adobe Reader anzeigen. Nachträglich erzeugte Revisionen (z.B. eine weitere Signatur oder eine Annotation) beeinträchtigen nicht die vorher angebrachte Signatur.

- Die Signatur ist nicht standardkonform.

Die PDF-Signatur ist nicht standardkonform. Die unsignierte Lücke im ByteRange ist kleiner als die eigentliche Signatur. Die Integrität der Signatur ist nicht verletzt. Mögliche Folge ist allerdings, dass andere Prüfkomponenten falschnegative Ergebnisse erzeugen könnten.

- Das PDF-Dokument ist mit einem Passwortschutz versehen und konnte nicht geöffnet werden.

Das PDF-Dokument ist mit einem Passwortschutz versehen. Es konnte daher nicht geöffnet und verarbeitet werden.

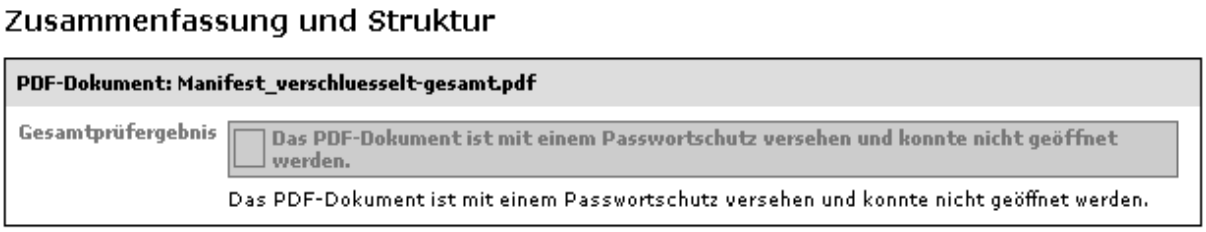


Abbildung 12: Meldung bei einem verschlüsselten PDF-Dokument

3.3.4.2 Hinweise mit informativem Charakter (nur PAdES)

Folgende Hinweise können bei einem PAdES-Dokument angezeigt werden, die nur einen informativen Charakter haben und die Signaturprüfung nicht beeinflussen:

- Es ist eine Signaturrichtlinie vorhanden, die nicht berücksichtigt wird.
- Das Signaturzertifikat passt nicht zum signierten Hashwert.
- Der Hashwert des Signaturzertifikats fehlt.
- Das PDF-Dokument ist nicht PAdES-konform.

Erläuterungen zu den Hinweisen:

- Es ist eine Signaturrichtlinie vorhanden, die nicht berücksichtigt wird.

In einem PAdES-Dokument kann eine Signaturrichtlinie hinterlegt werden. Damit gibt der Signierende an, welche Rolle und Verpflichtungen er mit der Signatur eingehen möchte und dass er damit Anforderungen an die Signaturprüfung stellt. Ist eine Signaturrichtlinie vorhanden, wird diese im Bereich "Signaturprüfungen" angezeigt, hat aber keine Auswirkungen auf die Prüfung.

- Das Signaturzertifikat passt nicht zum signierten Hashwert.

Bei einem PAdES-Dokument gemäß EU-Profilierung muss ein Signaturzertifikat beigefügt und dieses gehasht werden. Dieser Hashwert muss mit signiert werden. Im vorliegenden Fall stimmen der signierte Hashwert und der neu berechnete Hashwert über das Zertifikat nicht überein. Damit ist das Dokument nicht PAdES-konform gemäß EU-Profilierung. Im Fall einer positiven mathematischen Prüfung der Signatur und einer erfolgreichen Online-Prüfung des Zertifikats hat dieser Hinweis nur Informationscharakter.

- Der Hashwert des Signaturzertifikats fehlt.

Bei einem PAdES-Dokument gemäß EU-Profilierung muss das beigefügte Signaturzertifikat gehasht sein und dieser Hashwert muss mit signiert werden. Fehlt der Hashwert, ist das Dokument nicht PAdES-konform. Im Fall einer positiven mathematischen Prüfung der Signatur und einer erfolgreichen Online-Prüfung des Zertifikats hat dieser Hinweis nur Informationscharakter.

- Das PDF-Dokument ist nicht PAdES-konform.

Das geprüfte Dokument ist nicht PAdES-BES konform. Mögliche Ursachen sind:

a) In der CMS-Signatur befindet sich ein Signierzeitpunkt, obwohl dieses bei einer signierten PAdES-Revision nicht zulässig ist. Es wird, wenn vorhanden, der Signierzeitpunkt aus dem "Dictionary" verwendet.

b) Im "Dictionary" (Jedes signierte PDF-Dokument enthält alle Informationen zur digitalen Signatur gemäß ISO 32000 in einem "Dictionary".) ist ein Zertifikat vorhanden, obwohl dieses bei einer signierten PAdES-Revision nicht zulässig ist.

c) Der für PAdES-Revisionen vorgeschriebene Inhaltsdatentyp wurde nicht verwendet.

d) Die für PAdES-Revisionen vorgeschriebene Signaturversion wurde nicht verwendet. Die Signaturprüfung wird durch die Nichtkonformität nicht beeinflusst.

3.3.4.3 Hinweise, die zu einer Gelbprüfung führen

Folgende Hinweise können bei einem PDF-Dokument (auch PAdES) angezeigt werden, die zu einem finalen Gelbstatus der Signaturprüfung führen:

- Nur Teile der Revision wurden signiert.
- Die Signatur konnte nicht verarbeitet werden.
- Die Signatur ist nicht standardkonform.

Erläuterungen zu den Hinweisen:

- Nur Teile der Revision wurden signiert.

Die PDF-Signatur ist nicht standardkonform. Mögliche Folge: Inhalte werden durch externe Viewer angezeigt, nicht aber von der Signatur vor Manipulation geschützt. Deswegen sollten solche Signaturen nicht ungefragt akzeptiert werden, obwohl – rein technisch gesehen - die mathematische Signaturprüfung positiv verläuft. Dieses führt zum finalen Status "gelb" bei der Prüfung der Signatur.

- Die Signatur konnte nicht verarbeitet werden.

Die Signatur konnte nicht verarbeitet werden. Mögliche Ursachen sind: a) Die Signatur konnte nicht geparst werden. b) Die PDF-Revision enthält mehr als eine Signatur und nur einen Signierzeitpunkt. c) Für die Signatur wurde ein unbekannter Filter oder Signaturhandler verwendet. Es kann daher keine Aussage über die Integrität getroffen werden. Dieses führt zum finalen Status "gelb" bei der Prüfung der Signatur.

- Die Signatur ist nicht standardkonform.

Die Signatur ist nicht standardkonform, da sie sich nicht auf die PDF-Inhaltsdaten bezieht. Es besteht Manipulationsgefahr.

3.3.5 Zeile "Autor, Prüfergebnis und Erläuterung"

In dieser Zeile wird von links nach rechts zunächst das kumulierte Prüfergebnis mit dem Namen des Autors in einem farbig unterlegten Kasten und anschließend eine Erläuterung zum Prüfergebnis angezeigt.

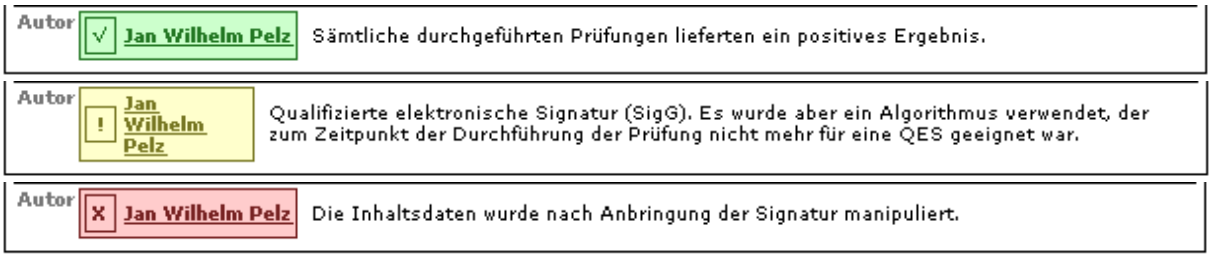


Abbildung 13: Kumulierte Prüfergebnisse im Bereich 1 "Zusammenfassung und Struktur"

3.3.5.1 Spalte "Autor" mit kumuliertem Prüfergebnis

In der Spalte "Autor" werden rechts neben der Feldbezeichnung "Autor" das kumulierte Prüfergebnis bezogen auf eine Signatur und der Name des Autors (der signierenden Person) in einem farbig unterlegten Kasten angezeigt. Folgende Status sind möglich:

- √ Grüner Kasten mit Haken
- ! Gelber Kasten mit Ausrufungszeichen
- X Roter Kasten mit Kreuz

Erläuterungen zu √ Grüner Kasten mit Haken:

Alle durchgeführten Einzelprüfungen besitzen den Status „grün“. Die elektronische Signatur und das zugeordnete Signaturzertifikat wurden mit positivem Ergebnis überprüft. Bei einer qualifizierten Signatur (erstellt mit einer Signaturkarte eines deutschen ZDAs) gehört dazu auch die Prüfung der Eignung der verwendeten Signaturalgorithmen (Inhaltsdatensignatur, Zertifikatssignatur) gemäß aktuellem Algorithmenkatalog der Bundesnetzagentur zum Signierzeitpunkt und zum Zeitpunkt der Durchführung der Prüfung. Damit ist die Unverfälschtheit (Integrität der signierten Inhaltsdaten, der Nachricht, des Dokuments) sichergestellt, der Signierende sicher identifiziert und seine Authentizität bestätigt.

Dieses kumulierte Prüfergebnis ist immer nur eine Momentaufnahme zum Zeitpunkt der Durchführung der Prüfung. Bei einer „Nachprüfung“ (z.B. nach einigen Jahren) kann der Status auch auf "gelb" wechseln, weil das Trustcenter keine Sperrinformationen zum Signaturzertifikat mehr bereitstellt oder weil der bei einer qualifizierten Signatur verwendete Signaturalgorithmus nicht mehr für die Prüfung einer qualifizierten Signatur geeignet ist.

Erläuterungen zu ! Gelber Kasten mit Ausrufungszeichen:

Mindestens eine der Einzelprüfungen besitzt den Status "gelb" und damit kein eindeutiges Ergebnis. Einzelprüfungen mit dem finalen Status „rot“ gibt es nicht.

Der Status der Signaturprüfung ist aus Empfängersicht unbestimmt. Die Ursache sollte in jedem Fall genauer analysiert werden. Häufig kommt dieses Prüfergebnis nämlich dadurch zustande, dass der Sperrstatus des Zertifikats nicht ermittelt werden konnte, weil z.B. der OCSP-Responder des Trustcenters temporär nicht erreichbar war. Im Teil "Prüfung des Zertifikats" hat die Einzelprüfung „Sperrstatus des Zertifikats“ in diesem Fall den Status "gelb". Eine "Nachprüfung" des Signaturzertifikats ist dann sinnvoll.

Der Status "gelb" kann aber auch endgültig sein, weil z. B. der Signierzeitpunkt nicht ermittelt werden konnte (In diesem Fall kann dann auch der Sperrstatus des Zertifikats nicht ermittelt werden) oder weil der bei einer qualifizierten Signatur verwendete Signaturalgorithmus nicht mehr für die Prüfung einer qualifizierten Signatur (Inhaltsdatensignatur, Zertifikatssignatur) geeignet ist. Bereits erzeugte qualifizierte elektronische Signaturen bleiben zwar auch dann

noch qualifiziert, wenn der zugrundeliegende Signaturalgorithmus nach der Signaturerzeugung seine Eignung verloren hat, sie büßen jedoch graduell und sukzessive ihren Beweiswert ein. In der Spalte Erläuterungen wird in diesem Fall immer der folgende Warnhinweis ausgegeben:

- Qualifizierte elektronische Signatur (SigG). Es wurde aber ein Algorithmus verwendet, der zum Zeitpunkt der Durchführung der Prüfung nicht mehr für eine qualifizierte Signatur geeignet war.

Der Status "gelb" wird bei einer qualifizierten Signatur auch dann angezeigt, wenn die Eignung des verwendeten Signaturalgorithmus nicht ermittelt werden konnte. In der Spalte Erläuterungen wird in diesem Fall immer der folgende Warnhinweis ausgegeben:

- Die Eignung eines Algorithmus konnte nicht ermittelt werden.

Erläuterungen zu Roter Kasten mit Kreuz:

Mindestens eine der Einzelprüfungen besitzt den Status „rot“, d.h. war abschließend nicht erfolgreich. Damit ist entweder die Unverfälschtheit der Inhaltsdaten (Integrität der Daten) nicht sichergestellt oder es konnte die signierende Person abschließend nicht sicher identifiziert werden.

Der Status „rot“ wird bei einer qualifizierten Signatur auch dann angezeigt, wenn der verwendete Signaturalgorithmus bereits zum Signierzeitpunkt nicht mehr für eine qualifizierte Signatur geeignet war. Signaturen, die nach dem Schwachwerden des zugrundeliegenden Signaturalgorithmus erzeugt wurden, sind von vornherein keine qualifizierten Signaturen. Schon bei der Erzeugung der Signatur konnte nämlich nicht mehr sichergestellt werden, dass der Signaturschlüssel-Inhaber die alleinige Kontrolle über die Mittel zur Erzeugung der Signatur hatte. In der Spalte Erläuterungen in diesem Fall wird immer die folgende Meldung ausgegeben:

- Fortgeschrittene Signatur und keine qualifizierte Signatur (SigG). Es wurde ein Algorithmus verwendet, der zum Signierzeitpunkt nicht mehr für eine qualifizierte Signatur geeignet war.

Das kumulierte Prüfergebnis mit dem Status "rot" ist in der Regel final. Nur bei temporär gesperrten Zertifikaten (im europäischen Ausland möglich) ist ein Statuswechsel möglich.

3.3.5.2 Name des Autors

In der Spalte "Autor" werden rechts neben der Feldbezeichnung "Autor" das kumulierte Prüfergebnis und der Name des Autors (der signierenden Person) in einem farblich unterlegten Kasten angezeigt. Der Name des Autors ist das Attribut "Name des Zertifikatseigentümers" aus dem Feld Inhaber [`subject`] des Signaturzertifikats. Das Attribut "Name" [`CommonName`] besteht in der Regel aus dem Vor- und Nachnamen des Zertifikatsinhabers, kann aber auch ein Pseudonym enthalten.

3.3.5.3 Spalte "Erläuterungen"

In der letzten Spalte rechts wird das Prüfergebnis erläutert.

Erläuterungen bei Prüfergebnis Grüner Kasten mit Haken

Es ist nur eine Meldung möglich:

- Sämtliche durchgeführten Prüfungen lieferten ein positives Ergebnis.

Erläuterungen bei Prüfergebnis Gelber Kasten mit Ausrufungszeichen:

Folgende Meldungen aus dem Bereich der Einzelprüfergebnisse sind möglich, die zu einem Gelbstatus des kumulierten Prüfergebnisses führen:

- Es liegt kein Signierzeitpunkt vor.
- Die Integrität der Signatur konnte nicht geprüft werden, da das Signaturzertifikat nicht vorhanden ist.
- Die Integrität der Signatur konnte nicht geprüft werden, da keine Inhaltsdaten vorliegen.
- Die Integrität der Signatur konnte nicht geprüft werden, da der Algorithmus nicht implementiert ist.
- Der Sperrstatus des Zertifikats konnte nicht ermitteln werden.
- Die Vertrauenswürdigkeit des Trustcenters konnte nicht ermittelt werden.
- Die Gültigkeit des Zertifikats konnte nicht überprüft werden.
- Die Signaturen der Zertifikatskette konnten nicht überprüft werden.
- Qualifizierte elektronische Signatur (SigG). Es wurde aber ein Algorithmus verwendet, der zum Zeitpunkt der Durchführung der Prüfung nicht mehr für eine qualifizierte Signatur geeignet war (nur bei einer qualifizierten Signatur, die mit einer Signaturkarte eines deutschen ZDAs erstellt wurde).
- Die Eignung eines Algorithmus konnte nicht ermittelt werden (nur bei einer qualifizierten Signatur, die mit einer Signaturkarte eines deutschen ZDAs erstellt wurde).

Erläuterungen bei Prüfergebnis Roter Kasten mit Kreuz:

Folgende Meldungen aus dem Bereich der Einzelprüfergebnisse sind möglich, die zu einem Rotstatus des kumulierten Prüfergebnisses führen:

- Die Inhaltsdaten wurden nach Anbringung der Signatur manipuliert.
- Die Signatur der OSCI-Nachricht ist inkorrekt.
- Das Attributzertifikat gehört nicht zum Signaturzertifikat.
- Das Zertifikat war zum Signierzeitpunkt gesperrt oder abgelaufen.
- Das Zertifikat ist gesperrt.
- Das Trustcenter ist nicht vertrauenswürdig.
- Das Zertifikat ist nicht gültig.
- Die Zertifikatskette ist nicht gültig.
- Fortgeschrittene Signatur und keine qualifizierte Signatur (SigG). Es wurde ein Algorithmus verwendet, der zum Signierzeitpunkt nicht mehr für eine qualifizierte Signatur geeignet war (nur bei einer qualifizierten Signatur, die mit einer Signaturkarte eines deutschen ZDAs erstellt wurde).

3.3.6 Anzeige der Prüfergebnisse von PDF-Portfolios"

Der Verification Interpreter unterstützt auch die Analyse von PDF-Portfolios und darin enthaltener PDF-Dokumente.

In einem PDF-Portfolio sind mehrere Dateien in einer integrierten PDF-Einheit gebündelt. Die

Dateien in einem Portfolio können in verschiedenen Formaten aus verschiedenen Anwendungsprogrammen vorliegen. Diese bleiben mit ihren spezifischen Eigenschaften erhalten, obwohl sie zu einer PDF-Portfolio-Datei zusammengesetzt werden. Der Verification Interpreter unterstützt nur die Analyse von PDF-Portfolios die erneut PDF-Dokumente enthalten. PDF-Portfolios und darin enthaltene PDF-Dokumente lassen sich im Adobe Reader öffnen und lesen.

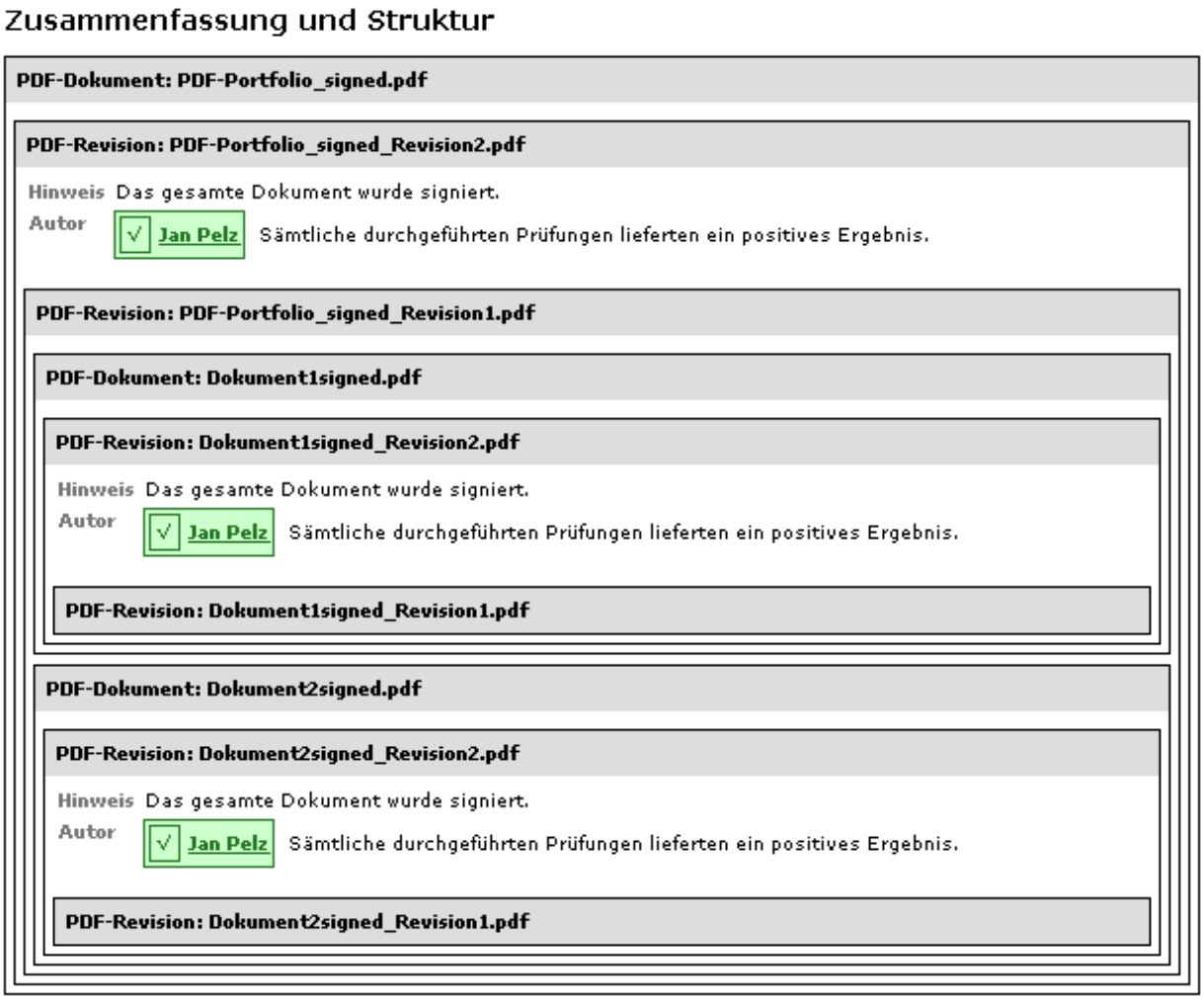


Abbildung 14: Bereich 1 Zusammenfassung und Struktur bei einem PDF-Portfolio mit zwei signierten PDF-Dokumenten

Im obigen Beispiel handelt es sich um ein PDF-Portfolio (Name: PDF-Portfolio_signed.pdf) mit zwei signierten PDF-Dokumenten (Dokument_1_signed.pdf und Dokument_2_signed.pdf). Beide Dokumente wurden signiert, dadurch wurde jeweils eine 2. Revision erzeugt. Die Signaturen umfassen jeweils das gesamte Dokument (Hinweis "Das gesamte Dokument wurde signiert"). Danach wurde ein PDF-Dokument (Name: PDF_Portfolio) erstellt, dass die beiden signierten Dokumente als Anhang enthält. Dadurch wurde die erste Revision des Dokuments erzeugt. Anschließend wurde das Dokument "PDF-Portfolio" signiert. Dadurch wurde eine zweite Revision erzeugt. Da keine Annotationen nach der Signatur angebracht wurden, existiert keine dritte Revision und als Hinweis wird wiederum angezeigt "Das gesamte Dokument wurde signiert".

3.4 Signaturzertifikate (Einzelprüfung)

Das Prüfprotokoll für die separate Zertifikatsprüfung unterscheidet sich vom Prüfprotokoll, das die Ergebnisse von Signaturprüfungen anzeigt. Der Unterschied liegt darin begründet, dass bei der separaten Zertifikatsprüfung ein Zertifikat zu einem angegebenen Prüfzeitpunkt geprüft wird. Der Prüfzeitpunkt beschreibt dabei den Zeitpunkt, zu dem der Sperrstatus des Zertifikats ermittelt werden soll.

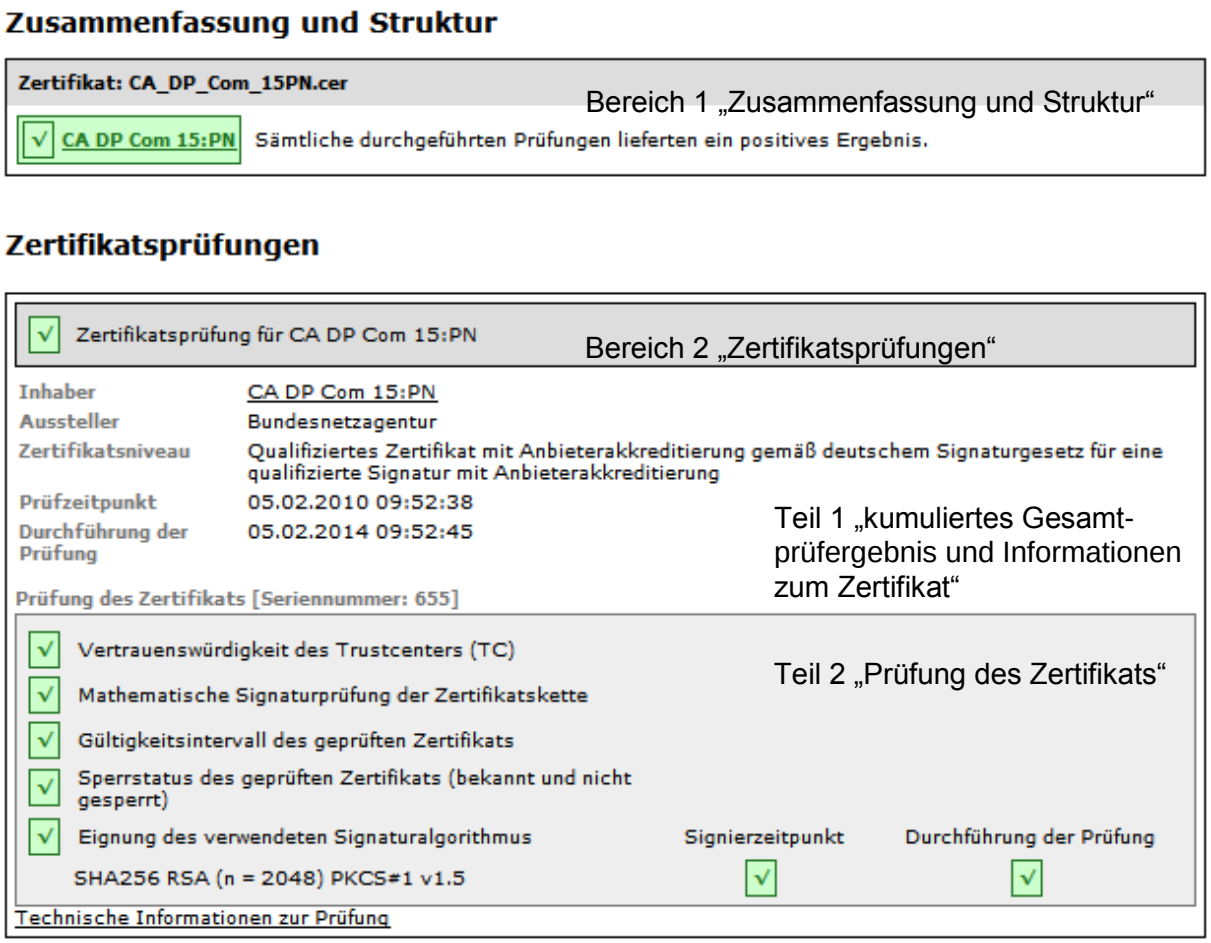


Abbildung 15: Bereich 1 "Struktur" und Bereich 2 "Zertifikatsprüfungen" bei der Prüfung eines einzelnen Zertifikats

3.4.1 Bereich 1: Zusammenfassung und Struktur

Im Bereich 1 "Zusammenfassung und Struktur" ist das Prüfprotokoll für die Prüfung von Zertifikaten wie folgt aufgebaut:

3.4.1.1 Zeile "Dateiname"

In der ersten, grau unterlegten Zeile wird hinter der Bezeichnung "Zertifikat" der Dateiname des geprüften Zertifikats angezeigt.

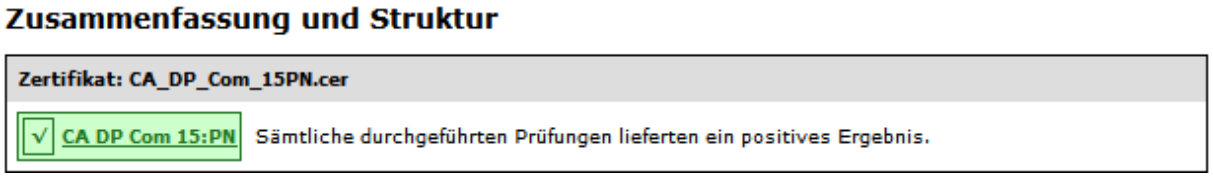


Abbildung 16: Bereich 1 "Struktur" bei der Prüfung eines einzelnen Zertifikats

3.4.1.2 Zeile "Zertifikatsinhaber, Prüfergebnis und Erläuterung"

In der Zeile "Zertifikatsinhaber" wird von links nach rechts zunächst das kumulierte Prüfergebnis der Zertifikatsprüfung mit dem Namen des Zertifikatsinhabers in einem farbig unterlegten Kasten und anschließend eine Erläuterung zum Prüfergebnis angezeigt.

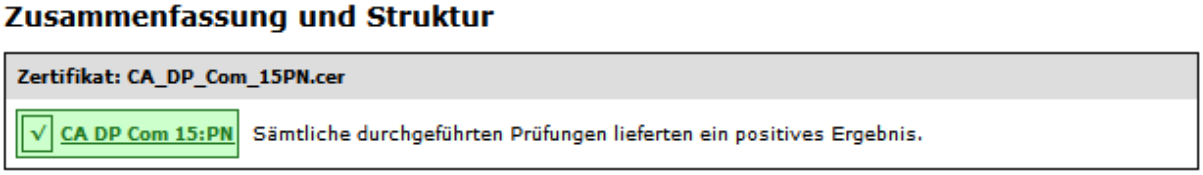


Abbildung 17: Bereich 1 "Zusammenfassung und Struktur" bei der Prüfung eines einzelnen Zertifikats

3.4.1.3 Spalte "kumuliertes Prüfergebnis"

In der ersten Spalte wird das kumulierte Prüfergebnis der Zertifikatsprüfung in einem farbig unterlegten Kasten angezeigt. Folgende Status sind möglich:

- Grüner Kasten mit Haken
- Gelber Kasten mit Ausrufungszeichen
- Roter Kasten mit Kreuz:

Erläuterungen zu Grüner Kasten mit Haken:

Alle durchgeführten Einzelprüfungen besitzen den Status „grün“. Das Signaturzertifikat wurde mit positivem Ergebnis überprüft. Bei einem qualifizierten Zertifikat gehört dazu auch die Prüfung der Eignung des zur Zertifikatssignatur verwendeten Signaturalgorithmus gemäß aktuellem Algorithmenkatalog der Bundesnetzagentur zum Signierzeitpunkt und zum Zeitpunkt der Durchführung der Prüfung. Damit ist der Zertifikatsinhaber sicher identifiziert und seine Authentizität bestätigt.

Dieses kumulierte Prüfergebnis ist immer nur eine Momentaufnahme zum Zeitpunkt der Durchführung der Prüfung. Bei einer „Nachprüfung“ (z.B. nach einigen Jahren) kann der Status auch auf "gelb" wechseln, weil das Trustcenter keine Sperrinformationen zum Signaturzertifikat mehr bereitstellt oder weil der bei der Signatur des Zertifikats verwendete Signaturalgorithmus nicht mehr für die Prüfung eines qualifizierten Zertifikats geeignet ist.

Erläuterungen zu Gelber Kasten mit Ausrufungszeichen:

Mindestens eine der Einzelprüfungen besitzt den Status "gelb" und damit kein eindeutiges Ergebnis. Einzelprüfungen mit dem finalen Status „rot“ gibt es nicht.

Der Status der Zertifikatsprüfung ist aus Empfängersicht unbestimmt. Die Ursache sollte in jedem Fall genauer analysiert werden. Häufig kommt dieses Prüfergebnis nämlich dadurch

zustande, dass der Sperrstatus des Zertifikats nicht ermittelt werden konnte, weil z.B. der OCSP-Responder des Trustcenters temporär nicht erreichbar war. Im Teil "Prüfung des Zertifikats" hat die Einzelprüfung „Sperrstatus des Zertifikats“ in diesem Fall den Status "gelb". Eine "Nachprüfung" des Signaturzertifikats ist dann sinnvoll.

Der Status "gelb" kann aber auch endgültig sein, weil der bei der Signatur des qualifizierten Zertifikats verwendete Signaturalgorithmus nicht mehr für die Prüfung eines qualifizierten Zertifikats geeignet ist. Bereits erzeugte qualifizierte elektronische Zertifikatssignaturen bleiben zwar auch dann noch qualifiziert, wenn der zugrundeliegende Signaturalgorithmus nach der Signaturerzeugung seine Eignung verloren hat, sie büßen jedoch graduell und sukzessive ihren Beweiswert ein.

Erläuterungen zu Roter Kasten mit Kreuz:

Mindestens eine der Einzelprüfungen besitzt den Status „rot“, d.h. war abschließend nicht erfolgreich. Damit konnte der Zertifikatsinhaber abschließend nicht sicher identifiziert werden.

Der Status „rot“ wird bei einem qualifizierten Zertifikat auch dann angezeigt, wenn der verwendete Signaturalgorithmus bereits zum Signierzeitpunkt des Zertifikats nicht mehr für eine qualifizierte Signatur geeignet war. Signaturen, die nach dem Schwachwerden des zugrundeliegenden Signaturalgorithmus erzeugt wurden, sind von vornherein keine qualifizierten Signaturen. Schon bei der Erzeugung der Signatur konnte nämlich nicht mehr sichergestellt werden, dass der Signaturschlüssel-Inhaber die alleinige Kontrolle über die Mittel zur Erzeugung der Signatur hatte.

Das kumulierte Prüfergebnis mit dem Status "rot" ist in der Regel final. Nur bei temporär gesperrten Zertifikaten (im europäischen Ausland möglich) ist ein Statuswechsel möglich.

3.4.1.4 Spalte "Name des Inhabers des Zertifikats"

In der zweiten Spalte wird der Name des Inhabers des Zertifikats angezeigt. Dieses ist der Name des Zertifikatseigentümers aus dem Feld Inhaber [`subject`] des Zertifikats. Das Attribut "Name" [`CommonName`] besteht in der Regel aus dem Vor- und Nachnamen des Zertifikatsinhabers, kann aber auch ein Pseudonym enthalten.

3.4.1.5 Spalte "Erläuterungen"

In der letzten Spalte wird das Ergebnis der Zertifikatsprüfung erläutert.

Erläuterungen bei Prüfergebnis Grüner Kasten mit Haken:

Es ist nur eine Meldung möglich:

- Sämtliche durchgeführten Prüfungen lieferten ein positives Ergebnis.

Erläuterungen bei Prüfergebnis Gelber Kasten mit Ausrufungszeichen:

Folgende Meldungen aus dem Bereich der Einzelprüfergebnisse sind möglich:

- Der Sperrstatus des Zertifikats konnte nicht ermittelt werden.
- Die Vertrauenswürdigkeit des Trustcenters konnte nicht ermittelt werden.
- Die Gültigkeit des Zertifikats konnte nicht überprüft werden.
- Die Signaturen der Zertifikatskette konnten nicht überprüft werden.

- Die Integrität der Signatur konnte nicht geprüft werden, da der Algorithmus nicht implementiert ist.

Zusätzlich bei einem qualifizierten Zertifikat, ausgestellt durch einen deutschen ZDA:

- Qualifizierte elektronische Signatur (SigG). Es wurde aber ein Algorithmus verwendet, der zum Zeitpunkt der Durchführung der Prüfung nicht mehr für eine qualifizierte Signatur geeignet war.
- Die Eignung eines Algorithmus konnte nicht ermittelt werden.

Erläuterungen bei Prüfergebnis Roter Kasten mit Kreuz:

Folgende Meldungen aus dem Bereich der Einzelprüfergebnisse sind möglich:

- Das Zertifikat war zum Signierzeitpunkt gesperrt oder abgelaufen.
- Das Zertifikat ist gesperrt.
- Das Trustcenter ist nicht vertrauenswürdig.
- Das Zertifikat ist nicht gültig.
- Die Zertifikatskette ist nicht gültig.

Zusätzlich bei einem qualifizierten Zertifikat, ausgestellt durch einen deutschen ZDA:

- Fortgeschrittene Signatur und keine qualifizierte Signatur (SigG). Es wurde ein Algorithmus verwendet, der zum Signierzeitpunkt nicht mehr für eine qualifizierte Signatur geeignet war.

3.4.2 Bereich 2: Zertifikatsprüfungen

In den folgenden Unterkapiteln wird der Bereich 2 "Zertifikatsprüfungen" des Prüfprotokolls für eine separate Zertifikatsprüfung erläutert.

- Im Teil 1 dieses Bereichs werden das kumulierte Prüfergebnis der Zertifikatsprüfung und allgemeine Informationen zum Zertifikat angezeigt. Dazu gehört der Name des Zertifikatsinhabers, der Aussteller des Zertifikats, das Zertifikatsniveau, Prüfzeitpunkt des Zertifikats (der Zeitpunkt zu dem der Sperrstatus ermittelt werden soll) und der Zeitpunkt der Durchführung der Prüfung.
- Im Teil 2 dieses Bereichs folgen die Ergebnisse der Zertifikatsprüfung. Dazu gehören die Ergebnisse folgender Einzelprüfungen: Vertrauenswürdigkeit des Trustcenters (Issuer Trust), die mathematische Prüfung der Zertifikatssignaturen (Signature), der Sperrstatus des Zertifikats (Revocation Status) und der Gültigkeitszeitraum (Validity Interval). Bei einem qualifizierten Zertifikat eines deutschen Zertifizierungsdiensteanbieters wird zusätzlich das Ergebnis der Eignung des zur Zertifikatssignatur verwendeten Signaturalgorithmus angezeigt. Dieser Teil entspricht vollständig dem allgemeinen Prüfprotokoll und wird ausführlich im Kapitel 4.3 „Prüfung des Zertifikats beschrieben.“

3.4.2.1 Teil 1 Prüfergebnis und Informationen zum Zertifikat

3.4.2.1.1 Zeile "Prüfergebnis und Name des Zertifikatsinhabers"

In der ersten Zeile "wird von links nach rechts zunächst das kumulierte Prüfergebnis der Zertifikatsprüfung und der Name des Zertifikatsinhabers in einem grau unterlegten Kasten angezeigt.

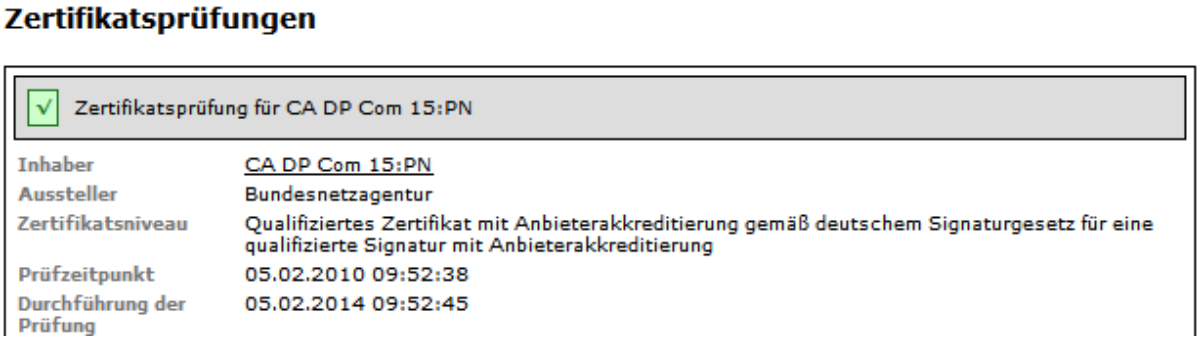


Abbildung 18: Teil 1 „Kumuliertes Prüfergebnis und Informationen zum Zertifikat“ bei der Prüfung eines einzelnen Zertifikats

3.4.2.1.2 Spalte "kumuliertes Prüfergebnis"

In der ersten Spalte wird das kumulierte Prüfergebnis der Zertifikatsprüfung in einem farbig unterlegten Kasten angezeigt. Folgende Status sind möglich:

- Grüner Kasten mit Haken
- Gelber Kasten mit Ausrufungszeichen
- Roter Kasten mit Kreuz:

Erläuterungen zu Grüner Kasten mit Haken:

Alle durchgeführten Einzelprüfungen besitzen den Status „grün“. Das Zertifikat wurde mit positivem Ergebnis überprüft. Bei einem qualifizierten Zertifikat gehört dazu auch die Prüfung der Eignung des zur Zertifikatssignatur verwendeten Signaturalgorithmus gemäß aktuellem Algorithmenkatalog der Bundesnetzagentur zum Signierzeitpunkt und zum Zeitpunkt der Durchführung der Prüfung. Damit ist der Zertifikatsinhaber sicher identifiziert und seine Authentizität bestätigt.

Dieses kumulierte Prüfergebnis ist immer nur eine Momentaufnahme zum Zeitpunkt der Durchführung der Prüfung. Bei einer „Nachprüfung“ (z.B. nach einigen Jahren) kann der Status auch auf "gelb" wechseln, weil das Trustcenter keine Sperrinformationen zum Signaturzertifikat mehr bereitstellt oder weil der bei der Signatur des Zertifikats verwendete Signaturalgorithmus nicht mehr für die Prüfung eines qualifizierten Zertifikats geeignet ist.

Erläuterungen zu Gelber Kasten mit Ausrufungszeichen:

Mindestens eine der Einzelprüfungen besitzt den Status "gelb" und damit kein eindeutiges Ergebnis. Einzelprüfungen mit dem finalen Status „rot“ gibt es nicht.

Der Status der Zertifikatsprüfung ist aus Empfängersicht unbestimmt. Die Ursache sollte in jedem Fall genauer analysiert werden. Häufig kommt dieses Prüfergebnis nämlich dadurch zustande, dass der Sperrstatus des Zertifikats nicht ermittelt werden konnte, weil z.B. der OCSP-Responders des Trustcenters temporär nicht erreichbar war. Im Teil "Prüfung des Zertifikats" hat die Einzelprüfung „Sperrstatus des Zertifikats“ in diesem Fall den Status "gelb". Eine "Nachprüfung" des Signaturzertifikats ist dann sinnvoll.

Der Status "gelb" kann aber auch endgültig sein, weil der bei der Signatur des qualifizierten Zertifikats verwendete Signaturalgorithmus nicht mehr für die Prüfung eines qualifizierten Zertifikats geeignet ist. Bereits erzeugte qualifizierte elektronische Zertifikatssignaturen bleiben zwar auch dann noch qualifiziert, wenn der zugrunde liegende Signaturalgorithmus nach

der Signaturerzeugung seine Eignung verloren hat, sie büßen jedoch graduell und sukzessive ihren Beweiswert ein.

Erläuterungen zu Roter Kasten mit Kreuz:

Mindestens eine der Einzelprüfungen besitzt den Status „rot“, d.h. war abschließend nicht erfolgreich. Damit konnte der Zertifikatsinhaber abschließend nicht sicher identifiziert werden.

Der Status „rot“ wird bei einem qualifizierten Zertifikat auch dann angezeigt, wenn der verwendete Signaturalgorithmus bereits zum Signierzeitpunkt des Zertifikats nicht mehr für eine qualifizierte Signatur geeignet war. Signaturen, die nach dem Schwachwerden des zugrundeliegenden Signaturalgorithmus erzeugt wurden, sind von vornherein keine qualifizierten Signaturen. Schon bei der Erzeugung der Signatur konnte nämlich nicht mehr sichergestellt werden, dass der Signaturschlüssel-Inhaber die alleinige Kontrolle über die Mittel zur Erzeugung der Signatur hatte.

Das kumulierte Prüfergebnis mit dem Status "rot" ist in der Regel final. Nur bei temporär gesperrten Zertifikaten (im europäischen Ausland möglich) ist ein Statuswechsel möglich.

3.4.2.1.3 Zeile "Name des Inhabers des Zertifikats"

In der Zeile Name des Inhabers des Zertifikats wird der Name des Inhabers des Zertifikats angezeigt. Dieses ist der Name des Zertifikatseigentümers aus dem Feld Inhaber [`subject`] des Zertifikats. Das Attribut "Name" [`CommonName`] besteht in der Regel aus dem Vor- und Nachnamen des Zertifikatsinhabers, kann aber auch ein Pseudonym enthalten.

3.4.2.1.4 Zeile "Aussteller des Zertifikats"

Angezeigt wird der Name des Ausstellers des geprüften Zertifikats. Dies ist der Organisationsname [Attribut: `OrganisationName`] des Ausstellers (CA, Trustcenters) aus dem Feld [`issuer`] des geprüften Zertifikats.

3.4.2.1.5 Zeile "Zertifikatsniveau"

Angezeigt wird das Niveau des Zertifikats. Dieses ist das Niveau, das erreicht wird, wenn das kumulierte Prüfergebnis in Ampelform den Status " Grüner Kasten mit Haken" erhalten hat.

Folgende Niveaus sind definiert:

- unbekannt
- gering
- Fortgeschrittenes Zertifikat gemäß einer einfachen Zertifizierungsrichtlinie
- Fortgeschrittenes Zertifikat gemäß einer normalisierten Zertifizierungsrichtlinie
- Fortgeschrittenes Zertifikat gemäß einer normalisierten Zertifizierungsrichtlinie mit privatem Schlüssel auf Smartcard
- Qualifiziertes Zertifikat gemäß der EU-Direktive 1999/93/EC für eine fortgeschrittene Signatur
- Qualifiziertes Zertifikat gemäß der EU-Direktive 1999/93/EC mit privatem Schlüssel auf Smartcard für eine qualifizierte Signatur
- Qualifiziertes Zertifikat gemäß deutschem Signaturgesetz für eine qualifizierte Signatur

- Qualifiziertes Zertifikat mit Anbieterakkreditierung gemäß deutschem Signaturgesetz für eine qualifizierte Signatur mit Anbieterakkreditierung

Die Bedeutung der einzelnen Zertifikatsniveaus wird ausführlich im Kapitel 6.1.4 beschrieben.

3.4.2.1.6 Zeile "Prüfzeitpunkt"

Angezeigt wird der Prüfzeitpunkt in der Form `TT.MM.JJJJ hh:mm:ss`. Der Prüfzeitpunkt ist der Zeitpunkt, zu dem der Sperrstatus des Zertifikats ermittelt wurde.

3.4.2.1.7 Zeile "Durchführung der Prüfung"

Angezeigt wird der Zeitpunkt der Durchführung der Prüfung in der Form `TT.MM.JJJJ hh:mm:ss`. Der Zeitpunkt der Durchführung der Prüfung ist der Zeitpunkt, zu dem das Zertifikat geprüft wurde.

3.4.2.2 Teil 2 „Prüfung des Zertifikats“

Im Teil 2 „Prüfung des Zertifikats“ folgen die Ergebnisse der Zertifikatsprüfung. Dazu gehören die Ergebnisse folgender Einzelprüfungen: Vertrauenswürdigkeit des Trustcenters (Issuer Trust), die mathematische Prüfung der Zertifikatssignaturen (Signature), der Sperrstatus des Zertifikats (Revocation Status) und der Gültigkeitszeitraum (Validity Interval). Bei einem qualifizierten Zertifikat eines deutschen Zertifizierungsdiensteanbieters wird zusätzlich das Ergebnis der Eignung des zur Zertifikatssignatur verwendeten Signaturalgorithmus angezeigt.

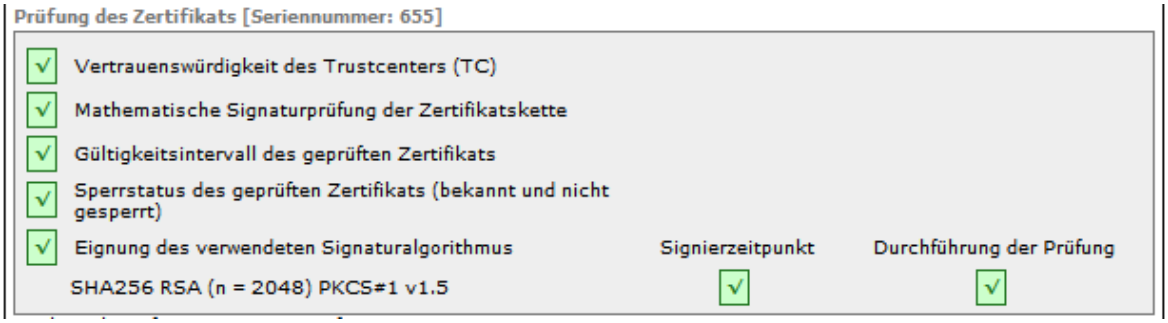


Abbildung 19: Teil 2 „Prüfung des Zertifikats

Dieser Teil entspricht vollständig dem allgemeinen Prüfprotokoll und wird ausführlich im Kapitel 4.3 „Prüfung des Zertifikats beschrieben.“

3.5 Gesamtprüfergebnis

Die Anzeige des Prüfprotokolls kann so konfiguriert angesprochen werden, dass ein Gesamtstatus über mehrere geprüfte Signaturen gebildet wird. In diesem Fall wird im Prüfprotokoll hinter der Bezeichnung "Gesamtprüfergebnis" das kumulierte Prüfergebnis in der Form eines Ampelstatus angezeigt. Die Anzeige ist für alle unterstützten Signaturformate identisch. Das Ergebnis bildet einen Gesamtstatus über die Prüfergebnisse der einzelnen Autorensignaturen.

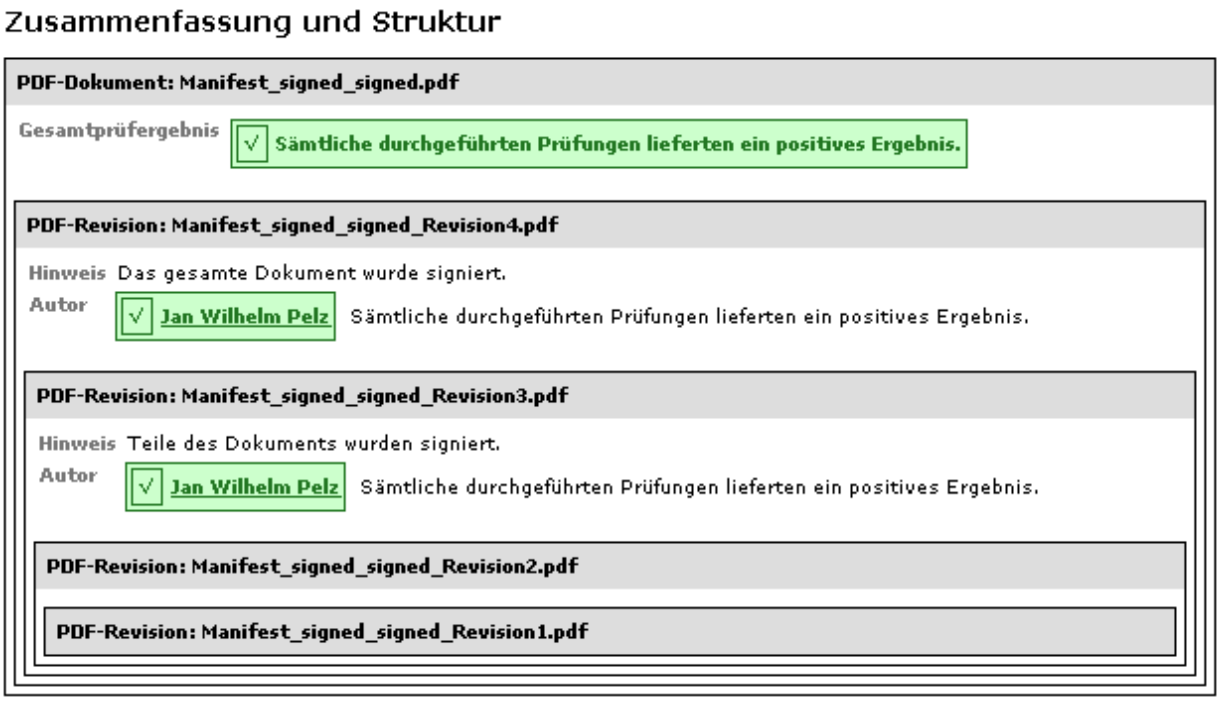


Abbildung 20: Bereich 1 Zusammenfassung und Struktur" bei PDF-Dokumenten mit mehreren Signaturen und der Ausgabe eines Gesamtstatus

Das Signaturniveau der einzelnen Signaturen wird beim Gesamtprüfergebnis nicht berücksichtigt. Gegebenenfalls wird auch über fortgeschrittene und qualifizierte elektronische Signaturen kumuliert. Die folgenden Status sind möglich:

- √ Grüner Kasten mit Haken
- ! Gelber Kasten mit Ausrufungszeichen
- X Roter Kasten mit Kreuz
- Grauer Kasten

Erläuterungen zu √ Grüner Kasten mit Haken:

Alle Signaturen wurden mit positivem Ergebnis (Ampelstatus "grün") geprüft. Als Erläuterung wird angezeigt: "Sämtliche durchgeführten Prüfungen lieferten ein positives Ergebnis."

Erläuterungen zu Gelber Kasten mit Ausrufungszeichen:

Mindestens ein Prüfergebnis bezogen auf eine Autorensignatur lieferte kein eindeutiges Ergebnis (Ampelstatus "gelb"). Als Erläuterung wird angezeigt: "Mindestens eine der Prüfungen lieferte kein eindeutiges Ergebnis."

Erläuterungen zu Roter Kasten mit Kreuz:

Mindestens ein Prüfergebnis bezogen auf eine Autorensignatur lieferte ein negatives Ergebnis (Ampelstatus "rot"). Als Erläuterung wird angezeigt: "Mindestens eine der durchgeführten Prüfungen lieferte ein negatives Ergebnis."

Erläuterungen zu Grauer Kasten:

Der Gesamtstatus konnte nicht ermittelt werden, weil keine Signaturen erkannt wurden. Dieser Status wird z.B. angezeigt, wenn ein nicht signiertes Dokument geprüft wurde. Als Erläuterung wird angezeigt: "Kein Gesamtstatus ermittelt, da unsigniert."

3.5.1 Fachliches Gesamtprüfergebnis bei PDF-Dokumenten

Bei der Prüfung von signierten PDF-Dokumenten gibt das Gesamtprüfergebnis aus fachlichen Erwägungen beim EGVP und beim Governikus Communicator lediglich den Prüfstatus der zuletzt angebrachten, also äußersten, Signatur an, wobei berücksichtigt wird, ob nach der zuletzt angebrachten Signatur noch mindestens eine weitere Revision erzeugt wurde, die nicht signiert wurde (Hinweis bei der signierten Revision "Teile des Dokuments wurden signiert."). In diesem Fall wird als Gesamtergebnis "rot" angezeigt mit der Meldung "die letzte Revision wurde nicht signiert".

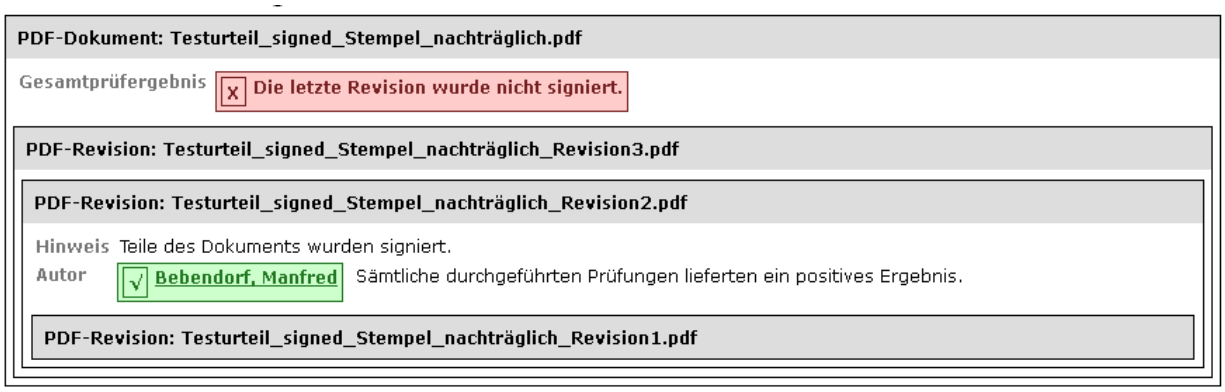


Abbildung 21: Bereich 1 "Zusammenfassung und Struktur" bei einem PDF-Dokument mit nicht signierter äußerer Revision

4 Bereich 2: "Signaturprüfungen"

In den folgenden Unterkapiteln wird der Bereich "Signaturprüfungen" des Prüfprotokolls erläutert. In diesem Bereich werden alle Prüfergebnisse, bezogen auf eine Signatur, angezeigt. Sollten mehrere Signaturen geprüft worden sein, wird für jede Signatur ein separater Block angezeigt.

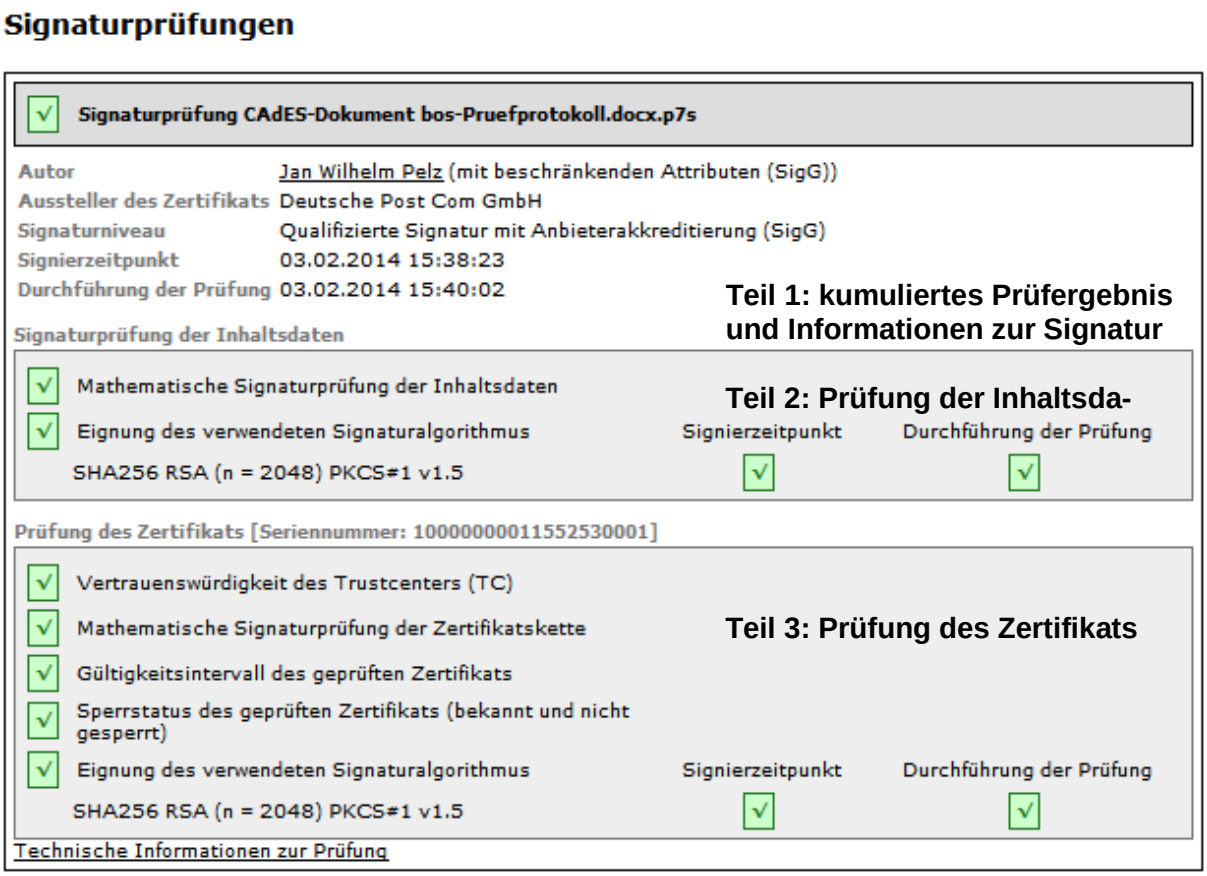


Abbildung 22: Bereich 2 "Signaturprüfungen des Prüfprotokolls"

Der Bereich "Signaturprüfungen" gliedert sich in drei Teile:

- Im Teil 1 wird das kumulierte Prüfergebnis mit allgemeinen Informationen zur Signatur angezeigt. Dazu gehört der Name des Signierenden, der Aussteller des Zertifikats, das Signaturniveau, der Signierzeitpunkt und der Zeitpunkt der Durchführung der Prüfung.
- Es folgt im Teil 2 "Signaturprüfung der Inhaltsdaten" die Anzeige des Ergebnisses der mathematischen Signaturprüfung. Bei einer qualifizierten Signatur, erzeugt mit einer Signaturkarte eines deutschen ZDAs, wird zusätzlich das Ergebnis der Eignung des zur Inhaltsdatensignatur verwendeten Signaturalgorithmus angezeigt.
- Im Teil 3 "Prüfung des Zertifikats" werden die Ergebnisse der Zertifikatsprüfung detailliert angezeigt. Dazu gehören die Ergebnisse folgender Einzelprüfungen: Vertrauenswürdigkeit des Trustcenters (Issuer Trust), die mathematische Prüfung der Zertifikatssignaturen (Signature), der Sperrstatus des Zertifikats (Revocation Status) und der Gültigkeitszeitraum (Validity Interval). Bei einem qualifizierten Zertifikat eines deutschen Zertifizierungsdiensteanbieters wird zusätzlich das Ergebnis der Eignung des zur Zertifikatssignatur verwendeten Signaturalgorithmus angezeigt.

4.1 Kumuliertes Prüfergebnis und Informationen zur Signatur

In den folgenden Unterkapiteln werden das kumulierte Prüfergebnis einer Signatur und die Anzeige der Kontextinformationen zur Signatur erläutert. Dazu gehören der Name des signierten Objekts, der Name des Signierenden, der Aussteller des Zertifikats, das Signaturniveau, der Signierzeitpunkt und der Zeitpunkt der Durchführung der Prüfung.

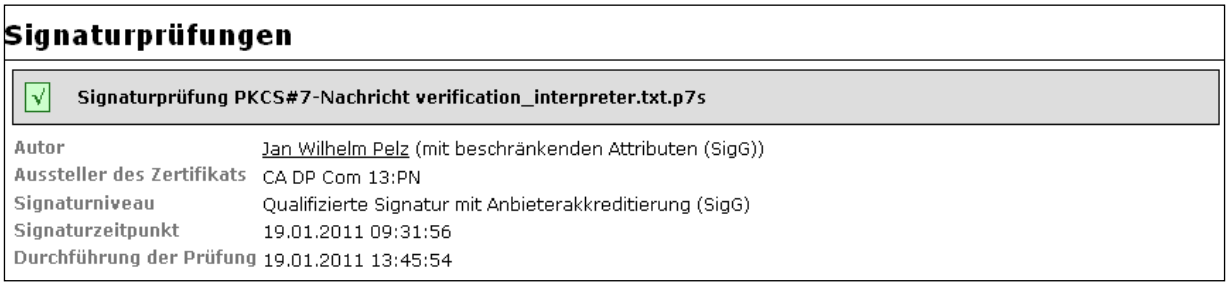


Abbildung 23: Teil 1 "Kumuliertes Prüfergebnis und Informationen zur Signatur"

4.1.1 Zeile "Prüfergebnis, Signaturformat und Dateiname/Container"

In der ersten grau unterlegten Zeile wird das kumulierte Prüfergebnis, bezogen auf die geprüfte Signatur, und der Name des signierten Objekts (signiertes Dokument, Revision, OSCI-Container) angezeigt.

4.1.1.1 Spalte "kumuliertes Prüfergebnis"

Die Zeile beginnt mit dem kumulierten Prüfergebnis in Ampelform. Die folgenden Status sind möglich:

- Grüner Kasten mit Haken
- Gelber Kasten mit Ausrufungszeichen
- Roter Kasten mit Kreuz

Erläuterungen zu Grüner Kasten mit Haken:

Alle durchgeführten Einzelprüfungen besitzen den Status „grün“. Die elektronische Signatur und das zugeordnete Signaturzertifikat wurden mit positivem Ergebnis überprüft. Bei einer qualifizierten Signatur (erstellt mit einer Signaturkarte eines deutschen ZDAs) gehört dazu auch die Prüfung der Eignung der verwendeten Signaturalgorithmen (Inhaltsdatensignatur, Zertifikatssignatur) gemäß aktuellem Algorithmenkatalog der Bundesnetzagentur zum Signierzeitpunkt und zum Zeitpunkt der Durchführung der Prüfung. Damit ist die Unverfälschtheit (Integrität der signierten Inhaltsdaten, der Nachricht, des Dokuments) sichergestellt, der Signierende sicher identifiziert und seine Authentizität bestätigt.

Dieses kumulierte Prüfergebnis ist immer nur eine Momentaufnahme zum Zeitpunkt der Durchführung der Prüfung. Bei einer „Nachprüfung“ (z.B. nach einigen Jahren) kann der Status auch auf "gelb" wechseln, weil das Trustcenter keine Sperrinformationen zum Signaturzertifikat mehr bereitstellt oder weil der bei einer qualifizierten Signatur verwendete Signaturalgorithmus nicht mehr für die Prüfung einer qualifizierten Signatur geeignet ist.

Erläuterungen zu Gelber Kasten mit Ausrufungszeichen:

Mindestens eine der Einzelprüfungen besitzt den Status "gelb" und damit kein eindeutiges Ergebnis. Einzelprüfungen mit dem finalen Status „rot“ gibt es nicht.

Der Status der Signaturprüfung ist aus Empfängersicht unbestimmt. Die Ursache sollte in jedem Fall genauer analysiert werden. Häufig kommt dieses Prüfergebnis nämlich dadurch zustande, dass der Sperrstatus des Zertifikats nicht ermittelt werden konnte, weil z.B. der OCSP-Responder des Trustcenters temporär nicht erreichbar war. Im Teil "Prüfung des Zertifikats" hat die Einzelprüfung „Sperrstatus des Zertifikats“ in diesem Fall den Status "gelb". Eine "Nachprüfung" des Signaturzertifikats ist dann sinnvoll.

Der Status "gelb" kann aber auch endgültig sein, weil z. B. der Signierzeitpunkt nicht ermittelt werden konnte (In diesem Fall kann dann auch der Sperrstatus des Zertifikats nicht ermittelt werden) oder weil der bei einer qualifizierten Signatur verwendete Signaturalgorithmus nicht mehr für die Prüfung einer qualifizierten Signatur (Inhaltsdatensignatur, Zertifikatssignatur) geeignet ist. Bereits erzeugte qualifizierte elektronische Signaturen bleiben zwar auch dann noch qualifiziert, wenn der zugrunde liegende Signaturalgorithmus nach der Signaturerzeugung seine Eignung verloren hat, sie büßen jedoch graduell und sukzessive ihren Beweiswert ein. In der Spalte Erläuterungen wird in diesem Fall immer der folgende Warnhinweis ausgegeben:

- Qualifizierte elektronische Signatur (SigG). Es wurde aber ein Algorithmus verwendet, der zum Zeitpunkt der Durchführung der Prüfung nicht mehr für eine qualifizierte Signatur geeignet war.

Der Status "gelb" wird bei einer qualifizierten Signatur auch dann angezeigt, wenn die Eignung des verwendeten Signaturalgorithmus nicht ermittelt werden konnte. In der Spalte Erläuterungen wird in diesem Fall immer der folgende Warnhinweis ausgegeben:

- Die Eignung eines Algorithmus konnte nicht ermittelt werden.

Welche der Einzelprüfungen den Status „gelb“ besitzen, kann der detaillierten Einzelergebnisdarstellung im Teil 2 "Signaturprüfung der Inhaltsdaten" und Teil 3 "Prüfung des Zertifikats" entnommen werden. Eine Erläuterung des "gelben" Einzelprüfergebnisses befindet sich am Ende des Bereichs unter der Zeile "Erläuterungen".

Erläuterungen zu Roter Kasten mit Kreuz:

Mindestens eine der Einzelprüfungen besitzt den Status „rot“, d.h. war abschließend nicht erfolgreich. Damit ist entweder die Unverfälschtheit der Inhaltsdaten (Integrität der Daten) nicht sichergestellt oder es konnte die signierende Person abschließend nicht sicher identifiziert werden.

Der Status „rot“ wird bei einer qualifizierten Signatur auch dann angezeigt, wenn der verwendete Signaturalgorithmus bereits zum Signierzeitpunkt nicht mehr für eine qualifizierte Signatur geeignet war. Signaturen, die nach dem Schwachwerden des zugrundeliegenden Signaturalgorithmus erzeugt wurden, sind von vornherein keine qualifizierten Signaturen. Schon bei der Erzeugung der Signatur konnte nämlich nicht mehr sichergestellt werden, dass der Signaturschlüssel-Inhaber die alleinige Kontrolle über die Mittel zur Erzeugung der Signatur hatte. In der Spalte Erläuterungen wird in diesem Fall wird immer die folgende Meldung ausgegeben:

- Fortgeschrittene Signatur und keine qualifizierte Signatur (SigG). Es wurde ein Algorithmus verwendet, der zum Signierzeitpunkt nicht mehr für eine qualifizierte Signatur geeignet war.

Das kumulierte Prüfergebnis mit dem Status "rot" ist in der Regel final. Nur bei temporär gesperrten Zertifikaten (im europäischen Ausland möglich) ist ein Statuswechsel möglich.

Welche der Einzelprüfungen den Status „rot“ besitzen, kann der detaillierten Einzelergebnisdarstellung im Teil 2 "Signaturprüfung der Inhaltsdaten" und Teil 3 "Prüfung des Zertifikats" entnommen werden. Eine Erläuterung des "roten" Einzelprüfergebnisses befindet sich am Ende des Bereichs unter der Zeile "Erläuterungen".

4.1.1.2 Spalte "Signaturformat und Name des signierten Objektes"

Angezeigt werden hinter dem kumulierten Prüfergebnis das signierte Dokumentenformat und der Name des signierten Dokuments. Der Name des Signaturformats entspricht der Angabe des Signaturformats in der Zeile "Dateiname" im Bereich 1 "Zusammenfassung und Struktur".

4.1.2 Zeile "Autor"

Angezeigt wird der Name des Signierenden. Dies ist das Attribut "Name des Zertifikatseigentümers" aus dem Feld Inhaber [`subject`] des Signaturzertifikats. Das Attribut Name [`CommonName`] besteht in der Regel aus dem Vor- und Nachnamen des Zertifikatsinhabers, kann aber auch ein Pseudonym enthalten.

4.1.2.1 Qualifiziertes Zertifikat gemäß CommonPKI-Spezifikation

Sollte es sich um ein qualifiziertes Zertifikat eines deutschen ZDAs handeln, ist der Name der im Identifikationsdokument (Personalausweis oder Reisepass) angegebene Vor- und Nachname des Zertifikatsinhabers. Durch die Angabe ":PN" hinter dem Namen wird bei qualifizierten Signaturzertifikaten deutscher Zertifizierungsdiensteanbieter (die konform zur CommonPKI-Spezifikation sind) angezeigt, dass es sich um ein Pseudonym handelt.

Die CommonPKI-Spezifikation Version 2.0, beschreibt im SigG-Profil eine Reihe von Zertifikatserweiterungen, die die Verwendung eines qualifizierten Signaturzertifikats beschränken, erweitern oder präzisieren. Damit werden die speziellen Anforderungen umgesetzt, die sich aus dem deutschen Signaturgesetz für qualifizierte Zertifikate ergeben (siehe § 5 SigG).

In diesem Fall wird in Klammern hinter dem Namen des Signierenden der Hinweis "mit beschränkenden Attributen (SigG)" angezeigt (siehe Abbildung 25).

4.1.3 Zeile "Aussteller des Zertifikats"

Angezeigt wird der Name des Ausstellers des geprüften Zertifikats. Dies ist der Organisationsname [Attribut: `OrganisationName`] des Ausstellers (CA, Trustcenters) aus dem Feld [`issuer`] des geprüften Zertifikats.

4.1.3.1 Qualifiziertes Zertifikat gemäß Common PKI-Spezifikation

Das Attribut Organisationsname [Attribut `organizationName`] ist bei einem qualifizierten Zertifikat eines deutschen ZDAs gemäß CommonPKI-Spezifikation der aus dem CA-Zertifikat des ZDA übernommene Organisationsname des Inhabers des CA-Zertifikats.

4.1.4 Zeile Ort der Signatur (nur bei *AdES-Dokumenten)

In signierten Dokumenten der *AdES-Formate kann durch den Signierenden angegeben werden, in welchem Land die Signatur angebracht wurde. Folgende Angaben sind möglich:

- Land [countryName]
- Ort [localityName]
- Postadresse [postaladdress]

4.1.5 Zeile "Signaturgrund" (nur bei *AdES-Dokumenten)

In signierten Dokumenten der *AdES-Formate besteht die Möglichkeit, dass der Signierende den Grund für die Signatur angibt. Folgende Angaben sind möglich und werden angezeigt:

- Nachweis der Quelle: Der Signierende gibt an, das Dokument erstellt, genehmigt und versendet zu haben.
- Nachweis des Empfangs: Der Signierende gibt an, das Dokument erhalten zu haben.
- Nachweis der Auslieferung: Ein Dienst gibt an, er habe das Dokument dem Empfänger in dessen Verfügungsbereich übermittelt.
- Nachweis des Versands: Der Sender gibt an, dass das Dokument versendet wurde (aber nicht notwendigerweise durch den Sender erstellt wurde).
- Nachweis der Bestätigung: Der Signierende gibt an, er habe den Inhalt des Dokuments genehmigt.
- Nachweis der Erzeugung: Der Signierende gibt an, er habe das Dokument erstellt (aber nicht notwendigerweise genehmigt und/oder gesendet).

Signaturort	Steiermark, 8010, Graz, Austria
Signaturgrund	Nachweis der Quelle
Signaturrichtlinie	http://xades-portal.etsi.org/protected/TestCases/Data/testPolicyBase64.txt

Abbildung 24: Zeilen "Signaturort, Signaturgrund und Signaturrichtlinie" bei * AdES-Dokumenten

4.1.6 Zeile "Signaturrichtlinie" (nur bei *AdES-Dokumenten)

In signierten Dokumenten der *AdES-Formate kann eine Signaturrichtlinie hinterlegt werden. Damit gibt der Signierende an, welche Rolle und Verpflichtungen er mit der Signatur eingehen möchte und dass er damit Anforderungen an die Signaturprüfung stellt.

Ist eine Signaturrichtlinie vorhanden, wird diese angezeigt, hat aber keine Auswirkungen auf die Prüfung. In diesem Fall wird im Strukturbereich des Prüfprotokolls der folgende Hinweis angezeigt:

- Es ist eine Signaturrichtlinie vorhanden, die nicht berücksichtigt wird.

4.1.7 Zeile "Signaturniveau"

Angezeigt wird das intendierte Niveau der elektronischen Signatur. Dieses ist das Niveau, das erreicht wird, wenn das kumulierte Prüfergebnis in Ampelform den Status "√ Grüner Kasten mit Haken" erhalten hat.

Folgende Niveaus sind definiert:

- Fortgeschrittene Signatur
- Fortgeschrittene Signatur mit qualifiziertem Zertifikat (EU)
- Qualifizierte Signatur (EU)

- Qualifizierte Signatur (SigG)
- Qualifizierte Signatur mit Anbieterakkreditierung (SigG)

Erläuterungen zum Signaturniveau

- Fortgeschrittene Signatur

Fortgeschrittene elektronische Signatur, die die Anforderungen gemäß Artikel 2 Absatz 2 Richtlinie 1999/93/EG erfüllt.

- fortgeschrittene Signatur mit qualifiziertem Zertifikat (EU)

Eine von einem qualifizierten Zertifikat unterstützte fortgeschrittene elektronische Signatur bezeichnet eine elektronische Signatur, die die Erfordernisse einer fortgeschrittenen elektronischen Signatur erfüllt und von einem der Definition in Artikel 2 Absatz 10 der Richtlinie 1999/93/EG entsprechenden qualifizierten Zertifikat (QZ) unterstützt wird.

- Qualifizierte Signatur (EU)

Die qualifizierte elektronische Signatur ist in der Richtlinie 1999/93/EG zwar nicht explizit als Begriff definiert. Es ist aber die Auffassung der EU-Kommission, dass eine qualifizierte elektronische Signatur auf einer fortgeschrittenen Signatur mit qualifiziertem Zertifikat basiert, die von einer sicheren Signaturerstellungseinheit (zertifizierte Smartcard) erstellt wird.

- Qualifizierte Signatur (SigG)

Qualifizierte Signatur konform zur Richtlinie 1999/93/EG, basierend auf den Anforderungen des deutschen Signaturgesetzes (SigG). Das Zertifikat wird herausgegeben von einem in Deutschland gemäß den Anforderungen des SigG angezeigten Zertifizierungsdiensteanbieter.

- Qualifizierte Signatur mit Anbieterakkreditierung (SigG)

Qualifizierte Signatur gemäß SigG. Das Zertifikat wird herausgegeben von einem in Deutschland gemäß den Anforderungen des SigG akkreditierten Zertifizierungsdiensteanbieter.

4.1.7.1 Herkunft der Signaturniveauinformationen

Das intendierte Niveau wird der Antwort des OCSP/CRL-Relays (XKMS-Response) entnommen und nicht dem geprüften Zertifikat. Das OCSP/CRL-Relay übernimmt den Niveaueintrag aus der Standardkonfiguration. Dort ist neben den Root- und Ausstellerzertifikaten und technischen Daten zur Verbindungskonfiguration auch für jede CA das Signaturniveau hinterlegt.

4.1.7.1.1 Qualifizierte Signatur (Signaturkarte deutscher ZDA)

Die Informationen wurden aus der sogenannten nationalen vertrauenswürdigen Liste (TSL) in die Standardkonfiguration übernommen. Diese TSL wird von der Bundesnetzagentur zum Download bereitgestellt und enthält neben allen (aktuell verwendeten) CA- und Robot-Zertifikaten auch Informationen zur Dienstequalität der ZDAs.

Der geltende Rechtsrahmen für die vorliegende vertrauenswürdige Liste für Deutschland ist die Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen und ihre Umsetzung in deutsches Recht und die Entscheidung der Kommission vom 16. Oktober 2009 über Maßnahmen zur Erleichterung der Nutzung elektronischer Verfahren über "einheitliche Ansprechpartner" gemäß der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates über Dienstleistungen im Binnenmarkt.

4.1.7.1.2 Qualifizierte Signatur (Signaturkarte aus dem EU-Ausland)

Ab der Version 3.5.3 des OCSP/CRL-Relays werden Prüfanfragen für qualifizierte Zertifikate aus dem EU-Ausland über ein XKMS-Gateway an sogenannte XKMS-Responder in den EU-Mitgliedsstaaten weiterleitet. Diese XKMS-Responder prüfen das Zertifikat und ermitteln auch den Sperrstatus des Zertifikats gegen das Trustcenter, das das Zertifikat ausgestellt hat. Der angefragte XKMS-Responder sendet seine XKMS-Response an das anfragende OCSP/CRL-Relay zurück.

4.1.8 Zeile "Signierzeitpunkt"

Angezeigt wird der Signierzeitpunkt in der Form `TT.MM.JJJJ hh:mm:ss`. Der Signierzeitpunkt ist der Zeitpunkt, zu dem die Signatur erzeugt oder angebracht wurde. Dieses ist in der Regel die lokale Clientzeit des PCs, auf dem die Signaturanwendungskomponente installiert ist, die die Signaturanbringung unterstützt hat. Kann der Signaturzeitpunkt nicht ermittelt werden, wird statt des Signaturzeitpunktes der Hinweis "k. A." für "keine Angabe" angezeigt. In diesem Fall kann zwar noch eine mathematische Signaturprüfung durchgeführt werden, nicht jedoch der Sperrstatus des Signaturzertifikats überprüft werden. Dieser Umstand führt immer zu einem finalen Gelbstatus im kumulierten Gesamtprüfergebnis mit der Meldung "Es liegt kein Signierzeitpunkt vor".

4.1.9 Zeile "Durchführung der Prüfung"

Angezeigt wird der Zeitpunkt der Durchführung der Prüfung in der Form `TT.MM.JJJJ hh:mm:ss`. Der Zeitpunkt der Durchführung der Prüfung ist der Zeitpunkt, zu dem die Signatur geprüft wurde (Mathematische Signaturprüfung der Inhaltsdaten, Eignung der verwendeten Algorithmen und Zertifikatsprüfung).

4.1.10 Zeile "Aussteller des Attributzertifikats" (nur bei Attributzertifikaten)

Ist zu einem Signaturzertifikat ein Attributzertifikat vorhanden, wird der Aussteller des Attributzertifikats angezeigt. Dies ist der Organisationsname [Attribut: `OrganisationName`] des Ausstellers (CA, Trustcenters) aus dem Feld [`issuer`] und in der Regel identisch mit dem Organisationsnamen des Ausstellers des Basiszertifikats.

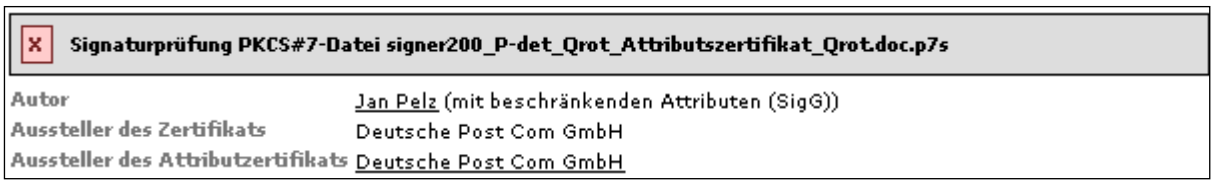


Abbildung 25: Zeile "Aussteller des Attributzertifikats"

4.2 Signaturprüfung der Inhaltsdaten

Im Teil "Signaturprüfung der Inhaltsdaten" werden das Ergebnis der mathematischen Signaturprüfung und die zur Signatur verwendeten Algorithmen angezeigt. Bei einer qualifizierten Signatur, erzeugt mit einer Signaturkarte eines deutschen Zertifizierungsdiensteanbieters, wird zusätzlich auch das Ergebnis der Prüfung der Eignung der verwendeten Algorithmen für die Inhaltsdatensignatur angezeigt.

4.2.1 Zeile "Mathematische Signaturprüfung der Inhaltsdaten"

Abbildung 26: Bereich 2 Teil 2 "Signaturprüfung der Inhaltsdaten"

In der Zeile "Mathematische Signaturprüfung" wird das Ergebnis der mathematischen Signaturprüfung angezeigt. Die folgenden Status sind möglich:

- Grüner Kasten mit Haken
- Gelber Kasten mit Ausrufungszeichen
- Roter Kasten mit Kreuz

Erläuterungen zu Grüner Kasten mit Haken:

Die Signatur konnte erfolgreich mathematisch mit dem Signaturprüfschlüssel aus dem Signaturzertifikat mit dem unter der Zeile „Eignung des verwendeten Signaturalgorithmus“ (Beschreibung siehe Kapitel 4.2.2) angegebenen Verfahren (Signaturalgorithmus) geprüft werden. Der signierte Inhalt des Dokumentes wurde nach der Signatur nicht verändert, die Integrität ist gegeben.

Erläuterungen zu Gelber Kasten mit Ausrufungszeichen:

Die mathematische Signaturprüfung konnte nicht durchgeführt werden oder es ist ein anderer Fehler aufgetreten, der die Prüfung beeinträchtigt. Folgende Fehler können auftreten und werden im unteren Bereich der Signaturprüfung unter der Zeile Erläuterung angezeigt:

- Die Integrität der Signatur konnte nicht geprüft werden, da das Signaturzertifikat nicht vorhanden ist.

Hinweis: Im Signaturzertifikat befindet sich der Signaturprüfschlüssel. Liegt dieser nicht vor, kann die Signatur mathematisch nicht geprüft werden.

- Die Integrität der Signatur konnte nicht geprüft werden, da keine Inhaltsdaten vorliegen.
- Die Integrität der Signatur konnte nicht geprüft werden, da der Algorithmus nicht implementiert ist.
- Es wurden nur Teile des Dokuments signiert (nur bei PDF-Inline-Signaturen).
- Eine Signaturprüfung ist nicht möglich, da eine unzulässige XPATH-Transformation

verwendet wurde (nur bei XAdES-Signaturen).

- Eine Signaturprüfung ist nicht möglich, da eine unzulässige XSLT-Transformation verwendet wurde (nur bei XAdES-Signaturen).
- Eine Signaturprüfung ist nicht möglich, da ein unbekannter Kanonisierungsalgorithmus verwendet wurde. (nur bei XAdES-Signaturen)

Erläuterungen zu Roter Kasten mit Kreuz:

Die mathematische Signaturprüfung mit dem Signaturprüfschlüssel aus dem Signaturzertifikat war nicht erfolgreich. Die Integrität der Inhaltsdaten ist nicht gegeben.

Folgende Fehler können auftreten und werden im unteren Bereich der Signaturprüfung unter der Zeile Erläuterung angezeigt:

- Die Inhaltsdaten wurden nach Anbringung der Signatur manipuliert.
- Die Signatur enthält illegalen Inhalt (nur bei PDF-Inline-Signaturen).
- Die Signatur der OSCI-Nachricht ist inkorrekt (nur bei OSCI-Nachrichten).

4.2.2 Zeile "Eignung des verwendeten Signaturalgorithmus"

Die Eignung des für die qualifizierte Signatur der Inhaltsdaten verwendeten Signaturalgorithmus wird auf Basis des von der Bundesnetzagentur veröffentlichten Algorithmenkatalogs

- zum Signierzeitpunkt und
- zum Zeitpunkt der Durchführung der Prüfung

ermittelt.

Die Anforderung ergibt sich aus dem § 2 Nr. 11 b des Signaturgesetzes, der besagt, dass Signaturanwendungskomponenten auch dann eine zuverlässige Prüfung und zutreffende Anzeige des Prüfergebnisses gewährleisten müssen, wenn die geprüfte Signatur auf einem Signaturalgorithmus, der gemäß aktuellem Algorithmenkatalog als nicht mehr geeignet und damit als nicht mehr hinreichend sicher eingestuft ist.

Die Prüfung der Eignung des verwendeten Signaturalgorithmus wird nur bei einer qualifizierten Signatur, erzeugt mit einer Signaturkarte eines deutschen ZDA, durchgeführt. In allen anderen Fällen besitzt das kumulierte Prüfergebnis den Status "grau" (keine Prüfung durchgeführt).

In der ersten Spalte der Zeile " Eignung des verwendeten Signaturalgorithmus" wird das kumulierte Prüfergebnis angezeigt. Die folgenden Status sind möglich:

- Grüner Kasten mit Haken
- Gelber Kasten mit Ausrufungszeichen
- Roter Kasten mit Kreuz
- Grauer Kasten

Erläuterungen zu Grüner Kasten mit Haken:

Der verwendete Signaturalgorithmus war zum Signierzeitpunkt für die Erzeugung einer qualifizierten elektronischen Signatur und zum Zeitpunkt der Durchführung der Prüfung für die Prüfung einer qualifizierten elektronischen Signatur gemäß aktuellem Algorithmenkatalog geeignet.

Abbildung 27: Ergebnis der Eignungsprüfung bei einem Algorithmus, der zum Signierzeitpunkt und zum Zeitpunkt der Durchführung der Prüfung für eine QES geeignet war

Erläuterungen zu ! Gelber Kasten mit Ausrufungszeichen:

Der verwendete Signaturalgorithmus war zum Zeitpunkt der Durchführung der Prüfung gemäß aktuellem Algorithmenkatalog nicht mehr für die Prüfung einer qualifizierten elektronischen Signatur geeignet. Zum Zeitpunkt der Signaturanbringung (Signierzeitpunkt) war die Eignung jedoch noch gegeben.

Abbildung 28: Ergebnis der Eignungsprüfung bei einem Algorithmus, der nur zum Zeitpunkt der Durchführung der Prüfung nicht mehr für die Prüfung einer QES geeignet war

Bereits erzeugte elektronische Signaturen bleiben auch dann noch qualifiziert, wenn der zugrundeliegende Algorithmus nach der Signatur seine Eignung verloren hat. Sie büßen jedoch graduell und sukzessive ihren Beweiswert ein. Das Prüfergebnis "gelb" wirkt sich auf das kumulierte Ergebnis der Signaturprüfung aus und ist in diesem Fall final. Am Ende des Bereichs "Signaturprüfungen" wird unter der Zeile "Erläuterungen" der folgende Warnhinweis ausgegeben:

- Qualifizierte elektronische Signatur (SigG). Es wurde aber ein Algorithmus verwendet, der zum Zeitpunkt der Durchführung der Prüfung nicht mehr für eine qualifizierte Signatur geeignet war.

Erläuterungen zu X Roter Kasten mit Kreuz:

Abbildung 29: Ergebnis der Eignungsprüfung bei einem Algorithmus, der schon zum Signierzeitpunkt nicht mehr für eine QES geeignet war

Der verwendete Signaturalgorithmus war bereits zum Signierzeitpunkt für die Erzeugung einer qualifizierten elektronischen Signatur nicht (mehr) geeignet. Signaturen, die nach dem Schwachwerden des zugrundeliegenden Signaturalgorithmus erzeugt wurden, sind von vornherein keine qualifizierten Signaturen. Schon bei der Erzeugung der Signatur konnte nämlich nicht mehr sichergestellt werden, dass der Signaturschlüssel-Inhaber die alleinige Kontrolle über die Mittel zur Erzeugung der Signatur hatte. Das Prüfergebnis "rot" wirkt sich auf das kumulierte Ergebnis der Signaturprüfung aus und ist in diesem Fall final. Am Ende des Bereichs "Signaturprüfungen" wird unter der Zeile "Erläuterungen" der folgende Warnhinweis ausgegeben:

- Fortgeschrittene Signatur und keine qualifizierte Signatur (SigG). Es wurde ein Algorithmus verwendet, der zum Signierzeitpunkt nicht mehr für eine qualifizierte Signatur geeignet war.

Erläuterungen zu Grauer Kasten:

Eine Prüfung der Eignung des verwendeten Signaturalgorithmus wurde nicht durchgeführt.

Abbildung 30: Eignungsprüfung des verwendeten Signaturalgorithmus bei einer fortgeschrittenen Signatur

4.2.2.1 Zeile "Angabe des verwendeten Signaturalgorithmus"

Unterhalb der Zeile mit dem angezeigten kumulierten Prüfergebnis wird der Name des verwendeten Signaturalgorithmus angezeigt.

Der angezeigte Name setzt sich wie folgt zusammen (von links nach rechts):

a) Bei einer RSA-Signatur:
   - Verwendeter Hashalgorithmus
   - RSA-Algorithmus mit Länge des Parameters n in Klammern
   - verwendetes Signaturschema (PKCS#1 v1.5 oder PKCS#1 v2.1 [PSS])

b) Bei einer DSA/ECDSA-Signatur:
   - verwendeter Hashalgorithmus
   - DSA/ECDSA-Algorithmus mit Länge der Parameter p (nur ECDSA) und q jeweils in Klammern

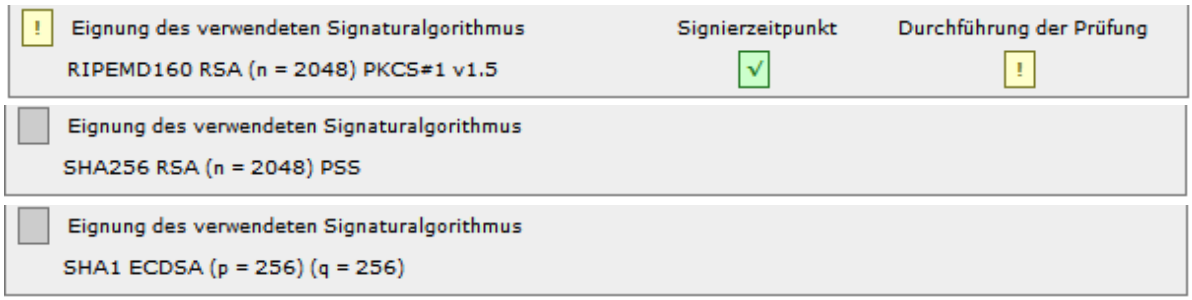


Abbildung 31: Anzeige des verwendeten Signaturalgorithmus

Hinweis: Am Ende des Prüfprotokolls befindet sich eine Liste aller geprüften Signaturalgorithmen. Angezeigt werden dort der Name des Teil-Algorithmus und das Datum des Ablaufs der Eignung gemäß aktuellem Algorithmenkatalog der Bundesnetzagentur (BNetzA) in Abhängigkeit vom Verwendungszweck (Anbringung einer Inhaltsdatensignatur, Prüfung einer Inhaltsdatensignatur, Anbringung einer Zertifikatssignatur, Prüfung einer Zertifikatssignatur).

4.2.2.2 Spalte Einzelprüfergebnis „Signierzeitpunkt“

In der Spalte „Signierzeitpunkt“ wird unter der Überschrift das Ergebnis der Eignungsprüfung des zur Signatur der Inhaltsdaten verwendeten Signaturalgorithmus zum Zeitpunkt der Signaturanbringung (Signierzeitpunkt) angezeigt.

Abbildung 32: Ergebnis der Eignungsprüfung des verwendeten Signaturalgorithmus einer Inhaltsdatensignatur zum Signierzeitpunkt

Die Eignung des verwendeten Signaturalgorithmus zum Zeitpunkt der Signaturanbringung (Signierzeitpunkt) wird nur bei einer qualifizierten Signatur, erzeugt mit einer Signaturkarte eines deutschen ZDA, ermittelt. In allen anderen Fällen besitzt das Prüfergebnis den Status "grau" (keine Prüfung durchgeführt). Folgende Status sind möglich:

- **grüner Kasten mit Haken**: Der Signaturalgorithmus war zum Signierzeitpunkt gemäß aktuellem Algorithmenkatalog für die Erzeugung einer qualifizierten elektronischen Signatur (Inhaltsdatensignatur) geeignet.
- **roter Kasten mit Kreuz**: Der Signaturalgorithmus war bereits zum Signierzeitpunkt gemäß aktuellem Algorithmenkatalog für die Erzeugung einer qualifizierten elektronischen Signatur (Inhaltsdatensignatur) nicht (mehr) geeignet.

4.2.2.3 Spalte Einzelprüfergebnis „Durchführung der Prüfung“

In der Spalte „Durchführung der Prüfung“ wird unter der Überschrift das Ergebnis der Eignungsprüfung des verwendeten Signaturalgorithmus zum Zeitpunkt der Durchführung der Signaturprüfung angezeigt.

Abbildung 33: Ergebnis der Eignungsprüfung des verwendeten Signaturalgorithmus einer Inhaltsdatensignatur zum Zeitpunkt der Durchführung der Signaturprüfung

Die Eignung des verwendeten Signaturalgorithmus zum Zeitpunkt der Durchführung der Prüfung wird nur bei einer qualifizierten Signatur, erzeugt mit einer Signaturkarte eines deutschen ZDA, ermittelt. In allen anderen Fällen besitzt das Prüfergebnis den Status "grau" (keine Prüfung durchgeführt). Folgende Status sind möglich:

- **grüner Kasten mit Haken**: Der Signaturalgorithmus war zum Zeitpunkt der Durchführung der Prüfung gemäß aktuellem Algorithmenkatalog für die Prüfung einer qualifizierten elektronischen Signatur (Inhaltsdatensignatur) geeignet.
- **Gelber Kasten mit Ausrufungszeichen:** Der verwendete Signaturalgorithmus war zum Zeitpunkt der Durchführung der Prüfung gemäß aktuellem Algorithmenkatalog nicht mehr für die Prüfung einer qualifizierten elektronischen Signatur geeignet. Zum Zeitpunkt der Signaturanbringung (Signierzeitpunkt) war die Eignung jedoch noch gegeben.
- **roter Kasten mit Kreuz**: Der Signaturalgorithmus war bereits zum Signierzeitpunkt gemäß aktuellem Algorithmenkatalog für die Erzeugung einer qualifizierten elektronischen Signatur (Inhaltsdatensignatur) nicht (mehr) geeignet. Signaturen, die nach dem Schwachwerden des zugrundeliegenden Signaturalgorithmus erzeugt wurden, sind von vornherein keine qualifizierten Signaturen. Daher wird auch hier ein rotes Prüfergebnis angezeigt.

4.2.2.4 Auswirkungen auf das Gesamtprüfergebnis

Unter der Bedingung, dass alle anderen Einzelprüfungen den Ampelstatus "grün" aufweisen, wirkt sich die Eignungsprüfung wie folgt auf das kumulierte Prüfergebnis einer qualifizierten elektronischen Signatur aus:

Eignung des Signaturalgorithmus (Inhaltsdatensignatur)		Kumuliertes Prüfergebnis der Eignungs-prüfung	Qualifizierte elektronische Signatur (QES)?
Signier-zeitpunkt	Zeitpunkt der Durchführung der Prüfung		
√ grün (ja)	√ grün (ja)	√ grün	QES
√ grün (ja)	! gelb (nein)	! gelb	QES mit einschränkendem Hinweis
x rot (nein)	x rot (nein)	x rot	keine QES

Tabelle 1: Ermittlung des kumulierten Prüfergebnisses

Alle geprüften Signaturalgorithmen werden am Ende des Prüfprotokolls tabellarisch zusammengefasst aufgeführt. Angezeigt werden der Name des Teil-Algorithmus, das Datum des Ablaufs der Eignung gemäß aktuellem Algorithmenkatalog der Bundesnetzagentur (BNetzA) in Abhängigkeit vom Verwendungszeck (Anbringung einer Inhaltsdatensignatur, Prüfung einer Inhaltsdatensignatur, Anbringung einer Zertifikatssignatur, Prüfung einer Zertifikatssignatur).

Auszug aus dem Algorithmenkatalog veröffentlicht von der Bundesnetzagentur am 27.03.2013

Algorithmusname	Typ	geeignet für	bis
PKCS#1 v1.5	Paddingalgorithmus	Anbringung von Zertifikatssignaturen	31.12.2017
PKCS#1 v1.5	Paddingalgorithmus	Anbringung von Inhaltsdatensignaturen	31.12.2015
PKCS#1 v1.5	Paddingalgorithmus	Prüfung von Zertifikats- und Inhaltsdatensignaturen	31.12.2019
RSA (n = 2048)	Schlüsselalgorithmus	Anbringung/Prüfung von Zertifikats- und Inhaltsdatensignaturen	31.12.2019
SHA256	Hashalgorithmus	Anbringung/Prüfung von Zertifikats- und Inhaltsdatensignaturen	31.12.2019

Abbildung 34: Anzeige der verwendeten Algorithmen für eine qualifizierte elektronische Signatur (SigG) mit Datum des Ablaufs der Eignung in Abhängigkeit vom Verwendungszeck

4.3 Prüfung des Zertifikats

Im dritten Teil "Prüfung des Zertifikats" des Bereichs Signaturprüfungen werden die Prüfergebnisse der Zertifikatsprüfung angezeigt. Dieses sind folgende Einzelprüfergebnisse:

- Vertrauenswürdigkeit des Trustcenters (Issuer Trust),
- Mathematische Prüfung der Zertifikatskette (Signature),
- Gültigkeitsintervall des geprüften Zertifikats (Validity Interval),
- Sperrstatus des geprüften Zertifikats (Revocation Status) und
- Eignung des verwendeten Signaturalgorithmus (nur bei einem qualifizierten Zertifikat).

Bei einem qualifizierten Signaturzertifikat, ausgestellt und qualifiziert signiert von einem deutschen ZDA, wird die Anzeige um das Ergebnis der Eignungsprüfung der verwendeten Algorithmen zum Signierzeitpunkt und zum Zeitpunkt der Durchführung der Prüfung ergänzt.

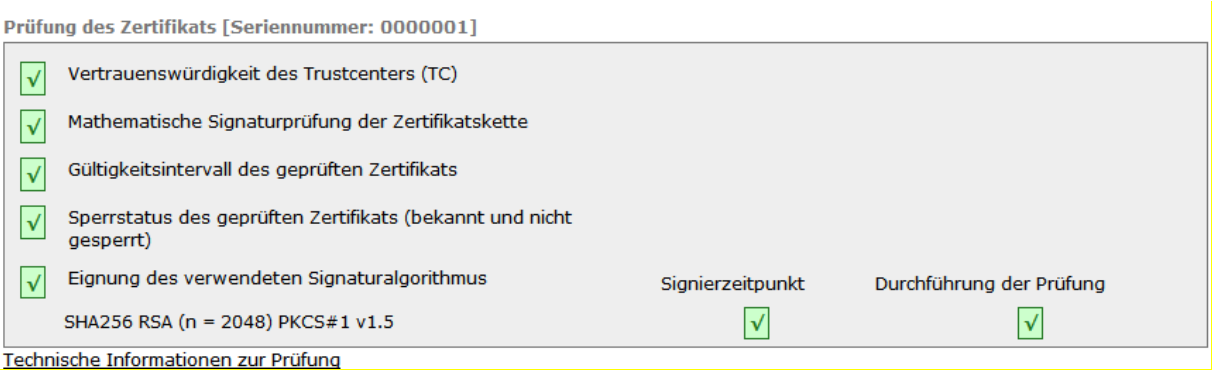


Abbildung 35: Teil 3 "Prüfung des Zertifikats"

Hinweis: Wird bei einer Signaturprüfung die Zertifikatsprüfung durch das OCSP/CRL-Relay nicht angefordert, erhalten alle vier Prüfmomente den Status "gelb".

4.3.1 Zeile "Prüfung des Zertifikats

In der Zeile " Prüfung des Zertifikats wird in eckigen Klammern die Seriennummer des geprüften Zertifikats angezeigt.

4.3.2 Zeile "Vertrauenswürdigkeit des Trustcenters"

In der Zeile "Vertrauenswürdigkeit des Trustcenters (TC)" wird angezeigt, ob die Zertifikatskette bis zur Wurzelinstanz erfolgreich gebildet werden konnte. Es handelt sich um eine technische Prüfung, die keine Aussage über die Qualität der Vertrauenswürdigkeit umfasst. In das Prüfergebnis fließen weitere Prüfschritte ein:

- Überprüfung des Sperrstatus (Revocation Status) aller zwischen dem zu prüfenden Zertifikat (in der Regel das Signaturzertifikat) und der Wurzelinstanz liegenden Zertifikate. Qualifizierte CA- und Rootzertifikate dürfen zum Zeitpunkt der Signatur der jeweils untergeordneten Zertifikats nicht gesperrt gewesen sein. Bei anderen Zertifikaten ist der maßgebliche Zeitpunkt häufig der Signaturzeitpunkt der Inhaltsdaten. Zur Erläuterung der verschiedenen Gültigkeitsmodelle siehe Kapitel 6.2.1. Hinweis: Die Prüfung des Sperrstatus des Signaturzertifikats erfolgt getrennt im Prüfschritt „Sperrstatus des geprüften Zertifikats“.
- Prüfung der Signaturen aller angeforderten OCSP-Antworten/CRL-Listen.

- Bei qualifizierten Signaturzertifikaten aus Deutschland wird geprüft, ob der Signaturzeitpunkt des Zertifikats innerhalb des Gültigkeitsintervalls (Validity Interval) des übergeordneten Zertifikats liegt. Diese Prüfung wird für jedes Zertifikat der Kette durchgeführt. Dieses Gültigkeitsmodell ergibt sich aus dem deutschen Signaturgesetz. Bei anderen Zertifikaten wird in der Regel geprüft, ob der Signaturzeitpunkt der Inhaltsdaten innerhalb des Gültigkeitszeitraums der Zertifikate oberhalb des zu prüfenden Signaturzertifikats lag (internationales Gültigkeitsmodell „Schale-Hybrid“). Zur Erläuterung der verschiedenen Gültigkeitsmodelle siehe Kapitel 6.2.1. Hinweis: Die Prüfung, ob der Signaturzeitpunkt der Inhaltsdaten innerhalb des Gültigkeitsintervalls des Signaturzertifikats liegt, erfolgt getrennt im Prüfschritt „Gültigkeitsintervall des geprüften Zertifikats“.

Folgende Status sind möglich:

- **Grüner Kasten mit Haken**: Die gesamte Zertifikatskette (ab dem zu prüfenden Zertifikat) bis zur Wurzelinstanz (selbstsigniertes Rootzertifikat) konnte erfolgreich hergestellt werden. Auch alle anderen Prüfschritte waren erfolgreich.
- **Gelber Kasten mit Ausrufungszeichen**: Mindestens einer der oben benannten Prüfschritte bei der Prüfung der Zertifikatskette konnte nicht durchgeführt werden. Es wird daher ein unbestimmter Status angezeigt.
- **Roter Kasten mit Kreuz**: Mindestens einer der oben benannten Prüfschritte bei der Prüfung der Zertifikatskette ist abschließend fehlgeschlagen.
- **Grauer Kasten**: Es wurde keine Prüfung durchgeführt. Mögliche Ursachen:
  - Eine zuvor notwendige Einzelprüfung konnte temporär nicht durchgeführt werden (Status "gelb")
  - Eine zuvor notwendige Einzelprüfung lieferte endgültig ein negatives Ergebnis (Status "rot"), sodass eine weitere Prüfung nicht mehr sinnvoll ist.
  - Eine zuvor notwendige Einzelprüfung wurde nicht durchgeführt (Status "grau") und es ist deshalb kein Prüfergebnis vorhanden.

Am Ende dieses Bereichs werden zusätzliche Erläuterungen zum Prüfergebnis unter der Zeile "Erläuterungen" angezeigt.

4.3.3 Zeile "Mathematische Signaturprüfung der Zertifikatskette"

In der Zeile "Mathematische Signaturprüfung" wird angezeigt, ob die Zertifikatssignaturen der Zertifikatskette mathematisch korrekt sind. Folgende Status sind möglich:

- **Grüner Kasten mit Haken**: Die Signaturen der Zertifikate der Kette konnten mit den jeweiligen Signaturprüfschlüsseln erfolgreich überprüft werden.
- **Gelber Kasten mit Ausrufungszeichen**: Mindestens eine mathematische Signaturprüfung konnte nicht durchgeführt werden. Es wird daher ein unbestimmter Status angezeigt.
- **Roter Kasten mit Kreuz**: Mindestens eine mathematische Signaturprüfung konnte nicht erfolgreich geprüft werden. Der Status ist final.
- **Grauer Kasten**: Es wurde keine Prüfung durchgeführt. Mögliche Ursachen:
  - Eine zuvor notwendige Einzelprüfung konnte temporär nicht durchgeführt werden (Status "gelb").
  - Eine zuvor notwendige Einzelprüfung lieferte endgültig ein negatives Ergebnis (Status "rot"), sodass eine weitere Prüfung nicht mehr sinnvoll ist.

- Eine zuvor notwendige Einzelprüfung wurde nicht durchgeführt (Status "grau") und es ist deshalb kein Prüfergebnis vorhanden.

Am Ende dieses Bereichs werden zusätzliche Erläuterungen zum Prüfergebnis unter der Zeile "Erläuterungen" angezeigt.

4.3.4 Zeile "Gültigkeitsintervall des geprüften Zertifikats"

In der Zeile "Gültigkeitsintervall des geprüften Zertifikats" wird angezeigt, ob der Signierzeitpunkt (der Inhaltsdaten) innerhalb des Gültigkeitszeitraums des Signaturzertifikats lag. Folgende Status sind möglich:

- **Grüner Kasten mit Haken**: Der Signierzeitpunkt lag innerhalb des Gültigkeitszeitraums des Signaturzertifikats.
- **Gelber Kasten mit Ausrufungszeichen**: Der oben benannte Prüfschritt konnte nicht durchgeführt werden. Ein möglicher Grund: das Zertifikat konnte nicht geparst werden. Es wird daher ein unbestimmter Status angezeigt.
- **Roter Kasten mit Kreuz**: Der Signierzeitpunkt lag außerhalb des Gültigkeitszeitraums des Signaturzertifikats.
- **Grauer Kasten**: Es wurde keine Prüfung durchgeführt. Mögliche Ursachen:
  - Eine zuvor notwendige Einzelprüfung konnte temporär nicht durchgeführt werden (Status "gelb").
  - Eine zuvor notwendige Einzelprüfung lieferte endgültig ein negatives Ergebnis (Status "rot"), sodass eine weitere Prüfung nicht mehr sinnvoll ist.
  - Eine zuvor notwendige Einzelprüfung wurde nicht durchgeführt (Status "grau") und es ist deshalb kein Prüfergebnis vorhanden.

Am Ende dieses Bereichs werden zusätzliche Erläuterungen zum Prüfergebnis unter der Zeile "Erläuterungen" angezeigt.

4.3.5 Zeile "Sperrstatus des geprüften Zertifikats"

In der Zeile "Sperrstatus des geprüften Zertifikats" wird angezeigt, ob das zu prüfende Zertifikat (in der Regel das Signaturzertifikat) zum Zeitpunkt der Signaturanbringung gesperrt war oder nicht.

In der ersten Spalte sind folgende Status möglich:

- **Grüner Kasten mit Haken**: Das zu überprüfende Zertifikat (in der Regel das Signaturzertifikat) war zum Zeitpunkt der Signaturanbringung (Signierzeitpunkt der Inhaltsdaten) nicht gesperrt. Angezeigt wird in diesem Fall in Klammern hinter dem Text "Sperrstatus des geprüften Zertifikats" der Hinweistext "nicht gesperrt".
- **Gelber Kasten mit Ausrufungszeichen**: Die Prüfung des Sperrstatus des Zertifikats konnte nicht durchgeführt werden. Eine Prüfung war möglicherweise deshalb nicht möglich, weil der Download der CRL fehlgeschlagen ist oder der angefragte OCSP-Responder des Trustcenters/ZDA temporär nicht erreichbar war. Es wird daher ein unbestimmter Status angezeigt.

- **Roter Kasten mit Kreuz**: Das Zertifikat war zum Signaturzeitpunkt gesperrt oder dem Trustcenter/ZDA unbekannt. Im Fall der Sperrung wird zusätzlich in Klammern hinter dem Text "Sperrstatus des geprüften Zertifikats" der Sperrgrund angegeben.[1]
- **Grauer Kasten**: Es wurde keine Prüfung durchgeführt, da eine zuvor notwendige Einzelprüfung temporär nicht durchgeführt werden konnte (wegen Status "gelb") oder eine zuvor notwendige Einzelprüfung endgültig ein negatives Ergebnis lieferte (Status "rot") oder eine zuvor notwendige Einzelprüfung nicht durchgeführt wurde (Status "grau") und deshalb kein Prüfergebnis vorhanden ist.

Am Ende dieses Bereichs werden zusätzliche Erläuterungen zum Prüfergebnis unter der Zeile "Erläuterungen" angezeigt.

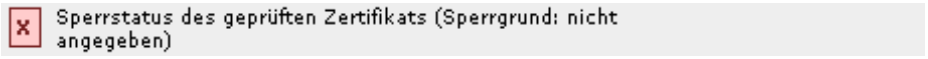


Abbildung 36: Teil 3 "Sperrgrund bei einem gesperrten Zertifikat"

4.3.5.1 Qualifiziertes Zertifikat eines deutschen ZDAs

Im §15 "Anforderungen an Produkte für qualifizierte elektronische Signaturen" der deutschen Signaturverordnung wird gefordert, dass "eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatsverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren".

Diesen Anforderungen genügt nur die Online-OCSP-Prüfung gemäß CommonPKI-Spezifikation. In einer normalen OCSP-Antwort meldet der OCSP-Responder des ZDA den Status des Zertifikats zurück mit "gut" oder "gesperrt" oder "unbekannt". Gemäß RFC2560 können diese Status-Informationen, die über den OCSP-Service geliefert wurden, aber aus einer CRL stammen, in der nur die Seriennummern gesperrter Zertifikate enthalten sind. Eine Positivaussage "Trustcenter hat das Zertifikat ausgestellt" ist nicht damit verbunden.

OCSP-Responder gemäß CommonPKI-Spezifikation ergänzen die Antwort um den Hashwert des Zertifikats, von dem die Statusinformation zurückgemeldet wurde. Das OCSP/CRL-Relay vergleicht den Hashwert des Zertifikats, zu dem die Statusinformation angefragt wurde, mit dem zurückgegebenen Hashwert in der OCSP-Antwort des OCSP-Responder. Stimmen beide Hashwerte überein, ist sichergestellt, dass das Zertifikat vom ZDA ausgestellt wurde.

Demnach zeigt bei einer qualifizierten Signatur, erzeugt mit einer Signaturkarte eines deutschen ZDAs, ein grünes Feld (Grüner Kasten mit Haken) an, dass das Zertifikat vom ZDA ausgestellt wurde und dass es zum Signierzeitpunkt nicht gesperrt war.

Angezeigt wird in diesem Fall in Klammern hinter dem Text "Sperrstatus des geprüften Zertifikats" der Hinweistext "bekannt und nicht gesperrt".

4.3.5.2 Anzeige des Sperrgrundes

Sollte ein Zertifikat gesperrt sein, wird zusätzlich in Klammern hinter dem Text "Sperrstatus des geprüften Zertifikats" der Sperrgrund angegeben. Folgende Sperrgründe sind möglich und werden ggf. angezeigt:

[1] Hinweis: Der OCSP-Responder des ZDA antwortet auch mit „unbekannt“, wenn ein qualifiziertes Zertifikat zwar durch den ZDA ausgestellt wurde, es aber zum Zeitpunkt der Signaturerstellung noch nicht online prüfbar war, da die Empfangsbestätigung für die Signaturkarte dem ZDA noch nicht vorlag.

- unspezifiziert
- Privater Schlüssel kompromittiert
- Privater CA-Schlüssel kompromittiert
- Name/andere Informationen über den Inhaber haben sich geändert
- Zertifikat ersetzt
- Zertifikat wird nicht mehr benötigt
- Zertifikat vorübergehend gesperrt
- Zertifikat abgelaufen und von Delta-CRL entfernt
- Attribut aus Zertifikat zurückgezogen
- Privater Schlüssel des Attributausstellers kompromittiert
- Kein Sperrgrund angegeben

4.3.6 Zeile "Eignung des verwendeten Signaturalgorithmus"

Die Eignung des für die Signatur eines qualifizierten Signaturzertifikats verwendeten Signaturalgorithmus wird auf Basis des von der Bundesnetzagentur veröffentlichten Algorithmenkatalogs

- zum Signierzeitpunkt des Zertifikats durch den ZDA und
- zum Zeitpunkt der Durchführung der Prüfung

ermittelt.

Die Anforderung ergibt sich aus dem § 2 Nr. 11 b des Signaturgesetzes, der besagt, dass Signaturanwendungskomponenten auch dann eine zuverlässige Prüfung und zutreffende Anzeige des Prüfergebnisses gewährleisten müssen, wenn die geprüfte Signatur auf einem Signaturalgorithmus, der gemäß aktuellem Algorithmenkatalog als nicht mehr geeignet und damit als nicht mehr hinreichend sicher eingestuft ist.

Die Eignung des für die Zertifikatssignatur verwendeten Signaturalgorithmus wird nur bei einem qualifizierten Zertifikat, ausgestellt von einem deutschen ZDA, überprüft. In allen anderen Fällen besitzt das kumulierte Prüfergebnis den Status "grau" (keine Prüfung durchgeführt).

In der ersten Spalte der Zeile " Eignung des verwendeten Signaturalgorithmus" wird das kumulierte Prüfergebnis angezeigt. Die folgenden Status sind möglich:

- Grüner Kasten mit Haken
- Gelber Kasten mit Ausrufungszeichen
- Roter Kasten mit Kreuz
- Grauer Kasten

Erläuterungen zu Grüner Kasten mit Haken:

Der verwendete Signaturalgorithmus war zum Signierzeitpunkt für die Erzeugung einer qualifizierten Signatur und zum Zeitpunkt der Durchführung der Prüfung für die Prüfung einer qualifizierten Signatur gemäß aktuellem Algorithmenkatalog geeignet.

Abbildung 37: Ergebnis der Eignungsprüfung bei einem Algorithmus, der zum Signierzeitpunkt für die Signatur eines qualifizierten Zertifikats und Zeitpunkt der Durchführung der Prüfung für die Prüfung der Signatur eines qualifizierten Zertifikats geeignet war

Erläuterungen zu ! Gelber Kasten mit Ausrufungszeichen:

Der verwendete Signaturalgorithmus war zum Zeitpunkt der Durchführung der Prüfung nicht mehr für die Prüfung einer qualifizierten elektronischen Signatur gemäß aktuellem Algorithmenkatalog geeignet. Zum Zeitpunkt der Signaturanbringung (Signierzeitpunkt) war die Eignung jedoch noch gegeben.

Abbildung 38: Ergebnis der Eignungsprüfung bei einem Algorithmus, der erst zum Zeitpunkt der Durchführung der Prüfung nicht mehr für die Prüfung der Signatur eines qualifizierten Zertifikats geeignet war

Bereits erzeugte elektronische Signaturen bleiben auch dann noch qualifiziert, wenn der zugrundeliegende Algorithmus nach der Signatur seine Eignung verloren hat. Sie büßen jedoch graduell und sukzessive ihren Beweiswert ein. Das Prüfergebnis "gelb" wirkt sich auf das kumulierte Ergebnis der Signaturprüfung aus und ist in diesem Fall final. Am Ende des Bereichs "Signaturprüfungen" wird unter der Zeile "Erläuterungen" der folgende Warnhinweis ausgegeben:

- Qualifizierte elektronische Signatur (SigG). Es wurde aber ein Algorithmus verwendet, der zum Zeitpunkt der Durchführung der Prüfung nicht mehr für eine qualifizierte Signatur geeignet war.

Erläuterungen zu X Roter Kasten mit Kreuz:

Abbildung 39: Ergebnis der Eignungsprüfung bei einem Algorithmus, der bereits zum Signierzeitpunkt nicht mehr für die Signatur eines qualifizierten Zertifikats geeignet war

Der verwendete Signaturalgorithmus war bereits zum Signierzeitpunkt gemäß aktuellem Algorithmenkatalog für die Signatur eines qualifizierten elektronischen Zertifikats nicht (mehr) geeignet. Signaturen, die nach dem Schwachwerden des zugrundeliegenden Signaturalgorithmus erzeugt wurden, sind von vornherein keine qualifizierten Signaturen. Schon bei der Erzeugung der Signatur konnte nämlich nicht mehr sichergestellt werden, dass der Signaturschlüssel-Inhaber die alleinige Kontrolle über die Mittel zur Erzeugung der Signatur hatte. Das Prüfergebnis "rot" wirkt sich auf das kumulierte Ergebnis der Signaturprüfung aus und ist in diesem Fall final. Am Ende des Bereichs "Signaturprüfungen" wird unter der Zeile "Erläuterungen" der folgende Warnhinweis ausgegeben:

- Fortgeschrittene Signatur und keine qualifizierte Signatur (SigG). Es wurde ein Algorithmus verwendet, der zum Signierzeitpunkt nicht mehr für eine qualifizierte Signatur geeignet war.

Erläuterungen zu Grauer Kasten:

Eine Prüfung der Eignung des verwendeten Signaturalgorithmus wurde nicht durchgeführt.

Abbildung 40: Eignungsprüfung des verwendeten Signaturalgorithmus bei einer fortgeschrittenen Signatur eines Zertifikats

4.3.6.1 Zeile "Angabe des verwendeten Signaturalgorithmus"

Unterhalb der Zeile mit dem angezeigten kumulierten Prüfergebnis wird der Name des verwendeten Signaturalgorithmus angezeigt.

Der angezeigte Name setzt sich wie folgt zusammen (von links nach rechts):

c) Bei einer RSA-Signatur:
   - Verwendeter Hashalgorithmus
   - RSA-Algorithmus mit Länge des Parameters n in Klammern
   - verwendetes Signaturschema (PKCS#1 v1.5 oder PKCS#1 v2.1 [PSS])

d) Bei einer DSA/ECDSA-Signatur:
   - verwendeter Hashalgorithmus
   - DSA/ECDSA-Algorithmus mit Länge der Parameter p (nur ECDSA) und q jeweils in Klammern

Abbildung 41: Anzeige des verwendeten Signaturalgorithmus

Hinweis: Am Ende des Prüfprotokolls befindet sich eine Liste aller geprüften Signaturalgorithmen. Angezeigt werden dort der Name des Teil-Algorithmus und das Datum des Ablaufs der Eignung gemäß aktuellem Algorithmenkatalog der Bundesnetzagentur (BNetzA) in Abhängigkeit vom Verwendungszweck (Anbringung einer Inhaltsdatensignatur, Prüfung einer Inhaltsdatensignatur, Anbringung einer Zertifikatssignatur, Prüfung einer Zertifikatssignatur).

4.3.6.2 Spalte Einzelprüfergebnis „Signierzeitpunkt“

In der Spalte „Signierzeitpunkt“ wird unter der Überschrift das Ergebnis der Eignungsprüfung des zur Signatur des Zertifikats verwendeten Signaturalgorithmus zum Zeitpunkt der Signaturanbringung (Signierzeitpunkt des Zertifikats) angezeigt.

Abbildung 42: Ergebnis der Eignungsprüfung des verwendeten Signaturalgorithmus einer Zertifikatssignatur zum Signierzeitpunkt

Die Eignung des verwendeten Signaturalgorithmus zum Zeitpunkt der Signaturanbringung (Signierzeitpunkt) wird nur bei der Signatur eines qualifizierten Zertifikats, ausgestellt von einem deutschen ZDA, ermittelt. In allen anderen Fällen besitzt das Prüfergebnis den Status "grau" (keine Prüfung durchgeführt). Folgende Status sind möglich:

- **grüner Kasten mit Haken**: Der Signaturalgorithmus war zum Signierzeitpunkt gemäß aktuellem Algorithmenkatalog für die Erzeugung einer qualifizierten elektronischen Signatur (Zertifikatssignatur) geeignet.
- **roter Kasten mit Kreuz**: Der Signaturalgorithmus war bereits zum Signierzeitpunkt gemäß aktuellem Algorithmenkatalog für die Erzeugung einer qualifizierten elektronischen Signatur (Zertifikatssignatur) nicht (mehr) geeignet.

4.3.6.3 Spalte Einzelprüfergebnis „Durchführung der Prüfung“

In der Spalte „Durchführung der Prüfung“ wird unter der Überschrift das Ergebnis der Eignungsprüfung des verwendeten Signaturalgorithmus zum Zeitpunkt der Durchführung der Signaturprüfung angezeigt.

Abbildung 43: Ergebnis der Eignungsprüfung des verwendeten Signaturalgorithmus einer Zertifikatssignatur zum Zeitpunkt der Durchführung der Signaturprüfung

Die Eignung des verwendeten Signaturalgorithmus zum Zeitpunkt der Durchführung der Prüfung wird nur bei der Prüfung der Signatur eines qualifizierten Zertifikats, ausgestellt von einem deutschen ZDA, ermittelt. In allen anderen Fällen besitzt das Prüfergebnis den Status "grau" (keine Prüfung durchgeführt). Folgende Status sind möglich:

- **grüner Kasten mit Haken**: Der Signaturalgorithmus war zum Zeitpunkt der Durchführung der Prüfung gemäß aktuellem Algorithmenkatalog für die Prüfung der Signatur eines qualifizierten Zertifikats geeignet.
- **Gelber Kasten mit Ausrufungszeichen:** Der verwendete Signaturalgorithmus war zum Zeitpunkt der Durchführung der Prüfung gemäß aktuellem Algorithmenkatalog nicht mehr für die Prüfung der Signatur eines qualifizierten Zertifikats geeignet. Zum Zeitpunkt der Signaturanbringung (Signierzeitpunkt) war die Eignung jedoch noch gegeben.
- **roter Kasten mit Kreuz**: Der Signaturalgorithmus war bereits zum Signierzeitpunkt gemäß aktuellem Algorithmenkatalog für die Signatur eines qualifizierten Zertifikats

nicht (mehr) geeignet. Signaturen, die nach dem Schwachwerden des zugrundeliegenden Signaturalgorithmus erzeugt wurden, sind von vornherein keine qualifizierten Signaturen. Daher wird auch hier ein rotes Prüfergebnis angezeigt.

4.3.6.4 Auswirkungen auf das Gesamtprüfergebnis

Unter der Bedingung, dass alle anderen Einzelprüfungen den Ampelstatus "grün" aufweisen, wirkt sich die Eignungsprüfung wie folgt auf das kumulierte Prüfergebnis einer qualifizierten elektronischen Signatur aus:

Eignung des Signaturalgorithmus (Zertifikatssignatur)		Kumuliertes Prüfergebnis der Eignungs-prüfung	Qualifizierte elektronische Signatur (QES)?
Signier-zeitpunkt	Zeitpunkt der Durchführung der Prüfung		
√ Grün (ja)	√ Grün (ja)	√ Grün	QES
√ Grün (ja)	! Gelb (nein)	! Gelb	QES mit einschränkendem Hinweis
X Rot (nein)	X rot (nein)	X Rot	keine QES

Tabelle 2: Ermittlung des kumulierten Prüfergebnisses

Alle geprüften Signaturalgorithmen werden am Ende des Prüfprotokolls tabellarisch zusammengefasst aufgeführt. Angezeigt werden der Name des Teil-Algorithmus, das Datum des Ablaufs der Eignung gemäß aktuellem Algorithmenkatalog der Bundesnetzagentur (BNetzA) in Abhängigkeit vom Verwendungszeck (Anbringung einer Inhaltsdatensignatur, Prüfung einer Inhaltsdatensignatur, Anbringung einer Zertifikatssignatur, Prüfung einer Zertifikatssignatur).

Auszug aus dem Algorithmenkatalog veröffentlicht von der Bundesnetzagentur am 27.03.2013

Algorithmusname	Typ	geeignet für	bis
PKCS#1 v1.5	Paddingalgorithmus	Anbringung von Zertifikatssignaturen	31.12.2017
PKCS#1 v1.5	Paddingalgorithmus	Anbringung von Inhaltsdatensignaturen	31.12.2015
PKCS#1 v1.5	Paddingalgorithmus	Prüfung von Zertifikats- und Inhaltsdatensignaturen	31.12.2019
RSA (n = 2048)	Schlüsselalgorithmus	Anbringung/Prüfung von Zertifikats- und Inhaltsdatensignaturen	31.12.2019
SHA256	Hashalgorithmus	Anbringung/Prüfung von Zertifikats- und Inhaltsdatensignaturen	31.12.2019

Abbildung 44: Anzeige der verwendeten Algorithmen für eine qualifizierte elektronische Signatur (SigG) mit Datum des Ablaufs der Eignung in Abhängigkeit vom Verwendungszeck

4.3.7 Link "Technische Informationen zur Prüfung"

Um die Qualität der Signatur und des Zertifikats genauer beurteilen zu können, sind folgende zusätzliche Informationen sinnvoll:

- der Staat, in dem das Trustcenter (Zertifizierungsdiensteanbieter) ansässig ist,
- die "Art der Überwachung" des Betriebs des Trustcenters (z.B. durch eine staatliche Stelle),
- das Zertifikatsniveau gemäß Zertifizierungsrichtlinie des Trustcenters,
- das Gültigkeitsmodell der Zertifikatsprüfung oder
- die Art der Statusprüfung (OCSP oder CRL).

Bei Unklarheiten oder im Fehlerfall ist es darüber hinaus hilfreich zu wissen, welches OCSP/CRL-Relay auf der Basis welcher Konfiguration geprüft hat.

Zu diesen und weiteren Informationen zur Zertifikatsprüfung gelangt man durch einen Klick auf den Link "Technische Informationen zur Prüfung", der sich am Ende des Prüfprotokolls befindet. Die technischen Informationen werden im Kapitel 6 ausführlich erläutert.

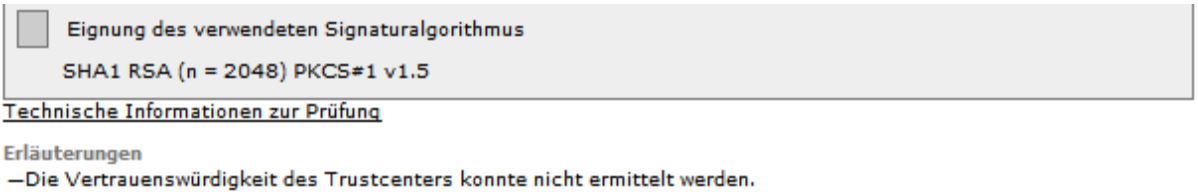


Abbildung 45: Link zu den technischen Informationen zur Prüfung und Erläuterungen

4.3.8 Zeile "Erläuterungen"

In der Zeile "Erläuterungen" werden alle Warnhinweise und Meldungen zu den einzelnen Prüfergebnissen aus dem Bereich Signaturprüfungen, Teil 2 und 3 angezeigt, die sich bei einer Einzelprüfung mit dem Status "gelb" und "rot" ergeben. Notwendige Erläuterungen zu den Warnhinweisen finden sich in den Kapiteln, in denen die Einzelprüfergebnisse dargestellt werden.

Folgende Meldungen aus dem Bereich der Einzelprüfergebnisse sind möglich, die zu einem Gelbstatus des kumulierten Prüfergebnisses führen:

- Es liegt kein Signierzeitpunkt vor.
- Die Integrität der Signatur konnte nicht geprüft werden, da das Signaturzertifikat nicht vorhanden ist.
- Die Integrität der Signatur konnte nicht geprüft werden, da keine Inhaltsdaten vorliegen.
- Die Integrität der Signatur konnte nicht geprüft werden, da der Algorithmus nicht implementiert ist.
- Es wurden nur Teile des Dokuments signiert (nur bei PDF-Inline-Signaturen).
- Eine Signaturprüfung ist nicht möglich, da eine unzulässige XPATH-Transformation verwendet wurde (nur bei XAdES-Signaturen).
- Eine Signaturprüfung ist nicht möglich, da eine unzulässige XSLT-Transformation verwendet wurde (nur bei XAdES-Signaturen).
- Eine Signaturprüfung ist nicht möglich, da ein unbekannter Kanonisierungsalgorithmus verwendet wurde (nur bei XAdES-Signaturen). [2]
- Der Sperrstatus des Zertifikats konnte nicht ermitteln werden.
- Die Vertrauenswürdigkeit des Trustcenters konnte nicht ermittelt werden.
- Die Gültigkeit des Zertifikats konnte nicht überprüft werden.
- Die Signaturen der Zertifikatskette konnten nicht überprüft werden.

[2] Vor der Signaturprüfung wird ein XML-Dokument durch eine spezielle Transformation "normalisiert". Dafür wird ein Kanonisierungsalgorithmus verwendet. Da dieser nicht bekannt ist, ist eine Signaturprüfung nicht möglich.

- Qualifizierte elektronische Signatur (SigG). Es wurde aber ein Algorithmus verwendet, der zum Zeitpunkt der Durchführung der Prüfung nicht mehr für eine qualifizierte Signatur geeignet war (nur bei einer qualifizierten Signatur, die mit einer Signaturkarte eines deutschen ZDAs erstellt wurde).
- Die Eignung eines Algorithmus konnte nicht ermittelt werden (nur bei einer qualifizierten Signatur, die mit einer Signaturkarte eines deutschen ZDAs erstellt wurde).

Folgende Meldungen aus dem Bereich der Einzelprüfergebnisse sind möglich, die zu einem Rotstatus des kumulierten Prüfergebnisses führen:

- Die Inhaltsdaten wurden nach Anbringung der Signatur manipuliert.
- Die Signatur enthält illegalen Inhalt (nur bei PDF-Inline-Signaturen).
- Die Signatur der OSCI-Nachricht ist inkorrekt (nur bei OSCI-Nachrichten).
- Das Attributzertifikat gehört nicht zum Signaturzertifikat.
- Das Zertifikat war zum Signierzeitpunkt gesperrt oder abgelaufen.
- Das Zertifikat ist gesperrt.
- Das Trustcenter ist nicht vertrauenswürdig.
- Das Zertifikat ist nicht gültig.
- Die Zertifikatskette ist nicht gültig.
- Fortgeschrittene Signatur und keine qualifizierte Signatur (SigG). Es wurde ein Algorithmus verwendet, der zum Signierzeitpunkt nicht mehr für eine qualifizierte Signatur geeignet war (nur bei einer qualifizierten Signatur, die mit einer Signaturkarte eines deutschen ZDAs erstellt wurde).

4.4 Zusätzliche Prüfung eines Attributzertifikats

Ein Attributzertifikat ist ein separates Zertifikat mit einer eindeutigen Referenz zum Signaturzertifikat. Als qualifiziertes Attributzertifikat enthält es mindestens ein Attribut, dass die Wirksamkeit einer qualifizierten Signatur beschränkt, erweitert oder präzisiert. Die CommonPKI-Spezifikation Version 2.0 profiliert im SigG-Profil entsprechende Attribute.

Ein Attributzertifikat wird wie ein Signaturzertifikat geprüft. Die Darstellung der Prüfergebnisse erfolgt in einem getrennten Teil direkt unter der Darstellung der Prüfergebnisse des zugehörigen Signaturzertifikats mit der Überschrift "Prüfung des Attributzertifikats".

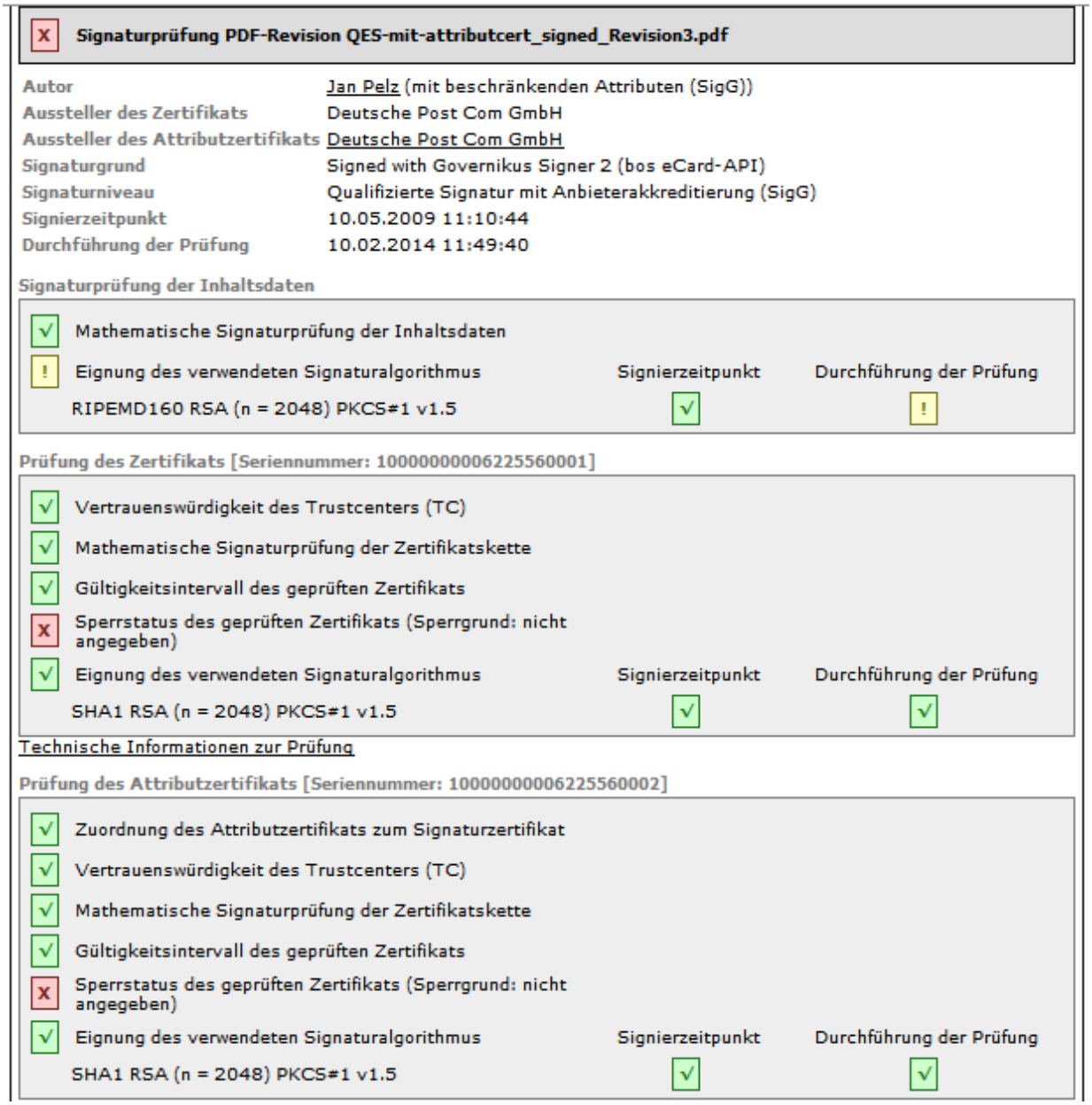


Abbildung 46: Teil 3 "Prüfung eines Attributzertifikats zu einem Signaturzertifikat"

Die Prüfergebnisse entsprechen der Anzeige der Prüfergebnisse für das geprüfte Signaturzertifikat mit folgenden Ergänzungen:

4.4.1 Zeile "Aussteller des Attributzertifikats" (nur bei Attributzertifikaten)

Ist zu einem Signaturzertifikat ein Attributzertifikat vorhanden, wird im Bereich 2 "Signaturprüfungen, Teil 1 „Kumuliertes Prüfergebnis und Informationen zur Signatur“, unter der Zeile Autor zusätzlich der Aussteller des Attributzertifikats angezeigt. Dies ist der Organisationsname [Attribut: `OrganisationName`] des Ausstellers (CA, Trustcenters) aus dem Feld [`issuer`] und in der Regel identisch mit dem Organisationsnamen des Ausstellers des Basiszertifikats.

4.4.2 Zeile "Zuordnung des Attributzertifikats zum Signaturzertifikat"

Es wird zusätzlich geprüft, ob das qualifizierte Attributzertifikat eindeutig dem qualifizierten Signaturzertifikat zugeordnet werden kann. Nur in diesem Fall sind die Attribute Bestandteil der abgegebenen Willenserklärung.

In der Zeile "Zuordnung des Attributzertifikats zum Signaturzertifikat" wird dieses Prüfergebnis angezeigt. Folgende Status sind möglich:

- **Grüner Kasten mit Haken**: Die eindeutige Zuordnung zum Signaturzertifikat/Basiszertifikat gemäß Common PKI-Spezifikation war erfolgreich. Damit ist es Bestandteil der Willenserklärung und muss beachtet werden.
- **Roter Kasten mit Kreuz**: Die Zuordnung zum Signaturzertifikat/Basiszertifikat ist endgültig gescheitert. Das Prüfergebnis wirkt sich auf das kumulierte Prüfergebnis aus. Es erhält den Status "rot". In den Erläuterungen am Ende des Bereichs "Signaturprüfungen" wird der folgende Hinweis angezeigt: "Das Attributzertifikat gehört nicht zum Signaturzertifikat."
- **Grauer Kasten**: Aus technischen Gründen ist keine Zuordnung möglich.

Sollten mehrere Attributzertifikate einem Signaturzertifikat zugeordnet sein, werden alle Atributzertifikate geprüft und die Prüfergebnisse untereinander angezeigt.

4.5 Teil 3: Nachprüfung eines Zertifikats bei OSCI-Nachrichten

Sollte das kumulierte Prüfergebnis bei einer geprüften OSCI-Nachricht den Status "gelb" aufweisen, kann eine Nachprüfung des Signaturzertifikats sinnvoll sein. Häufig kommt dieses Prüfergebnis nämlich dadurch zustande, dass der Sperrstatus des Zertifikats nicht ermittelt werden konnte, weil das angefragte Trustcenter temporär nicht erreichbar war. Im Teil "Prüfung des Zertifikats" wird in diesem Fall mindestens die Prüfung des Sperrstatus den Status "gelb" aufweisen. In diesem Fall ist eine "Nachprüfung" des Sperrstatus des Signaturzertifikats sinnvoll. Der Status "gelb" kann aber auch endgültig sein, wenn z. B. der Signierzeitpunkt der Inhaltsdaten nicht ermittelt werden konnte. In diesem Fall macht eine "Nachprüfung" des Signaturzertifikats keinen Sinn.

Eine Nachprüfung wird immer durchgeführt bei OSCI-Nachrichten, die qualifizierte ECDSA-signierte Zertifikate, ausgestellt durch einen deutschen ZDA, enthalten (z. B. qualifizierte nPA-Zertifikate). Im Laufzettel sind nämlich nur das Signaturzertifikat und die Prüfergebnisse enthalten, nicht aber das CA-Zertifikat des ZDA. Dieses wird aber benötigt, um die Eignung des zur Zertifikatssignatur verwendeten Algorithmus überprüfen zu können.

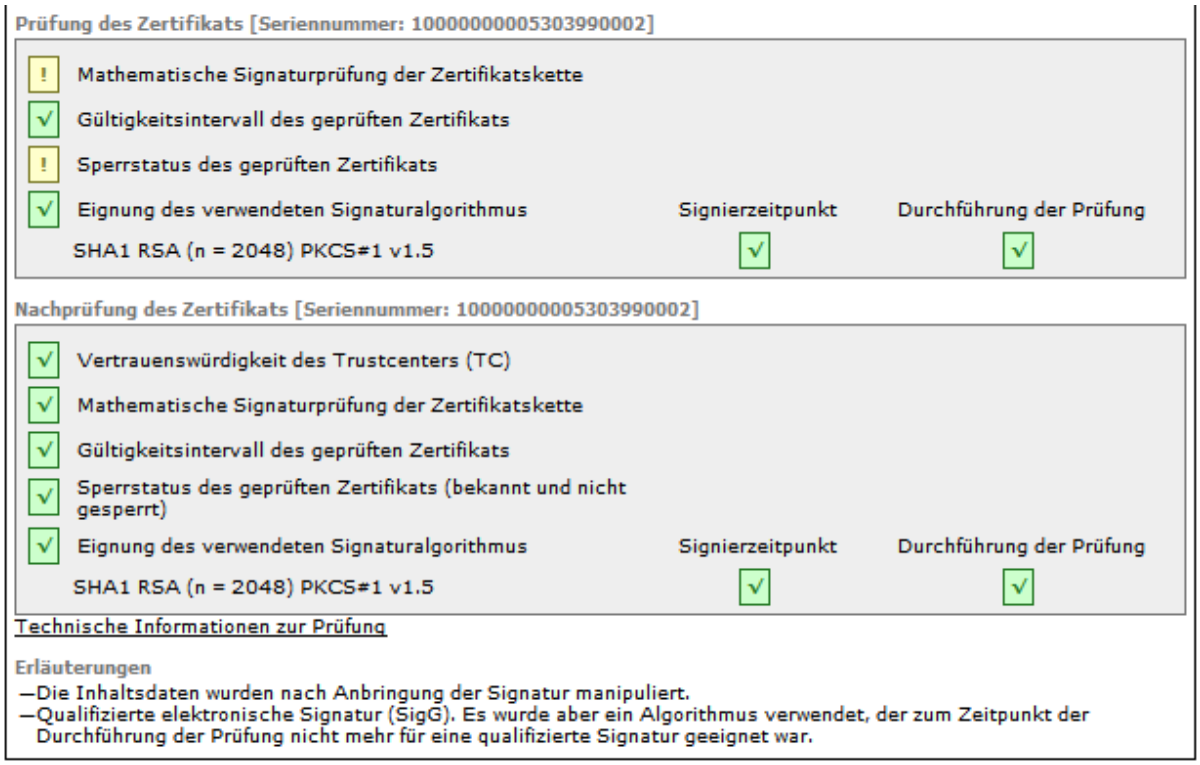


Abbildung 47: Teil 3 "Nachprüfung eines Zertifikats bei OCSI-Nachrichten"

Das Ergebnis der Nachprüfung wird als Voreinstellung nur dann an das Ergebnis der Prüfung des Zertifikats angehängt, falls alle Einzelprüfungen erfolgreich waren. Das Ergebnis einer angezeigten Nachprüfung wirkt sich auf den Status des kumulierten Prüfergebnisses aus.

5 Bereich 3: Zertifikate

Um eine elektronische Signatur einer Person zuordnen zu können, wird ein digitales Zertifikat verwendet. Es enthält Angaben, welche den Inhaber des privaten Signaturschlüssels identifizieren. Durchgesetzt haben sich Zertifikate nach Standard X.509; aktuell ist die Version 3.

Dieses Kapitel beschreibt den Bereich 3 des Prüfprotokolls, in dem die Inhalte von Zertifikaten angezeigt werden.

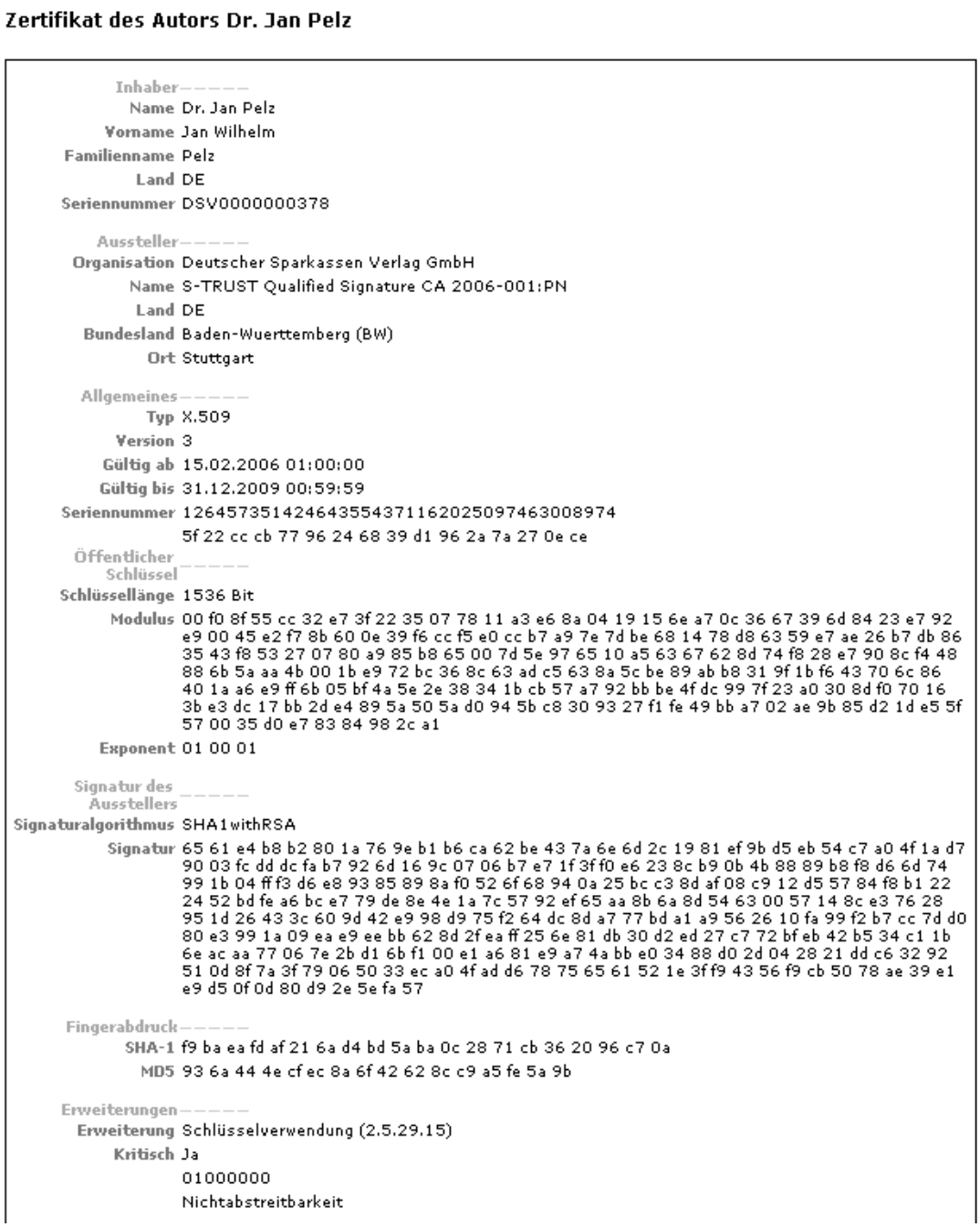


Abbildung 48: Bereich 3 "Zertifikate“ des Prüfprotokolls"

Das Kapitel gliedert sich in mehrere Unterkapitel. Im Kapitel 5.1 wird zunächst erläutert, welche Art der Anzeige im Prüfprotokoll gewählt wurde und welche Inhalte angezeigt werden können. In den folgenden Kapiteln folgt anschließend eine Beschreibung aller vorgeschriebenen und optionalen Inhalte eines (Signatur-)Zertifikats in der Reihenfolge ihrer Nennung im RFC 5280 und der CommonPKI-Spezifikation:

5.1 Anzeige von Zertifikatsinhalten im Prüfprotokoll

Die Struktur eines Zertifikats basiert auf ASN.1, eine abstrakte Beschreibungssprache zur eindeutigen Definition von Datenstrukturen und Inhalten, ohne auf die rechnerinterne Darstellung einzugehen sowie Festlegungen zur Umsetzung von Datenstrukturen in ein eindeutiges Format über sogenannte Kodierungsregeln. Diese sind auf Bitebene völlig eindeutig und damit für Zertifikate geeignet, die digital signiert sind und plattformübergreifend ausgetauscht werden sollen.

Zertifikate sind daher, auch in der Textansicht, nur schwer lesbar. Feldnamen, Erweiterungen, IDs und Werte aus dem Zertifikat werden daher im Prüfprotokoll verständlich "übersetzt". Angezeigt werden im Prüfprotokoll in der Detailansicht der Zertifikate immer alle Zertifikatsinhalte. Dabei wird sichergestellt, dass alle im

- RFC 5280 und in der
- CommonPKI-Spezifikation Version 2.0

profilierten Zertifikatsfelder und Erweiterungen menschenlesbar übersetzt werden. Die vorgeschriebenen und optionalen Inhalte eines Zertifikats werden dabei in der Reihenfolge, wie im RFC und der CommonPKI-Spezifikation aufgeführt, beschrieben. Dazu gehören auch die optionalen Attribute in qualifizierten Signaturzertifikaten und/oder in qualifizierten Attributzertifikaten (ausgestellt von deutschen Zertifizierungsdiensteanbietern), die die Wirksamkeit einer qualifizierten elektronischen Signatur einschränken, erweitern oder präzisieren.

Bitte beachten Sie in diesem Zusammenhang, dass ein Zertifikat nicht alle in den folgenden Kapitel beschriebenen Inhalte enthalten muss. Eine verständliche Anzeige bei Zertifikaten aus der EU kann ebenso nicht immer sichergestellt werden, da jedes Trustcenter eigene Zertifikatserweiterungen (sogenannte private Extensions) definieren kann. Werden diese in einer gültigen ASN.1-Struktur erzeugt, können sie aber zumindest in einer rudimentären Ansicht (mit OIDs) angezeigt werden.

Erläuterung: RFC 5280 und CommonPKI-Spezifikation Version 2.0

Der RFC 5280 ist Teil einer Familie von Standards für die X.509 Public Key Infrastructure (PKI) für das Internet. Der RFC 5280 profiliert grundlegend das Format und die Semantik von Zertifikaten.

Die CommonPKI-Spezifikation Version 2.0 beschreibt ein Profil über international verbreitete und anerkannte Standards für elektronische Signaturen, Verschlüsselungen und Public-Key-Infrastrukturen. Im Januar 2009 ist die Spezifikation gemeinsam von T7 und TeleTrusT verabschiedet worden. Sowohl Anbieter von Signaturanwendungskomponenten als auch die deutschen Trustcenter-Betreiber waren an der Erarbeitung der Spezifikation beteiligt und stellen auch konforme Zertifikate aus. Die CommonPKI-Spezifikation referenziert und profiliert die relevanten Standards, wie RFC 5280, 3739 und ETSI QC, CPN.

5.2 Inhaber eines Zertifikats

Anzeigt werden alle im Zertifikat vorhandenen Informationen zum Inhaber [Feld `subject`] des Zertifikats (Inhaberattribute).

Abbildung 49: Bereich "Inhaber eines Zertifikats"

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

- Name [`commonName`]
- Familienname (Nachname) [`surName`]
- Vorname(n) [`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 [`stateOrProvinceName`]
- Land [`countryName`]
- Namensunterscheider [`distinguishedNameQualifier`]
- Domainname [`domainComponent`]
- Straße [`streetAddress`]
- Postleitzahl [`postalCode`]
- Postanschrift [`postalAddress`]
- E-Mail-Adresse [`emailAddress`]

- Pseudonym [pseudonym]
- Seriennummer [serialNumber]

Hinweis: Das Attribut "Seriennummer" wird im Gegensatz zur Zertifikatsseriennummer als Namensunterscheider verwendet, sollte ein Inhaber z.B. mehrere Zertifikate mit ansonsten identischen Angaben zum Inhaber besitzen.

5.2.1 Qualifiziertes Zertifikat gemäß CommonPKI SigG-Profil

Der Name [Attribut commonName] ist gemäß Common PKI-Profil das einzige Pflichtattribut, das im Feld "Inhaber" angegeben werden muss. Der Inhabername muss bezogen auf alle von der Zertifizierungsstelle während ihrer gesamten Lebensdauer ausgestellten Zertifikate einzigartig sein.

Das Attribut "Name" setzt sich zusammen aus dem im Identifikationsdokument (Personalausweis oder Reisepass) angegebenen Vor- und Nachnamen des Zertifikatsinhabers. Durch das Signaturgesetz (SigG) werden auch ausdrücklich Pseudonyme erlaubt, wenn diese als Pseudonym gekennzeichnet sind. Im CommonPKI SigG-Profil wird bei einem Pseudonym daher der Suffix ":PN" vorgeschrieben.

5.2.2 Qualifiziertes Attributzertifikat gemäß CommonPKI SigG-Profil

Bei Attributzertifikaten wird das zugehörige Basiszertifikat (Signaturzertifikat) referenziert. Angezeigt werden aus dem Feld "Inhaber des Attributzertifikats" [Feld subject] – soweit vorhanden - der Organisationsname des Ausstellers des Basiszertifikats [Attribut organization des Feldes Issuer des Basiszertifikats] und die Seriennummer des Basiszertifikats [baseCertificateID], entnommen aus dem Feld SerialNumber des Basiszertifikats. Attributzertifikate sind nur in Deutschland weiter verbreitet.

Qualifizierte Attributzertifikate dürfen gemäß CommonPKI SigG-Profil nur ausgestellt werden, wenn ein qualifiziertes Basiszertifikat (Signaturzertifikat) existiert. In diesem Fall muss die baseCertificateID-Option verwendet werden.

Abbildung 50: Bereich "Inhaber eines Attributzertifikats"

5.3 Aussteller eines Zertifikats

Angezeigt werden alle im Zertifikat vorhandenen Informationen zum Aussteller [Feld issuer]. Die folgenden Attribute können nach RFC 5280 und RFC 3739 (Internet X.509 Public Key Infrastructure: Qualified Certificates Profile) verwendet werden:

- Name [commonName]
- Familienname (Nachname) [surName]
- Vorname(n) [givenName]

- Titel [title]
- Initialen [initials]
- Generationskennzeichen [generationQualifier]
- Organisation [organizationName]
- Organisationseinheit [organizationalUnitName]
- Ort [localityName]
- Bundesland [stateOrProvinceName]
- Land (c) [countryName]
- Namensunterscheider [distinguishedNameQualifier]
- Domainname [domainComponent]
- Pseudonym [pseudonym]
- Seriennummer [serialNumber]

Hinweis: Das Attribut "Seriennummer" wird im Gegensatz zur Zertifikatsseriennummer als Namensunterscheider verwendet.

Abbildung 51: Bereich "Aussteller"

5.3.1 Qualifiziertes Signaturzertifikat gemäß Common PKI-Profil

Gemäß Common PKI-Profil müssen die Attribute im Feld "Aussteller" des Signaturzertifikates identisch sein mit den Attributen im Feld "Inhaber" im korrespondierenden CA-Zertifikat, um hilfsweise die Kettenbildung über diese Felder zu ermöglichen. Pflichtattribute sind gemäß SigG-Profil nur die Attribute "Land" [Attribut countryName] und "Organisation" [Attribut organizationName]. Das Attribut "Organisation" soll dem Namen der Organisation entsprechen, den der Zertifizierungsdiensteanbieter operativ führt.

Im Attribut "Name" steht bei qualifizierten CA-Zertifikaten nach CommonPKI SigG-Profil der aus dem CA-Zertifikat übernommene Name [Attribut commonName] des Inhabers des CA-Zertifikats. Qualifizierte CA-Zertifikate müssen auf eine natürliche Person ausgestellt werden und verwenden deshalb ein Pseudonym in der Form [Name] mit dem Zusatz ":PN".

5.4 Allgemeine Informationen

5.4.1 Zeilen "Typ" und "Version"

Alle Signaturzertifikate sind immer konform zur Version 3 des Zertifikatstyps X509, da nur in dieser Version Erweiterungen enthalten sein dürfen [Feld version]; Attributzertifikate sind an der Version 1 zu erkennen [Feld version.AttCertVersion].

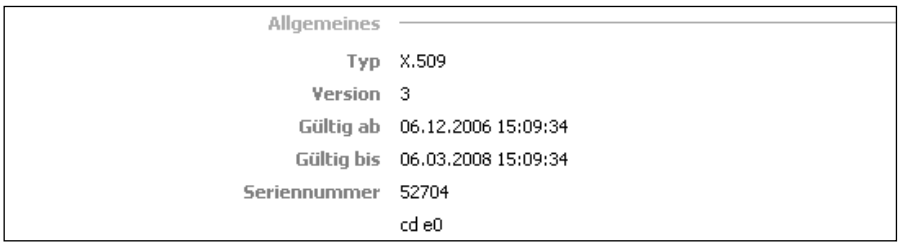


Abbildung 52: Allgemeine Informationen zum Zertifikat

5.4.2 Zeile "Algorithmus"

Angezeigt wird der vom Aussteller (Zertifizierungsdiensteanbieter, Trustcenter) verwendete Algorithmus zur Signatur des Zertifikats [Feld `signature`]. Er muss identisch sein zum Eintrag in der Zeile "Algorithmus" im Bereich "Signatur des Ausstellers" [Feld `signatureAlgorithm`].

5.4.3 Zeilen "gültig ab" und "gültig bis" (Gültigkeitszeitraum)

Angezeigt wird der Gültigkeitszeitraum [Feld `validity`, bei Attributzertifikaten `attrCertValidityPeriod`] des Zertifikats in der Form

- gültig ab Datum
- gültig bis Datum

Bei "gültig ab" wird das Datum, ab dem das Zertifikat gültig ist, in der Form `Tag.Monat.Jahr Stunde:Minute:Sekunde (tt.mm.jjjj hh:mm.ss)` [`notBefore`; bzw. `notBeforeTime`] angezeigt.

Bei "gültig bis" 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).` [`notAfter`; bzw. `notAfterTime`] angezeigt.

Hinweis: Das CommonPKI SigG-Profil schreibt gemäß Signaturverordnung (siehe § 14 SigV) bei qualifizierten Signaturzertifikaten deutscher Zertifizierungsdiensteanbieter eine maximale Gültigkeitsdauer von 5 Jahren vor.

5.4.4 Zeile "Seriennummer"

Angezeigt wird die Seriennummer des Zertifikats [Feld `SerialNumber`] in Ziffern und hexadezimal. Die Zertifikatsnummer muss innerhalb eines Zertifizierungsbereichs einer CA (gleicher Aussteller) gemäß RFC 5280 und CommonPKI-Spezifikation eindeutig sein.

5.5 Öffentlicher Schlüssel aus dem Zertifikat

Im Bereich "öffentlicher Schlüssel" [Feld `subjectPublicKeyInfo`] werden der öffentliche Schlüssel des Zertifikatsinhabers [`subjectPublicKey`] und technische Informationen zum öffentlichen Schlüssel [`algorithm`] angezeigt.

5.5.1 RSA-Schlüssel

RSA ist ein asymmetrisches kryptographisches Verfahren, das zur digitalen Signatur oder Verschlüsselung benutzt wird. Es verwendet ein Schlüsselpaar, bestehend aus einem privaten Signaturschlüssel, der zum Signieren verwendet wird, und einem öffentlichen Signatur-

prüfschlüssel, mit dem man Signaturen prüft. Der private Schlüssel muss geheim gehalten werden.

Bei Verschlüsselung fungiert der private Teil als Entschlüsselungsschlüssel, der öffentliche Teil des Schlüssels als Verschlüsselungsschlüssel.

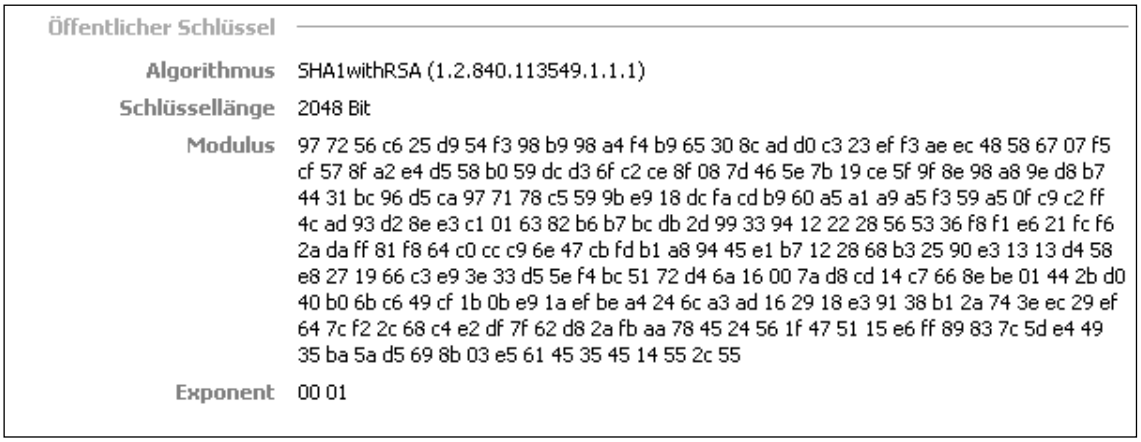


Abbildung 53: Bereich "öffentlicher Schlüssel" (RSA-Schlüssel)

5.5.1.1 Zeile "Algorithmus"

Angezeigt werden der Name des Algorithmus, auf dem der öffentliche Schlüssel des Zertifikatsinhabers basiert, und in Klammern seine OID.

5.5.1.2 Zeile "Schlüssellänge"

Angezeigt wird die RSA-Schlüssellänge in Bit.

5.5.1.3 Zeilen "Modulus" und "Exponent"

Der öffentliche Schlüssel von RSA wird durch Modulus und Exponent bestimmt.

5.5.2 ECDSA-Schlüssel

ECDSA ist die Abkürzung für "Elliptic Curve Digital Signature Algorithmus". Dieses ist eine Variante des Digital Signature Algorithm (DSA), die Elliptische-Kurven-Kryptographie verwendet. Der nPA nutzt z. B. (zukünftig) dieses Verfahren, um qualifizierte Signaturen zu erzeugen.

Bei ECDSA-Schlüsseln hat die Anzeige die folgende Form:

Öffentlicher Schlüssel	
Parameterversion	2
Körpertyp-OID	1.2.840.10045.1.1
Körperparameter	01 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
Kurvenparameter A	01 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fc
Kurvenparameter B	51 95 3e b9 61 8e 1c 9a 1f 92 9a 21 a0 b6 85 40 ee a2 da 72 5b 99 b3 15 f3 b8 b4 89 91 8e f1 09 e1 56 19 39 51 ec 7e 93 7b 16 52 c0 bd 3b b1 bf 07 35 73 df 88 3d 2c 34 f1 ef 45 1f d4 6b 50 3f 00
Seed	d0 9e 88 00 29 1c b8 53 96 cc 67 17 39 32 84 aa a0 da 64 ba
Kurvenpunkt	04 00 c6 85 8e 06 b7 04 04 e9 cd 9e 3e cb 66 23 95 b4 42 9c 64 81 39 05 3f b5 21 f8 28 af 60 6b 4d 3d ba a1 4b 5e 77 ef e7 59 28 fe 1d c1 27 a2 ff a8 de 33 48 b3 c1 85 6a 42 9b f9 7e 7e 31 c2 e5 bd 66 01 18 39 29 6a 78 9a 3b c0 04 5c 8a 5f b4 2c 7d 1b d9 98 f5 44 49 57 9b 44 68 17 af bd 17 27 3e 66 2c 97 ee 72 99 5e f4 26 40 c5 50 b9 01 3f ad 07 61 35 3c 70 86 a2 72 c2 40 88 be 94 76 9f d1 66 50
Ordnung	01 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fa 51 86 87 83 bf 2f 96 6b 7f cc 01 48 f7 09 a5 d0 3b b5 c9 b8 89 9c 47 ae bb 6f b7 1e 91 38 64 09
Cofactor	01
Parameter W	00 04 01 7f 83 0a bb 63 15 89 31 b3 9d d4 dc e8 70 b1 b3 7c b4 e5 af ac a0 6d 5c 50 ea e5 37 ac a9 72 d1 cf af 0c 0b ab a8 77 23 6f d2 e3 42 0d 75 2f 4c 7b d1 49 93 49 f9 a2 f6 34 ca f8 3a 65 51 3e d0 47 01 0d e8 9b ee 78 0a 67 11 9c 94 d2 58 af d0 5e 23 12 2c ae 27 c5 77 56 ca 84 60 51 98 87 de d6 1f 26 16 81 c7 2d 06 66 42 e8 cc b1 6c 3a f2 48 40 aa 37 b0 b9 08 07 25 e3 c3 c0 74 8c 5d b0 9c 06 a3

Abbildung 54: Bereich "öffentlicher Schlüssel" (ECDSA-Schlüssel)

5.6 Signatur des Ausstellers im Zertifikat

Angezeigt werden hier zuerst der Name des Signaturalgorithmus, der vom Aussteller (Zertifizierungsdiensteanbieter) zur Signatur des Zertifikats (TBS-Bereich des Zertifikats) verwendet wurde, und die Signatur über den TBS-Teil des Zertifikats, erzeugt durch den Zertifizierungsdiensteanbieter.

Signatur des Ausstellers	
Signaturalgorithmus	SHA1withRSA
Signatur	65 61 e4 b8 b2 80 1a 76 9e b1 b6 ca 62 be 43 7a 6e 6d 2c 19 81 ef 9b d5 eb 54 c7 a0 4f 1a d7 90 03 fc dd dc fa b7 92 6d 16 9c 07 06 b7 e7 1f 3f f0 e6 23 8c b9 0b 4b 88 89 b8 f8 d6 6d 74 99 1b 04 ff f3 d6 e8 93 85 89 8a f0 52 6f 68 94 0a 25 bc c3 8d af 08 c9 12 d5 57 84 f8 b1 22 24 52 bd fe a6 bc e7 79 de 8e 4e 1a 7c 57 92 ef 65 aa 8b 6a 8d 54 63 00 57 14 8c e3 76 28 95 1d 26 43 3c 60 9d 42 e9 98 d9 75 f2 64 dc 8d a7 77 bd a1 a9 56 26 10 fa 99 f2 b7 cc 7d d0 80 e3 99 1a 09 ea e9 ee bb 62 8d 2f ea ff 25 6e 81 db 30 d2 ed 27 c7 72 bf eb 42 b5 34 c1 1b 6e ac aa 77 06 7e 2b d1 6b f1 00 e1 a6 81 e9 a7 4a bb e0 34 88 d0 2d 04 28 21 dd c6 32 92 51 0d 8f 7a 3f 79 06 50 33 ec a0 4f ad d6 78 75 65 61 52 1e 3f f9 43 56 f9 cb 50 78 ae 39 e1 e9 d5 0f 0d 80 d9 2e 5e fa 57

Abbildung 55: Anzeige "Signatur des Ausstellers"

5.6.1 Zeile "Signaturalgorithmus"

Angezeigt wird der vom Aussteller (Zertifizierungsdiensteanbieter, Trustcenter) verwendete Algorithmus zur Signatur des Zertifikats [Feld `signatureAlgorithm`]. Er muss identisch sein mit dem Eintrag in der Zeile "Algorithmus" im Bereich "Allgemeines" [Feld `signature`].

5.6.2 Zeile "Signatur"

Angezeigt wird die Signatur des Ausstellers (Trustcenters, Zertifizierungsdiensteanbieter) [`signatureValue`] als hexadezimaler Ausdruck.

5.7 Fingerabdruck des Zertifikats

Der Fingerabdruck (Fingerprint) ist der durch den Verification Interpreter berechnete Hashwert einer auf das angezeigte Zertifikat (TBS-Teil des Zertifikats) angewendeten Hash-Funktion. Berechnet und angezeigt werden folgende Hashwerte: SHA1 und MD5. Die Hashwerte sind nicht Bestandteil des angezeigten Zertifikats.

5.7.1 Zeilen "UID des Ausstellers" und "UID des Inhabers"

Angezeigt wird ein Identifikationskennzeichen für den Aussteller des Zertifikats als Zeichenkette [Feld `issuerUniqueID`] bzw. für den Inhaber des Zertifikats als Zeichenkette [Feld `subjectUniqueID`].

5.7.1.1 Qualifiziertes Signaturzertifikat gemäß Common PKI-Profil

Beide Felder sollen gemäß CommonPKI SigG-Profil bei qualifizierten Zertifikaten nicht verwendet werden, da sie für die eindeutige Konstruktion der Verifikationsketten bei der Prüfung von Zertifikaten nicht geeignet sind. Vielmehr wird eine Kettenbildung über den `issuer.DName/subject.DName` oder über die Erweiterung `SubjectKeyIdentifier` (CA-Zertifikat) bzw. `AuthorityKeyIdentifier` (Nutzerzertifikat [EE-Zertifikat]) durchgeführt.

5.8 Allgemeine Zertifikatserweiterungen

Im folgenden Kapitel werden alle in dem RFC 5280 definierten Standarderweiterungen und privaten Erweiterungen, andere relevante Erweiterungen aus dem RFC 3739 (Qualified Certificates Profile) und jeweils eine Erweiterung aus dem RFC 2560 und der CommonPKI-Spezifikation (SigG-Profil) beschrieben:

a) Standarderweiterungen gemäß RFC 5280:

- Ausstellerschlüssel-ID und Inhaberschlüssel-ID
- Schlüsselverwendung
- Zertifizierungsrichtlinien
- Richtlinienzuordnungen
- Alternativer Name des Inhabers
- Alternativer Name des Ausstellers
- Verzeichnisattribute des Inhabers
- Allgemeine Einschränkungen (nur in CA-Zertifikaten)
- Beschränkung des Namensraums (nur in CA-Zertifikaten)
- Richtlinienbeschränkungen (nur in CA-Zertifikaten)
- Erweiterte Schlüsselverwendung
- Distributionspunkt für CRLs
- Unterdrückung jeder Policy
- neueste CRL

b) Im RFC 5280 definierte private Erweiterungen:

- Authority Information Access
- Subject Information Access

c) Im RFC 3739 definierte private Erweiterungen für qualifizierte Signaturzertifikate und eine Erweiterung aus dem RFC 2560:

- BiometricData
- Angaben zum qualifizierten Zertifikat
- keine OCSP-Prüfung

d) CommonPKI SigG-Profil

- Seriennummer der Chipkarte

Alle beschriebenen Erweiterungen besitzen immer die folgende Unterstruktur

- Erweiterungs-ID (ggf. auch mehrere)
- Kritikalitätsflag
- Inhalt (Werte)

Das Kritikalitätsflag signalisiert gemäß RFC, ob die Erweiterung durch eine Anwendung verarbeitet werden können muss. Da eine Signaturanwendungskomponente allerdings generisch ist und in der Regel nicht in einen fachlichen Workflow eingebunden ist, wird die Erweiterung nur - wie vom Signaturgesetz gefordert - vollständig angezeigt. Damit ist dann zumindest grundsätzlich eine nachgelagerte Verarbeitung möglich. Der Wert des Kritikalitätsflags wird unter dem Namen der Erweiterung wie folgt angezeigt: kritisch: "ja" oder "nein".

5.8.1 Erweiterungen "Aussteller- und Inhaberschlüssel-ID"

Die Ausstellerschlüssel-ID [Extension `AuthorityKeyIdentifier`] erlaubt eine eindeutige Identifizierung des öffentlichen Schlüssels des Ausstellerzertifikats in einem Signaturzertifikat. Die korrespondierende Inhaberschlüssel-ID [Extension `subjectKeyIdentifier`] erlaubt in einem Ausstellerzertifikat die eindeutige Erkennung dieses Zertifikats. Die Erweiterung "Ausstellerschlüssel-ID" hat die folgende allgemeine Form:

Feld	Wert
Erweiterung	Ausstellerschlüssel-ID (OID)
kritisch	ja/nein
Schlüssel-ID	
Name des Ausstellers	
Seriennummer des Ausstellerzertifikats	

Tabelle 3: Erweiterung "Ausstellerschlüssel-ID"

Die Erweiterung Inhaberschlüssel-ID hat die folgende allgemeine Form:

Feld	Wert
Erweiterung	Inhaberschlüssel—ID (OID)
kritisch	ja/nein
Schlüssel-ID	

Tabelle 4: Erweiterung "Inhaberschlüssel-ID"

Die Schlüssel-ID der Erweiterung "Inhaberschlüssel-ID" des Ausstellerzertifikats muss identisch sein mit der Schlüssel-ID der Erweiterung "Ausstellerschlüssel-ID" aus dem Nutzerzertifikat (EE-Zertifikat), um die Bildung von Zertifikatsketten zu ermöglichen. Gemäß RFC ist die Erweiterung eine Pflichtangabe in entsprechenden Zertifikaten. Sie sollte nicht als kritisch markiert sein.

Die Schlüssel-ID der Erweiterung "Inhaberschlüssel-ID" kann auch in Nutzerzertifikaten (EE-Zertifikaten) verwendet werden.

Der Name des Ausstellers in der Erweiterung "Ausstellerschlüssel-ID" kann gemäß CommonPKI-Spezifikation enthalten:

- einen Internet Domain Namen (dNSName, RFC1034) und/oder
- einen DirectoryName (z.B. eine X500-Adresse beliebigen Inhalts) und/oder
- eine URI (uniformResourceIdentifier definiert in RFC1630, z.B. eine URL) und/oder
- eine IP-Adresse (iPAddress) und/oder
- eine OID (OtherName)

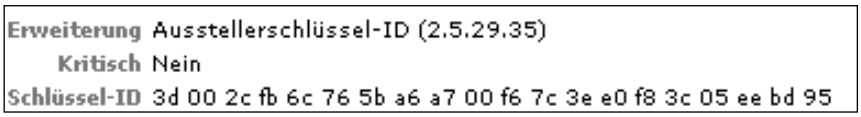


Abbildung 56: Anzeige Erweiterung "Ausstellerschlüssel-ID"

5.8.2 Erweiterung "Schlüsselverwendung"

In dieser Erweiterung wird der Zweck, für den der öffentliche Schlüssel des Zertifikats verwendet werden darf [Extension `keyUsage`], angezeigt. Diese Erweiterung hat eine herausragende Bedeutung und muss nach RFC 5280 und nach der CommonPKI-Spezifikation vorhanden und als kritisch markiert sein. Sie muss demnach von der Anwendung verarbeitet werden können. Da eine Signaturanwendungskomponente allerdings generisch ist und in der Regel nicht direkt in einen fachlichen Workflow eingebunden ist, wird der Inhalt der Erweiterung - wie auch vom Signaturgesetz gefordert - im Prüfprotokoll nur vollständig angezeigt.

Die Erweiterung hat die folgende allgemeine Form:

Feld	Wert
Erweiterung	Schlüsselverwendung (OID)
kritisch	ja
Zertifikatsverwendung	Zulässige Werte

Tabelle 5: Erweiterung "Schlüsselverwendung"

Gemäß RFC sind folgende Verwendungszwecke möglich:

- Digitale Signatur (0)
- Nichtabstreitbarkeit (1)
- Schlüsselverschlüsselung (2)
- Datenverschlüsselung (3)
- Schlüsselvereinbarung (4)
- Zertifikatssignatur (5)
- CRL-Signatur (6)
- nur Verschlüsselung (7)
- nur Entschlüsselung (8)

Erläuterungen zu "Digitale Signatur (0)":

Die Schlüsselverwendung "Digitale Signatur" [Wert: `digitalSignature`] bezeichnet einen öffentlichen Schlüssel, der für die Prüfung von digitalen Signaturen verwendet werden soll und dabei NICHT den Zweck der Nichtabstreitbarkeit erfüllt (siehe auch den folgenden Verwendungszweck). Sie wird häufig im Bereich der fortgeschrittenen elektronischen Signatur nach Signaturgesetz und für Zertifikate für die Authentifizierung verwendet.

Erläuterungen zu "Nichtabstreitbarkeit (1)":

Die Schlüsselverwendung "Nichtabstreitbarkeit" oder "Bekenntnis zu einem Inhalt" [Wert: `nonRepudiation` oder `contentCommitment`] ist gesetzt, wenn der öffentliche Schlüssel zur Prüfung von digitalen Signaturen verwendet werden soll, mit denen Unterschriften geleistet werden und der Signierende sich zu dem signierten Inhalt bekennen will. Bei einer qualifizierten elektronischen Signatur nach deutschem Signaturgesetz entfaltet diese Signatur, bis auf einige spezielle gesetzlich festgelegte Ausnahmen, eine Rechtswirkung wie eine eigenhändige Unterschrift.

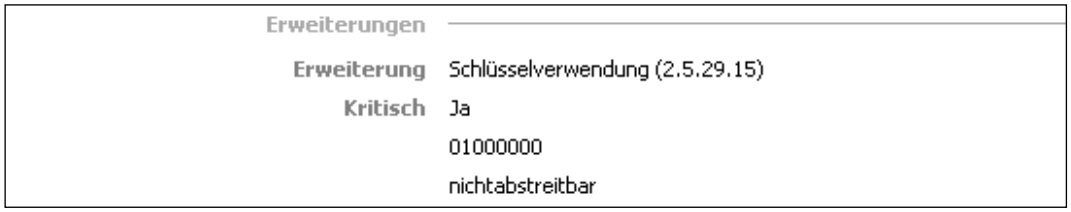


Abbildung 57: Anzeige Erweiterung "Schlüsselverwendung"

Erläuterungen zu "Schlüsselverschlüsselung (2)":

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

Erläuterungen zu "Datenverschlüsselung (3)":

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

Erläuterungen zu "Schlüsselvereinbarung (4)":

Die Schlüsselverwendung "Schlüsselvereinbarung" [`keyAgreement`] ist gesetzt, wenn der Diffie-Hellman-Algorithmus für die Schlüsselvereinbarung verwendet werden soll.

Erläuterungen zu "Zertifikatssignatur (5)":

Die Schlüsselverwendung "Zertifikatssignatur" [`keycertSign`] wird nur bei CA-Zertifikaten verwendet, wenn der Schlüssel für die Verifikation von Signaturen auf Zertifikaten verwendet wird.

Erläuterungen zu "CRL-Signatur (6)":

Die Schlüsselverwendung "CRL-Signatur" [`CRLSign`] wird nur bei CA-Zertifikaten verwendet, wenn der Schlüssel für die Verifikation von CRL-Signaturen verwendet wird.

Erläuterungen zu "nur Verschlüsselung (7)":

Die Schlüsselverwendung "nur Verschlüsselung" [`encipherOnly`] ist gesetzt, wenn der Diffie-Hellman-Algorithmus für die Schlüsselvereinbarung verwendet werden soll.

Erläuterungen zu "nur Entschlüsselung (8)":

Die Schlüsselverwendung "nur Entschlüsselung" [`decipherOnly`] ist gesetzt, wenn der Diffie-Hellman-Algorithmus für die Schlüsselvereinbarung verwendet werden soll.

5.8.2.1 Profilierung gemäß CommonPKI SigG-Profil

Gemäß CommonPKI SigG-Profil darf bei qualifizierten Signaturzertifikaten deutscher Zertifizierungsdiensteanbieter einzig diese Schlüsselverwendung und keine andere gesetzt sein. Gleichwohl bietet dieser Umstand keine Gewähr dafür, dass nicht andere Zertifikate (z.B. auch fortgeschrittene Signaturzertifikate deutscher Trustcenter oder bei qualifizierten Zertifikaten aus der EU, die den Anforderungen der Richtlinie 1999/93/EG genügen, diese und andere zusätzliche Schlüsselverwendungen gesetzt sind. Die Schlüsselverwendung "Nichtabstreitbarkeit" eignet sich daher nicht zur Klassifizierung eines qualifizierten elektronischen Zertifikats.

5.8.3 Erweiterung "Zertifizierungsrichtlinien"

In der Erweiterung "Zertifizierungsrichtlinien" [Extension `certificatePolicies`] sind die Bedingungen festgelegt, unter denen ein Nutzer-Zertifikat herausgegeben wurde und unter denen es verwendet werden darf. In einem CA-Zertifikat verwendet, wird durch die Erweiterung der Satz von Richtlinien für den Zertifizierungspfad begrenzt, die dieses Zertifikat enthalten.

Um die Interoperabilität sicherzustellen, wird in RFC 5280 empfohlen, dass die Erweiterung nur eine OID enthalten soll, die die Qualität der Zertifizierungsrichtlinie festlegt. Optional ist aber auch eine Reihe von weiteren Kennzeichen möglich.

Die Erweiterung hat die folgende allgemeine Form:

Feld	Wert
Erweiterung	Zertifizierungsrichtlinien (OID)
kritisch	ja/nein
Richtlinien-Information 1	
Zertifizierungsrichtlinien-ID	OID, die die Richtlinie repräsentiert
Richtlinienbeschreibung 1	
CPS-URI	URL des Certificate Practice Statements
Beschreibung	Referenz zu einer Beschreibung, explizite Beschreibung, Name der Organisation etc.)
Richtlinienbeschreibung 2	...
Richtlinien-Information 2	...

Tabelle 6: Erweiterung "Zertifizierungsrichtlinien"

Die URI verlinkt auf das Certification Practice Statement (CPS). Wird in einem CA-Zertifikat die OID anyPolicy (2 5 29 32 0) verwendet, wird durch die Erweiterung der Satz von Richtlinien für den Zertifizierungspfad nicht mehr begrenzt.

5.8.3.1 Profilierung gemäß CommonPKI SigG-Profil

Eine besondere Bedeutung hat diese Erweiterung bei qualifizierten Signaturzertifikaten aus Deutschland, die konform zum CommonPKI SigG-Profil sind. Wird die OID mit dem Wert [`id-commonpki-cp-accredited` (1 3 36 8 1 1)] verwendet, bedeutet dies, dass eine Zertifizierungsrichtlinie vorliegt, in der beschrieben ist, dass es sich um ein Zertifikat handelt, welches den Anforderungen an ein qualifiziertes Zertifikat mit Anbieterakkreditierung nach deutschem Signaturgesetz (SigG) genügt. Die Erweiterung sollte gemäß CommonPKI SigG-Profil nicht als kritisch markiert sein.

5.8.4 Erweiterung "Richtlinienzuordnungen"

Die Erweiterung "Richtlinienzuordnungen" [Extension `policyMappings`] wird nur bei CA-Zertifikaten verwendet.

5.8.5 Erweiterung "Alternativer Name des Inhabers"

Die Erweiterung "Alternativer Name des Inhabers" [Extension `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. Die Erweiterung hat die folgende allgemeine Form:

Feld	Wert
Erweiterung	Alternativer Name des Inhabers
kritisch	ja/nein
	Technischer Name

Tabelle 7: Erweiterung "Alternativer Name des Inhabers"

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

5.8.5.1 Profilierung gemäß Common PKI-Profil

Nach CommonPKI-Spezifikation sollte hier die LDAP-URL angegeben sein, über die das CA-Zertifikat heruntergeladen werden kann. Diese Erweiterung sollte gemäß CommonPKI-Spezifikation nicht als kritisch markiert sein.

5.8.6 Erweiterung "Alternativer Name des Ausstellers"

Die Erweiterung "Alternativer Name des Ausstellers" [Extension `issuerAlternativeName`] besteht aus einer Liste von alternativen (technischen) Namen für den Aussteller des Zertifikats. Die Erweiterung hat die folgende allgemeine Form:

Feld	Wert
Erweiterung	Alternativer Name des Ausstellers
kritisch	ja/nein
	Technischer Name

Tabelle 8: Erweiterung "Alternativer Name des Ausstellers"

Der technische Name kann RFC 822-Namen, DNS-Namen, X.400 Adressen, EDI-Namen, URIs oder IP-Adressen sein - im Grunde ist jedes strukturierte Namensschema verwendbar.

5.8.6.1 Profilierung gemäß Common PKI-Profil

Nach Common PKI-Spezifikation sollte hier die LDAP-URL angegeben sein, über die das Zertifikat heruntergeladen werden kann. Diese Erweiterung sollte gemäß CommonPKI-Spezifikation nicht als kritisch markiert sein.

5.8.7 Erweiterung "Verzeichnisattribute des Inhabers"

Die Erweiterung "Verzeichnisattribute des Inhabers" [Extension `subjectDirectoryAttributes`] ist dafür gedacht, zusätzliche Informationen (Attribute) über den Inhaber bereitzustellen. Die Erweiterung hat die folgende allgemeine Form:

Feld	Wert
Erweiterung	Verzeichnisattribute des Inhabers
Kritisch	ja/nein
Attribut 1	z. B. die Postanschrift
Attribut 2	...

Tabelle 9: Erweiterung "Verzeichnisattribute des Inhabers"

5.8.7.1 Profilierung gemäß CommonPKI SigG-Profil

Qualifizierte Zertifizierungsdiensteanbieter aus Deutschland können diese Erweiterung für rechtlich zugelassene Identifikationsdaten verwenden. Diese Informationen können in Attributzertifikaten als Attribut verwendet werden. Gemäß CommonPKI SigG-Profil dürfen nur folgende Attributtypen verwendet werden:

- Name [`commonName`]
- Nachname [`surName`]
- Vorname(n) [`givenName`]
- Titel [`title`]
- Postanschrift [`postalAdress`]
- Geburtstag [`dateOfBirth`]
- Geburtsort [`placeOfBirth`]
- Geschlecht [`Gender`]
- Geburtsland [`countryOfCitizenship`]
- Aufenthaltsland [`countryOfResidence`]
- Geburtsname [`nameAtBirth`]

Diese Erweiterung sollte gemäß CommonPKI SigG-Profil nicht als kritisch markiert sein.

5.8.8 Erweiterung "Allgemeine Einschränkungen"

Die Erweiterung "Allgemeine Einschränkungen" [Extension `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.

5.8.9 Erweiterung "Beschränkung des Namensraums"

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

5.8.10 Erweiterung "Richtlinienbeschränkungen"

Die Erweiterung "Richtlinienbeschränkungen" [Extension `policyConstraints`] findet sich nur in CA-Zertifikaten. Sie legt fest, dass in Zertifikaten, die dem CA-Zertifikat im Zertifizierungspfad folgen, Policy-Identifier (OIDs) definiert werden müssen und/oder verbietet das Policy Mapping in untergeordneten Zertifikaten.

5.8.11 Erweiterung "Erweiterte Schlüsselverwendung"

Die Erweiterung "Erweiterte Schlüsselverwendung" [Extension `extendedKeyUsage`] kann zusätzlich die Verwendungsmöglichkeiten des öffentlichen Schlüssels des Zertifikats einschränken oder erweitern. Die Erweiterung hat die folgende allgemeine Form:

Feld	Wert
Erweiterung	Erweiterte Schlüsselverwendung
kritisch	ja
Zertifikatsverwendung	Liste von OIDs (siehe unten)

Tabelle 10: Erweiterung "Erweiterte Schlüsselverwendung"

Folgende Bezeichner können verwendet werden:

- TLS web server authentication
- TLS web client authentication
- Code-Signing
- Email-Protection
- Zeitstempeldienst
- OCSP-Responder-Signatur

Zeitstempeldienstzertifikate müssen nach RFC 3161 den Verwendungszweck "Zeitstempeldienst" und nur diesen Verwendungszweck besitzen. RFC 3161 verlangt, dass die Erweiterung `ExtendedKeyUsage` bei dieser erweiterten Schlüsselverwendung als kritisch markiert werden muss. Sie muss demnach von der Anwendung verarbeitet werden können. Da eine Signaturanwendungskomponente allerdings generisch ist und in der Regel nicht direkt in einen fachlichen Workflow eingebunden ist, wird der Inhalt der Erweiterung - wie auch vom Signaturgesetz gefordert - im Prüfprotokoll nur vollständig angezeigt.

5.8.11.1 Profilierung gemäß Common PKI-Profil

Zusätzlich zu dieser erweiterten Schlüsselverwendung darf gemäß CommonPKI SigG-Profil bei qualifizierten Zeitstempelzertifikaten noch die Schlüsselverwendung `nonRepudiation` verwendet werden.

Bei OCSP-Responder-Zertifikaten muss die erweiterte Schlüsselverwendung "OCSP-Responder-Signatur" und nur diese Schlüsselverwendung gesetzt sein. Die Erweiterung `ExtendedKeyUsage` ist als kritisch zu markieren.

5.8.12 Erweiterung "Distributionspunkt für CRL"

Die Erweiterung "Distributionspunkt für CRL" [Extension `CRLDistributionPoint`] liefert Informationen darüber, wie Sperrinformationen zu dem Zertifikat bezogen werden können. Die Erweiterung hat die folgende allgemeine Form:

Feld	Wert
Erweiterung	Distributionspunkt für CRL (OID)
kritisch	Nein
Distributionspunkt Name 1	Eindeutiger Name
Sperrinformationen zu	Zulässige Werte siehe unten
Herausgeber der Sperrliste	Name
Distributionspunkt Name 2	...

Tabelle 11: Erweiterung "Distributionspunkt für CRL"

Der Name des Distributionspunkts für CRL kann der volle "Distinguished Name" (Eindeutiger Gesamtname eines LDAP-Objekts) sein oder auch die URL zum Download der CRL (LDAP und/oder HTTP).

CRLs können nur eine Auswahl der gesperrten Zertifikate enthalten. In diesem Fall ist anzugeben, zu welchen Sperrgründen Seriennummern enthalten sind. Zulässig ist eine Auswahl folgender Sperrgründe:

- privater Schlüssel kompromittiert
- privater CA-Schlüssel kompromittiert
- Name/andere Informationen über den Inhaber haben sich geändert
- Zertifikat ersetzt
- Zertifikat wird nicht mehr benötigt
- Zertifikat vorübergehend gesperrt
- Attribut aus Zertifikat zurückgezogen
- Privater Schlüssel des Attributausstellers kompromittiert

Wird kein Sperrgrund angegeben, wird die CRL für alle benannten Sperrgründe verwendet. In der Regel wird in der Erweiterung auch angegeben, wer der Herausgeber der Sperrliste ist. Dieses sind in der Regel ausgewählte Attribute aus dem Feld "Inhaber" des Zertifikats, von dem die Sperrliste signiert worden ist, wie z. B.:

- Land [`countryName`]
- Organisation [`organizationName`]
- Organisationseinheit [`organizationalUnitName`]
- Name [`commonName`]

5.8.12.1 Profilierung gemäß Common PKI-Profil

CAs müssen gemäß CommonPKI-Spezifikation CRLs zum Download via LDAP bereitstellen. Die Bereitstellung via http ist demgegenüber optional. Wird eine LDAP-URL angegeben, muss auch der Herausgeber der Zertifikatssperrliste angegeben werden. Diese Erweiterung sollte nicht als kritisch markiert sein.

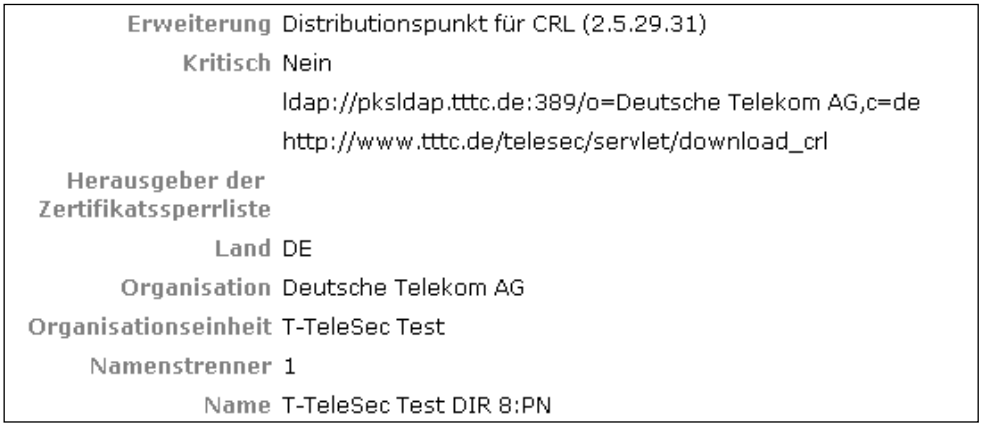


Abbildung 58: Anzeige Erweiterung "Distributionspunkt für CRL"

5.8.13 Erweiterung "Unterdrückung jeder Policy"

Die Erweiterung wird nur in Zertifikaten verwendet, die für CAs herausgeben werden, wenn verhindert werden soll, dass diese die OID `anyPolicy` (2 5 29 32 0) für weitere Zertifikate im Pfad verwenden.

5.8.14 Erweiterung "neueste CRL"

Die Erweiterung "neueste CRL" beschreibt, wie Delta-CRL-Informationen erhalten werden können. Sie hat dieselbe Syntax wie die Erweiterung "Distributionspunkt für CRL". Diese Erweiterung sollte gemäß RFC 5280 nicht als kritisch markiert sein.

5.8.15 Erweiterung Zugangsinformationen des Ausstellers

Die Erweiterung "Zugangsinformationen des Ausstellers" [private Extension gemäß RFC 5280 `authorityInformationAccess`] definiert, wie weitere Informationen und Services der ausstellenden CA genutzt werden können. Die Erweiterung hat die folgende allgemeine Form:

Feld	Wert
Erweiterung	Zugangsinformationen des Ausstellers (PKIX OID)
kritisch	nein
Zugangsart 1	OID für Zugangsart
	Zugangsort (in der Form einer URL)
Zugangsart 2	...

Tabelle 12: Erweiterung "Zugangsinformationen des Ausstellers"

5.8.15.1 Profilierung gemäß CommonPKI SigG-Profil

Bei qualifizierten Signaturzertifikaten, die konform zum CommonPKI SigG-Profil sind, 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`].

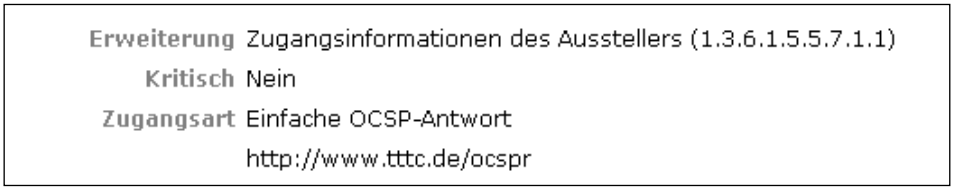


Abbildung 59: Anzeige Erweiterung "Zugangsinformationen des Ausstellers"

Für den Fall, dass ein Trustcenter einen OCSP-Service anbietet, muss diese Erweiterung mit der URL des Services gemäß CommonPKI-Spezifikation angegeben werden.

5.8.16 Erweiterung Zugangsinformationen des Inhabers

Die Erweiterung "Zugangsinformationen des Inhabers" [private Extension gemäß RFC 5280 `subjectInformationAccess`] definiert, wie weitere Informationen und Services des Inhabers des Zertifikats genutzt werden können. Die Erweiterung hat die folgende allgemeine Form:

Feld	Wert
Erweiterung	Zugangsinformationen des Inhabers (PKIX OID)
kritisch	nein
Zugangsart 1	OID für Zugangsart
	Zugangsort (in der Form einer URL)
Zugangsart 2	...

Tabelle 13: Erweiterung "Zugangsinformationen des Inhabers"

5.8.16.1 Profilierung gemäß Common PKI-Profil

Wenn der Inhaber des Zertifikats eine CA ist, können hier folgende Informationen zu weiteren CA-Diensten beschrieben werden: die OID "CA-Repository" [`id-ad-caRepository`] weist auf die folgende Angabe einer URL für ein Verzeichnis hin, das von der CA ausgestellte Zertifikate enthält. Je nach Zugangsart kann eine LDAP, http oder ftp URL angegeben sein. Die OID "Zeitstempeldienst" [`id-ad-timeStamping`] zeigt an, dass die CA einen Zeitstempeldienst gemäß RFC 3161 anbietet. Es folgen dann immer Zugangsinformationen als http-URL (wie in CommonPKI-Spezifikation, Part 4 definiert).

5.8.17 Erweiterung "BiometricData"

Erweiterung für gehashte biometrische Informationen, wie z. B. die Angabe des Hash-Algorithmus, mit dem das biometrische Datenimage gehasht wurde [private qc Extension gemäß RFC 3739 `BiometricInfo`].

5.8.18 Erweiterung "Angaben zum qualifizierten Zertifikat"

In der Erweiterung "Angaben zum qualifizierten Zertifikat" [private qc Extension gemäß RFC 3739 `qcStatements`] werden qualifizierte Zertifikatstatements aufgelistet.

Die Erweiterung hat die folgende allgemeine Form:

Feld	Wert
Erweiterung	Angaben zum qualifizierten Zertifikat (PKIX OID)
kritisch	nein
Statement 1	OID für das Statement
	Weitere Informationen
Statement 2	...

Tabelle 14: Erweiterung "Angaben zum qualifizierten Zertifikat"

5.8.18.1 Profilierung gemäß Common PKI SigG-Profil

Gemäß CommonPKI-Spezifikation sind folgende ETSI-Statements (siehe ETSI TS 101 862 v1.3.3: Qualified Certificate profile) möglich:

- Zertifikat konform mit EU-Direktive 1999/93/EC [`id-etsi-qcs-QcCompliance`]
- Privater Schlüssel auf Smartcard gemäß EU-Richtlinie 1999/93/EC Anhang 3 [`id-etsi-qcs-QcSSCD`]
- Aufbewahrung externer Identifikationsdokumente durch CA [`id-etsi-qcs-QcRetentionPeriod`]
- Monetäre Beschränkung [`id-etsi-qcs-QcLimitValue`]

Zu Statement "Zertifikat konform mit EU-Direktive 1999/93/EC": Das Statement wird vom Aussteller des Zertifikats gesetzt, wenn er ein qualifiziertes Zertifikat ausgestellt hat, das konform ist zu der in nationales Recht umgesetzten EU-Direktive 1999/93/EC, in dessen Land der ZDA ansässig ist. Ist das Zertifikat vom einem ZDA aus Deutschland, handelt es sich um ein SigG-konformes qualifiziertes Zertifikat.

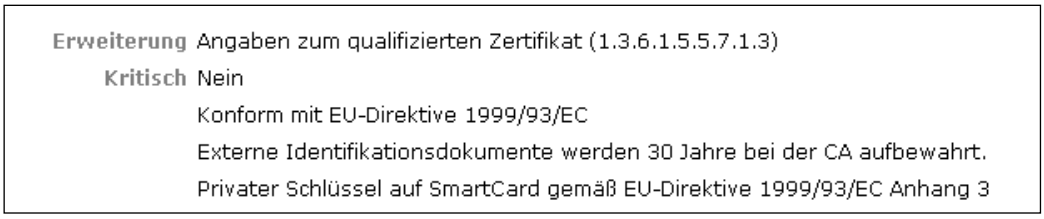


Abbildung 60: Anzeige Erweiterung "Angaben zum qualifizierten Zertifikat"

Zu dem Statement "Privater Schlüssel auf Smartcard gemäß EU-Richtlinie 1999/93/EC Anhang 3": Das Statement wird gesetzt, wenn der zum öffentlichen Schlüssel korrespondierende private Schlüssel auf einer Smartcard gespeichert ist und es sich bei dieser Smartcard um eine sichere Signaturerstellungseinheit gemäß der in nationales Recht umgesetzten EU-Direktive 1999/93/EC EU-Richtlinie 1999/93/EC, Anhang 3 handelt.

Die CommonPKI-Spezifikation schreibt für eine qualifizierte elektronische Signatur die beiden zuerst genannten Statements zwingend vor (siehe Common PKI Part 1 – Page 38). Im EU-Kontext stellt nur die Kombination beider Statements sicher, dass eine QES intendiert ist.

Zu Statement "Aufbewahrung externer Identifikationsdokumente": Das Statement zeigt an, wie viele Jahre externe Identifikationsdokumente (z. B. Kopie des Personalausweises) beim

Zertifizierungsdiensteanbieter nach Ablauf der Zertifikatsgültigkeit aufbewahrt werden. Dadurch ist es möglich, für den genannten Zeitraum im Streitfall die zu einem Zertifikat gehörende physische Person zu identifizieren.

Zu Statement "Monetäre Beschränkung": Das Statement schränkt den finanziellen Verfügungsrahmen des Zertifikatsinhabers ein. Es besitzt folgende Form: Zahlenwert mit Währungsangabe.

Die Erweiterung "Angaben zum qualifizierten Zertifikat" sollte gemäß CommonPKI-Spezifikation nicht als kritisch markiert sein.

5.8.19 Erweiterung "keine OCSP-Prüfung"

Die Erweiterung "keine OCSP-Prüfung" [private qc Extension gemäß RFC 2560 `OCSPNo-chec`] wird nur bei OCSP-Responder-Zertifikaten verwendet und schreibt vor, dass keine OCSP-Prüfung für diese Zertifikate durchgeführt wird.

5.8.20 Erweiterung "Attributzertifikat"

Die Erweiterung "Attributzertifikat" [CommonPKI SigG-Profil private Extension `Liability-LimitationFlag`] kann die Werte "vorhanden" oder "nicht vorhanden" besitzen. Der Wert "vorhanden" zeigt an, dass ein Attributzertifikat zu dem qualifizierten Signaturzertifikat existiert, durch das die Verwendung des Signaturzertifikats beschränkt, erweitert oder präzisiert wird.

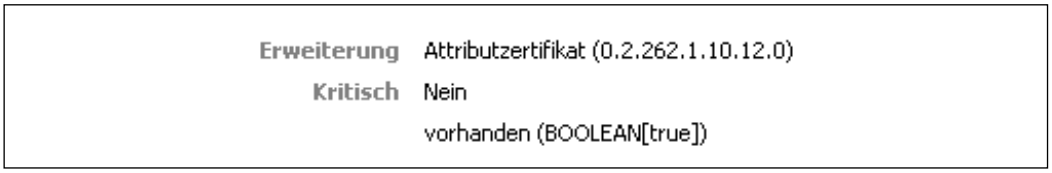


Abbildung 61: Anzeige Erweiterung "Attributzertifikat" vorhanden

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, sodass diese Information dann im Signaturzertifikat nicht vorhanden sein kann.

Die Erweiterung sollte gemäß CommonPKI-Spezifikation nicht als kritisch markiert sein.

5.8.21 Erweiterung "Datum Zertifikatserzeugung"

Die Erweiterung "Datum Zertifikatserzeugung" [CommonPKI SigG-Profil private Extension `DateOfCertGen`] zeigt das Datum an, an dem das Zertifikat erzeugt wurde. Die Form ist: `Tag.Monat.Jahr Stunde:Minute:Sekunde (tt.mm.jjjj hh:mm.ss).`

5.8.22 Erweiterung "Seriennummer der Chipkarte"

Die Erweiterung "Seriennummer der Chipkarte" [CommonPKI SigG-Profil, private Extension: `ICSSN`] zeigt die Seriennummer der Signaturkarte an, auf der der zum öffentlichen Schlüssel korrespondierende private Schlüssel abgespeichert wurde.

5.9 Inhaberattribute nach Common PKI SigG-Profil

Die CommonPKI-Spezifikation Version 2.0 beschreibt im SigG-Profil eine Reihe von Zertifikatserweiterungen, die die Wirksamkeit einer qualifizierten Signatur beschränken, erweitern oder präzisieren. Damit werden u. a. die speziellen Anforderungen umgesetzt, die sich aus dem deutschen Signaturgesetz für qualifizierte Zertifikate ergeben. Diese Attribute können sich in einem qualifizierten Signaturzertifikat selbst (technisch dann als Extension [Erweiterung]) oder in einem separaten qualifizierten Attributzertifikat (technisch dann als Attribut) befinden, welches eindeutig auf ein qualifiziertes Basiszertifikat (Signaturzertifikat) referenzieren muss.

Folgende Attribute werden in der Spezifikation profiliert:

- Vertretungsmacht,
- bestätigte/r Beruf/Berufsausübung,
- monetäre Beschränkung,
- altersabhängige Einschränkung,
- allgemeine Einschränkung und die
- Zusatzinformation.

Alle Attribute besitzen immer die Unterstruktur, ID, Kritikalitätsflag und Werte. Der Wert des Kritikalitätsflags wird unter dem Namen der Erweiterung wie folgt angezeigt: kritisch: "ja" oder "nein". Bei allen Inhaberattributen soll gemäß CommonPKI-Spezifikation das Kritikalitätsflag auf den Wert “Kritisch = Nein” gesetzt sein.

Das Kritikalitätsflag signalisiert gemäß RFC, ob die Erweiterung durch eine Anwendung verarbeitet werden können muss oder nicht. Da eine Signaturanwendungskomponente allerdings generisch ist und in der Regel nicht direkt in einen fachlichen Workflow eingebunden ist, wird als ausreichende Verarbeitung die vollständige Anzeige des Inhalts der Erweiterung angenommen. Damit ist dann zumindest grundsätzlich eine nachgelagerte Verarbeitung möglich. Die vollständige Anzeige des Inhalts qualifizierter Zertifikate ist in jedem Fall auch durch das Signaturgesetz vorgeschrieben.

Die einzelnen Attribute werden in den folgenden Kapiteln ausführlich erläutert.

5.9.1 Attribut "Vertretungsmacht"

Das Attribut "Vertretungsmacht" [Attribut oder Extension `id-commonpki-at-procuration`] wird verwendet, wenn ein Zertifikatsinhaber für eine andere Person Unterschriften leisten darf. In der Regel hat die Einschränkung folgenden Aufbau:

- Feld Vertretung gemäß Landesrecht von [Feld `country`], und/oder
- Feld Art der Vertretung `[stypeOfSubstitution]` und/oder
- Feld Vertretene Person `[signingFor]`.

Im Feld "Vertretung gemäß Landesrecht" wird das Land angezeigt, dessen Recht der Vertretung zugrunde liegt. Gemäß CommonPKI SigG-Profil ist dieses ein Wert mit zwei Zeichen, wie z. B. DE für Deutschland.

Der Wert im Feld "Art der Vertretung" beschreibt die Art der Vertretung, wie z.B. Prokura, mit einer maximalen Feldlänge von 128 Zeichen.

Das Feld "vertretene Person" kann folgende Attribute der vertretenen Person umfassen:

- Aufenthaltsland `[countryOfResidence]`

- Bundesland `[stateOrProvinceName]`
- Domainname `[domainComponent]`
- Familienname (Nachname) `[surName]`
- Geburtsland `[countryOfCitizenship]`
- Geburtsname `[nameAtBirth]`
- Geburtsort `[placeOfBirth]`
- Geburtstag `[dateOfBirth]`
- Generationskennzeichen `[generationQualifier]`
- Geschlecht `[Gender]`
- Initialen `[initials]`
- Land `[countryName]`
- Name `[commonName]`
- Namensunterscheider `[distinguishedNameQualifier]`
- Organisation `[organizationName]`
- Organisationseinheit `[organizationalUnitName]`
- Ort `[localityName]`
- Postadresse `[postalAdress]`
- Seriennummer `[serialNumber]`
- Titel `[title]`
- Vorname(n) `[givenName]`

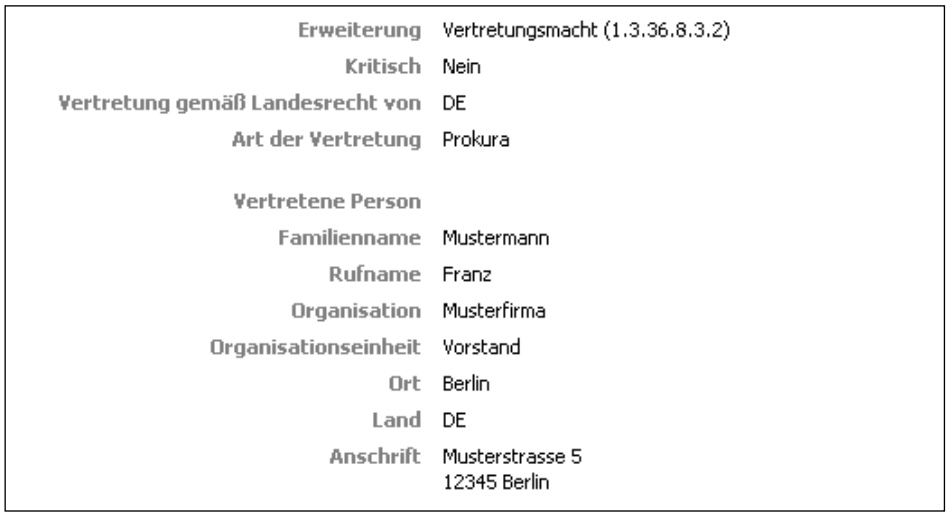


Abbildung 62: Attribut "Vertretungsmacht gemäß CommonPKI SigG-Profil"

Anstatt der vertretenen Person kann auch eine Zertifikatsreferenz angegeben werden [Feld `certRef`], die auf ein Signaturzertifikat der vertretenen Person verweist. Es muss sich hierbei um ein qualifiziertes Signaturzertifikat handeln. In diesem Fall wird der Name des Ausstellers des Zertifikats angezeigt [Feld `Issuer`], für das die Vertretung erteilt wurde, und die Seriennummer dieses Zertifikats [Feld `Serial`].

Angezeigt werden alle im Zertifikat vorhandenen Einträge zu diesem Attribut. Das Attribut muss gemäß CommonPKI SigG-Profil angezeigt werden. Als Erweiterung sollte das Attribut nicht als kritisch markiert sein. Dieses Attribut kann in einem Attributzertifikat auch als Attribut verwendet werden.

5.9.2 Attribut "bestätigter Beruf"

Das Attribut "bestätigter Beruf/bestätigte Berufsbezeichnung oder -ausübung" [Attribut oder Extension `id-commonpki-at-admission`] bzw. [Attribut oder Extension `id-commonpki-at-namingAuthorities`] wird verwendet, um einen Beruf oder eine Berufsausübung zu bestätigen. Damit verbunden ist häufig auch die Berechtigung, bestimmte Aufgaben erledigen zu dürfen. Angezeigt werden alle im Zertifikat vorhandenen Einträge zu diesem Attribut. Das Attribut hat den folgenden Aufbau für einen Bestätigungseintrag:

5.9.2.1 Bestätigende Institution

Angezeigt wird der Name der bestätigenden Institution [`admissionAuthority`] oder der Institution, die ein bestätigtes (amtliches) Register führt [`namingAuthority`]. Angezeigt werden alle vorhandenen Inhaber-Attribute (X.501, wie z. B. Name [`commonName`], Organisation [`organizationName`], Organisationseinheit [`organizationalUnitName`], Ort [`localityName`], Land [`countryName`] und die Postanschrift [`postalAdress`].

Als `namingAuthority` 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.

Der Name kann als Text [`namingauthorityText`] (Name, Land, Name des Registers) und/oder als Nummer (`ObjectIdentifier`) [`namingauthorityID`] angegeben werden, wenn diese bei www.teletrust.de und/oder als URL [`namingauthorityUrl`] geführt wird. Die Berufsbezeichnung kann als Text [`professionItems`] und bei von TeleTrusT geführten NamingAuthorities, die Berufsbezeichnungen festgelegt haben, als OID [`professionOIDs`] geführt werden. Zusätzlich kann noch die Registernummer im Titelregister [`registrationNumber`] angegeben sein.

5.9.2.2 Berufsinformation

Es folgt die Anzeige des Berufs [`professionInfo`] im Feld Berufseintrag und bei Register führenden Institutionen, soweit vorhanden, die Registernummer [`registrationNumber`] für diesen Eintrag.

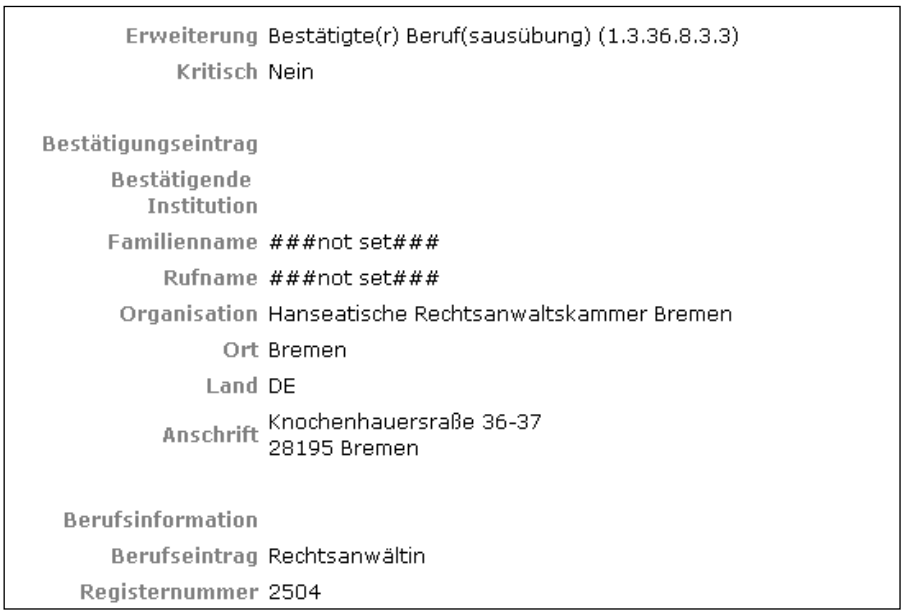


Abbildung 63: Erweiterung bestätigter Beruf (einer namingAuthority) gemäß CommonPKI SigG-Profil

Die Syntax des Attributs erlaubt mehrere Bestätigungseinträge, die dann alle angezeigt werden.

5.9.3 Attribut "monetäre Beschränkung"

Das Attribut "monetäre Beschränkung" schränkt den finanziellen Verfügungsrahmen des Zertifikatsinhabers ein und besitzt die Form "Zahlenwert Währung". Die Währung wird gemäß ISO4217CurrencyCode interpretiert.

Das Attribut muss gemäß CommonPKI SigG-Profil angezeigt werden. Als Erweiterung sollte das Attribut nicht als kritisch markiert sein. Dieses Attribut kann in einem Attributzertifikat auch als Attribut verwendet werden. Gemäß CommonPKI SigG-Profil ist das Attribut "monetäre Beschränkung" ein optionales Statement in der Zertifikatserweiterung "Angaben zum qualifizierten Zertifikat" [`qcStatement`] mit der Statement-ID `id-etsi-qcs-QcLimit Value`. Das Statement ersetzt im Attributzertifikat die Erweiterung `id-commonpki-at-MonetaryLimit` (im Signaturzertifikat das entsprechende Attribut), die seit dem 31.12.2003 nicht mehr verwendet werden soll. Sollte es sich um ein älteres Zertifikat handeln, wird auch diese Erweiterung/dieses Attribut interpretiert und angezeigt. Angezeigt werden alle im Zertifikat vorhandenen Einträge zu diesem Attribut.

5.9.4 Attribut "altersabhängige Einschränkung"

Im Attribut "altersabhängige Einschränkung" [Attribut oder Extension `id-commonpki-at-declarationOfMajority`] können folgende Altersangaben angezeigt werden.

- das Mindestalter des Zertifikatseigentümers und/oder
- ob der Zertifikatsinhaber volljährig ist und/oder
- das Geburtsdatum.

In das Feld "Mindestalter des Zertifikatsinhabers" (nicht jünger als xx Jahre) [`notYounger Than`]) kann jedes beliebige Alter eingetragen sein.

Der Eintrag "Volljährigkeit" [Feld `fullageAtCountry`] umfasst die Angabe, ob der Zertifikatsinhaber volljährig ist: Volljährigkeit: ja/nein [`fullage`] und die Angabe des Landes, nach dessen Recht die Volljährigkeit festgestellt wurde.

Das Geburtsdatum [Feld `dateOfBirth`] wird in der Form `tt.mm.jjjj` angezeigt.

Angezeigt werden alle im Zertifikat vorhandenen Einträge zu diesem Attribut.

5.9.5 Attribut "Einschränkung"

Das Attribut "Einschränkung" [Attribut oder Extension `id-commonpki-at-restriction`] enthält, wenn vorhanden, einen Freitext der maximalen Länge von 1024 Zeichen, der die Nutzung des Zertifikats in irgendeiner Form beschränkt. Angezeigt werden alle im Zertifikat vorhandenen Einträge zu diesem Attribut.

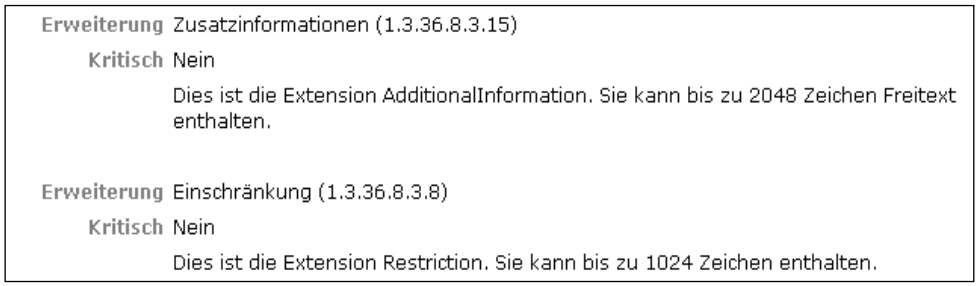


Abbildung 64: Attribute "Einschränkung" und "Zusatzinformationen" gemäß CommonPKI SigG-Profil

5.9.6 Attribut "Zusatzinformationen"

Das Attribut "Zusatzinformationen" [`id-commonpki-at-additionalInformation`] enthält, wenn vorhanden, einen Freitext der maximalen Länge von 2048 Zeichen, der die Nutzung des Zertifikats nicht beschränken darf. Angezeigt werden alle im Zertifikat vorhandenen Einträge zu diesem Attribut.

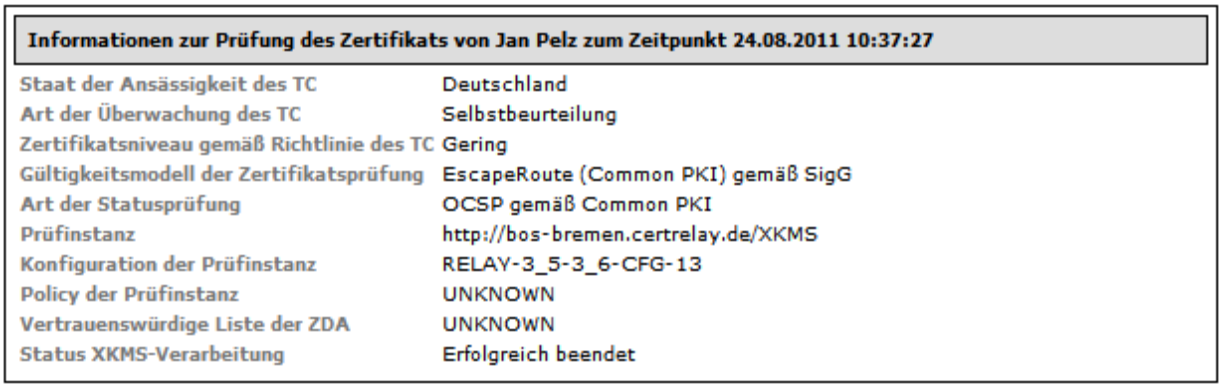
6 Bereich 4: Technische Informationen

Um die Qualität der Signatur und des Zertifikats genauer beurteilen zu können, sind zusätzliche Informationen sinnvoll wie:

- der Staat, in dem das Trustcenter ansässig ist,
- die "Art der Überwachung" des Betriebs des Trustcenters (z.B. durch eine staatliche Stelle),
- das Zertifikatsniveau gemäß Zertifizierungsrichtlinie des Trustcenters,
- das Gültigkeitsmodell der Zertifikatsprüfung oder
- die Art der Statusprüfung (OCSP oder CRL).

Bei Unklarheiten oder im Fehlerfall ist es darüber hinaus hilfreich zu wissen, welches OCSP/CRL-Relay auf der Basis welcher Konfiguration geprüft hat.

In den folgenden Unterkapiteln werden diese technischen Informationen detailliert beschrieben.



Informationen zur Prüfung des Zertifikats von Jan Pelz zum Zeitpunkt 24.08.2011 10:37:27	
Staat der Ansässigkeit des TC	Deutschland
Art der Überwachung des TC	Selbstbeurteilung
Zertifikatsniveau gemäß Richtlinie des TC	Gering
Gültigkeitsmodell der Zertifikatsprüfung	EscapeRoute (Common PKI) gemäß SigG
Art der Statusprüfung	OCSP gemäß Common PKI
Prüfinstanz	http://bos-bremen.certrelay.de/XKMS
Konfiguration der Prüfinstanz	RELAY-3_5-3_6-CFG-13
Policy der Prüfinstanz	UNKNOWN
Vertrauenswürdige Liste der ZDA	UNKNOWN
Status XKMS-Verarbeitung	Erfolgreich beendet

Abbildung 65: Technische Informationen zur Prüfung

6.1 Informationen zum Trustcenter

6.1.1 Zeile "Zuordnung der technischen Informationen zum Zertifikat"

In der Zeile "Informationen zur Prüfung des Zertifikats" werden der Name des Zertifikatsinhabers und der Zeitpunkt der Durchführung der Prüfung angegeben, um eine Zuordnung zu den Prüfergebnissen zu erleichtern. Es handelt sich beim Namen um das Attribut "Name" [`commonName`] aus dem Feld "Inhaber" [`subject`] des Zertifikats.

6.1.2 Zeile "Staat in dem der ZDA ansässig ist"

Angezeigt wird in der Zeile "Staat in dem der ZDA ansässig ist" das Land aus der europäischen Union, in dem das Trustcenter bzw. der Zertifizierungsdiensteanbieter, der das Signaturzertifikat ausgestellt hat, ansässig ist.

Die Information wird der Antwort des OCSP/CRL-Relays (XKMS-Response) entnommen und nicht dem geprüften Zertifikat. Das OCSP/CRL-Relay übernimmt diese Information aus der Standardkonfiguration. Dort ist neben den Root- und Ausstellerzertifikaten und technischen Daten zur Verbindungskonfiguration auch für jedes Trustcenter hinterlegt, in welchem Staat

es ansässig ist bzw. für jeden Zertifizierungsdiensteanbieter hinterlegt, in welchem Staat er überwacht wird bzw. akkreditiert ist.

6.1.3 Zeile "Art der Überwachung" des Trustcenters

Angezeigt wird in dieser Zeile die Art der Überwachung des Trustcenters/Zertifizierungsdiensteanbieters. Folgende Überwachungsqualitäten werden angezeigt.

Anzeige	Erläuterung
a) Überwachungsarten für Trustcenter, die keine qualifizierten Zertifikate ausstellen	
Selbstbeurteilung	Interne Selbstbeurteilung
unabhängige Bewertung auf Dokumentenbasis	Überprüfung auf Einhaltung der geltenden Anforderungen durch eine unabhängige, externe Stelle basierend auf der Überprüfung von Dokumenten
Interner Compliance Audit	Interne periodische Überprüfung auf Einhaltung der geltenden Anforderungen
Überwachung ohne Compliance Audit	Der ZDA wird durch eine öffentliche, nationale oder internationale Stelle/ Behörde auf Einhaltung des geltenden Rechts überwacht.
externer Compliance Audit	Regelmäßige Überprüfung der Einhaltung der geltenden Anforderungen durch externe, unabhängige Prüfer
externer Compliance Audit zertifiziert	Regelmäßige Überprüfung der Einhaltung der geltenden Anforderungen durch externe, unabhängige Prüfer. Der ZDA wird dabei in Übereinstimmung mit einem entsprechenden Standard zertifiziert.
b) Überwachungsarten für Trustcenter/ZDAs, die im Kontext der Ausgabe von qualifizierten Zertifikaten und qualifizierten Signaturkarten relevant sind	
Überwachung mit externem Compliance Audit	Regelmäßige Überprüfung der Einhaltung der geltenden Anforderungen durch externe, unabhängige Prüfer. Der ZDA wird zusätzlich durch eine öffentliche, nationale oder internationale Stelle/Behörde auf Einhaltung des geltenden Rechts überwacht.
Akkreditierung mit externem Compliance Audit	Regelmäßige Überprüfung der Einhaltung der geltenden Anforderungen durch externe, unabhängige Prüfer. Der ZDA ist zusätzlich durch eine öffentliche, nationale oder internationale Stelle/ Behörde akkreditiert und wird auf Einhaltung des geltenden Rechts überwacht.

Tabelle 15: Art der Überwachung

6.1.3.1 Zertifizierungsdiensteanbieter aus der EU

Die EU-Richtlinie zur elektronischen Signatur1999/93/EC sieht vor, dass die Mitgliedstaaten ein angemessenes System zur Überwachung der auf ihrem Staatsgebiet ansässigen ZDA einrichten, die qualifizierte Zertifikate herausgeben, damit die Einhaltung der Bestimmungen der Richtlinie gewährleistet wird. Dabei werden zwei Überwachungsmodelle unterschieden: Beaufsichtigung und Akkreditierung. Im Beaufsichtigungsmodell erklärt und verpflichtet sich der ZDA, dass er die Anforderungen (des jeweiligen Signaturgesetzes, welches die EU-Richtlinie in nationales Gesetz umsetzt) bei Betriebsaufnahme einhält und auch weiter erfüllen wird. Er wird dann als ZDA bei einer nationalen Aufsichtsstelle oder Behörde gelistet. Der

ZDA akzeptiert, dass diese Stelle periodisch überprüft, ob er die postulierten Anforderungen auch wirklich einhält. Im Akkreditierungsmodell hat die Stelle oder Behörde vor Aufnahme des ZDA-Betriebs überprüft, ob der ZDA die gesetzlichen Anforderungen (die für akkreditierte ZDA höher sein können) einhält und die Konformität zertifiziert und listet.

In beiden Modellen verpflichtet sich die ZDA zur Einhaltung der Anforderungen und gesetzlichen Regeln. Diese Compliance[3] wird auch auditiert[4]. In der Regel durch die nationale Aufsichtsstelle oder Behörde selbst oder durch dazu beauftragte externe Prüfer.

6.1.3.2 Zertifizierungsdiensteanbieter aus Deutschland

Zertifizierungsdiensteanbieter aus Deutschland, die qualifizierte Zertifikate herausgeben, erreichen das Überwachungsniveau "Überwachung mit externem Compliance Audit". Akkreditierte ZDA erreichen das Niveau "Akkreditierung mit externem Compliance Audit".

Die Information bezüglich der Überwachungsqualität wird der Antwort des OCSP/CRL-Relays (XKMS-Response) entnommen und nicht dem geprüften Zertifikat. Das OCSP/CRL-Relay übernimmt diese Information aus der Standardkonfiguration. Dort ist neben den Root- und Ausstellerzertifikaten und technischen Daten zur Verbindungskonfiguration auch für jedes Trustcenter/jeden Zertifizierungsdiensteanbieter/jede CA diese Information hinterlegt. Der Eintrag in der Standardkonfiguration wird bei qualifizierten ZDA aus Deutschland aus der sogenannten nationalen TSL in die Konfiguration übernommen. Im nicht qualifizierten Bereich finden sich diese Informationen in den von den Trustcentern bereitgestellten CP- und CPS-Dokumenten. Diese Dokumente beschreiben die Regeln und Richtlinien, nach denen Zertifizierungsdienste Zertifikate ausstellen.

6.1.4 Zeile "Zertifikatsniveau gemäß Zertifizierungsrichtlinie des TC"

Angezeigt wird in der Zeile "Zertifikatsniveau gemäß Zertifizierungsrichtlinie des TC" des Trustcenters/Zertifizierungsdiensteanbieters. Folgende Zertifikatniveaus sind definiert:

[3] Unter Compliance wird hier die Pflicht des ZDA zur Befolgung der „relevanten Regeln“ verstanden. Dazu gehört auch die organisatorische Sicherstellung der Übereinstimmung des Handelns des ZDA mit relevanten Vorschriften (eigenem Regelwerk oder gesetzlichen Anforderungen).

[4] Als Audit wird ein Untersuchungsverfahren verstanden, das dazu dient, Prozesse hinsichtlich der Erfüllung von Anforderungen und Richtlinien zu bewerten.

Anzeige	Erläuterung
a) Zertifikatsniveau für Trustcenter, die keine qualifizierten Zertifikate ausstellen	
unbekannt	unbestimmt
gering	Das Zertifikat wurde von einem Trustcenter erstellt gemäß einer Zertifizierungsrichtlinie (Certificate Policy) oder die Qualitätsbewertung ist durch andere Maßnahmen möglich. Geringes Vertrauen in das Zertifikat.
Fortgeschrittenes Zertifikat gemäß einer einfachen Zertifizierungsrichtlinie	Das Zertifikat wurde von einem ZDA erstellt, dessen Zertifizierungsrichtlinie dem ETSI TS 102 042-Standard für einfache Zertifizierungsrichtlinien (Lightweight Certificate Policy=LCP) oder einem vergleichbaren Standard genügt. Dies bedingt nur ein mittleres Vertrauen in das Zertifikat mit wenig anspruchsvollen Anforderungen an die Zertifizierung.
Fortgeschrittenes Zertifikat gemäß einer normalisierten Zertifizierungsrichtlinie	Das Zertifikat wurde von einem ZDA gemäß einer Zertifizierungsrichtlinie in Übereinstimmung mit dem ETSI TS 102 042-Standard für normalisierte Zertifizierungsrichtlinien (Normalised Certificate Policy=NCP) oder einem vergleichbaren Standard erstellt. Zertifikate nach NCP bieten die gleiche Qualität, wie die nach der Qualified Certificate Policy (QCP) definierten Zertifikate (definiert in der ETSI TS 101 456), ohne die rechtlichen Auflagen durch die EU-Direktive 1999/93/EG zu erfüllen und ohne die Verwendung einer sicheren Signaturerstellungseinheit (SSEE, Smartcard die den Anforderungen der EU-Direktive 1999/93/EG genügt) für den privaten Schlüssel vorzuschreiben.
Fortgeschrittenes Zertifikat gemäß einer normalisierten Zertifizierungsrichtlinie mit privatem Schlüssel auf Smartcard	Das Zertifikat wurde von einem ZDA erstellt, dessen Zertifizierungsrichtlinie dem ETSI TS 102 042-Standard für normalisierte Zertifizierungsrichtlinien oder einem vergleichbaren Standard genügt, wobei die Verwendung einer sicheren Signaturerstellungseinheit (SSEE, Smartcard die den Anforderungen der EU-Direktive 1999/93/EG, Anhang III erfüllt) für den privaten Schlüssel vorgeschrieben ist (Normalised Certificate Policy Plus=NCP+). Zertifikate nach NCP+ bieten die gleiche Qualität wie die nach der Qualified Certificate Policy (QCP) definierten Zertifikate (definiert in der ETSI TS 101 456), ohne die rechtlichen Auflagen durch die EU-Direktive 1999/93/EG zu erfüllen.

Tabelle 16: Zertifikatsniveau gemäß Zertifizierungsrichtlinie des ZDA (1)

Die Informationen bezüglich des Zertifikatsniveaus werden der Antwort des OCSP/CRL-Relays (XKMS-Response) entnommen und nicht dem geprüften Zertifikat. Das OCSP/CRL-Relay übernimmt diese Information aus der Standardkonfiguration. Dort ist neben den Root- und Ausstellerzertifikaten und technischen Daten zur Verbindungskonfiguration auch für jedes Trustcenter/jeden Zertifizierungsdiensteanbieter/jede CA diese Information hinterlegt. Der Eintrag in der Standardkonfiguration wird bei qualifizierten ZDA aus Deutschland aus der sogenannten nationalen TSL in die Konfiguration übernommen. Im nicht qualifizierten Bereich finden sich diese Informationen in den von den Trustcentern bereitgestellten CP- und CPS-Dokumenten. Diese Dokumente beschreiben die Regeln und Richtlinien, nach denen Zertifizierungsdienste Zertifikate ausstellen.

b) Zertifikatsniveau für Trustcenter/ZDAs, die im Kontext der Ausgabe von qualifizierten Zertifikaten und qualifizierter Signaturkarten relevant sind	
Qualifiziertes Zertifikat gemäß der EU-Direktive 1999/93/EC für eine fortgeschrittene Signatur	Das Zertifikat wurde von einem ZDA erstellt, dessen Zertifizierungsrichtlinie dem ETSI TS 101 456-Standard für qualifizierte Zertifikate (Qualified Certificate Policy, QCP) oder einem vergleichbaren Standard genügt. Zertifikate nach QCP entsprechen den Anforderungen des Anhangs I der EU-Direktive 1999/93/EG und sind von einem ZDA ausgestellt. Die Zertifikate genügen dem Anhang II, wobei eine sichere Signaturerstellungseinheit (SSEE, zertifizierte Signaturkarte) für den privaten Schlüssel nicht verwendet wird. Die Signatur entfaltet daher nicht die rechtliche Wirksamkeit, wie die eigenhändige Unterschrift (siehe Artikel 5.2 der EU-Direktive 1999/93/EG).
Qualifiziertes Zertifikat gemäß der EU-Direktive 1999/93/EC mit privatem Schlüssel auf Smartcard für eine qualifizierte Signatur	Das Zertifikat wurde von einem ZDA erstellt, dessen Zertifizierungsrichtlinie dem ETSI TS 101 456-Standard für qualifizierte Zertifikate (Qualified Certificate Policy Plus, QCP+) oder einem vergleichbaren Standard genügt, wobei die Verwendung einer sicheren Signaturerstellungseinheit für den privaten Schlüssel vorgeschrieben ist. Zertifikate nach QCP+ entsprechen den Anforderungen des Anhangs I der EU-Direktive 1999/93/EG und sind von einem ZDA ausgestellt. Die Zertifikate genügen dem Anhang II, der private Schlüssel befindet sich auf einer sicheren Signaturerstellungseinheit, die die Anforderungen der EU-Direktive 1999/93/EG, Anhang III erfüllt. In diesem Fall entfaltet die Signatur weitestgehend die gleiche rechtliche Wirksamkeit, wie die eigenhändige Unterschrift (siehe Artikel 5.2 der EU-Direktive 1999/93/EG).
Qualifiziertes Zertifikat gemäß deutschem Signaturgesetz für eine qualifizierte Signatur	Qualifiziertes Zertifikat gemäß deutschem Signaturgesetz. Der private Schlüssel befindet sich auf einer sicheren Signaturerstellungseinheit. Die Signatur erfüllt damit auch die Anforderungen an eine qualifizierte Signatur gemäß der EU-Direktive 1999/93/EC.
Qualifiziertes Zertifikat mit Anbieterakkreditierung gemäß deutschem Signaturgesetz für eine qualifizierte Signatur mit Anbieterakkreditierung	Qualifiziertes Zertifikat von einem ZDA mit Anbieterakkreditierung gemäß deutschem Signaturgesetz. Der private Schlüssel befindet sich auf einer sicheren Signaturerstellungseinheit. Die Signatur erfüllt damit auch die Anforderungen an eine qualifizierte Signatur gemäß der EU-Direktive 1999/93/EC.

Tabelle 17: Zertifikatsniveau gemäß Zertifizierungsrichtlinie des ZDA (2)

6.2 Zertifikatsprüfung und Prüfinstanz

6.2.1 Zeile "Gültigkeitsmodell der Zertifikatsprüfung"

Angezeigt wird in dieser Zeile das Gültigkeitsmodell der Zertifikatsprüfung. Das Gültigkeitsmodell beschreibt, in welcher Form die Gültigkeit der Zertifikate der Kette in Abhängigkeit vom Signierzeitpunkt in Inhaltsdaten und den Zertifikatssignaturen zu bewerten ist. Das OCSP/CRL-Relay bzw. nachgeordnete XKMS-Responder in den EU-Ländern können Zertifikate gemäß

- Schale-Hybrid
- Kettenprüfung
- EscapeRoute

prüfen.

Erläuterungen zu Schale-Hybrid:

Das Gültigkeitsmodell Schale-Hybrid wird grundsätzlich im RFC 5280 definiert und ist weltweit verbreitet. Alle Zertifikate der Kette oberhalb des zu prüfenden Zertifikats müssen zum Signierzeitpunkt über die Inhaltsdaten gültig gewesen sein (Signaturzeitpunkt liegt innerhalb der Gültigkeitsintervalle der Zertifikate und diese waren zum Signierzeitpunkt nicht gesperrt).

Erläuterungen zu Kette

Im Gültigkeitsmodell Kette wird geprüft, ob die Zertifikatssignatur zu einem Zeitpunkt erfolgte, zu dem das darüber liegende Zertifikat gültig war (Signierzeitpunkt liegt innerhalb des Gültigkeitsintervalls des Zertifikats und das Zertifikat ist zu diesem Zeitpunkt nicht gesperrt).

Erläuterungen zu EscapeRoute

Das Gültigkeitsmodell EscapeRoute ist definiert in der CommonPKI-Spezifikation und setzt die Anforderungen für die Prüfung qualifizierter elektronischer Zertifikate (ausgestellt von deutschen Zertifizierungsdiensteanbietern) um, die sich aus dem deutschen Signaturgesetz (SigG) ergeben. Es ist eine Kombination der Gültigkeitsmodelle Schale-Hybrid und Kette mit zusätzlicher Sperrgrundbewertung.

Bei der EscapeRoute-Prüfung wird zunächst geprüft, ob alle Zertifikate der Kette oberhalb des zu prüfenden Zertifikats zum Signierzeitpunkt der Inhaltsdaten gültig waren (Signierzeitpunkt liegt innerhalb des Gültigkeitsintervalls des Zertifikats und das Zertifikat ist zu diesem Zeitpunkt nicht gesperrt). Dieses entspricht dem Gültigkeitsmodell Schale-Hybrid. Ist dieses nicht der Fall, wird gemäß EscapeRoute alternativ geprüft, ob die Zertifikatssignatur zu einem Zeitpunkt erfolgte, zu dem das darüber liegende Zertifikat gültig war (Signierzeitpunkt liegt innerhalb des Gültigkeitsintervalls des Zertifikats und das Zertifikat ist zu diesem Zeitpunkt nicht gesperrt). Dieses entspricht dem Gültigkeitsmodell Kette. Sowohl bei Gültigkeitsmodell Schale-Hybrid als auch bei der alternativen Kettenprüfung wird zusätzlich geprüft, ob das darüber liegende Zertifikat nach Anbringung der Zertifikatssignatur mit einem kompromittierenden Sperrgrund gesperrt wurde.

Die Information bezüglich des zu verwendenden Gültigkeitsmodells werden der Antwort des OCSP/CRL-Relays (XKMS-Response) entnommen und nicht dem geprüften Zertifikat. Das OCSP/CRL-Relay übernimmt diese Information aus der Standardkonfiguration. Dort ist neben den Root- und Ausstellerzertifikaten und technischen Daten zur Verbindungskonfiguration auch für jedes Trustcenter/jeden Zertifizierungsdiensteanbieter/jede CA diese Information hinterlegt. Die Informationen zum Gültigkeitsmodell finden sich in der Regel in den von den Trustcentern bereitgestellten CP- und CPS-Dokumenten. Diese Dokumente beschreiben

auch die Regeln und Richtlinien, nach denen von Zertifizierungsdiensten ausgestellte Zertifikate zu prüfen sind.

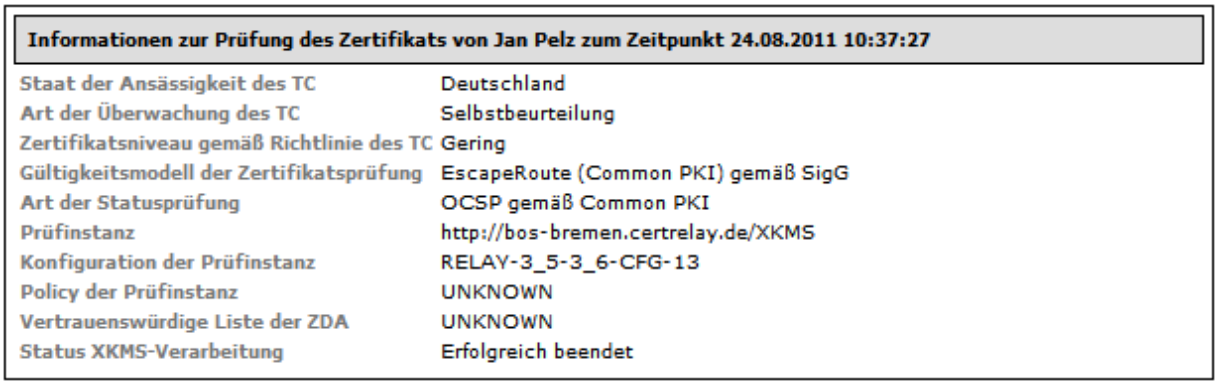
6.2.2 Zeile "Art der Statusprüfung"

Angezeigt wird in der Zeile "Art der Statusprüfung", wie der Sperrstatus des Zertifikats ermittelt wurde. Folgende Arten der Statusprüfung werden durch das OCSP/CRL-Relay unterstützt:

- **OCSP gemäß Common PKI**: Vom OCSP/CRL-Relay wurde eine Online-OCSP-Anfrage gemäß CommonPKI-Spezifikation durchgeführt. In der durch den ZDA qualifiziert signierten Antwort wird neben der Sperrstatusinformation auch der Hashwert des Zertifikats zurückgegeben. Das OCSP/CRL-Relay kann so feststellen, ob das Zertifikat dem ZDA tatsächlich bekannt ist. In Deutschland ist dieses Verfahren für die Prüfung qualifizierter Zertifikate quasi vorgeschrieben.
- **OCSP**: OCSP-Anfrage gemäß RFC2560. Dem OCSP-Responder wird eine CertificateID übergeben, die aus der Seriennummer des User-Zertifikats und Teilen des Aussteller-Zertifikats gebildet wurde. Der OCSP-Responder antwortet dann mit dem Status des Zertifikats. Die Status-Informationen können aus einer CRL stammen, in der nur die Seriennummern gesperrter Zertifikate enthalten sind. Eine Positivaussage "Trustcenter hat das Zertifikat ausgestellt" ist nicht damit verbunden.
- **CRL**: Bei der CRL-Prüfung wird geprüft, ob sich Sperrinformationen zum Zertifikat in der aktuellen Sperrliste des Herausgebers befinden. In der durch die CA signierten Certificate Revocation List (CRL) werden Seriennummern von gesperrten Zertifikaten durch die ausstellende CA eingetragen. Zusätzlich sind der Sperrgrund sowie ein Sperrzeitpunkt enthalten. Die CRLs werden vom OCSP/CRL-Relay regelmäßig aktualisiert. Es handelt sich um eine reine Negativprüfung. Eine Positivaussage "Trustcenter hat das Zertifikat ausgestellt" ist nicht damit verbunden.
- **LDAP**: Bei der LDAP-Abfrage wird online beim Trustcenter über deren LDAP-Server abgefragt, ob das Zertifikat im Verzeichnisdienst vorhanden ist. Das Prüfergebnis ist nicht vom Trustcenter autorisiert.
- **Kombiniert CRL und LDAP:** Die kombinierte CRL-LDAP-Prüfung ermöglicht es, die Sperrstatusinformation aus der CRL zu entnehmen und gleichzeitig festzustellen, ob das Zertifikat auch im Verzeichnisdienst vorhanden ist. Das LDAP-Prüfergebnis ist nicht vom Trustcenter autorisiert.
- **Keine Prüfung**: Es wurde keine Prüfung durchgeführt

6.2.3 Zeile "Prüfinstanz"

Angezeigt wird in der Zeile "Prüfinstanz" die URL des OCSP/CRL-Relays oder des XKMS-Responders, der die Prüfung gegen das Trustcenter/den ZDA tatsächlich durchgeführt hat.



Informationen zur Prüfung des Zertifikats von Jan Pelz zum Zeitpunkt 24.08.2011 10:37:27	
Staat der Ansässigkeit des TC	Deutschland
Art der Überwachung des TC	Selbstbeurteilung
Zertifikatsniveau gemäß Richtlinie des TC	Gering
Gültigkeitsmodell der Zertifikatsprüfung	EscapeRoute (Common PKI) gemäß SigG
Art der Statusprüfung	OCSP gemäß Common PKI
Prüfinstanz	http://bos-bremen.certrelay.de/XKMS
Konfiguration der Prüfinstanz	RELAY-3_5-3_6-CFG-13
Policy der Prüfinstanz	UNKNOWN
Vertrauenswürdige Liste der ZDA	UNKNOWN
Status XKMS-Verarbeitung	Erfolgreich beendet

Abbildung 66: Informationen zur Prüfinstanz

6.2.4 Zeile "Konfiguration der Prüfinstanz"

Angezeigt wird in der Zeile "Konfiguration der Prüfinstanz" ein Identifier, der die Konfiguration des OCSP/CRL-Relays oder des XKMS-Responders beschreibt, der die Prüfung gegen das Trustcenter durchgeführt hat.

6.2.5 Zeile "Policy der Prüfinstanz"

Hier kann eine OID oder URL angegeben werden, die zu einer Policy führt, die das Prüfverhalten der Prüfinstanz beschreibt.

6.2.6 Zeile "Vertrauenswürdige Liste der ZDA"

Bei einem qualifizierten Zertifikat aus einem EU-Land wird in der Zeile "Vertrauenswürdige Liste der ZDA" eine eindeutige Identifizierung der vertrauenswürdigen Liste der beaufsichtigten bzw. akkreditierten Zertifizierungsdiensteanbieter angezeigt, auf deren Basis die Qualitätsinformationen zum Zertifikat bzw. zur Signatur und zum Zertifizierungsdiensteanbieter beruhen. Diese wird von der Prüfinstanz geliefert und sollte die folgende Form haben: Link zur maschinenlesbaren TSL des Landes, in dem der Zertifizierungsdiensteanbieter, dessen Zertifikat geprüft wurde, überwacht wird oder akkreditiert ist und die Versionsnummer (sequenceNumber).

6.2.7 Zeile "XKMS-Verarbeitung"

Die XML Key Management Specification (XKMS) definiert ein Protokoll zur einfachen Validierung von Zertifikaten. Der Verification Interpreter verwendet XKMS (die Methode "validate"), um Validierungsanfragen an das OCSP/CRL-Relay zu stellen und erhält XKMS-Antworten mit den Prüfergebnissen vom OCSP/CRL-Relay zurück. Den Status der XKMS-Verarbeitung und mögliche Fehlergründe werden bei Bedarf auch im Bereich "Technische Informationen" angezeigt.

6.2.7.1 Zeile "Status der XKMS-Verarbeitung"

In der Zeile "Status XKMS-Verarbeitung" werden folgende Informationen über den Status der Bearbeitung der Validierungsanfrage und/oder der XKMS-Antwort angezeigt:

- **Fehler bei Empfänger:** Beim Empfänger ist ein Fehler bei der Verarbeitung aufgetreten. Das Ergebnis ist final.
- **Fehler durch Senderanfrage:** Es ist ein Fehler durch die Senderanfrage aufgetreten. Das Ergebnis ist final.
- **Erfolgreich beendet:** Die Verarbeitung wurde erfolgreich beendet. Das Ergebnis ist final. Wenn nicht alle angefragten Informationen bereitgestellt werden konnten, wird zusätzlich in der Zeile "Erläuterung zum Status der XKMS-Verarbeitung" ein entsprechender Hinweis gegeben.
- unbekannt

6.2.7.2 Zeile "Erläuterung"

In der Zeile "Erläuterung" werden bei Bedarf Zusatzinformationen angezeigt, die Fehler in der Verarbeitung näher erläutern:

- **Vorgang fehlgeschlagen:** Der Empfänger hat versucht, die Anfrage zu bearbeiten. Der Vorgang ist fehlgeschlagen.
  a) Wenn der Status "Fehler durch Senderanfrage" ist, liegt die Fehlerursache beim Sender (z. B. weil das Schema nicht validiert werden konnte oder weil die angefragte Operation nicht unterstützt wird.)
  b) Wenn der Status "Fehler bei Verarbeitung durch Empfänger" ist, liegt die Fehlerursache beim Empfänger (z.B. Datenbankfehler).
- **Informationen nicht vollständig:** Die Verarbeitung war grundsätzlich erfolgreich und wurde final abgeschlossen. Allerdings konnte nur ein Teil der angeforderten Informationen bereitgestellt werden.
- **Operation durch Empfänger nicht unterstützt:** Die durch den Sender angefragte Operation kann durch den Empfänger nicht ausgeführt werden, da sie nicht unterstützt wird.
- **keine Authentifizierung:** Die Verarbeitung wurde durch den Empfänger abgelehnt, weil die vom Sender übermittelte Authentifizierung fehlte oder fehlerhaft ist.
- Unbekannt

6.2.8 Zeile "interner Fehler"

In der Zeile "Interner Fehler" werden interne Fehlermeldungen des angefragten OCSP/CRL-Relays angezeigt. Folgende Fehlermeldungen werden zurückgemeldet:

- **angefragter OCSP-Responder temporär nicht erreichbar:** Der angefragte OCSP-Responder war zum Zeitpunkt der Anfrage durch das OCSP/CRL-Relay temporär nicht erreichbar. Entweder hat der OCSP-Responder innerhalb von 90 Sekunden (Defaultwert) gar nicht oder mit einem „try later“ geantwortet.
- **Sperrstatusdienst für angefragtes Zertifikat durch Trustcenter eingestellt:** Es wurde eine Zertifikatsanfrage an das OCSP/CRL-Relay gestellt. Der Aussteller des Zertifikats ist zwar im OCSP/CRL-Relay konfiguriert, hat jedoch für das angefragte Zertifikat den Sperrstatusdienst eingestellt. Diese Information ist der Konfiguration des OCSP/CRL-Relays entnommen worden.

- **Unbekannter Aussteller oder nicht konfiguriertes Ausstellerzertifikat:** Es wurde eine Zertifikatsanfrage an das OCSP/CRL-Relay gestellt. Entweder ist der Aussteller dem OCSP/CRL-Relay unbekannt oder das zum angefragten Signaturzertifikat korrespondierende Ausstellerzertifikat ist nicht in der Konfiguration des OCSP/CRL-Relays vorhanden.
- **Übergebener Prüfzeitpunkt in der Zukunft:** Der in der Anfrage an das OCSP/CRL-Relay übergebene Zeitpunkt, zu dem das OCSP/CRL-Relay das Zertifikat prüfen soll, lag in der Zukunft.
- **Nächster Responder temporär nicht erreichbar:** Es wurde eine Zertifikatsanfrage (zu einem qualifizierten Zertifikat aus dem EU-Ausland) an das OCSP/CRL-Relay gestellt. Diese werden vom OCSP/CRL-Relay automatisch an ein zentrales Gateway geleitet und von dort weiter an den zuständigen XKMS-Responder in einem EU-Land. Dieser war jedoch temporär nicht erreichbar, so dass die Anfrage nicht bearbeitet werden konnte.
- **Chainloop bei Weiterleitung an Responder:** Es wurde eine Zertifikatsanfrage (zu einem Zertifikat aus dem EU-Ausland) an das OCSP/CRL-Relay gestellt, die an einen XKMS-Responder weitergeleitet wurde. Dieser hat wiederum eine Weiterleitung durchgeführt usw. Irgendwo in der Kette der beteiligten Responder ist es zu einem Fehler in Form einer Endlosschleife gekommen.
- **Identifier in Anfrage zu lang:** Ein interner Identifier, der zur Absicherung von Angriffen auf die Kommunikation zwischen anfragendem Client und OCSP/CRL-Relay dient, entspricht nicht der Norm.
- **Unverständlich:** Es wurde eine unverständliche, nicht spezifikationskonforme XKMS-Anfrage an das OCSP/CRL-Relay gestellt.
- **Signatur der Anfrage nicht korrekt:** Die Signatur der XKMS-Anfrage konnte nicht geprüft werden. Das OCSP/CRL-Relay akzeptiert auch nicht-signierte Anfragen.
- **Nicht-zulässiges Zertifikatsformat:** Das in der XKMS-Anfrage an das OCSP/CRL-Relay übermittelte Zertifikat ist nicht standardkonform (X509V3 bzw. V1) und konnte daher nicht geprüft werden.
- Qualität der Zertifikate der Kette nicht konsistent
- Unbekannt

7 Bereich "Übertragungsinformation"

Um eine Manipulation der vom OCSP/CRL-Relay zurückgegebenen Prüfergebnisse in der XKMS-Antwort ausschließen zu können, werden folgende Prüfungen durchgeführt:

Das OCSP/CRL-Relay signiert seine XKMS-Antwort, um Manipulationen bei der Rückmeldung der Ergebnisse auszuschließen. Diese Signatur wird durch den Verification Interpreter mathematisch geprüft. Dieses ist möglich, weil in der SAK, die den Verification Interpreter nutzt, das Signaturzertifikat mit dem Signaturprüfschlüssel des konfigurierten OCSP/CRL-Relays vorgehalten wird.

Es wird überprüft, ob die in der XKMS-Anfrage übermittelten Zertifikate und der Prüfzeitpunkt sowie die Request-IDs mit den in der Antwort übermittelten Zertifikaten, dem Prüfzeitpunkt sowie den Request-IDs übereinstimmen. Damit wird sichergestellt, dass die Prüfinformationen in der XKMS-Antwort (Issuer Trust, Signature, Validity Interval und Revocation Status) tatsächlich den Status der in der Anfrage übermittelten Zertifikate zum übermittelten Prüfzeitpunkt darstellen.

Der Bereich "Übertragungsinformation" wird am Anfang des Prüfprotokolls nur dann angezeigt, wenn die Signaturprüfung nicht positiv verlaufen ist.

Abbildung 67: Bereich "Übertragungsinformation" bei "Gelb"-Prüfung

7.1 Zeile "Prüfinstanz und Prüfergebnis mit Erläuterung"

Das Ergebnis der Prüfung hat im Fehlerfall die folgende Form: In der Zeile "Prüfinstanz und Prüfergebnis mit Erläuterung" werden von links nach rechts zunächst das Prüfergebnis mit dem Namen der Prüfinstanz (Attribut "Name" [`CommonName`] aus dem Signaturzertifikat der Prüfinstanz) in einem farbig unterlegten Kasten und anschließend eine Erläuterung zum Prüfergebnis angezeigt.

7.1.1 Spalten "Name der Prüfinstanz" mit Prüfergebnis und Erläuterung

In der Spalte "Name der Prüfinstanz" werden rechts neben der Feldbezeichnung "Zertifikat" das Ergebnis der mathematischen Signaturprüfung und der Name der Prüfinstanz in einem farbig unterlegten Kasten angezeigt. Folgende Status sind möglich:

- √ Grüner Kasten mit Haken
- ! Gelber Kasten mit Ausrufungszeichen
- X Roter Kasten mit Kreuz:

Erläuterungen zu √ Grüner Kasten mit Haken:

Den in der XKMS-Antwort übermittelten Informationen kann vertraut werden. Die Überprüfung der Signatur der XKMS-Antwort des OCSP/CRL-Relays verlief erfolgreich. Die in der XKMS-Anfrage übermittelten Zertifikate und der Prüfzeitpunkt sowie die Request-IDs stim-

men mit den in der Antwort übermittelten Zertifikaten, dem Prüfzeitpunkt sowie den Request-IDs überein. Dieses Prüfergebnis wird nicht angezeigt.

Erläuterungen zu Gelber Kasten mit Ausrufungszeichen

Bei der Prüfung der Signatur der XKMS-Antwort des OCSP/CRL-Relays ist ein Fehler aufgetreten. Es gibt zwei Ursachen für diesen Status:

Die Prüfung der Signatur der XKMS-Antwort des OCSP/CRL-Relays konnte nicht durchgeführt werden, da die XKMS-Antwort nicht signiert wurde, aber signiert sein sollte oder die XKMS-Antwort signiert wurde, obwohl sie nicht signiert sein sollte. Die in der XKMS-Anfrage übermittelten Zertifikate und der Prüfzeitpunkt sowie die Request-IDs stimmen aber mit den in der Antwort übermittelten Zertifikaten, dem Prüfzeitpunkt sowie den Request-IDs überein. Damit kann den in der XKMS-Antwort übermittelten Informationen nur bedingt vertraut werden. Die Prüfergebnisse aus der XKMS-Antwort (Issuer Trust, Signature, Validity Interval und Revocation Status) werden nicht ausgewertet. Das Gesamtprüfergebnis und die vier Einzelprüfergebnisse zur Zertifikatsprüfung werden in diesem Fall auf "gelb" gesetzt. Die technischen Informationen zur Prüfung werden ebenso ignoriert. Daher wird auch das intendierte Signaturniveau nicht ausgewertet und als Folge die Eignung der Algorithmen nicht überprüft werden. In der Spalte "Erläuterungen" wird angezeigt "Die Signatur der Serverantwort konnte nicht überprüft werden".

Die Verbindung zur Prüfinstanz wurde mit einer Fehlermeldung unterbrochen, z. B. durch ein Timeout oder weil die angefragte Prüfinstanz temporär oder wegen einer fehlerhaften Konfiguration nicht erreichbar war. In diesem Fall existiert keine XKMS-Antwort. Das Gesamtprüfergebnis und die vier Einzelprüfergebnisse zur Zertifikatsprüfung werden in diesem Fall auf "gelb" gesetzt. Da die technischen Informationen zur Prüfung nicht vorhanden sind, kann auch das intendierte Signaturniveau nicht bestimmt und als Folge die Eignung der Algorithmen nicht überprüft werden. In der Spalte "Erläuterungen" wird angezeigt "Beim Versuch den Server zu erreichen ist ein Fehler aufgetreten".

Erläuterungen zu Roter Kasten mit Kreuz:

Den in der XKMS-Antwort übermittelten Informationen kann nicht vertraut werden. Bei der Prüfung der Signatur der XKMS-Antwort des OCSP/CRL-Relays ist ein Fehler aufgetreten.

Mindestens eine der folgenden Prüfungen ist fehlgeschlagen:

- Die Überprüfung der Signatur der XKMS-Antwort des OCSP/CRL-Relays ist fehlgeschlagen. Die Signatur konnte mit dem Signaturprüfschlüssel (aus dem Signaturzertifikat) nicht entschlüsselt werden oder der originale und der neu berechnete Hashwert stimmen nicht überein. In der Spalte "Erläuterungen" wird angezeigt "Die Signaturprüfung der Serverantwort ist fehlgeschlagen".
- Die in der XKMS-Anfrage übermittelten Zertifikate und der Prüfzeitpunkt sowie die Request-IDs stimmen mit den in der Antwort übermittelten Zertifikaten, dem Prüfzeitpunkt sowie den Request-IDs in mindestens einem Fall nicht überein. Damit ist nicht mehr sichergestellt, dass die Prüfinformationen in der XKMS-Antwort (Issuer Trust, Signature, Validity Interval und Revocation Status) tatsächlich der Status der in der Anfrage übermittelten Zertifikate zum übermittelten Prüfzeitpunkt darstellen. In der Spalte "Erläuterungen" wird angezeigt "Die Serverantwort wurde korrumpiert".

In beiden Fällen besteht Manipulationsgefahr. Das Gesamtprüfergebnis und die vier Einzelprüfergebnisse zur Zertifikatsprüfung werden in diesem Fall auf "gelb" gesetzt. Die technischen Informationen zur Prüfung werden ebenso ignoriert. Daher wird auch das intendierte Signaturniveau nicht ausgewertet und als Folge die Eignung der Algorithmen nicht überprüft werden.

7.1.2 Spalte "Name der Prüfinstanz"

In der Spalte "Name der Prüfinstanz" wird rechts neben der Feldbezeichnung "Zertifikat" der Name der Prüfinstanz in einem farbig unterlegten Kasten angezeigt. Der Name der Prüfinstanz ist das Attribut "Name des Zertifikatseigentümers" aus dem Feld Inhaber [`subject`] des Signaturzertifikats. Das Attribut "Name" [`CommonName`] besteht in der Regel bei technischen Zertifikaten aus einem Pseudonym. Genauere Informationen zur Prüfinstanz (OCSP/CRL-Relay) befinden sich bei einer erfolgreichen Prüfung der Prüfinstanzsignatur in den "Informationen zur Zertifikatsprüfung" (URL der Prüfinstanz und Konfiguration der Prüfinstanz).

7.1.3 Zeile "Fehler"

In dieser Zeile wird bei einer Exception die Fehlermeldung angezeigt.

8 Verzeichnis der Abbildungen und Tabellen

Abbildungen

Abbildung 1: Aufbau Prüfprotokoll 7

Abbildung 2: Grundaufbau Bereich 1 "Zusammenfassung und Struktur" 14

Abbildung 3: Zusammenfassung und Struktur bei einer signierten OSCI-Nachricht (1.2) 15

Abbildung 4: nicht gesendete OSCI-Nachricht mit verschlüsseltem Inhaltsdatencontainer ...17

Abbildung 5: kumulierte Prüfergebnisse im Bereich 1 "Zusammenfassung und Struktur" 17

Abbildung 6: Bereich 1 "Zusammenfassung und Struktur" bei CMS/PKCS#7-Dokumenten..21

Abbildung 7: Anzeige einer nicht interpretierten Datei 21

Abbildung 8: PKCS#7-Signatur ohne Dokumenteninhalt 22

Abbildung 9: PKCS#7-Signatur ohne Dokumenteninhalt und ohne Originaldokument 22

Abbildung 10: kumulierte Prüfergebnisse im Bereich 1 "Zusammenfassung und Struktur" ...23

Abbildung 11: Bereich 1 "Zusammenfassung und Struktur bei einem PDF-Dokument mit zwei Signaturen".....26

Abbildung 12: Meldung bei einem verschlüsselten PDF-Dokument.....28

Abbildung 13: Kumulierte Prüfergebnisse im Bereich 1 "Zusammenfassung und Struktur"...30

Abbildung 14: Bereich 1 Zusammenfassung und Struktur bei einem PDF-Portfolio mit zwei signierten PDF-Dokumenten.....33

Abbildung 15: Bereich 1 "Struktur" und Bereich 2 "Zertifikatsprüfungen" bei der Prüfung eines einzelnen Zertifikats 34

Abbildung 16: Bereich 1 "Struktur" bei der Prüfung eines einzelnen Zertifikats.....35

Abbildung 17: Bereich 1 "Zusammenfassung und Struktur" bei der Prüfung eines einzelnen Zertifikats.....35

Abbildung 18: Teil 1 „Kumuliertes Prüfergebnis und Informationen zum Zertifikat“ bei der Prüfung eines einzelnen Zertifikats 38

Abbildung 19: Teil 2 „Prüfung des Zertifikats 40

Abbildung 20: Bereich 1 Zusammenfassung und Struktur" bei PDF-Dokumenten mit mehreren Signaturen und der Ausgabe eines Gesamtstatus.....41

Abbildung 21: Bereich 1 "Zusammenfassung und Struktur" bei einem PDF-Dokument mit nicht signierter äußerer Revision 42

Abbildung 22: Bereich 2 "Signaturprüfungen des Prüfprotokolls".....43

Abbildung 23: Teil 1 "Kumuliertes Prüfergebnis und Informationen zur Signatur" 44

Abbildung 24: Zeilen "Signaturort, Signaturgrund und Signaturrichtlinie" bei * AdES-Dokumenten.....47

Abbildung 25: Zeile "Aussteller des Attributzertifikats" 49

Abbildung 26: Bereich 2 Teil 2 "Signaturprüfung der Inhaltsdaten".....50

Abbildung 27: Ergebnis der Eignungsprüfung bei einem Algorithmus, der zum Signierzeitpunkt und zum Zeitpunkt der Durchführung der Prüfung für eine QES geeignet war 52

Abbildung 28: Ergebnis der Eignungsprüfung bei einem Algorithmus, der nur zum Zeitpunkt der Durchführung der Prüfung nicht mehr für die Prüfung einer QES geeignet war 52

Abbildung 29: Ergebnis der Eignungsprüfung bei einem Algorithmus, der schon zum Signierzeitpunkt nicht mehr für eine QES geeignet war 52

Abbildung 30: Eignungsprüfung des verwendeten Signaturalgorithmus bei einer fortgeschrittenen Signatur 53

Abbildung 31: Anzeige des verwendeten Signaturalgorithmus 53

Abbildung 32: Ergebnis der Eignungsprüfung des verwendeten Signaturalgorithmus einer Inhaltsdatensignatur zum Signierzeitpunkt 54

Abbildung 33: Ergebnis der Eignungsprüfung des verwendeten Signaturalgorithmus einer Inhaltsdatensignatur zum Zeitpunkt der Durchführung der Signaturprüfung 54

Abbildung 34: Anzeige der verwendeten Algorithmen für eine qualifizierte elektronische Signatur (SigG) mit Datum des Ablaufs der Eignung in Abhängigkeit vom Verwendungszeck 55

Abbildung 35: Teil 3 "Prüfung des Zertifikats" 56

Abbildung 36: Teil 3 "Sperrgrund bei einem gesperrten Zertifikat" 59

Abbildung 37: Ergebnis der Eignungsprüfung bei einem Algorithmus, der zum Signierzeitpunkt für die Signatur eines qualifizierten Zertifikats und Zeitpunkt der Durchführung der Prüfung für die Prüfung der Signatur eines qualifizierten Zertifikats geeignet war 61

Abbildung 38: Ergebnis der Eignungsprüfung bei einem Algorithmus, der erst zum Zeitpunkt der Durchführung der Prüfung nicht mehr für die Prüfung der Signatur eines qualifizierten Zertifikats geeignet war 61

Abbildung 39: Ergebnis der Eignungsprüfung bei einem Algorithmus, der bereits zum Signierzeitpunkt nicht mehr für die Signatur eines qualifizierten Zertifikats geeignet war 61

Abbildung 40: Eignungsprüfung des verwendeten Signaturalgorithmus bei einer fortgeschrittenen Signatur eines Zertifikats 62

Abbildung 41: Anzeige des verwendeten Signaturalgorithmus 62

Abbildung 42: Ergebnis der Eignungsprüfung des verwendeten Signaturalgorithmus einer Zertifikatssignatur zum Signierzeitpunkt 63

Abbildung 43: Ergebnis der Eignungsprüfung des verwendeten Signaturalgorithmus einer Zertifikatssignatur zum Zeitpunkt der Durchführung der Signaturprüfung 63

Abbildung 44: Anzeige der verwendeten Algorithmen für eine qualifizierte elektronische Signatur (SigG) mit Datum des Ablaufs der Eignung in Abhängigkeit vom Verwendungszeck 64

Abbildung 45: Link zu den technischen Informationen zur Prüfung und Erläuterungen 65

Abbildung 46: Teil 3 "Prüfung eines Attributzertifikats zu einem Signaturzertifikat" 67

Abbildung 47: Teil 3 "Nachprüfung eines Zertifikats bei OCSI-Nachrichten" 69

Abbildung 48: Bereich 3 "Zertifikate“ des Prüfprotokolls" 70

Abbildung 49: Bereich "Inhaber eines Zertifikats" 72

Abbildung 50: Bereich "Inhaber eines Attributzertifikats" 73
Abbildung 51: Bereich "Aussteller" 74
Abbildung 52: Allgemeine Informationen zum Zertifikat 75
Abbildung 53: Bereich "öffentlicher Schlüssel" (RSA-Schlüssel) 76
Abbildung 54: Bereich "öffentlicher Schlüssel" (ECDSA-Schlüssel) 77
Abbildung 55: Anzeige "Signatur des Ausstellers" 77
Abbildung 56: Anzeige Erweiterung "Ausstellerschlüssel-ID" 80
Abbildung 57: Anzeige Erweiterung "Schlüsselverwendung" 81
Abbildung 58: Anzeige Erweiterung "Distributionspunkt für CRL" 88
Abbildung 59: Anzeige Erweiterung "Zugangsinformationen des Ausstellers" 89
Abbildung 60: Anzeige Erweiterung "Angaben zum qualifizierten Zertifikat" 90
Abbildung 61: Anzeige Erweiterung "Attributzertifikat" vorhanden 91
Abbildung 62: Attribut "Vertretungsmacht gemäß CommonPKI SigG-Profil" 93
Abbildung 63: Erweiterung bestätigter Beruf (einer namingAuthority) gemäß CommonPKI SigG-Profil 95
Abbildung 64: Attribute "Einschränkung" und "Zusatzinformationen" gemäß CommonPKI SigG-Profil 96
Abbildung 65: Technische Informationen zur Prüfung 97
Abbildung 66: Informationen zur Prüfinstanz 104
Abbildung 67: Bereich "Übertragungsinformation" bei "Gelb"-Prüfung 107

Tabellen

Tabelle 1: Ermittlung des kumulierten Prüfergebnisses 55
Tabelle 2: Ermittlung des kumulierten Prüfergebnisses 64
Tabelle 3: Erweiterung "Ausstellerschlüssel-ID" 79
Tabelle 4: Erweiterung "Inhaberschlüssel-ID" 80
Tabelle 5: Erweiterung "Schlüsselverwendung" 80
Tabelle 6: Erweiterung "Zertifizierungsrichtlinien" 83
Tabelle 7: Erweiterung "Alternativer Name des Inhabers" 84
Tabelle 8: Erweiterung "Alternativer Name des Ausstellers" 84
Tabelle 9: Erweiterung "Verzeichnisattribute des Inhabers" 85
Tabelle 10: Erweiterung "Erweiterte Schlüsselverwendung" 86
Tabelle 11: Erweiterung "Distributionspunkt für CRL" 87
Tabelle 12: Erweiterung "Zugangsinformationen des Ausstellers" 88
Tabelle 13: Erweiterung "Zugangsinformationen des Inhabers" 89
Tabelle 14: Erweiterung "Angaben zum qualifizierten Zertifikat" 90
Tabelle 15: Art der Überwachung 98
Tabelle 16: Zertifikatsniveau gemäß Zertifizierungsrichtlinie des ZDA (1) 100
Tabelle 17: Zertifikatsniveau gemäß Zertifizierungsrichtlinie des ZDA (2) 101