Governikus KG

Governikus Communicator

Anwenderhandbuch

Governikus Prüfprotokoll

Verification Interpreter Version 3_16_0

Governikus Communicator Justiz Edition 3.8.1

Dokumentenversion 1.0

22.03.2021

Inhaltsverzeichnis

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.

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

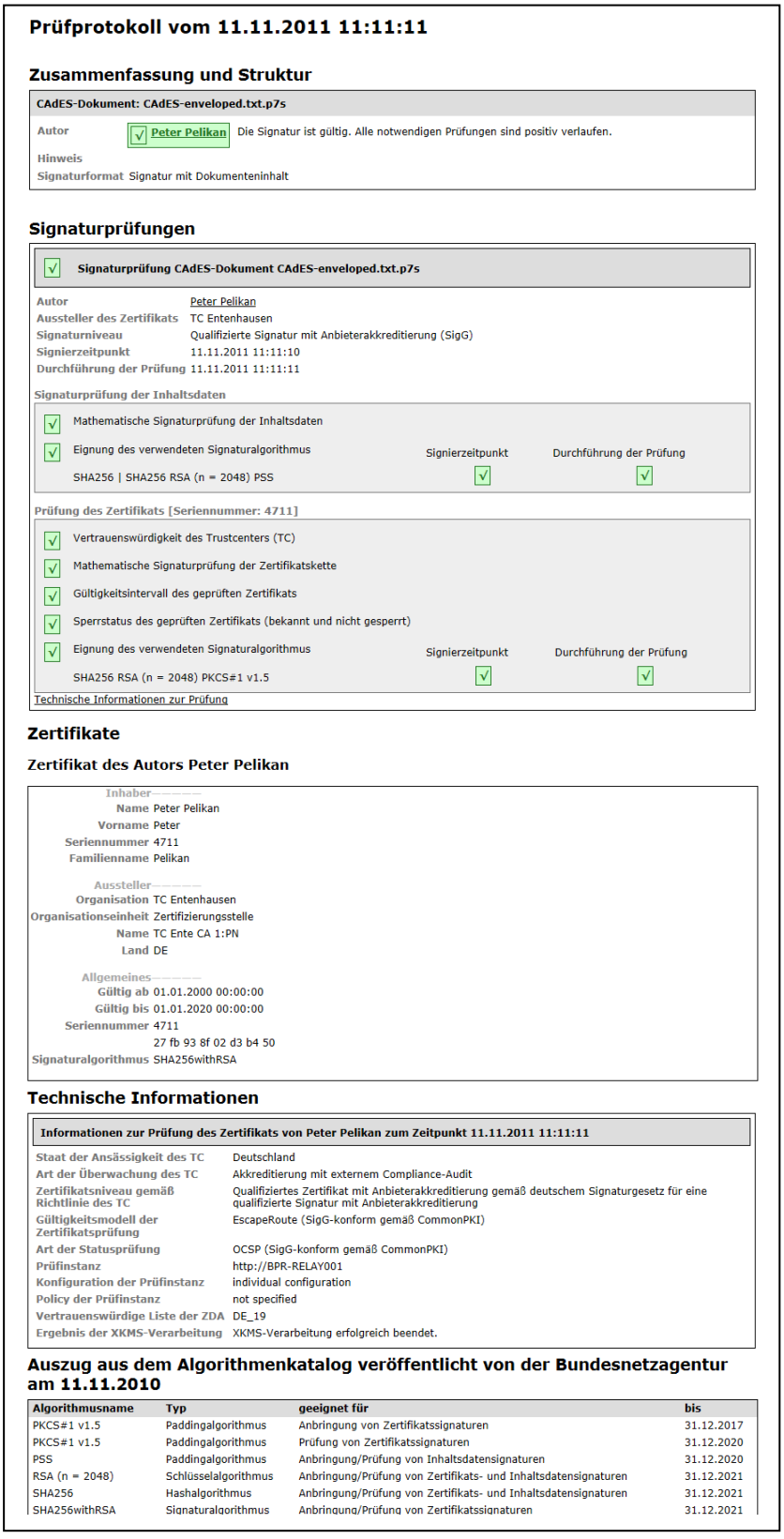
Dieses Anwenderhandbuch erläutert das Governikus Prüfprotokoll (zukünftig Prüfprotokoll), das die Ergebnisse der Prüfung einer elektronischen Signatur anzeigt. Das Prüfprotokoll gliedert sich in vier Hauptbereiche:

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 11.11.2011 11:11:11

Zusammenfassung und Struktur

CAdES-Dokument: CAdES-enveloped.txt.p7s

Autor √ Peter Pelikan — Die Signatur ist gültig. Alle notwendigen Prüfungen sind positiv verlaufen.

Hinweis

Signaturformat Signatur mit Dokumenteninhalt

Signaturprüfungen

√ Signaturprüfung CAdES-Dokument CAdES-enveloped.txt.p7s

Autor	Peter Pelikan
Aussteller des Zertifikats	TC Entenhausen
Signaturniveau	Qualifizierte Signatur mit Anbieterakkreditierung (SigG)
Signierzeitpunkt	11.11.2011 11:11:10
Durchführung der Prüfung	11.11.2011 11:11:11

Signaturprüfung der Inhaltsdaten

√ Mathematische Signaturprüfung der Inhaltsdaten

√ Eignung des verwendeten Signaturalgorithmus — Signierzeitpunkt √ — Durchführung der Prüfung √

SHA256 | SHA256 RSA (n = 2048) PSS

Prüfung des Zertifikats [Seriennummer: 4711]

√ 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
Name Peter Pelikan
Vorname Peter
Seriennummer 4711
Familienname Pelikan

Aussteller
Organisation TC Entenhausen
Organisationseinheit Zertifizierungsstelle
Name TC Ente CA 1:PN
Land DE

Allgemeines
Gültig ab 01.01.2000 00:00:00
Gültig bis 01.01.2020 00:00:00
Seriennummer 4711
27 fb 93 8f 02 d3 b4 50
Signaturalgorithmus SHA256withRSA

Technische Informationen

Informationen zur Prüfung des Zertifikats von Peter Pelikan zum Zeitpunkt 11.11.2011 11:11:11

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 (SigG-konform gemäß CommonPKI)
Art der Statusprüfung	OCSP (SigG-konform gemäß CommonPKI)
Prüfinstanz	http://BPR-RELAY001
Konfiguration der Prüfinstanz	individual configuration
Policy der Prüfinstanz	not specified
Vertrauenswürdige Liste der ZDA	DE_19
Ergebnis der XKMS-Verarbeitung	XKMS-Verarbeitung erfolgreich beendet.

Auszug aus dem Algorithmenkatalog veröffentlicht von der Bundesnetzagentur am 11.11.2010

Algorithmusname	Typ	geeignet für	bis
PKCS#1 v1.5	Paddingalgorithmus	Anbringung von Zertifikatssignaturen	31.12.2017
PKCS#1 v1.5	Paddingalgorithmus	Prüfung von Zertifikatssignaturen	31.12.2020
PSS	Paddingalgorithmus	Anbringung/Prüfung von Inhaltsdatensignaturen	31.12.2020
RSA (n = 2048)	Schlüsselalgorithmus	Anbringung/Prüfung von Zertifikats- und Inhaltsdatensignaturen	31.12.2021
SHA256	Hashalgorithmus	Anbringung/Prüfung von Zertifikats- und Inhaltsdatensignaturen	31.12.2021
SHA256withRSA	Signaturalgorithmus	Anbringung/Prüfung von Zertifikatssignaturen	31.12.2021

Abbildung 1: Aufbau Prüfprotokoll

Bereich 1 "Zusammenfassung und Struktur"

Im Bereich 1 "Zusammenfassung und Struktur" des Prüfprotokolls wird das Prüfergebnis in Ampelform zusammengefasst. Folgende Prüfstatus sind möglich:

-  Grüner Kasten mit Haken: Die Signatur ist gültig.
-  Gelber Kasten mit Ausrufungszeichen: Das Prüfergebnis ist unbestimmt.
-  Roter Kasten mit Kreuz: Die Signatur ist ungültig.

Eine detaillierte Beschreibung der Zeile "Autor, Prüfergebnis und Erläuterung" befindet sich im Kapitel 3.1.

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.

Bereich 2 "Signaturprüfungen"

Im Bereich 2 "Signaturprüfungen" werden die detaillierten Prüfergebnisse und Kontextinformationen zur geprüften Signatur und die detaillierten 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 Prüfung der 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.

Bereich 3 "Zertifikate"

Im Bereich 3 "Zertifikate" des Prüfprotokolls wird der Inhalt des geprüften Signaturzertifikats angezeigt. Die Darstellung wird ggf. für jedes weitere Zertifikat wiederholt. Der Bereich "Zertifikate" des Prüfprotokolls wird ausführlich in Kapitel 5 beschrieben.

Bereich 4 "Zertifikate" Technische Informationen

Im Bereich 4 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 beschrieben.

Sollte der Antwort des OCSP/CRL-Relay nicht vertraut werden können, wird am Anfang des Prüfprotokolls eine entsprechende Fehlermeldung angezeigt. Erläuterungen hierzu finden sich im Kapitel 7.

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

2 Rechtlicher und technischer Hintergrund

Aufbau und Inhalt des Prüfprotokolls ergeben sich wesentlich aus den Anforderungen der eIDAS-Verordnung an die Prüfung einer qualifizierten elektronischen Signatur und die Anzeige des Prüfergebnisses. Diese werden im Kapitel 2.1 kurz skizziert. In der eIDAS-Verordnung werden verschiedene Signaturniveaus definiert, die im Kapitel 2.2 vorgestellt werden. Das Kapitel 2.3 informiert darüber, welche Signaturformate geprüft werden können und über den technischen Ablauf einer Signaturprüfung über die Governikus-Infrastruktur.

2.1 Prüfung von qualifizierten elektronischen Signaturen gemäß eIDAS-Verordnung

Bei der Prüfung einer qualifizierten elektronischen Signatur gemäß eIDAS-Verordnung, Artikel 32, Absatz 1 ist mit dem Verfahren für die Validierung einer qualifizierten elektronischen Signatur die Gültigkeit einer qualifizierten elektronischen Signatur zu bestätigen, wenn

- das der Signatur zugrundeliegende Zertifikat zum Zeitpunkt des Signierens ein qualifiziertes Zertifikat für elektronische Signaturen war, dass die Anforderungen des Anhangs I erfüllt,
- das qualifizierte Zertifikat von einem qualifizierten Vertrauensdiensteanbieter ausgestellt wurde und zum Zeitpunkt des Signierens gültig war,
- die Signaturvalidierungsdaten den Daten entsprechen, die dem vertrauenden Beteiligten bereitgestellt werden,
- der eindeutige Datensatz, der den Unterzeichner im Zertifikat repräsentiert, dem vertrauenden Beteiligten korrekt bereitgestellt wird,
- die etwaige Benutzung eines Pseudonyms dem vertrauenden Beteiligten eindeutig angegeben wird, wenn zum Zeitpunkt des Signierens ein Pseudonym benutzt wurde,
- die elektronische Signatur von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde,
- die Unversehrtheit der unterzeichneten Daten nicht beeinträchtigt ist und
- die Anforderungen des Artikels 26 zum Zeitpunkt des Signierens erfüllt waren.

Gemäß Artikel 32, Absatz 2 eIDAS-Verordnung muss das zur Validierung der qualifizierten elektronischen Signatur verwendete System dem vertrauenden Beteiligten das korrekte Ergebnis des Validierungsprozesses bereitstellen und dem Validierenden ermöglichen, etwaige Sicherheitsprobleme zu erkennen.

2.2 Niveaus elektronischer Signaturen

In der eIDAS-Verordnung werden die Niveaus fortgeschrittene elektronische Signatur, fortgeschrittene elektronische Signatur mit qualifiziertem Zertifikat sowie qualifizierte elektronische Signatur definiert. Gemäß Artikel 51, Übergangsmaßnahmen, gelten dabei sichere Signaturerstellungseinheiten, deren Übereinstimmung mit den Anforderungen gemäß Artikel 3 Absatz 4 der Richtlinie 1999/93/EC festgestellt wurde, als qualifizierte Signaturerstellungseinheiten gemäß der eIDAS-Verordnung sowie qualifizierte Zertifikate, die gemäß der Richtlinie 1999/93/EC für natürliche Personen ausgestellt worden sind, bis zu ihrem Ablauf als qualifizierte Zertifikate für elektronische Signaturen gemäß der eIDAS-Verordnung.

Dementsprechend werden folgende Signaturniveaus während der Prüfung festgestellt, wenn die Bedingungen erfüllt sind:

- Fortgeschrittene elektronische Signatur,
- Fortgeschrittene elektronische Signatur mit qualifiziertem Zertifikat,
- Qualifizierte elektronische Signatur

Neben qualifizierten Signaturen werden in der eIDAS-Verordnung erstmalig auch elektronische Siegel für juristische Personen definiert (siehe Artikel 35 und 36). Die Anforderungen an diese Siegel sowie deren Validierung entsprechen sinngemäß den Anforderungen an qualifizierte elektronische Signaturen gemäß eIDAS-Verordnung. Definiert werden

- Fortgeschrittenes elektronisches Siegel,
- Fortgeschrittenes elektronisches Siegel mit qualifiziertem Zertifikat und
- Qualifiziertes elektronisches Siegel.

2.3 Ablauf der Signaturprüfung

Für die Prüfung elektronischer Signaturen und die Anzeige des Prüfergebnisses in Client-Anwendungen der Governikus KG sind in der Regel zwei Komponenten zuständig. Die Erkennung und Analyse der Signaturstruktur sowie die mathematische Signaturprüfung erfolgt durch das in die Anwendung integrierte Kryptomodul "Verification Interpreter". 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) und
- 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. Das 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.

Qualifizierte elektronische Signaturen werden durch den Verification Interpreter konform zu den Anforderungen der eIDAS-Verordnung. Einschlägig ist hierbei der Artikel 32 der eIDAS-Verordnung: „Anforderungen an die Validierung qualifizierter elektronischer Signaturen“. Dieses gilt auch für die Prüfung qualifizierter elektronischer Zertifikate durch das OCSP/CRL-Relay und die Anzeige der Prüfergebnisse durch den Verification Interpreter.

Prüfung von qualifizierten Signaturen aus anderen EU-Mitgliedstaaten als Deutschland

Qualifizierte elektronische Zertifikate, die nicht von deutschen Vertrauensdiensteanbietern ausgestellt werden, sondern von Trustcentern aus anderen EU-Mitgliedstaaten, können auch über die Governikus-Infrastruktur geprüft werden.

Der Prüfdienst wird ausschließlich zentral durch die Governikus KG bereitgestellt. OCSP/CRL-Relays der Betreiber leiten dafür eingehende Prüfanfragen (XKMS-Requests) zu qualifizierten Zertifikaten aus EU-Mitgliedstaaten automatisch an diesen zentralen Dienst

weiter. Prüfantworten (XKMS-Responses) werden von diesem Dienst an das anfragende OCSP/CRL-Relay zurückgesendet, welches die Prüfantwort an die anfragende Instanz (Client) zurückleitet.

Einschränkungen der Prüfbarkeit

Es können nur qualifizierte elektronische Zertifikate geprüft werden, deren Aussteller in der jeweils aktuellen maschinenlesbaren nationalen Trusted List geführt sind. Ist dieses nicht der Fall, sind die notwendigen CA- und Rootzertifikate für den Aufbau der Zertifikatskette nicht vorhanden und es gibt keinen Nachweis über die Qualität des Signaturzertifikats und keinen Vertrauensanker. Auch ist die Governikus KG darauf angewiesen, dass diese Listen sehr zeitnah aktualisiert werden, sollten Trustcenter neue CA-Zertifikate verwenden.

Die Suspendierung von Signaturzertifikaten wird als problematisch für elektronische Signaturen angesehen. Daher ist eine Suspendierung in Deutschland für qualifizierte Zertifikate auch nicht zulässig, gleichwohl bei einigen Trustcentern in der EU üblich. Hintergrund: Wird ein Signaturzertifikat nach dem Ende der Suspendierung wieder für gültig erklärt und danach geprüft, liefert ein OCSP-Responder eine positive OCSP-Antwort („good“) zurück. Der Antwort ist also nicht zu entnehmen, ob dieses Zertifikat ggf. einmal suspendiert war. Wenn dieses der Fall war, könnte es zum Beispiel auch zum Signaturzeitpunkt suspendiert (= temporär gesperrt) gewesen sein. Dann wäre aber keine nach deutschem Recht gültige Signatur erzeugt worden.

Sollte der Governikus KG bekannt sein, dass ein Trustcenter Nutzerzertifikate suspendiert, wird daher bei einer sonst gültigen Signatur zusätzlich der folgende Warnhinweis angezeigt:

- Das Trustcenter suspendiert Zertifikate. Es kann nicht festgestellt werden, ob das Zertifikat zum Signaturzeitpunkt ggf. suspendiert war.

Die Entfernung von Sperrinformationen aus CRLs nach Ablauf der Zertifikatsgültigkeit ist problematisch, weil Signaturzertifikate in der Regel auch nach Ablauf ihrer Gültigkeit geprüft werden und im Sperrfall dieses zu Falschpositivprüfungen führen könnte. Sollte der Governikus KG bekannt sein, dass ein Trustcenter Sperrinformationen nach Ablauf der Gültigkeit entfernt, wird zusätzlich der folgende Warnhinweis angezeigt:

- Der Sperrstatusdienst für das angefragte Zertifikat wurde durch das Trustcenter eingestellt.

Berücksichtigung spezieller signaturrechtlicher und technischer Anforderungen aus den einzelnen EU-Mitgliedstaaten

Die Prüfung von qualifizierten elektronischen Signaturen aus den EU-Mitgliedstaaten erfolgt gemäß internationaler Standards (RFC, ETSI). Etwaige besondere technische Anforderungen einzelner Mitgliedstaaten, dazu gehört auch die Eignung der eingesetzten Kryptoalgorithmen, werden bei der Prüfung nicht berücksichtigt. Auch kann nicht sichergestellt werden, dass alle trustcenterspezifischen Anforderungen der Governikus KG bekannt sind und konfiguriert werden konnten. Im Prüfprotokoll wird daher immer der folgende Hinweis angezeigt:

- Das geprüfte Zertifikat wurde durch einen (qualifizierten) Vertrauensdiensteanbieter aus einem anderen EU-Mitgliedstaat als Deutschland ausgestellt. Die Prüfung wurde auf Basis der durch die nationale Aufsichtsbehörde zur Verfügung gestellten Trusted List durchgeführt. Der Dienste-Identifier wurde als Trusted Anchor verwendet. Die Prüfung wurde konform zu den aktuellen europäischen Standards/Normen der eIDAS-Verordnung durchgeführt.

2.4 Unterstützte Signaturformate und Signaturalgorithmen

Signierte Dokumente liegen in unterschiedlichen Signaturformaten vor. Das Modul "Verification Interpreter" unterstützt die im Folgenden aufgeführten Signaturformate. Bitte beachten Sie, dass Clientanwendungen den Umfang der unterstützten Signaturformate einschränken können.

OSCI-Nachrichten mit XML-Signaturen

- **Asynchrone OSCI-Nachrichten** mit Laufzettel gemäß OSCI 1.2-Spezifikation und ausgewählte **synchrone Nachrichtentypen** (Abwicklungsantwort, Abwicklungsauftrag, Bearbeitungsauftrag, Weiterleitungsantwort, Annahmeauftrag).

Dokumente mit CAdES-Signaturen (detached oder attached)

- **CAdES-Baseline-Signaturen**
  CAdES-Signatur und Dokument werden auch erkannt, wenn sie sich in einem **ASiC-Container** des Typs S (simple) befinden.

Signierte E-Mails und De-Mail-Nachrichten

- **E-Mails mit S/MIME-Signaturen**
  Unterstützt werden E-Mails im Plain-Text-Format (Endung .eml) sowie das proprietäre Export-Format mit der Endung .msg, wenn der Export aus den Outlook-Versionen 2007, 2010, 2013 oder 2016 erfolgt.
- **De-Mail-Signaturen** (DKIM) bis Header-Version 1.2 und Version Spezifikation 1.6 sowie Mischformen.

Signierte PDF-Dokumente

- **PDF-Dokumente mit eingebetteten PAdES-Baseline-Signaturen**
  Bestimmte Alt-Signaturen (Legacy-Formate) nach ISO 32000 werden auch unterstützt.

Dokumente mit XML-Signaturen

- **XAdES-Baseline-Signaturen**

Zeitstempel

- **TSP** gemäß RFC 3161.

Bitte beachten Sie: Anwendungen, die den Verification Interpreter verwenden, können den Umfang der unterstützten Signaturformate einschränken.

Unterstützte Signaturalgorithmen

Der Verification Interpreter unterstützt eine Vielzahl von Signaturalgorithmen. Darunter auch die Signaturalgorithmen (Hashfunktionen, Paddingverfahren, RSA-, DSA- und ECDSA-Algorithmen), die für qualifizierte elektronische Signaturen verwendet werden können oder konnten.

Bei einer qualifizierten elektronischen Signatur wird durch den Verification Interpreter auch die Eignung des verwendeten Signaturalgorithmus zum Signaturzeitpunkt und zum Zeitpunkt der Durchführung der Prüfung ermittelt.

2.5 Algorithmenkatalog der Anwendung Governikus des IT-PLR

Für die Ermittlung der Eignung von Signaturalgorithmen bei qualifizierten elektronischen Signaturen (ausgestellt von qualifizierten Vertrauensdiensteanbietern, die von der Bundesnetzagentur als nationaler Aufsichtsbehörde einen qualifizierten Status verliehen bekommen haben) wird der jeweils aktuelle Algorithmen-Katalog der „Anwendung Governikus des IT-PLR“ verwendet. Der Katalog enthält zusätzlich aus Vertrauensschutzerwägungen die Eignungsangaben aus dem letzten Algorithmenkatalog der Bundesnetzagentur von 2017. Dabei wird für jeden Algorithmus immer das hinsichtlich der Eignung günstigste Ablaufdatum aus beiden Katalogen verwendet.

Für fortgeschrittene elektronische Signaturen wird die Eignung der verwendeten Algorithmen nicht ermittelt.

3 Bereich 1: Zusammenfassung und Struktur

Im ersten Bereich des Prüfprotokolls "Zusammenfassung und Struktur" wird das Signaturformat, die Struktur der signierten Datei 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 Signaturformat und der Dateiname des signierten Dokuments angezeigt.
- In der Zeile "Autor" wird immer der Name des Autors (Name des Signierenden), das Ergebnis der Signaturprüfung (der dem Autor zugeordneten Signatur) in Ampelform (grün, gelb, rot) sowie eine Erläuterung zum Prüfergebnis angezeigt.

In den nächsten Zeilen folgen ggf. formatspezifische Kontextinformationen.

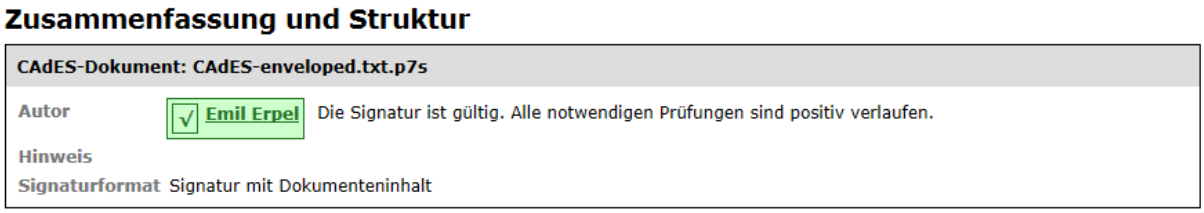


Abbildung 2: Grundaufbau Bereich 1 "Zusammenfassung und Struktur"

Konnte keine Signatur ermittelt werden, wird die folgende Meldung angezeigt: "keine Signatur gefunden: [`Dateiname`]".

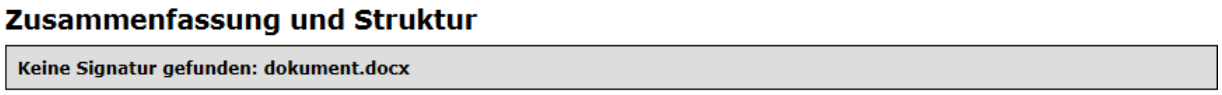


Abbildung 3: Anzeige „keine Signatur gefunden“

Der Grundaufbau des Bereichs "Zusammenfassung und Struktur" gilt für alle unterstützen Signaturformate. Dazu gehört auch die Anzeige des Ergebnisses der Signaturprüfung, die für alle Signaturformate identisch ist und im folgenden Kapitel 3.1 erläutert wird. Die unterstützten Signaturformate unterscheiden sich allerdings hinsichtlich ihrer Komplexität und der angezeigten formatspezifischen Kontextinformationen. In den Unterkapiteln 3.2 und in den folgenden Kapiteln werden diese formatspezifischen Besonderheiten dargestellt.

3.1 Prüfergebnis: Zeile "Autor, Prüfergebnis und Erläuterung"

In der Zeile "Autor mit Prüfergebnis und Erläuterung" wird von links nach rechts zunächst das Ergebnis der Signaturprüfung mit dem Namen des Signierenden (Autor) in einem farbig unterlegten Kasten und anschließend eine Erläuterung des Ergebnisses angezeigt.

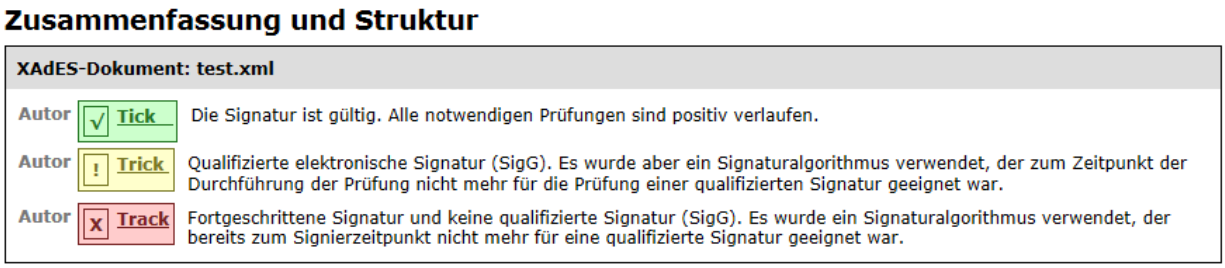


Abbildung 4: Anzeige des Gesamtprüfergebnisses und der Erläuterung im Bereich 1 "Zusammenfassung und Struktur"

3.1.1 Ergebnis der Signaturprüfung

Rechts neben der Feldbezeichnung "Autor" wird das Ergebnis der Signaturprüfung und der Name der signierenden Person (wie im Zertifikat angegeben) in einem farbig unterlegten Kasten angezeigt. Folgende Status sind möglich:

- Grüner Kasten mit Haken: Die Signatur ist gültig.
- Gelber Kasten mit Ausrufungszeichen: Das Prüfergebnis ist unbestimmt.
- Roter Kasten mit Kreuz: Die Signatur ist ungültig.

Erläuterungen zu Grüner Kasten mit Haken:

Ein grüner Kasten mit Haken bedeutet, dass die Signatur gültig ist. Alle notwendigen Einzelprüfungen wurden durchgeführt und sind positiv verlaufen. Damit ist die Unverfälschtheit (Integrität der signierten Inhaltsdaten, der Nachricht, des Dokuments) sichergestellt, der Signierende sicher identifiziert und seine Authentizität bestätigt.

Dieses 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 "unbestimmt" wechseln, weil z.B. der Sperrstatus des Zertifikats nicht mehr ermittelt werden kann oder weil, im Fall einer qualifizierten Signatur, der für die Signatur verwendete Signaturalgorithmus inzwischen nicht mehr für die Prüfung einer qualifizierten Signatur geeignet ist.

Erläuterungen zu Gelber Kasten mit Ausrufungszeichen:

Ein gelber Kasten mit Ausführungszeichen signalisiert, das mindestens eine notwendige Einzelprüfung einen unbestimmten Status besitzt weil sie z.B. nicht durchgeführt werden konnte. Es kann nicht entschieden werden, ob die Signatur gültig oder ungültig ist.

Die Ursache für den unbestimmten Status sollte in jedem Fall genauer analysiert werden. Häufig kommt dieses Prüfergebnis nämlich dadurch zustande, dass der Sperrstatus des Zertifikats nicht ermittelt werden konnte (In diesem Fall hat die Einzelprüfung „Sperrstatus des Zertifikats“ den Status "gelb"). Nach einem gewissen Zeitraum ist in diesem Fall eine erneute Prüfung sinnvoll.

Bei der Prüfung einer qualifizierten Signatur kann der Status "gelb" auch ein endgültiges Ergebnis anzeigen, wenn der verwendete Signaturalgorithmus zum Zeitpunkt der Durchführung der Prüfung nicht mehr für die Prüfung einer qualifizierten Signatur geeignet war. In der Spalte Erläuterungen wird in diesem Fall der folgende Warnhinweis ausgegeben:

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

Bereits erzeugte qualifizierte elektronische Signaturen bleiben zwar auch dann noch qualifiziert, wenn der zugrundeliegende Signaturalgorithmus nach der Signaturerzeugung seine Sicherheitseignung verloren hat, sie büßen jedoch graduell und sukzessive ihren Beweiswert ein. Der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung kann dadurch erschüttert werden.

Erläuterungen zu  Roter Kasten mit Kreuz:

Ein roter Kasten mit Kreuz  bedeutet, dass die Signatur ungültig ist. Mindestens eine notwendige Einzelprüfung ist abschließend fehlgeschlagen. Damit ist entweder die Unverfälschtheit der Inhaltsdaten (Integrität der Daten) nicht sichergestellt oder es konnte die signierende Person abschließend nicht sicher identifiziert werden.

Bei der Prüfung einer qualifizierten Signatur besitzt der Status "rot" eine besondere Warnfunktion, wenn der verwendete Signaturalgorithmus bereits zum Zeitpunkt der Erzeugung der Signatur nicht mehr für die Erzeugung einer qualifizierten Signatur geeignet war. In diesem Fall wird der folgende Warnhinweis ausgegeben:

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

Bereits bei der Erzeugung der Signatur war nicht mehr sichergestellt, dass der Signaturschlüssel-Inhaber die alleinige Kontrolle über die Mittel zur Erzeugung der Signatur hatte. Es handelt sich daher bei der erzeugten Signatur von vornherein nicht um eine qualifizierte elektronische Signatur.

3.1.2 Name des Autors

Rechts neben dem Prüfergebnis wird der Name der signierenden Person in einem farbig unterlegten Kasten angezeigt. Der Name besteht in der Regel aus dem Vor- und Nachnamen des Zertifikatsinhabers, so wie er im Zertifikat hinterlegt wurde ([`subject`] [`CommonName`]). Bitte beachten Sie: Nur bei einer gültigen Signatur konnte der Signierende sicher identifiziert und seine Authentizität bestätigt werden, d.h. kann der Namensangabe im Zertifikat vertraut werden.

3.1.3 Spalte "Erläuterungen"

In der letzten Spalte rechts wird das Prüfergebnis erläutert. Ist die Signatur gültig (grüner Kasten mit Haken) wird ausschließlich die folgende Meldung angezeigt:

- Die Signatur ist gültig. Alle notwendigen durchgeführten Prüfungen lieferten ein positives Ergebnis.

Ist der Status der Signaturprüfung unbestimmt (gelber Kasten mit Ausrufungszeichen) oder die Signatur ungültig (Roter Kasten mit Kreuz) wird als Erläuterungstext in der Regel das erste unbestimmte Einzelprüfergebnis bzw. das erste negative Einzelprüfergebnis angezeigt. Es gibt allerdings zwei Ausnahmen, die wegen ihrer besonderen Warnfunktion immer an dieser Stelle angezeigt werden:

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

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

3.2 OSCI-Nachrichten (OSCI 1.2)

In diesem Kapitel wird der Aufbau des Bereichs 1 "Zusammenfassung und Struktur" für OSCI-Nachrichten gemäß Spezifikation Version 1.2 beschrieben.

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 Struktur der geprüften OCSI-Nachricht.

3.2.1 Zeile Name der OSCI-Nachricht

In der ersten Zeile wird grau unterlegt hinter der Bezeichnung des Signaturformats "OSCI-Nachricht" der Name der OSCI-Nachricht angezeigt.

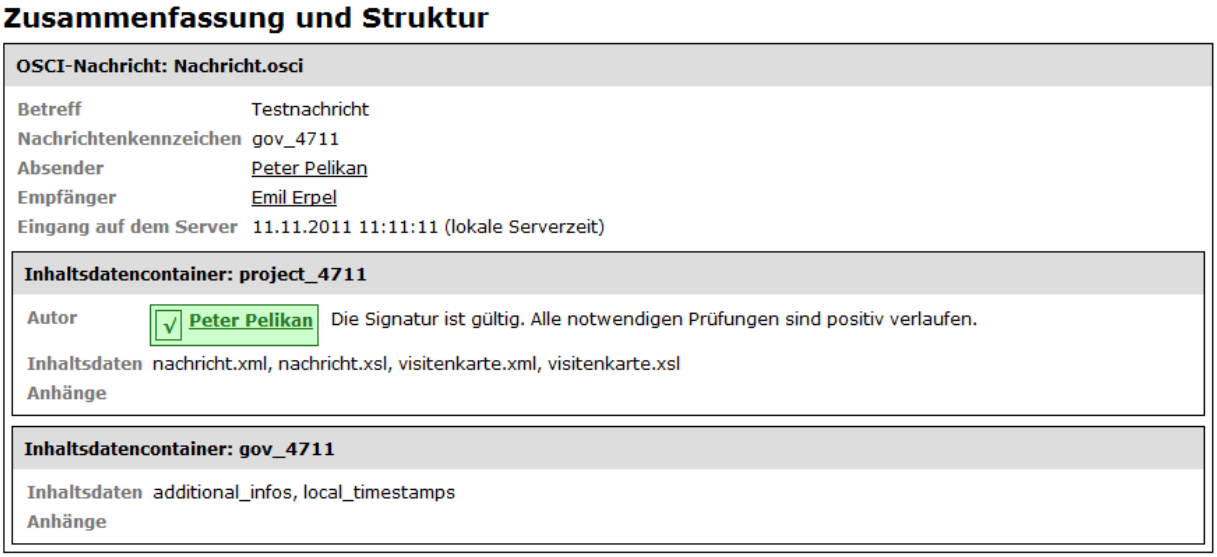


Abbildung 5: Zusammenfassung und Struktur bei einer signierten OSCI-Nachricht (1.2)

3.2.2 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.

3.2.2.1 Zeile "Betreff"

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

3.2.2.2 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.

3.2.2.3 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. Das Zertifikat mit dem angezeigten Namen wird im Bereich 3 des Prüfprotokolls angezeigt.

3.2.2.4 Optionale Zeile "weitere Absender"

In der optionalen Zeile wird, sofern die Anzeige für das Prüfprotokoll angefordert wurde und das Zertifikat in der OSCI-Nachricht vorhanden ist, der Name eines weiteren Absenders [Feld `subject`, Attribut `commonName`] angezeigt. Das Zertifikat mit dem angezeigten Namen wird im Bereich 3 des Prüfprotokolls angezeigt.

3.2.2.5 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. Das Zertifikat mit dem angezeigten Namen wird im Bereich 3 des Prüfprotokolls angezeigt.

3.2.2.6 Optionale Zeile "Weitere Empfänger"

In der optionalen Zeile wird, sofern die Anzeige angefordert wurde und das Zertifikat in der OSCI-Nachricht vorhanden ist, der Name eines weiteren Empfängers [Feld `subject`, Attribut `commonName`] angezeigt. Das Zertifikat mit dem angezeigten Namen wird im Bereich 3 des Prüfprotokolls angezeigt.

3.2.2.7 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 Zeitstempeldienstes 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.

3.2.2.8 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 6: nicht gesendete OSCI-Nachricht mit verschlüsseltem Inhaltsdatencontainer

3.2.3 Signaturprüfergebnis: Zeile "Autor, Prüfergebnis und Erläuterung"

In der Zeile "Autor mit Prüfergebnis und Erläuterung" wird von links nach rechts zunächst das Ergebnis der Signaturprüfung mit dem Namen des Signierenden (Autor) in einem farbig unterlegten Kasten und anschließend eine Erläuterung des Ergebnisses angezeigt. Folgende Prüfstatus sind möglich:

- Grüner Kasten mit Haken: Die Signatur ist gültig.
- Gelber Kasten mit Ausrufungszeichen: Das Prüfergebnis ist unbestimmt.
- Roter Kasten mit Kreuz: Die Signatur ist ungültig.

Eine detaillierte Beschreibung der Zeile "Autor, Prüfergebnis und Erläuterung" befindet sich im Kapitel 3.1.

3.2.4 Zeile "Inhaltsdaten"

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

3.2.5 Zeile "Anhänge"

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

3.3 CAdES-Signaturen

In diesem Kapitel wird der Aufbau des Bereichs 1 "Zusammenfassung und Struktur" für CAdES-Signaturen beschrieben.

Das CAdES-Signaturformat erlaubt es, dass Signaturen detached (losgelöst) oder enveloped vorliegen können. Bei einer Enveloped-Signatur ist das Dokument ein Teil der Signatur. In diesem Fall wird die Nachricht gemäß ASN.1 codiert und in die Signaturstruktur eingefügt. Bei einer Detached-Signatur liegen Signatur und Dokument in getrennten Dateien getrennt vor.

Bitte beachten Sie bei Detached-Signaturen: Die Zuordnung der Signatur zum Dokument erfolgt automatisch über den Dateinamen. Diese müssen beim Dokument und bei der Signatur identisch sein. Beispiel: dokument.docx – dokument.docx.p7s.

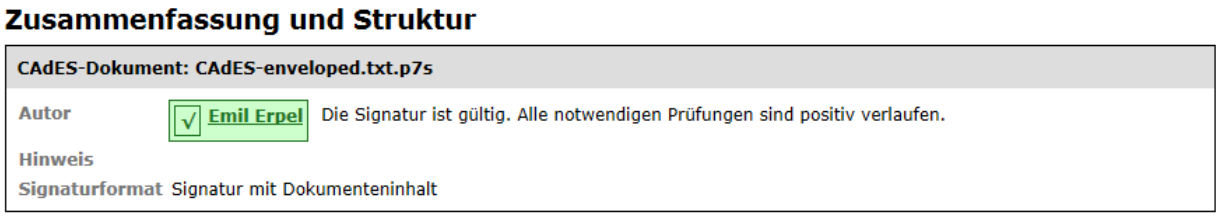


Abbildung 7: Bereich 1 "Zusammenfassung und Struktur" bei CAdES-Signaturen

Signatur und Dokument der Detached-Form können auch verarbeitet werden, wenn sie sich in einem ASiC-Container befinden. Die Beschreibung des Bereichs 1 "Zusammenfassung und Struktur" einer detached CAdES-Signatur in einem ASiC-Container befindet sich im Kapitel 3.3.5.

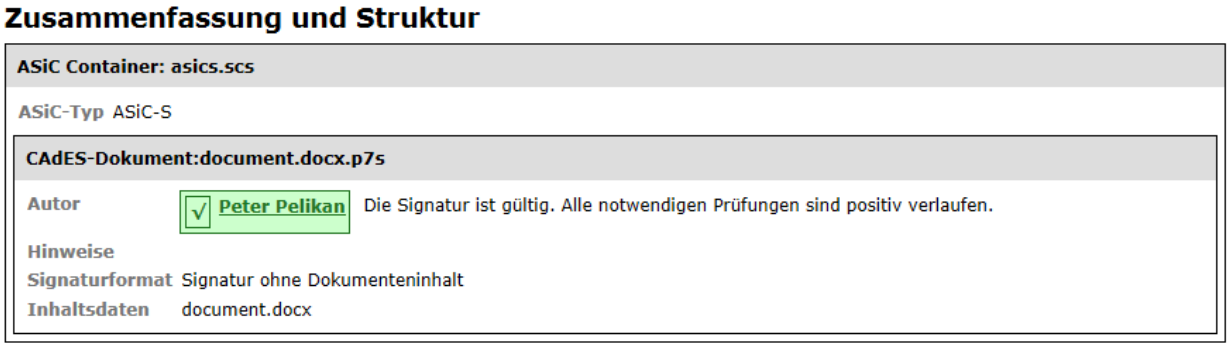


Abbildung 8: Bereich 1 "Zusammenfassung und Struktur" bei einer CAdES-Signatur in einem ASiC-Container

CAdES-Signaturen können eine unterschiedliche Komplexität aufweisen. Dafür wurden in einem ETSI-Standard (Baseline Profile ETSI TS 103173 v.2.2.1) vier verschiedene "Baseline-Level" definiert:

- Der B-Level ist der Basis-Level für fortgeschrittene und qualifizierte elektronische Signaturen. Er enthält vorgeschriebene Attribute, wie z.B. den Signierzeitpunkt (claimed signing time) und das Signaturzertifikat. Die Attribute werden mitsigniert.
- Der T-Level umfasst eine Signatur des B-Levels und den Nachweis der Existenz der Signatur zu einem Zeitpunkt durch einen Zeitstempel (Signaturzeitstempel). Sollte eine T-Signatur vorliegen, wird auch der Signaturzeitstempel geprüft.

- Der LT-Level ist der Long Term Level, der zusätzlich zum T-Level auch alle notwendigen Widerrufsprüfungen in der Signatur enthält, um die Signatur später noch einmal offline validieren zu können (wie zum Beispiel alle Zertifikate der Kette und die OCSP-Antworten). Es ist geplant den LT-Level ab Governikus 4.0 zu unterstützen, da der implementierte Validierungsalgorithmus im Verification Interpreter die Prüfung von LT-Signaturen nur unzureichend unterstützt.
- Der LTA-Level umfasst eine LT-Level-Signatur mit zusätzlichen Archivzeitstempeln. Werden die Archivzeitstempel rechtzeitig vor dem Schwachwerden der Signaturalgorithmen angebracht, können dadurch die Integrität der Inhaltsdaten sowie der Beweiswert der Inhaltsdatensignatur und der Widerrufsinformationen sichergestellt werden. Der LTA-Level wird noch nicht unterstützt, da zurzeit die weitere Standardisierung im Kontext der eIDAS-Verordnung im Bereich Beweiswertbewahrung abgewartet wird.

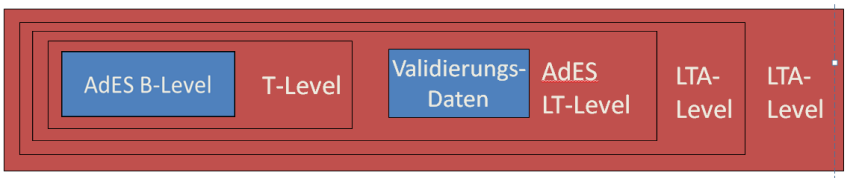


Abbildung 9: Struktur einer CAdES-LTA-Signatur

In den folgenden Unterkapiteln wird Bereich 1 "Zusammenfassung und Struktur" für CAdES-Signaturen beschrieben.

3.3.1 Zeile "CAdES-Dokument"

In der ersten Zeile wird grau unterlegt hinter der Bezeichnung des Signaturformats "CAdES-Dokument" der Name der Datei angezeigt, die die Signatur enthält. Kann eine CAdES-Signatur nicht verarbeitet werden, wird hier die Meldung angezeigt: "Nicht interpretierte Datei: [`Dateiname`]".

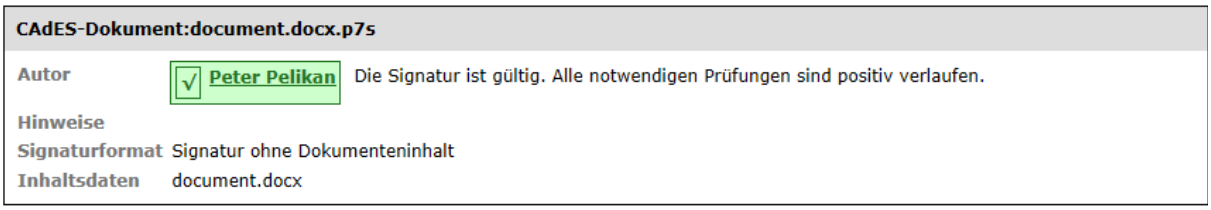


Abbildung 10: CAdES-Signatur ohne Dokumenteninhalt

3.3.2 Signaturprüfergebnis: Zeile "Autor, Prüfergebnis und Erläuterung"

In der Zeile "Autor mit Prüfergebnis und Erläuterung" wird von links nach rechts zunächst das Ergebnis der Signaturprüfung mit dem Namen des Signierenden (Autor) in einem farbig unterlegten Kasten und anschließend eine Erläuterung des Ergebnisses angezeigt. Folgende Prüfstatus sind möglich:

- Grüner Kasten mit Haken: Die Signatur ist gültig.
- Gelber Kasten mit Ausrufungszeichen: Das Prüfergebnis ist unbestimmt.
- Roter Kasten mit Kreuz: Die Signatur ist ungültig.

Eine detaillierte Beschreibung der Zeile "Autor, Prüfergebnis und Erläuterung" befindet sich im Kapitel 3.1.

3.3.3 Zeile "Signaturformat"

CAdES-Signaturen können in zwei Formen vorliegen. Angezeigt wird im Prüfprotokoll hinter der Bezeichnung "Signaturformat", ob die Signatur losgelöst (detached) in einer separaten Datei vorliegt oder sich im signierten Dokument befindet (enveloped):

- Signatur ohne Dokumenteninhalt
- Signatur mit Dokumenteninhalt

3.3.4 Optionale Zeile "Inhaltsdaten" bei einer Detached-Signatur

Sollte es sich um eine Detached-Signatur handeln, wird hinter der Bezeichnung "Inhaltsdaten" der Name des signierten Dokuments angegeben, auf den sich die Signatur bezieht. Ist das Feld leer, konnte das signierte Dokument nicht ermittelt werden. In diesem Fall konnte auch die mathematische Signaturprüfung nicht durchgeführt werden, da der Hashwert über das Dokument nicht neu berechnet werden konnte. Dieses führt zu einem unbestimmten Prüfergebnis. Im Bereich 2 "Signaturprüfungen", Teil 2 "mathematische Signaturprüfung" ist der Status der mathematischen Signaturprüfung in diesem Fall unbestimmt (Gelber Kasten mit Ausrufungszeichen) und es wird die Erläuterung angezeigt: "Die Signatur konnte mathematisch nicht geprüft werden, da die Inhaltsdaten nicht vorliegen".

3.3.5 Detached CAdES-Signatur in einem ASiC-Container

Signatur und Dokument der Detached-Form können auch verarbeitet werden, wenn sie sich in einem ASiC-Container befinden. ASiC-Container besitzen eine Struktur, um signierte Daten gemeinsam mit Signaturen oder auch Zeitstempeln in einem Container zu speichern. Unterstützt werden ausschließlich ASiC-Container des Typs S (simple). Beim Typ S darf sich nur eine Signatur oder ein Zeitstempel und ein Dokument (das signiert/zeitgestempelt wurde) im Container befinden.

Der Bereich 1 "Zusammenfassung und Struktur" für CAdES-signierte Dokumente in einem ASiC-Container im Vergleich zur CAdES-Signatur die zusätzlichen Angaben "Dateiname des ASiC-Containers" und "Typ des ASiC-Containers".

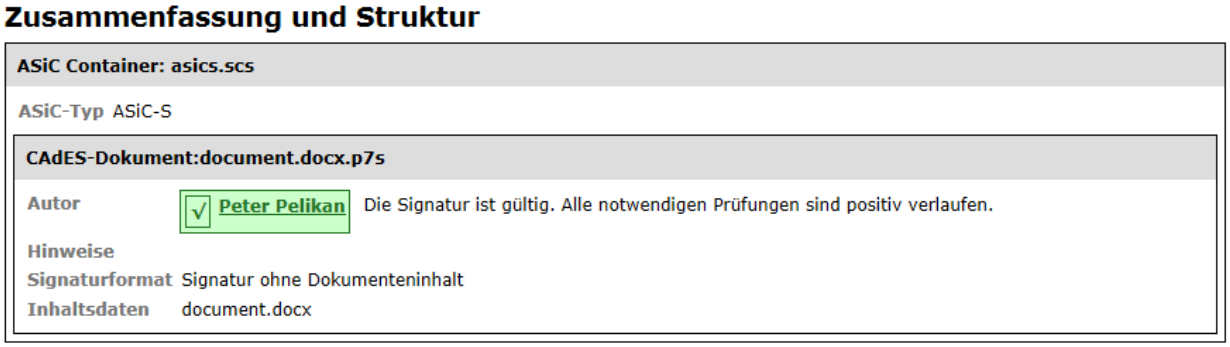


Abbildung 11: Bereich 1 "Zusammenfassung und Struktur" eines einem ASiC-Container

Befinden sich mehr als zwei Dateien in einem ASiC-S-Container oder kann der Containerinhalt nicht verarbeitet werden (weil z.B. die Inhaltsdaten fehlen), wird nur der Containername angezeigt (siehe Abbildung 12).

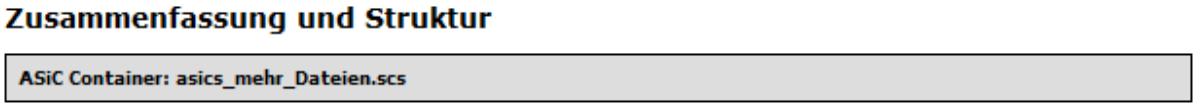


Abbildung 12: Meldung bei einem ASiC-Container mit mehr als zwei Dateien

3.3.5.1 Zeile „ASiC-Container“

In der ersten Zeile wird grau unterlegt hinter der Bezeichnung "ASiC-Container" der Name des Containers (Endung häufig .asics oder .scs) angezeigt, der die Signatur und das Dokument enthält.

3.3.5.2 Zeile "ASiC-Typ"

Die Spezifikation des ASiC-Containers kennt zwei Typen. Angezeigt wird entweder der Typ S (simple) oder der Typ E (extended). In einem Container des Typs S darf sich nur eine Signatur befinden, die auf ein Dokument verweist, das signiert wurde.

3.4 PAdES-Signaturen

In diesem Kapitel wird der Aufbau des Bereichs 1 "Zusammenfassung und Struktur" für PDF/PAdES-Signaturen beschrieben.

3.4.1 Struktur und Komplexität von PDF/PAdES-Signaturen

Das PDF-Dateiformat unterstützt die inkrementelle Dokumentenaktualisierung. Jedes Mal, wenn das PDF-Dokument nach einer Veränderung (z.B. einer Anmerkung, Graphikmarkierung) gespeichert wird, wird eine sogenannte neue "Revision" der PDF-Datei erstellt. Eine Signatur erzeugt auch immer eine neue Revision, die vorherige Revisionen mit einschließt. Enthält ein PDF-Dokument mehrere Signaturen, sind sie daher auch ineinander verschachtelt. Die Anzeige im Bereich 1 "Zusammenfassung und Struktur" stellt diese Struktur graphisch dar (siehe Abbildung 13).

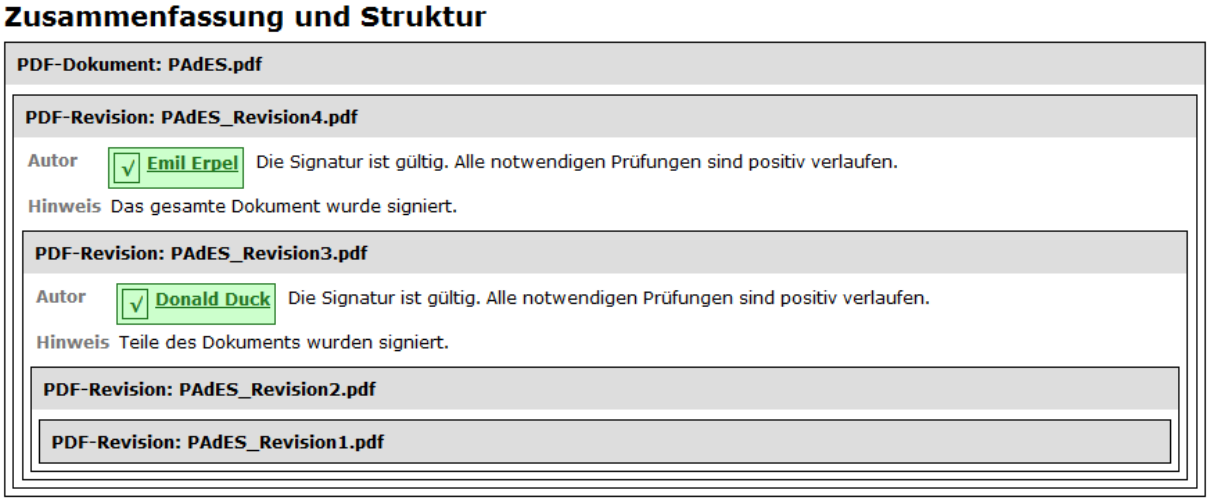


Abbildung 13: Bereich 1 "Zusammenfassung und Struktur bei einem PDF-Dokument mit zwei Signaturen"

Im Beispiel enthält die PDF-Datei „PAdES.pdf“ zwei Signaturen, wobei die äußere Signatur (PAdES_Revision4.pdf) auch die andere Signatur (PAdES_Revision3.pdf) und den Dokumenteninhalt (in zwei Revisionen) umschließt. Die signierten Revisionen eines PDFs lassen sich im Adobe Reader im Fenster "Unterschrifteneigenschaften", Reiter "Dokument" über den Button "unterschriebene Version anzeigen" anzeigen.

PDF-Portfolios

Unterstützt wird auch die Prüfung von PDF-Portfolios, wenn sie ausschließlich PDF-Dokumente (mit PDF-Inline-Signaturen) enthalten. Auch die Portfolio-Datei selbst kann signiert sein. Die Anzeige im Bereich 1 "Zusammenfassung und Struktur" stellt auch die Struktur eines PDF-Portfolios graphisch dar (siehe Abbildung 14).

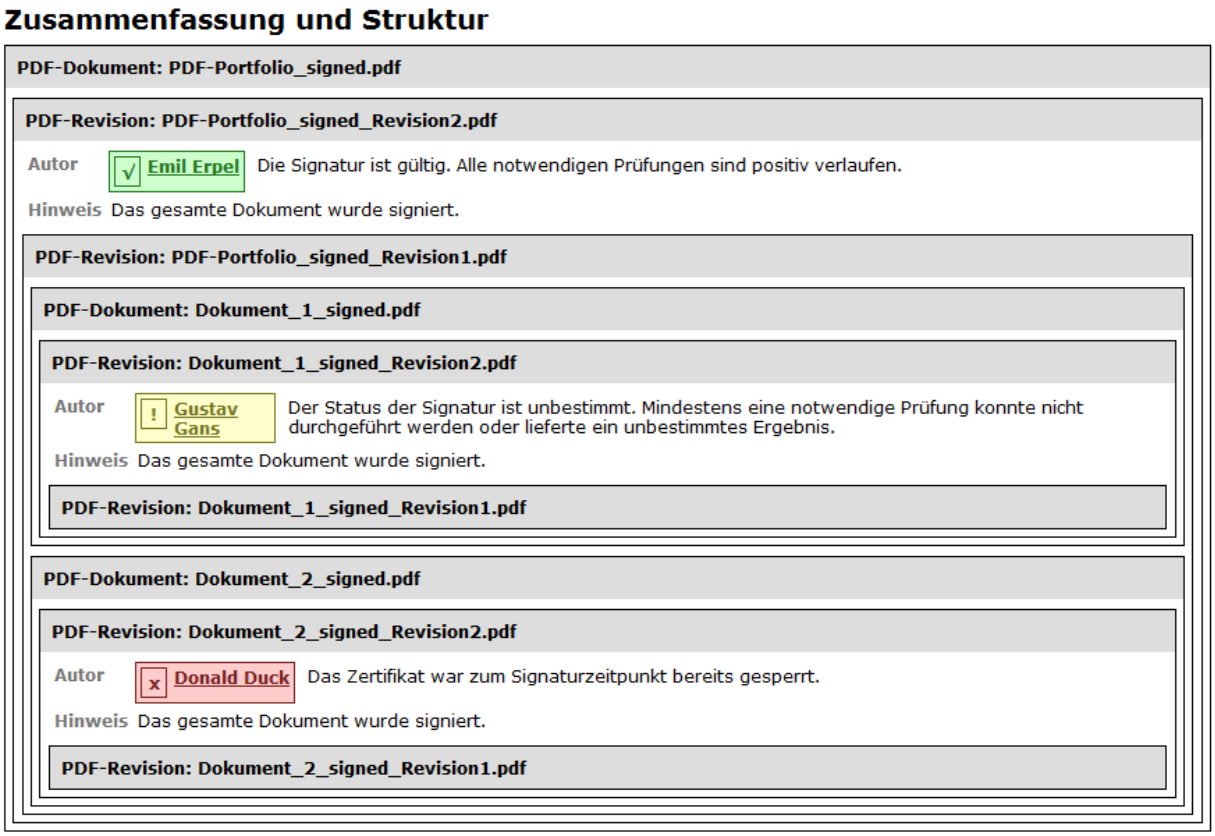


Abbildung 14: Bereich 1 Zusammenfassung und Struktur bei einem PDF-Portfolio mit zwei signierten PDF-Dokumenten

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 erstellt, das die beiden signierten Dokumente als Anhang enthält. Dadurch wurde die erste Revision dieses 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".

PAdES-Signaturen

PAdES-Signaturen können eine unterschiedliche Komplexität aufweisen. Dafür wurden in einem ETSI-Standard (Baseline Profile ETSI TS 103172 Version 2.2.2) vier verschiedene "Baseline-Level" definiert.

- Der B-Level ist der Basis-Level für fortgeschrittene und qualifizierte elektronische Signaturen. Er enthält vorgeschriebene Attribute, wie z.B. den Signierzeitpunkt (claimed signing time) und das Signaturzertifikat. Die Attribute werden mitsigniert.
- Der T-Level umfasst eine Signatur des B-Levels und den Nachweis der Existenz der Signatur zu einem Zeitpunkt durch einen Zeitstempel (Signaturzeitstempel). Sollte eine T-Signatur vorliegen, wird auch der Signaturzeitstempel geprüft.
- Der LT-Level ist der Long Term Level, der zusätzlich zum T-Level auch alle notwendigen Widerrufsprüfungen in der Signatur enthält, um die Signatur später noch einmal offline validieren zu können (wie zum Beispiel alle Zertifikate der Kette und die OCSP-

Antworten). Es ist geplant den LT-Level ab Governikus 4.0 zu unterstützen, da der implementierte Validierungsalgorithmus im Verification Interpreter die Prüfung von LT-Signaturen nur unzureichend unterstützt.

- Der LTA-Level umfasst eine LT-Level-Signatur mit zusätzlichen Archivzeitstempeln. Werden die Archivzeitstempel rechtzeitig vor dem Schwachwerden der Signaturalgorithmen angebracht, können dadurch die Integrität der Inhaltsdaten sowie der Beweiswert der Inhaltsdatensignatur und der Widerrufsinformationen sichergestellt werden. Der LTA-Level wird noch nicht unterstützt, da zurzeit die weitere Standardisierung im Kontext der eIDAS-Verordnung im Bereich Beweiswertbewahrung abgewartet wird.

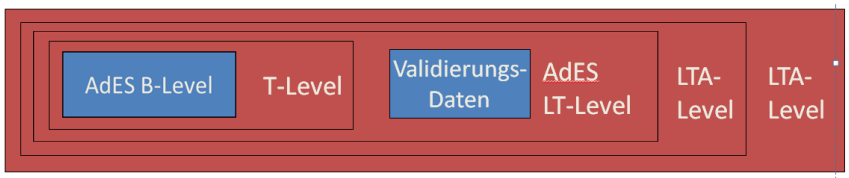


Abbildung 15: Struktur einer PAdES-LTA-Signatur

In den folgenden Unterkapiteln wird Bereich 1 "Zusammenfassung und Struktur" für PAdES-Signaturen beschrieben.

3.4.2 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.

Ist das PDF-Dokument mit einem Passwortschutz versehen, kann es nicht geöffnet und verarbeitet werden. Eine Signaturprüfung ist in diesem Fall nicht möglich und es wird der folgende Hinweis angezeigt:

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

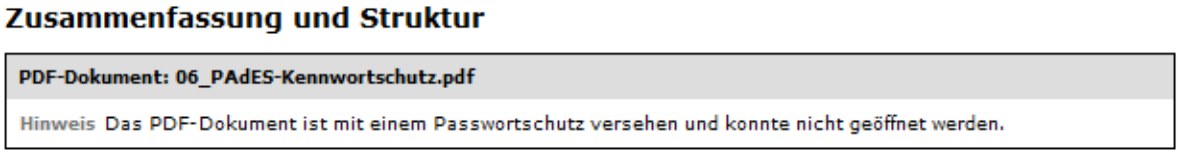


Abbildung 16: Bereich 1 "Zusammenfassung und Struktur" bei einem PDF-Dokument mit Kennwortschutz"

3.4.3 Zeile "PDF-Revision"

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

3.4.4 Signaturprüfergebnis: Zeile "Autor, Prüfergebnis und Erläuterung"

In der Zeile "Autor mit Prüfergebnis und Erläuterung" wird von links nach rechts zunächst das Ergebnis der Signaturprüfung mit dem Namen des Signierenden (Autor) in einem farbig unterlegten Kasten und anschließend eine Erläuterung des Ergebnisses angezeigt. Folgende Prüfstatus sind möglich:

-  Grüner Kasten mit Haken: Die Signatur ist gültig.
-  Gelber Kasten mit Ausrufungszeichen: Das Prüfergebnis ist unbestimmt.
-  Roter Kasten mit Kreuz: Die Signatur ist ungültig.

Eine detaillierte Beschreibung der Zeile "Autor, Prüfergebnis und Erläuterung" befindet sich im Kapitel 3.1.

3.4.5 Zeile "Hinweise"

In der Zeile „Hinweise“ werden Eigenschaften der PAdES-Signatur angezeigt, die die Sicherheit der Signaturprüfung nicht beeinflussen.

Folgende Hinweise können angezeigt werden:

- Das gesamte Dokument wurde signiert
- Teile des Dokuments wurden signiert
- Das PDF-Dokument ist nicht PAdES-konform.
- Das Signaturzertifikat passt nicht zum signierten Hashwert.
- Der Hashwert des Signaturzertifikats fehlt.
- Nicht zulässiger Eintrag in der Datenstruktur, die die Signaturinformationen enthält.

Erläuterungen:

- Das gesamte Dokument wurde signiert

Eine PDF-Signatur kann das gesamte Dokument oder nur Teile des Dokuments einschließen. Umfasst die Signatur das gesamte Dokument, wurde nach der Signaturanbringung keine weitere Revision des Dokuments erzeugt wurde. Der Hinweis beeinflusst das Prüfergebnis nicht.

- Teile des Dokuments wurden signiert

Eine PDF-Signatur kann das gesamte Dokument oder nur Teile des Dokuments einschließen. Umfasst die Signatur nicht das gesamte Dokument, wurde nach der Signaturanbringung mindestens eine weitere Revision erzeugt. Es ist in diesem Fall zu empfehlen, sich davon zu überzeugen, dass die nicht signierte Revision keine Inhalte enthält, die 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 Anmerkung) verändern technisch den vorher signierten Inhalt nicht. Der Hinweis beeinflusst das Prüfergebnis nicht.

- Das PDF-Dokument ist nicht PAdES-konform.

Die Signatur ist nicht PAdES-konform. Da die Nichtkonformität sicherheitsunkritisch ist, beeinflusst sie das Prüfergebnis nicht. Mögliche Ursachen für diesen Hinweis 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.

- Das Signaturzertifikat passt nicht zum signierten Hashwert.

Bei einer PAdES-Signatur gemäß Baselineprofil muss das Signaturzertifikat beigefügt werden. Dieses Zertifikat muss gehasht werden; der Hashwert wird mitsigniert. Passt das Signaturzertifikat nicht zum signierten Hashwert, stimmen der signierte Hashwert und der neu berechnete Hashwert über das Zertifikat nicht überein. Trotzdem kann die mathematische Signaturprüfung erfolgreich sein, wenn der im beigefügten Signaturzertifikat vorhandene öffentliche Signaturprüfschlüssel erfolgreich die Signatur entschlüsseln konnte.

- Der Hashwert des Signaturzertifikats fehlt.

Bei einer PAdES-Signatur gemäß Baselineprofil muss das Signaturzertifikat beigefügt werden. Dieses Zertifikat muss gehasht werden; der Hashwert wird mitsigniert. Fehlt der Hashwert, kann die mathematische Signaturprüfung trotzdem positiv verlaufen, wenn der im beigefügten Signaturzertifikat vorhandene öffentliche Signaturprüfschlüssel erfolgreich die Signatur entschlüsseln konnte.

- Nicht zulässiger Eintrag in der Datenstruktur, die die Signaturinformationen enthält.

Es gibt einen nicht standardkonformen Eintrag in der Datenstruktur, die die Signaturinformationen enthält, wie zum Beispiel ein zusätzlicher Signaturzeitpunkt in der CMS-Signatur, der gemäß PAdES-Spezifikation dort nicht zulässig ist. Da diese Nichtkonformität nicht sicherheitskritisch ist, beeinflusst sie das Prüfergebnis nicht.

3.5 Einzelprüfung von Zertifikaten

In diesem Kapitel wird der Aufbau des Bereichs 1 "Zusammenfassung und Struktur" für die separate Zertifikatsprüfung beschrieben. 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.

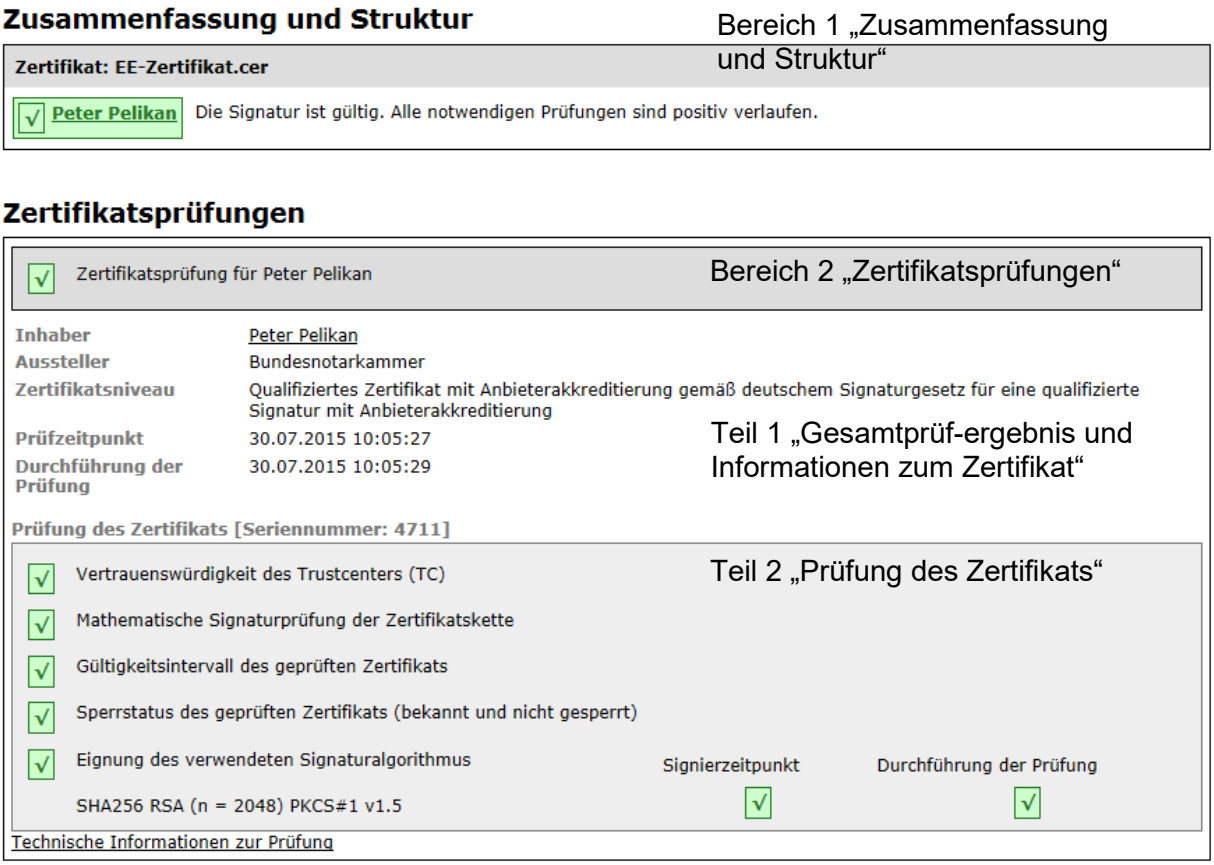


Abbildung 17: Bereich 1 "Struktur" und Bereich 2 "Zertifikatsprüfungen" bei der Prüfung eines einzelnen Zertifikats

3.5.1 Bereich 1: Zusammenfassung und Struktur

In den folgenden Unterkapiteln wird Bereich 1 "Zusammenfassung und Struktur" des Prüfprotokolls für die separate Zertifikatsprüfung beschrieben.

3.5.1.1 Zeile "Dateiname"

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

3.5.1.2 Zeile "Zertifikatsinhaber, Prüfergebnis und Erläuterung"

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

3.5.1.3 Spalte "Prüfergebnis"

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

-  Grüner Kasten mit Haken: Das Zertifikat ist gültig zum Prüfzeitpunkt.
-  Gelber Kasten mit Ausrufungszeichen: Das Prüfergebnis ist unbestimmt.
-  Roter Kasten mit Kreuz: Das Zertifikat ist ungültig zum Prüfzeitpunkt.

Erläuterungen zu  Grüner Kasten mit Haken:

Ein grüner Kasten mit Haken bedeutet, dass das Zertifikat zum angegebenen Prüfzeitpunkt gültig ist. Alle notwendigen Einzelprüfungen wurden durchgeführt und sind positiv verlaufen. Damit ist der Zertifikatsinhaber sicher identifiziert und seine Authentizität bestätigt.

Dieses 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 "unbestimmt" wechseln, weil z.B. der Sperrstatus des Zertifikats nicht mehr ermittelt werden kann oder weil, im Fall eines qualifizierten Zertifikats, der für die Signatur des Zertifikats verwendete Signaturalgorithmus inzwischen nicht mehr für die Prüfung einer qualifizierten Zertifikatssignatur geeignet ist.

Erläuterungen zu  Gelber Kasten mit Ausrufungszeichen:

Ein gelber Kasten mit Ausführungszeichen signalisiert, das mindestens eine notwendige Einzelprüfung einen unbestimmten Status besitzt weil sie z.B. nicht durchgeführt werden konnte. Endgültig fehlgeschlagene Einzelprüfungen gibt es nicht. Es kann nicht entschieden werden, ob die Signatur gültig oder ungültig ist.

Die Ursache für den unbestimmten Status sollte in jedem Fall genauer analysiert werden. Häufig kommt dieses Prüfergebnis nämlich dadurch zustande, dass der Sperrstatus des Zertifikats nicht ermittelt werden konnte (In diesem Fall hat die Einzelprüfung „Sperrstatus des Zertifikats“ den Status "gelb"). Nach einem gewissen Zeitraum ist in diesem Fall eine erneute Prüfung sinnvoll.

Bei der Prüfung einer qualifizierten Zertifikatsignatur kann der Status "gelb" auch ein endgültiges Ergebnis anzeigen, wenn der für die Zertifikatssignatur verwendete Signaturalgorithmus zum Zeitpunkt der Durchführung der Prüfung nicht mehr für die Prüfung einer qualifizierten Zertifikatsignatur geeignet war. In der Spalte Erläuterungen wird in diesem Fall der folgende Warnhinweis ausgegeben:

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

Bereits erzeugte qualifizierte elektronische Signaturen bleiben zwar auch dann noch qualifiziert, wenn der zugrundeliegende Signaturalgorithmus nach der Signaturerzeugung seine Sicherheitseignung verloren hat, sie büßen jedoch graduell und sukzessive ihren Beweiswert ein. Der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung, der sich auf Grund der Prüfung ergibt, kann dadurch erschüttert werden.

Erläuterungen zu Roter Kasten mit Kreuz:

Ein roter Kasten mit Kreuz bedeutet, dass das Zertifikat zum angegebenen Prüfzeitpunkt ungültig ist. Mindestens eine notwendige Einzelprüfung ist abschließend fehlgeschlagen. Damit konnte die signierende Person abschließend nicht sicher identifiziert werden.

Bei der Prüfung einer qualifizierten Zertifikatssignatur besitzt der Status "rot" eine besondere Warnfunktion, wenn der verwendete Signaturalgorithmus bereits zum Zeitpunkt der Erzeugung der Signatur nicht mehr für die Erzeugung einer qualifizierten Zertifikatssignatur geeignet war. In diesem Fall wird der folgende Warnhinweis ausgegeben:

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

Bereits bei der Erzeugung der Signatur war nicht mehr sichergestellt, dass der Signaturschlüssel-Inhaber die alleinige Kontrolle über die Mittel zur Erzeugung der Signatur hatte. Es handelt sich bei der erzeugten Signatur von vornherein daher nicht um eine qualifizierte elektronische Signatur.

3.5.1.4 Spalte "Name des Inhabers des Zertifikats"

Rechts neben dem Prüfergebnis wird der Name des Inhabers des Zertifikats in einem farbig unterlegten Kasten angezeigt. Angezeigt wird der Name des Signierenden oder der signierenden Organisation. Bei Signaturzertifikaten besteht der Name besteht in der Regel aus dem Vor- und Nachnamen des Zertifikatsinhabers, so wie er im Zertifikat hinterlegt wurde ([`subject`] [`CommonName`]). Bei Siegelzertifikaten muss der `CommonName` den Namen enthalten, der normalerweise von der legalen Person (Organisation) verwendet wird, um sich selbst darzustellen. Dieser Name muss nicht exakt mit dem vollständig registrierten Organisationsnamen übereinstimmen.

3.5.1.5 Spalte "Erläuterungen"

In der letzten Spalte rechts wird das Prüfergebnis erläutert. Ist das Zertifikat gültig (grüner Kasten mit Haken) wird ausschließlich die folgende Meldung angezeigt:

- Alle notwendigen durchgeführten Prüfungen lieferten ein positives Ergebnis.

Ist der Status der Zertifikatsprüfung unbestimmt (gelber Kasten mit Ausrufungszeichen) oder die Signatur ungültig (Roter Kasten mit Kreuz) wird als Erläuterungstext in der Regel das erste unbestimmte Einzelprüfergebnis bzw. das erste negative Einzelprüfergebnis des Prüfprotokolls angezeigt. Es gibt allerdings zwei Ausnahmen, die wegen ihrer besonderen Warnfunktion immer an dieser Stelle angezeigt werden:

- Qualifizierte elektronische Signatur. Es wurde aber ein Algorithmus verwendet, der zum Zeitpunkt der Durchführung der Prüfung nicht mehr für eine qualifizierte elektronische Signatur geeignet war.
- Fortgeschrittene Signatur und keine qualifizierte Signatur. Es wurde ein Algorithmus verwendet, der bereits zum Signierzeitpunkt nicht mehr für eine qualifizierte elektronische Signatur geeignet war.

3.5.2 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 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.“

3.5.2.1 Teil 1 Prüfergebnis und Informationen zum Zertifikat

3.5.2.1.1 Zeile "Prüfergebnis und Name des Zertifikatsinhabers"

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

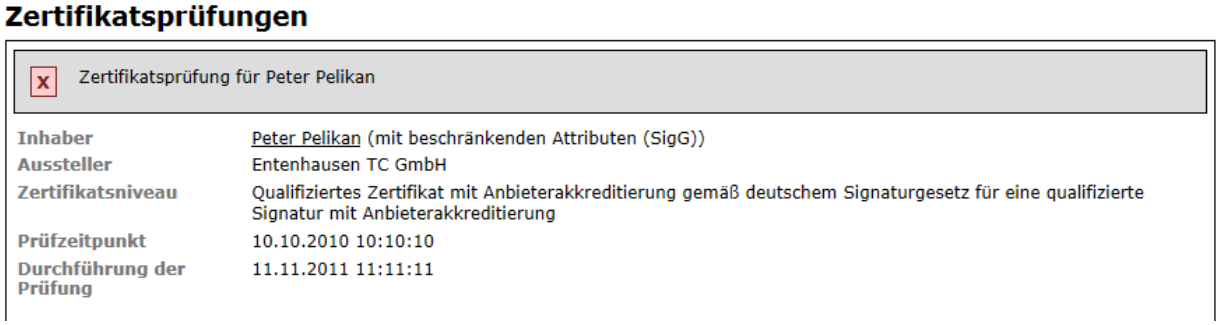


Abbildung 18: Teil 1 „Prüfergebnis und Informationen zum Zertifikat“ bei der Prüfung eines einzelnen Zertifikats

3.5.2.1.2 Spalte "Prüfergebnis"

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

- Grüner Kasten mit Haken: Das Zertifikat ist gültig.
- Gelber Kasten mit Ausrufungszeichen: Das Prüfergebnis ist unbestimmt.
- Roter Kasten mit Kreuz: Das Zertifikat ist ungültig.

Die Bedeutung der drei Status wird im Kapitel 3.5.1.3 erläutert.

3.5.2.1.3 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.

3.5.2.1.4 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.

3.5.2.1.5 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 Signaturrichtlinie oder eIDAS-Verordnung für eine fortgeschrittene elektronische Signatur
- Qualifiziertes Zertifikat gemäß Signaturrichtlinie oder eIDAS-Verordnung mit privatem Schlüssel auf Smartcard für eine qualifizierte elektronische Signatur

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

3.5.2.1.6 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.

3.5.2.1.7 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.

3.5.2.2 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 wird zusätzlich das Ergebnis der Eignung des zur Zertifikatssignatur verwendeten Signaturalgorithmus angezeigt.

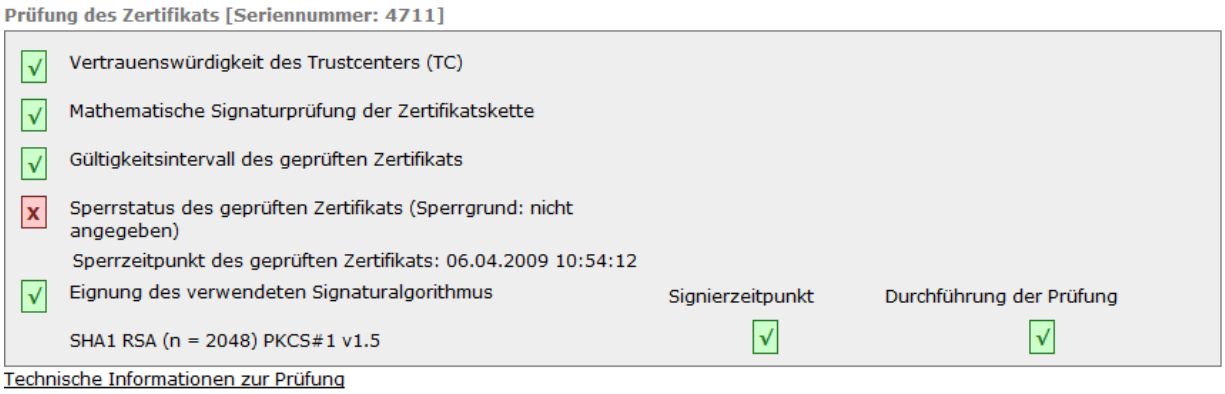


Abbildung 19: Teil 2 „Prüfung des Zertifikats

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

3.6 Anzeige 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 Signaturen.

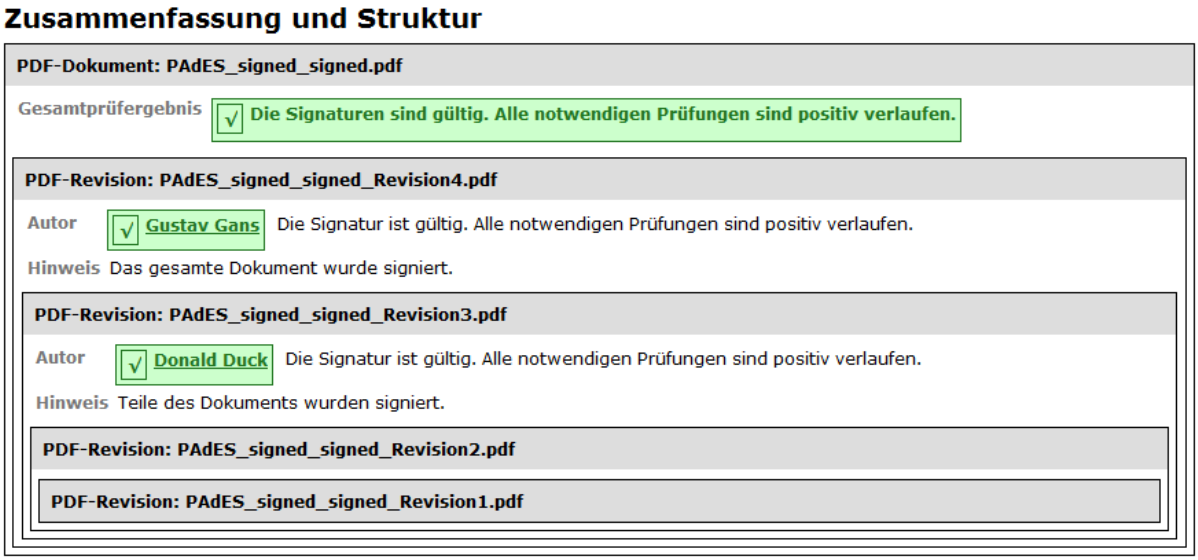


Abbildung 20: Bereich 1 Zusammenfassung und Struktur" bei PDF-Dokumenten mit mehreren Signaturen und der Ausgabe eines Gesamtstatus

3.6.1 Zeile „Gesamtprüfergebnis“

In der Zeile wird hinter der Bezeichnung "Gesamtprüfergebnis" das kumulierte Prüfergebnis aller geprüften Signaturen angezeigt. Das Signaturniveau der einzelnen Signaturen wird beim Gesamtprüfergebnis nicht berücksichtigt, d.h., gegebenenfalls wird auch über fortgeschrittene und qualifizierte elektronische Signaturen kumuliert. Die folgenden Status sind möglich:

- Grüner Kasten mit Haken: Die Signatur ist gültig/die Signaturen sind gültig. Alle notwendigen Prüfungen sind positiv verlaufen.
- Gelber Kasten mit Ausrufungszeichen: Mindestens eine notwendige Prüfung konnte nicht durchgeführt werden oder lieferte ein unbestimmtes Ergebnis.
- Roter Kasten mit Kreuz: Die Signatur ist ungültig/Mindestens eine Signatur ist ungültig. Mindestens eine notwendige Prüfung ist negativ verlaufen.
- Grauer Kasten: Kein Prüfergebnis vorhanden, da keine Signatur gefunden werden konnte.

Ein grüner Kasten mit Haken bedeutet, dass alle Signaturen gültig sind. Alle notwendigen Einzelprüfungen wurden durchgeführt und sind positiv verlaufen. Als Erläuterung wird angezeigt: "Die Signatur ist gültig/die Signaturen sind gültig. Alle notwendigen Prüfungen sind positiv verlaufen."

Ein gelber Kasten mit Ausführungszeichen signalisiert, das mindestens eine Signaturprüfung einen unbestimmten Status besitzt. Endgültig fehlgeschlagene Signaturprüfungen gibt es nicht. Als Erläuterung wird angezeigt: Mindestens eine notwendige Prüfung konnte nicht durchgeführt werden oder lieferte ein unbestimmtes Ergebnis."

Ein roter Kasten mit Kreuz bedeutet, dass mindestens eine Signatur ungültig ist. Als Erläuterung wird angezeigt: "Mindestens eine Signatur ist ungütig. Mindestens eine notwendige Prüfung ist negativ verlaufen."

Ein Grauer Kasten zeigt an, dass der Gesamtstatus nicht ermittelt werden konnte. Als Erläuterung wird angezeigt: "Kein Prüfergebnis vorhanden, da keine Signatur gefunden werden konnte."

3.6.2 Fachliches Gesamtprüfergebnis bei signierten PDF-Dokumenten

Bei der Prüfung von signierten PDF-Dokumenten kann über das fachliche Gesamtprüfergebnis eine mögliche Manipulationsgefahr berücksichtigt werden (siehe dazu auch Kapitel 3.4.5). Diese kann bei PAdES-Signaturen nicht ausgeschlossen werden, wenn

a) die digitale Signatur nur Teile des PDFs umschließt, also mindestens eine nach der digitalen Signatur erstellte Revision existiert und/oder

b) die digitale Signatur zwar das gesamte PDF umschließt, es aber mindestens eine weitere digitale Signatur gibt und dazwischen mindestens eine unsignierte Revision existiert.

Beide Angriffe sind keine technisch-mathematischen Angriffe auf PAdES-Signaturen, sondern liegen in den vielfältigen Arten der PDF-Gestaltung durch den PDF-Standard selbst begründet.

Bei der Anzeige des fachlichen Gesamtstatus sind zwei Fälle zu unterscheiden:

1. Eine unter a) und/oder b) beschriebene Manipulationsgefahr existiert nicht. In diesem Fall sind folgende Prüfergebnisse möglich:
   - Grüner Kasten mit Haken: Die Signatur ist gültig/die Signaturen sind gültig. Alle notwendigen Prüfungen sind positiv verlaufen.
   - Gelber Kasten mit Ausrufungszeichen: Mindestens eine notwendige Prüfung konnte nicht durchgeführt werden oder lieferte ein unbestimmtes Ergebnis.
   - Roter Kasten mit Kreuz: Die Signatur ist ungültig/Mindestens eine Signatur ist ungültig. Mindestens eine notwendige Prüfung ist negativ verlaufen.
2. Eine unter a) und/oder b) beschriebene Manipulationsgefahr existiert. In diesem Fall wird das folgende Prüfergebnisse unabhängig von dem Gesamtprüfergebnis der Einzelsignatur/Einzelsignaturen angezeigt (siehe Abbildung 21):
   - Roter Kasten mit Kreuz: Eine Manipulation des Inhalts kann nicht ausgeschlossen werden.

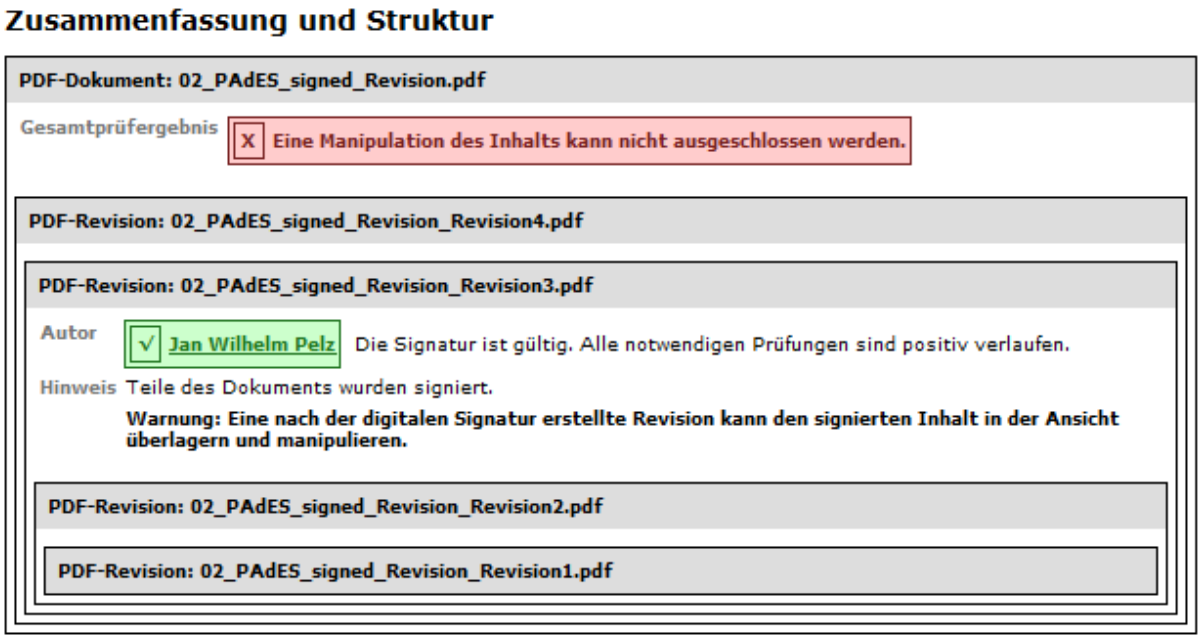


Abbildung 21: Bereich 1 "Zusammenfassung und Struktur" bei einem signierten, manipulationsgefährdeten PDF-Dokument mit fachlichem Gesamtstatus (Fall a))

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.

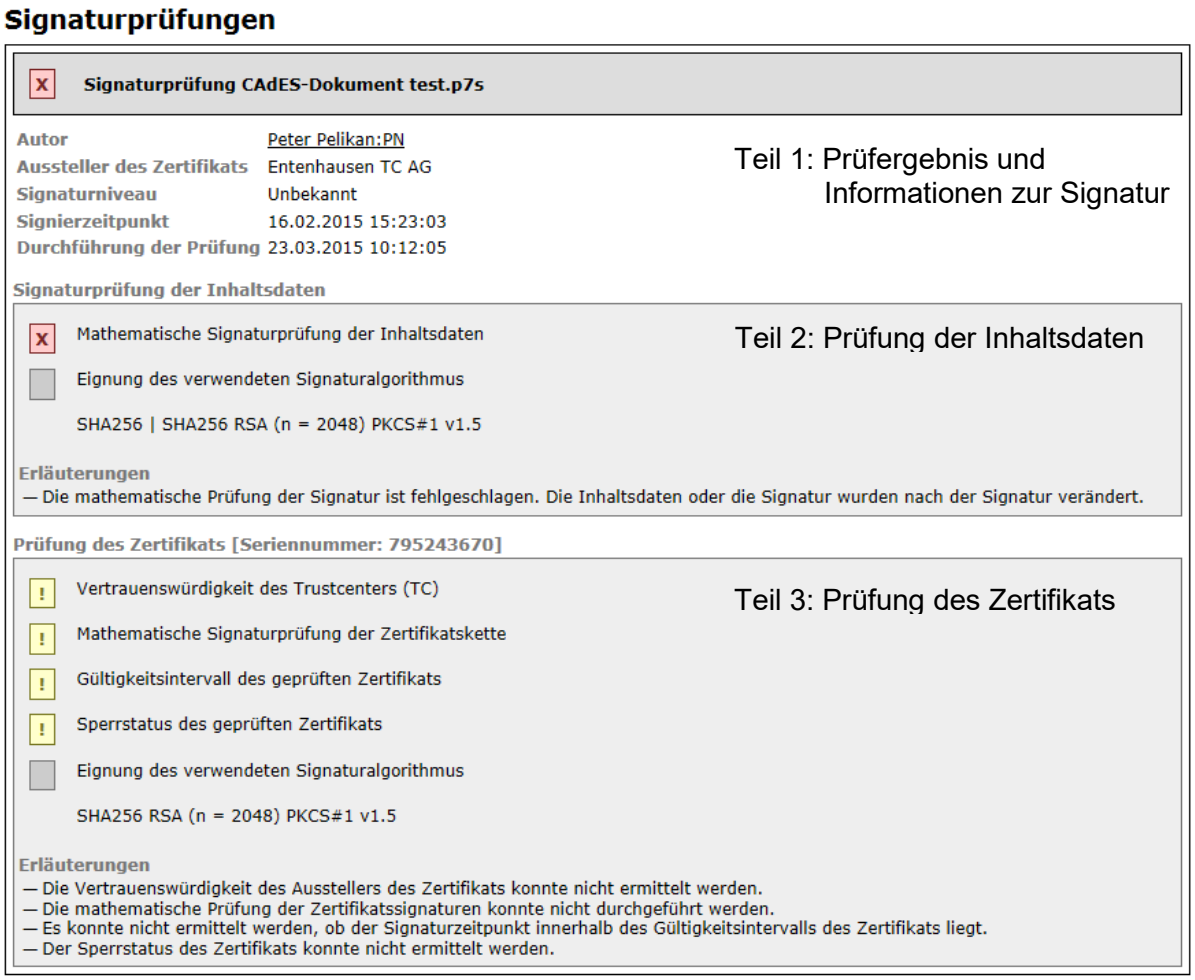


Abbildung 22: Bereich 2 "Signaturprüfungen"

Der Bereich "Signaturprüfungen" gliedert sich in drei Teile:

- Im Teil 1 wird das Ergebnis der Signaturprüfung 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 elektronischen Signatur 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 wird zusätzlich das Ergebnis der Eignung des zur Zertifikatssignatur verwendeten Signaturalgorithmus angezeigt.

Sollte eine Einzelprüfung zu einem unbestimmten Ergebnis führen oder fehlschlagen (Status gelb oder rot), wird am Ende des Teils 2 und 3 jeweils unter der Überschrift "Erläuterungen" der Grund für den jeweiligen Prüfstatus kurz erläutert.

4.1 Prüfergebnis und Kontextinformationen zur Signatur und zum Signierenden

In den folgenden Unterkapiteln werden das Ergebnis einer Signaturprüfung 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.

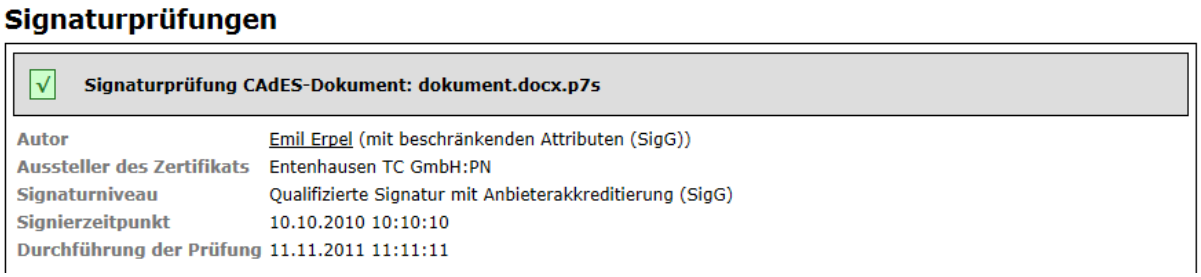


Abbildung 23: Teil 1 "Ergebnis der Signaturprüfung und Informationen zur Signatur und zum Signierenden"

4.1.1 Zeile "Prüfergebnis, Signaturformat und Dateiname des signierten Dokuments"

In der ersten grau unterlegten Zeile werden das Ergebnis der Signaturprüfung und der Name des signierten Objekts (signiertes Dokument, Revision, OSCI-Container) angezeigt.

4.1.1.1 Spalte „Ergebnis der Signaturprüfung“

In der Zeile wird zunächst das Ergebnis der Signaturprüfung in einem farbig unterlegten Kasten angezeigt. Die folgenden Status sind möglich:

- Grüner Kasten mit Haken: Die Signatur ist gültig.
- Gelber Kasten mit Ausrufungszeichen: Das Prüfergebnis ist unbestimmt.
- Roter Kasten mit Kreuz: Die Signatur ist ungültig.

Erläuterungen zu Grüner Kasten mit Haken:

Ein grüner Kasten mit Haken bedeutet, dass die Signatur gültig ist. Alle notwendigen Einzelprüfungen wurden durchgeführt und sind positiv verlaufen. Damit ist die Unverfälschtheit (Integrität der signierten Inhaltsdaten, der Nachricht, des Dokuments) sichergestellt, der Signierende sicher identifiziert und seine Authentizität bestätigt.

Erläuterungen zu  Gelber Kasten mit Ausrufungszeichen:

Ein gelber Kasten mit Ausführungszeichen signalisiert, das mindestens eine notwendige Einzelprüfung einen unbestimmten Status besitzt weil sie z.B. nicht durchgeführt werden konnte. Endgültig fehlgeschlagene Einzelprüfungen gibt es nicht. Es kann nicht entschieden werden, ob die Signatur gültig oder ungültig ist.

Erläuterungen zu  Roter Kasten mit Kreuz:

Ein roter Kasten mit Kreuz  bedeutet, dass die Signatur ungültig ist. Mindestens eine notwendige Einzelprüfung ist abschließend fehlgeschlagen. Damit ist entweder die Unverfälschtheit der Inhaltsdaten (Integrität der Daten) nicht sichergestellt oder es konnte die signierende Person abschließend nicht sicher identifiziert werden.

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".

4.1.1.3 Zeile "Autor"

Angezeigt wird der Name des Signierenden oder der signierenden Organisation. Bei Signaturzertifikaten besteht der Name besteht in der Regel aus dem Vor- und Nachnamen des Zertifikatsinhabers, so wie er im Zertifikat hinterlegt wurde ([`subject`] [`CommonName`]). Bei Siegelzertifikaten muss der `CommonName` den Namen enthalten, der normalerweise von der legalen Person (Organisation) verwendet wird, um sich selbst darzustellen. Dieser Name muss nicht exakt mit dem vollständig registrierten Organisationsnamen übereinstimmen.

Bei einem qualifizierten Zertifikat handelt es sich beim Namen des Autors um den im Identifikationsdokument angegebenen Vor- und Nachnamen. Bei deutschen qualifizierten Zertifikaten, die unter den Anforderungen des Signaturgesetzes ausgestellt wurden, wird durch die Angabe ":PN" hinter dem Namen wird angezeigt, dass es sich um ein Pseudonym handelt.

4.1.2 Zeile "Aussteller des Zertifikats"

Angezeigt wird der Name des Ausstellers des geprüften Zertifikats. Dies ist der Organisationsname [Attribut: `OrganisationName`] des Ausstellers (CA, Trustcenter) aus dem Feld [`issuer`] des geprüften Zertifikats. Bei einem qualifizierten Zertifikat ist der Organisationsname der aus dem CA-Zertifikat des Vertrauensdiensteanbieters übernommene Name des Inhabers des CA-Zertifikats.

4.1.3 Optionale Zeile "Aussteller des Attributzertifikats"

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.

4.1.4 Zeile "Signaturniveau"

Angezeigt wird das intendierte Niveau der elektronischen Signatur. Dieses ist auch das tatsächliche Signaturniveau, das erreicht wird, wenn das Ergebnis der Signaturprüfung den Status "gültig" ( Grüner Kasten mit Haken) erhalten hat.

Die eIDAS-Verordnung definiert Anforderungen an fortgeschrittene und qualifizierte elektronische Signaturen. Dabei gelten gemäß Artikel 51 der eIDAS-Verordnung Übergangsmaßnahmen für qualifizierte Signaturkarten, die unter der EU-Signaturrichtlinie 1999/93/EC (und dem deutschen Signaturgesetz) ausgegeben wurden: Signaturerstellungseinheiten, deren Übereinstimmung mit den Anforderungen gemäß Artikel 3 Absatz 4 der Richtlinie 1999/93/EC festgestellt wurde, gelten als qualifizierte Signaturerstellungseinheiten gemäß der eIDAS-Verordnung, qualifizierte Zertifikate, die gemäß der Richtlinie 1999/93/EC für natürliche Personen ausgestellt worden sind, gelten bis zu ihrem Ablauf als qualifizierte Zertifikate für elektronische Signaturen gemäß der eIDAS-Verordnung. Dementsprechend wird bei der Angabe des Signaturniveaus nicht mehr zwischen dem deutschen Signaturgesetz und der eIDAS-Verordnung unterschieden. Folgende Signaturniveaus werden während der Prüfung ermittelt und angezeigt:

- Fortgeschrittene elektronische Signatur,
- Fortgeschrittene elektronische Signatur mit qualifiziertem Zertifikat und
- Qualifizierte elektronische Signatur.

Neben qualifizierten Signaturen werden in der eIDAS-Verordnung erstmalig auch elektronische Siegel für juristische Personen definiert (siehe Artikel 35 und 36). Die Anforderungen an diese Siegel sowie deren Validierung entsprechen sinngemäß den Anforderungen an qualifizierte elektronische Signaturen gemäß eIDAS-Verordnung. Definiert sind:

- Fortgeschrittenes elektronisches Siegel,
- Fortgeschrittenes elektronisches Siegel mit qualifiziertem Zertifikat und
- Qualifiziertes elektronisches Siegel.

Herkunft der Informationen zum Signaturniveau

Das intendierte Signaturniveau basiert nicht auf Angaben im geprüften Zertifikat (QC-Statement) sondern wird bei der Zertifikatsprüfung ermittelt. Verwendet wird das in der Konfiguration des angefragten OCSP/CRL-Relays hinterlegte Niveau. Dort ist neben den Root- und Ausstellerzertifikaten und technischen Daten zur Verbindungskonfiguration auch für jede CA das Signaturniveau hinterlegt. Die Konfiguration des OCSP/CRL-Relays wird durch die Governikus KG bereitgestellt (Name „Standardkonfiguration“), kann aber auch durch den Betreiber des OCSP/CRL-Relays ergänzt oder modifiziert werden (Name „Individualkonfiguration“). Ob die Angabe im Prüfprotokoll der Standard- oder einer betreiberspezifischen Individualkonfiguration entnommen wurde, wird im Bereich "technische Informationen" in der Zeile "Konfiguration der Prüfinstanz" des Prüfprotokolls angezeigt (siehe auch Kapitel 6.2.4).

Wird bei einer intendierten qualifizierten Signatur als Informationsquelle der Wert „Standardkonfiguration `[Versionsnummer]`“ angezeigt, stammt die Niveauangabe aus einer Vertrauenslsiste (TL). Diese Liste wird von der zuständigen Aufsichtsbehörde zum Download bereitgestellt und enthält neben den CA-Zertifikaten, die einen Dienst (Dienste-Identifier) identifizierten, vor allem Informationen zur Qualität der angebotenen Dienste jedes Vertrauensdiensteanbieters.

Die Prüfung eines qualifizierten Zertifikats aus einem anderen EU-Mitgliedstaat als Deutschland erfolgt nicht durch die OCSP/CRL-Relays der Betreiber, sondern über einen durch die Governikus KG zentral bereitgestellten XKMS-Responder. Die Angaben zum Zertifikats-

bzw. Signaturniveau im Prüfprotokoll basieren in diesem Fall auf der Auswertung der Trusted List des jeweiligen EU-Mitgliedstaates durch den XKMS-Responder.

4.1.5 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 das Signaturzertifikat überprüft werden. Dieser Umstand führt immer zu einem unbestimmten Prüfergebnis. Als Erläuterung wird am Ende des Teils 2 "Prüfung der Inhaltsdaten" die folgende Erläuterung angezeigt:

- Die Signatur konnte geprüft werden, da ein Signaturzeitpunkt nicht ermittelt werden konnte.

4.1.6 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).

4.1.7 Optional: Zeile "Signaturgrund" (nur bei *AdES-Signaturen)

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

- Nachweis der Quelle
- Nachweis des Empfangs
- Nachweis der Auslieferung
- Nachweis des Versands
- Nachweis der Bestätigung
- Nachweis der Erzeugung

Erläuterungen zum Signaturgrund

- 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).

4.1.8 Optional: Zeile "Signaturrichtlinie" (nur bei *AdES- Signaturen)

In signierten Dokumenten der *AdES-Formate (genauer im SignerInfo) kann eine Signaturrichtlinie angegeben werden oder der Link zu einer Signaturrichtlinie hinterlegt werden. Damit gibt der Signierende an, welche Rolle und Verpflichtungen er mit der Signatur eingehen möchte und/oder dass er Anforderungen an die Signaturprüfung stellt. Ist ein Eintrag vorhanden, wird dieser angezeigt. Die Richtlinie wird bei der Prüfung der Signatur nicht berücksichtigt.

4.1.9 Optional. Zeile Signaturort (nur bei *AdES- Signaturen)

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

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

4.1.9.1 Optional: Zeile Hinweise"

Folgende Hinweise können angezeigt werden:

- Der mitsignierte Hashwert und der neu berechnete Hashwert über das beigefügte Signaturzertifikat stimmen nicht überein.

Der Hinweis hat informativen Charakter. Einer standardkonformen *AdES-Signatur muss das Signaturzertifikat beigefügt sein; der Hashwert dieses Zertifikats ist mit zu signieren. Ob der signierte Hashwert und der neue berechnete Hashwert über das Zertifikat übereinstimmen, wird bei der Signaturprüfung überprüft. Ist dieses nicht der Fall, wurde entweder a) das Zertifikat nach dem Hashen oder b) vor der Signatur der Hashwert verändert. Damit ist das Dokument nicht *AdES-konform gemäß Baseline Profile. Die mathematische Signaturprüfung kann trotzdem positiv verlaufen, wenn sich im beigefügten Signaturzertifikat der zum privaten Signaturschlüssel korrespondierende öffentliche Signaturprüfschlüssel befindet.

- Der Hashwert des Signaturzertifikats fehlt.

Sollte der Hashwert des Signaturzertifikats fehlen ist das signierte Dokument nicht *AdES-konform gemäß Baseline Profile. Die mathematische Signaturprüfung kann trotzdem positiv verlaufen, wenn sich im beigefügten Signaturzertifikat der zum privaten Signaturschlüssel korrespondierende öffentliche Signaturprüfschlüssel befindet.

4.2 Signaturprüfung der Inhaltsdaten

Im Teil "Signaturprüfung der Inhaltsdaten" werden das Ergebnis der mathematischen Signaturprüfung und die zur Signatur verwendeten Algorithmen angezeigt. Bei der Prüfung einer qualifizierten elektronischen Signatur wird zusätzlich auch das Ergebnis der Prüfung der Eignung der verwendeten Algorithmen aus Basis des verwendeten Algorithmenkatalogs (siehe dazu die ausführliche Erläuterung im Kapitel 2.5) für die Inhaltsdatensignatur angezeigt.

In den folgenden Unterkapiteln werden die Einzelprüfergebnisse ausführlich erläutert.

4.2.1 Zeile "Mathematische Signaturprüfung der Inhaltsdaten"

Abbildung 24: 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: Prüfung erfolgreich.
- ! Gelber Kasten mit Ausrufungszeichen: Unbestimmtes Prüfergebnis.
- X Roter Kasten mit Kreuz: Prüfung fehlgeschlagen.

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 führte zu einem unbestimmten Prüfergebnis. Das Zustandekommen dieses Prüfergebnisses kann unterschiedliche Ursachen haben. Eine notwendige Bedingung für die mathematische Signaturprüfung ist eine erfolgreiche Analyse des Dokuments und das Erkennen und das Auswerten der Signaturstruktur mit der Signatur und dem Signaturzertifikat. Sollte es in diesem Kontext zu Problemen kommen, kann möglicherweise eine mathematische Signaturprüfung nicht durchgeführt werden. Dieser Umstand führt zu einem unbestimmten Status der Signaturprüfung. Es kann auch vorkommen, dass die Signatur zwar mathematisch geprüft werden kann, sie aber in einer Form nicht standardkonform ist, die zu sicherheitskritischen Mängeln führt. Auch dieser Umstand führt zu einem unbestimmten Status der Signaturprüfung. Eine Erläuterung wird am Ende des Teils 2 „Prüfung der Inhaltsdaten unter der Zeile „Erläuterungen“ angezeigt“.

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. Das Zustandekommen dieses Prüfergebnisses kann unterschiedliche Ursachen haben. Eine Erläuterung wird am Ende des Teils 2 „Prüfung der Inhaltsdaten unter der Zeile „Erläuterungen“ angezeigt“.

4.2.2 Zeile "Eignung des verwendeten Signaturalgorithmus"

Die Eignung des für die qualifizierte elektronische Signatur der Inhaltsdaten verwendeten Signaturalgorithmus wird auf Basis des verwendeten Algorithmenkatalogs zum Signierzeitpunkt und zum Zeitpunkt der Durchführung der Prüfung ermittelt. Die Prüfung wird nur bei einer qualifizierten elektronischen Signatur durchgeführt.

Ein Signaturalgorithmus setzt sich aus mehreren Teil-Algorithmen zusammen, die zusammen den verwendeten „Signaturalgorithmus“ bilden. Die einzelnen Teil-Algorithmen werden hinsichtlich ihrer Eignung getrennt bewertet. Für das Ergebnis der Eignung des Signaturalgorithmus gilt: Ist einer der Teil-Algorithmen für die Anbringung oder Prüfung einer qualifizierten Signatur als nicht mehr geeignet klassifiziert, wird der gesamte Signaturalgorithmus als nicht mehr geeignet angesehen. Welche Teil-Algorithmen für den Signaturalgorithmus verwendet wurden, wird unter der Zeile „Eignung des verwendeten Signaturalgorithmus" angezeigt.

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 für die Inhaltsdatensignatur 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 (alle Teil-Algorithmen waren geeignet).

Abbildung 25: Ergebnis der Eignungsprüfung eines Signaturalgorithmus, der zum Signierzeitpunkt und zum Zeitpunkt der Durchführung der Prüfung für eine qualifizierte elektronische Signatur geeignet war

Erläuterungen zu Gelber Kasten mit Ausrufungszeichen:

Der für die Inhaltsdatensignatur verwendete Signaturalgorithmus war zum Zeitpunkt der Durchführung der Prüfung gemäß verwendetem Algorithmenkatalog nicht mehr für die Prüfung einer qualifizierten elektronischen Signatur geeignet (mindestens ein Teil-Algorithmus war nicht mehr geeignet). Zum Zeitpunkt der Signaturanbringung (Signierzeitpunkt) war die Eignung jedoch noch gegeben.

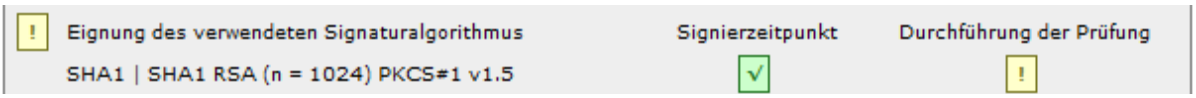


Abbildung 26: Ergebnis der Eignungsprüfung eines Signaturalgorithmus, der nur zum Zeitpunkt der Durchführung der Prüfung nicht mehr für eine qualifizierte elektronische Signatur geeignet war

Bereits erzeugte qualifizierte elektronische Signaturen bleiben auch dann noch qualifiziert, wenn der zugrundeliegende Signaturalgorithmus nach der Erzeugung 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. Es wurde aber ein Algorithmus verwendet, der zum Zeitpunkt der Durchführung der Prüfung nicht mehr für eine qualifizierte elektronische Signatur geeignet war.

Erläuterungen zu Roter Kasten mit Kreuz:

Abbildung 27: Ergebnis der Eignungsprüfung eines Signaturalgorithmus, der schon zum Signierzeitpunkt nicht mehr für eine qualifizierte elektronische Signatur geeignet war

Der für die Inhaltsdatensignatur verwendete Signaturalgorithmus war bereits zum Signierzeitpunkt für die Erzeugung einer qualifizierten elektronischen Signatur nicht (mehr) geeignet (mindestens ein Teil-Algorithmus war nicht mehr geeignet). Signaturen, die nach dem Schwachwerden des zugrundeliegenden Signaturalgorithmus erzeugt wurden, sind von vornherein keine qualifizierten elektronischen 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. Es wurde ein Algorithmus verwendet, der zum Signierzeitpunkt nicht mehr für eine qualifizierte elektronische Signatur geeignet war.

Erläuterungen zu Grauer Kasten:

Eine Prüfung der Eignung des verwendeten Signaturalgorithmus wurde nicht durchgeführt. Sie ist signaturrechtlich nur erforderlich bei der Prüfung von qualifizierten elektronischen Signaturen. Der verwendete Signaturalgorithmus wird auch in diesem Fall angezeigt.

4.2.2.1 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 28: Ergebnis der Eignungsprüfung des verwendeten Signaturalgorithmus einer Inhaltsdatensignatur zum Signierzeitpunkt

Folgende Status sind möglich:

- **grüner Kasten mit Haken**: Der Signaturalgorithmus war zum Signierzeitpunkt gemäß aktuellem Algorithmenkatalog für die Erzeugung einer qualifizierten elektronischen Signatur geeignet (alle Teil-Algorithmen waren geeignet).
- **roter Kasten mit Kreuz**: Der Signaturalgorithmus war bereits zum Signierzeitpunkt gemäß aktuellem Algorithmenkatalog für die Erzeugung einer qualifizierten elektronischen Signatur nicht (mehr) geeignet (mindestens ein Teil-Algorithmus war nicht (mehr) geeignet).

4.2.2.2 Spalte Einzelprüfergebnis „Durchführung der Prüfung“

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

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 geeignet (alle Teil-Algorithmen waren 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 (mindestens ein Teil-Algorithmus war nicht (mehr) 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 nicht (mehr) geeignet (mindestens ein Teil-Algorithmus war 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.

4.2.2.3 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 über beide Zeitpunkte	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
rot (nein)	rot (nein)	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 aus Basis des verwendeten Algorithmenkatalog in Abhängigkeit vom Verwendungszeck (Anbringung einer Inhaltsdatensignatur, Prüfung einer Inhaltsdatensignatur, Anbringung einer Zertifikatssignatur, Prüfung einer Zertifikatssignatur).

4.2.2.4 Zeile "Angabe des verwendeten Signaturalgorithmus"

Unterhalb der Zeile mit dem angezeigten Prüfergebnis wird der Name des verwendeten Signaturalgorithmus angezeigt. Der Signaturalgorithmus setzt sich aus mehreren Teil-Algorithmen zusammen, die zusammen den verwendeten „Signaturalgorithmus“ bilden. Die einzelnen Teil-Algorithmen werden getrennt hinsichtlich ihrer Eignung bewertet. Für das kumulierte Prüfergebnis gilt: Ist einer der unten benannten Teilalgorithmen nicht mehr für die Anbringung oder Prüfung einer qualifizierten elektronischen Signatur als geeignet klassifiziert, wird der gesamte Signaturalgorithmus als nicht mehr geeignet angesehen.

Der zusammengesetzte Signaturalgorithmus enthält - in Abhängigkeit vom gewählten Signaturformat und Signaturverfahren - folgende Teilalgorithmen (von links nach rechts):

- **Hashalgorithmus I:**
  Der Hashalgorithmus I wird für das Hashen der Inhaltsdaten verwendet und wird immer angezeigt.
- **Optional: Hashalgorithmus II:**
  Der Hashalgorithmus II existiert nur bei detached CMS-/CAdES-Signaturen und XML-/XAdES-Signaturen sowie bei Zeitstempeln. Er wird bei diesen Formaten für das Hashen der zu signierenden Attribute des SignerInfo sowie bei Zeitstempeln für das Hashen des TimestampTokenInfo verwendet.
- **Schlüsselalgorithmus** mit Bitlängen von Parametern:
  Ist das eigentliche kryptographische Verfahren zum Signieren und wird immer angezeigt
- **Optional: Paddingalgorithmus:**
  Der Paddingalgorithmus wird nur bei RSA-Signaturen verwendet um den berechneten Hashwert aufzufüllen. Er wird nur angezeigt, wenn eine RSA-Signatur erzeugt wurde.

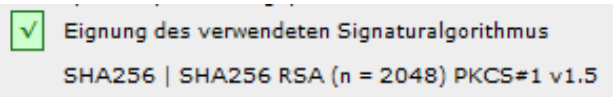


Abbildung 29: Angezeigter Signaturalgorithmus

Erläuterung Hashalgorithmus

Ein Hashalgorithmus ist ein standardisiertes kryptographisches Verfahren zur Berechnung eines eindeutigen (kurzen) Hashwerts über beliebige digitale Daten. Er wird verwendet, um die Integrität von digitalen Daten zu sichern. Wenn zwei Dokumente (Inhaltsdaten) den gleichen Hashwert besitzen, ist die Gleichheit der Dokumente garantiert (nach Stand von Wis-

senschaft und Technik), wenn ein im verwendeten Algorithmenkatalog als geeignet klassifizierter Hashalgorithmus verwendet wurde. Ein solcher Hashalgorithmus garantiert, dass es praktisch unmöglich ist, dass zwei verschiedene Dokumente den gleichen Hashwert besitzen können.

Der im Prüfprotokoll angegebene erste Hashalgorithmus (**Hashalgorithmus I**) ist der Algorithmus, der verwendet wurde, um den Hashwert der Inhaltsdaten (des Dokuments) zu erzeugen. Dieser Hashwert wird abgelegt im sogenannten SignerInfo des signierten Dokuments. Das SignerInfo ist ein Bereich enthält noch weitere Inhalte (sogenannte Attribute) wie das Signaturzertifikat, den Signaturzeitpunkt, die technischen Namen der verwendeten Teil-Algorithmen und der erzeugte Signaturwert selbst.

Der bei detached CMS-CAdES-Signaturen, XML/XAdES-Signaturen und bei Zeitstempeln angegebene Hashalgorithmus (**Hashalgorithmus II**) ist der Algorithmus, der verwendet wurde um die zu signierenden Attribute des SignerInfo zu hashen. Dieses sind unter anderem der Hashalgorithmus der Inhaltsdaten, das Signaturzertifikat, der Signaturzeitpunkt und die technischen Namen der verwendeten Teil-Algorithmen. Der Signaturwert selbst ist ein sogenanntes unsigniertes Attribut und wird später hinzugefügt.

Erläuterung Schlüsselalgorithmus

Der an dritter Stelle angegebene Schlüsselalgorithmus (**Schlüsselalgorithmus**) ist das asymmetrische kryptographische Verfahren, das zum Signieren selbst verwendet wurde. Es verwendet ein Schlüsselpaar, bestehend aus einem privaten und einem öffentlichen Schlüsselteil. Der private Schlüsselteil ist die Basis für die Signaturerzeugung, der öffentliche Schlüsselteil (der im Signaturzertifikat enthalten ist) ist die Basis, um die Signatur zu prüfen.

Folgende asymmetrische kryptographische Signaturverfahren sind grundsätzlich für eine qualifizierte elektronische Signatur geeignet, wenn bestimmte Parameterlängen verwendet werden:

1. RSA,
2. DAS und
3. ECDSA.

RSA wurde von Rivest, Shamir und Adleman 1977 zum Erzeugen und Verifizieren digitaler Signaturen explizit beschrieben. DSA (Digital Signature Algorithm) ist ein Verfahren, das vom National Institute of Standards and Technology (NIST) in den USA 1984 spezifiziert wurde. Daneben gibt es Varianten des DSA, die auf sogenannten „Punktegruppen elliptischer Kurven über endlichen Körpern“ basieren. In Deutschland verwendet wird nur die Variante ECDSA. ECDSA ist eine Alternative zu RSA und ein grundsätzlich anderes mathematisches Verfahren, dass auf Signaturkarten vermehrt zum Einsatz kommt, wie z.B. beim elektronischen Personalausweis. ECDSA ist beim Signieren und Signaturprüfen schneller bei gleichem Sicherheitsniveau, da die Bitlängen der Systemparameter kürzer sind.

Die Sicherheit der oben genannten Verfahren beruht auf bestimmten sogenannten „mathematischen Problemen[1]“, die verhindern, dass aus Signaturen und öffentlichen Signaturprüfschlüsseln auf den privaten Schlüsselteil geschlossen werden kann. Dieses ist der Fall, wenn die besten heute bekannten Algorithmen für notwendige mathematische Operationen (Faktorisieren ganzer Zahlen, Berechnen diskreter Logarithmen) verwendet werden, die die Leistungsfähigkeit der heutigen Rechnertechnik berücksichtigt und wenn geeignete System-

[1] 1: Faktorisierungsproblem für ganze Zahlen, 2: Problem der Berechnung diskreter Logarithmen in der multiplikativen Gruppe von F, 3: Diskretes-Logarithmus-Problem in einer elliptischen Kurve über einem Restklassenkörper modulo einer Primzahl p oder einem Körper der Charakteristik 2.

parameter gewählt werden. Hinter dem verwendeten Signaturverfahren werden daher auch die verwendeten Parameterlängen angegeben (RSA: Parameter n, DSA und den Varianten auf der Basis elliptischer Kurven: Parameter p oder m und q). Ihre Länge wird bei der Beurteilung der Eignung des Schlüsselalgorithmus auf der Basis des verwendeten Algorithmenkatalog mit berücksichtigt.

Erläuterung Paddingalgorithmus (nur bei RSA-Signaturen)

Damit RSA-signiert werden kann, muss der Hashwert in einem Vorverarbeitungsschritt „aufgefüllt“ werden. Vor dem Signieren wird daher noch ein **Paddingalgorithmus** eingesetzt, der den Hashwert verlängert.

Am Ende des Prüfprotokolls befindet sich eine Liste aller geprüften Teil-Algorithmen. Angezeigt werden dort der Name des Teil-Algorithmus (ggf. mit Bitlänge des verwendeten Parameters in Klammern) und das Datum des Ablaufs der Eignung auf Basis des verwendeten Algorithmenkatalogs in Abhängigkeit vom Verwendungszweck (Anbringung einer Inhaltsdatensignatur, Prüfung einer Inhaltsdatensignatur, Anbringung einer Zertifikatssignatur, Prüfung einer Zertifikatssignatur).

Auszug aus dem Algorithmenkatalog SOG-IS plus (Bundesnetzagentur 2017/SOG-IS Agreed Cryptographic Mechanisms V1.1) veröffentlicht von der Governikus KG am 01.06.2018

Algorithmusname	Typ	geeignet für	bis
PKCS#1 v1.5	Paddingalgorithmus	Anbringung von Zertifikatssignaturen	31.12.2018
PKCS#1 v1.5	Paddingalgorithmus	Anbringung von Inhaltsdatensignaturen	31.12.2017
PKCS#1 v1.5	Paddingalgorithmus	Prüfung von Zertifikats- und Inhaltsdatensignaturen	31.12.2022
RSA (n = 2048)	Schlüsselalgorithmus	Anbringung von Zertifikats- und Inhaltsdatensignaturen	31.12.2022
RSA (n = 2048)	Schlüsselalgorithmus	Prüfung von Zertifikats- und Inhaltsdatensignaturen	31.12.2024
SHA256	Hashalgorithmus	Anbringung/Prüfung von Zertifikats- und Inhaltsdatensignaturen	Ohne Ablaufdatum
SHA256withRSA	Signaturalgorithmus	Anbringung von Zertifikats- und Inhaltsdatensignaturen	31.12.2022
SHA256withRSA	Signaturalgorithmus	Prüfung von Zertifikats- und Inhaltsdatensignaturen	31.12.2024

Abbildung 30: Anzeige der verwendeten Teil-Algorithmen für eine qualifizierte elektronische Signatur mit Datum des Ablaufs der Eignung in Abhängigkeit vom Verwendungszeck

4.2.2.5 Zeile „Erläuterungen“ für die mathematische Signaturprüfung

Unter der Zeile „Erläuterungen“ werden die Ursachen angezeigt, die zu einem unbestimmten Status (Gelbprüfung) der mathematischen Signaturprüfung oder zu einem Fehlschlagen der Prüfung (Rotprüfung) geführt haben.

Ursachen für einen unbestimmten Status

a) alle unterstützten Signaturformate

- Die Signatur konnte geprüft werden, da ein Signaturzeitpunkt nicht ermittelt werden konnte.
- Die Signatur konnte mathematisch nicht geprüft werden, da das Zertifikat (und damit der Signaturprüfschlüssel) nicht vorliegt.
- Die Signatur konnte mathematisch nicht geprüft werden, da die Inhaltsdaten nicht vorliegen.
- Die mathematische Prüfung der Signatur konnte nicht durchgeführt werden, da der Algorithmus nicht implementiert ist.
- Es konnte nicht ermittelt werden, ob der Signaturalgorithmus für eine qualifizierte elektronische Signatur geeignet ist.

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

b) nur bei PAdES-Signaturen

- Nur Teile der Revision wurden signiert.
  Wenn nur Teile der Revision signiert wurden, kann es sein, dass Inhalte durch externe Viewer angezeigt werden, die nicht durch die Signatur vor einer Manipulation geschützt werden. Solche Signaturen sollten nicht ungefragt akzeptiert werden, obwohl – rein technisch gesehen - die mathematische Signaturprüfung positiv verlaufen kann.
- Die Signatur konnte nicht verarbeitet werden.
  Die Signatur konnte nicht verarbeitet werden, weil a) die Signatur fehlerhaft ist und daher nicht geparst werden konnte oder b) die PDF-Revision mehr als eine Signatur und nur einen Signierzeitpunkt enthält oder c) ein unbekannter Filter verwendet wurde oder d) ein unbekannter Signaturhandler verwendet wurde.
- Die Signatur ist nicht standardkonform.
  Die Signatur bezieht sich nicht auf die Inhaltsdaten und ist daher nicht standardkonform. Es besteht konkret die Möglichkeit, dass die Signatur verändert wurde.

c) nur bei XAdES-Signaturen

- Eine Signaturprüfung ist nicht möglich, da eine unzulässige XPATH-Transformation verwendet wurde.
- Eine Signaturprüfung ist nicht möglich, da eine unzulässige XSLT-Transformation verwendet wurde.
- Eine Signaturprüfung ist nicht möglich, da ein unbekannter Kanonisierungsalgorithmus verwendet wurde.
  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. Dieses führt zu einem unbestimmten Status der mathematischen Signaturprüfung.

Ursachen für ein Fehlschlagen der Prüfung

a) alle unterstützten Signaturformate

- Die mathematische Prüfung der Signatur ist fehlgeschlagen. Die Inhaltsdaten oder die Signatur wurden nach der Signatur verändert.
- Fortgeschrittene Signatur und keine qualifizierte elektronische Signatur. Es wurde ein Algorithmus verwendet, der zum Signierzeitpunkt nicht mehr für eine qualifizierte elektronische Signatur geeignet war.

b) nur bei PDF/PAdES-Signaturen

- Die Signatur enthält illegalen Inhalt (nur bei PDF-Inline-Signaturen).

c) nur bei OSCI-Nachrichten

- Die Signatur der OSCI-Nachricht ist inkorrekt (nur bei OSCI-Nachrichten).

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

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

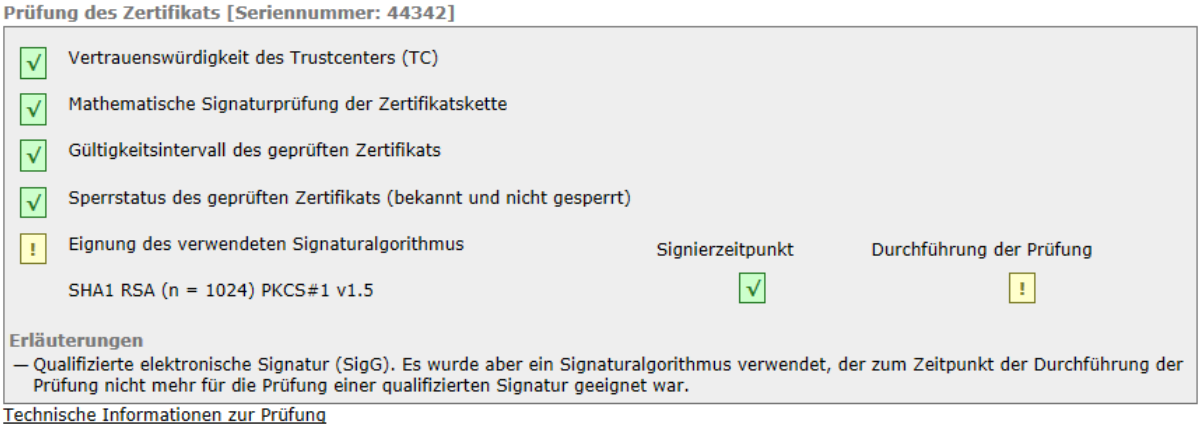


Abbildung 31: Teil 3 "Prüfung des Zertifikats"

Wird bei einer Signaturprüfung die Zertifikatsprüfung durch das OCSP/CRL-Relay nicht angefordert, erhalten alle vier Prüfmomente einen unbestimmten Status.

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 des 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 Signaturzertifikaten wird in Abhängigkeit vom konfigurierten Gültigkeitsmodell (Kette, Schale-Hybrid, Escape-Route) geprüft, ob der Signaturzeitpunkt des Zertifikats (Kettenmodell) oder der Signaturzeitpunkt der Inhaltsdaten (Modell Schale-Hybrid) innerhalb des Gültigkeitsintervalls (Validity Interval) des übergeordneten Zertifikats liegt. Diese Prüfung wird für jedes Zertifikat der Kette durchgeführt. 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 führte zu einem unbestimmten Ergebnis, weil er z.B. nicht durchgeführt werden konnte.
- **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.

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 führte zu einem unbestimmten Ergebnis.
- **Roter Kasten mit Kreuz**: Mindestens eine mathematische Signaturprüfung ist fehlgeschlagen. 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.

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 liegt. Folgende Status sind möglich:

- **Grüner Kasten mit Haken**: Der Signierzeitpunkt liegt innerhalb des Gültigkeitszeitraums des Signaturzertifikats.
- **Gelber Kasten mit Ausrufungszeichen**: Die Prüfung führte zu einem unbestimmten Ergebnis.
- **Roter Kasten mit Kreuz**: Der Signierzeitpunkt liegt 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.

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 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 Ermittlung des Sperrstatus des Zertifikats führte zu einem unbestimmten Ergebnis. In den Erläuterungen am Ende des Teils 3 wird – soweit ermittelbar – die Ursache für den unbestimmten Status angezeigt.
- **Roter Kasten mit Kreuz**: Das Zertifikat war zum Signaturzeitpunkt gesperrt oder dem Trustcenter unbekannt.
- **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.

Abbildung 32: Teil 3 "Sperrgrund und Sperrzeitpunkt bei einem gesperrten Zertifikat"

Besonderheiten beim Sperrstatus bei Zertifikaten (Positiv-Negativ-Prüfung)

Gemäß RFC2560 ist es zulässig, dass Status-Informationen einer OCSP-Antwort aus einer CRL stammen, in der nur die Seriennummern gesperrter Zertifikate enthalten sind. Eine Positivaussage "Trustcenter hat das Zertifikat ausgestellt" ist nicht damit verbunden. Optional können OCSP-Responder gemäß RFC (und dieses war auch in der CommonPKI-Spezifikation für qualifizierte Zertifikate so vorgeschrieben) die OCSP-Antwort um den Hashwert des Zertifikats, von dem die Statusinformation zurückgemeldet wurde, ergänzen.

Das OCSP/CRL-Relay vergleicht dann 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 auch tatsächlich vom Vertrauensdiensteanbieter ausgestellt wurde (Positiv-Negativ-Prüfung). Ein grüner Kasten mit Haken bedeutet in diesem Fall:

- **Grüner Kasten mit Haken**: Das Zertifikat (in der Regel das Signaturzertifikat) war zum Zeitpunkt der Signaturanbringung (Signierzeitpunkt der Inhaltsdaten) nicht gesperrt und wurde durch den Vertrauensdiensteanbieter tatsächlich ausgestellt. Angezeigt wird in diesem Fall in Klammern hinter dem Text "Sperrstatus des geprüften Zertifikats" der Hinweistext "bekannt und nicht gesperrt".

4.3.5.1 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:

- unbekannt
- 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

Kompromittierung des privaten Schlüssels

Der Sperrgrund "Privater Schlüssel kompromittiert" führt immer zum Sperrstatus "rot", unabhängig vom Sperrzeitpunkt. Alle Signaturen, die jemals mit dem kompromittierten privaten Schlüssel erzeugt wurden, sind ungültig (Gesamtprüfergebnis "rot"). Als Kompromittierung

wird der Umstand bezeichnet, dass der Eigentümer des privaten Schlüssels keine alleinige Kontrolle mehr über den privaten Schlüssel besitzt und daher Signaturen auch rückwirkend manipuliert werden können.

Der Sperrstatus "rot" durch Kompromittierung kann durch den erfolgreichen Nachweis der Existenz der Signatur zu einem bestimmten Zeitpunkt durch einen Signaturzeitstempel (Level-T-Signatur, siehe Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**) aufgehoben werden, wenn der Widerruf (Sperrung) nach der Erzeugung des Zeitstempels erfolgte. In diesem Fall kann nämlich nachgewiesen werden, dass die Signaturerstellung vor der Kompromittierung des Schlüssels erfolgt sein muss.

4.3.6 Zeile "Sperrzeitpunkt des geprüften Zertifikats"

Ist das geprüfte Zertifikat gesperrt, wird hinter der Bezeichnung „Sperrzeitpunkt des geprüften Zertifikats“ der Sperrzeitpunkt in der Form `TT.MM.JJJJ hh:mm:ss` angezeigt.

4.3.7 Zeile "Eignung des verwendeten Signaturalgorithmus"

Die Eignung des für die Signatur eines qualifizierten Signaturzertifikats verwendeten Signaturalgorithmus wird auf Basis des verwendeten Algorithmen-katalogs zum Signierzeitpunkt des Zertifikats und zum Zeitpunkt der Durchführung der Prüfung ermittelt. Die Eignung des für die Zertifikatssignatur verwendeten Signaturalgorithmus wird nur bei einem qualifizierten elektronischen Zertifikat überprüft.

Der für die Zertifikatssignatur verwendete Signaturalgorithmus setzt sich aus mehreren Teil-Algorithmen zusammen, die zusammen den verwendeten „Signaturalgorithmus“ bilden. Die einzelnen Teil-Algorithmen werden hinsichtlich ihrer Eignung getrennt bewertet. Für das Ergebnis der Eignung des Signaturalgorithmus gilt: Ist einer der Teil-Algorithmen für die Anbringung oder Prüfung einer qualifizierten elektronischen Signatur als nicht mehr geeignet klassifiziert, wird der gesamte Signaturalgorithmus als nicht mehr geeignet angesehen. Welche Teil-Algorithmen für den Signaturalgorithmus verwendet wurden, wird unter der Zeile „Eignung des verwendeten Signaturalgorithmus" angezeigt.

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 für die Zertifikatssignatur verwendete Signaturalgorithmus war zum Signierzeitpunkt für die Erzeugung einer qualifizierten elektronischen Signatur und zum Zeitpunkt der Durchführung der Prüfung für die Prüfung einer qualifizierten Signatur auf Basis des verwendeten Algorithmenkatalogs geeignet (alle Teil-Algorithmen waren geeignet).

Abbildung 33: Ergebnis der Eignungsprüfung eines Signaturalgorithmus, der zum Signierzeitpunkt und zum Zeitpunkt der Durchführung der Prüfung für eine qualifizierte elektronische Signatur geeignet war

Erläuterungen zu ! Gelber Kasten mit Ausrufungszeichen:

Der für die Zertifikatssignatur verwendete Signaturalgorithmus war zum Zeitpunkt der Durchführung der Prüfung nicht mehr für die Prüfung einer qualifizierten elektronischen Signatur auf Basis des verwendeten Algorithmenkatalogs geeignet (mindestens ein Teil-Algorithmus war nicht (mehr) geeignet). Zum Zeitpunkt der Signaturanbringung (Signierzeitpunkt) war die Eignung jedoch noch gegeben.

Abbildung 34: Ergebnis der Eignungsprüfung eines Signaturalgorithmus, der erst zum Zeitpunkt der Durchführung der Prüfung nicht mehr für die Prüfung einer qualifizierten elektronischen Signatur geeignet war

Bereits erzeugte qualifizierte elektronische Signaturen bleiben auch dann noch qualifiziert, wenn der zugrundeliegende Signaturalgorithmus nach der Erzeugung 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. Es wurde aber ein Algorithmus verwendet, der zum Zeitpunkt der Durchführung der Prüfung nicht mehr für eine qualifizierte elektronische Signatur geeignet war.

Erläuterungen zu X Roter Kasten mit Kreuz:

Abbildung 35: Ergebnis der Eignungsprüfung bei einem Algorithmus, der bereits zum Signierzeitpunkt nicht mehr für die qualifizierte elektronische Signatur geeignet war

Der für die Zertifikatssignatur verwendete Signaturalgorithmus war bereits zum Signierzeitpunkt auf Basis des verwendeten Algorithmenkatalogs für die Signatur eines qualifizierten elektronischen Zertifikats nicht (mehr) geeignet (mindestens ein Teil-Algorithmus war 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. Es wurde ein Algorithmus verwendet, der zum Signierzeitpunkt nicht mehr für eine qualifizierte elektronische Signatur geeignet war.

Erläuterungen zu Grauer Kasten:

Eine Prüfung der Eignung des verwendeten Signaturalgorithmus wurde nicht durchgeführt.

4.3.7.1 Zeile "Angabe des verwendeten Signaturalgorithmus"

Unterhalb der Zeile mit dem angezeigten kumulierten Prüfergebnis wird der Name des verwendeten Signaturalgorithmus angezeigt. Der Signaturalgorithmus setzt sich aus mehreren Teil-Algorithmen zusammen, die zusammen den verwendeten „Signaturalgorithmus“ bilden. Die einzelnen Teil-Algorithmen werden getrennt hinsichtlich ihrer Eignung bewertet. Für das kumulierte Prüfergebnis gilt: Ist einer der unten benannten Teilalgorithmen nicht mehr für die Anbringung oder Prüfung einer qualifizierten elektronischen Signatur als geeignet klassifiziert, wird der gesamte Signaturalgorithmus als nicht mehr geeignet angesehen.

Der zusammengesetzte Name des Signaturalgorithmus beinhaltet folgende Teilalgorithmen (von links nach rechts):

- Hashalgorithmus:
  Der Hashalgorithmus wird verwendet um den TBS-Teil des Zertifikats zu hashen.
- Schlüsselalgorithmus mit Bitlängen von Parametern:
  Der Schlüsselalgorithmus bezeichnet das eigentliche kryptographische Verfahren zum Signieren.
- Paddingalgorithmus:
  Wird nur bei RSA-Signaturen verwendet um den berechneten Hashwert aufzufüllen und wird nur angezeigt, wenn eine RSA-Signatur erzeugt wurde.

Hintergrundinformationen zu diesen Algorithmen befinden sich im Kapitel 4.3.7.1.

4.3.7.2 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) angezeigt. Folgende Status sind möglich:

- **grüner Kasten mit Haken**: Der Signaturalgorithmus war zum Signierzeitpunkt gemäß aktuellem Algorithmenkatalog für die Erzeugung einer qualifizierten elektronischen Signatur geeignet (alle Teil-Algorithmen waren geeignet).
- **roter Kasten mit Kreuz**: Der Signaturalgorithmus war bereits zum Signierzeitpunkt gemäß aktuellem Algorithmenkatalog für die Erzeugung einer qualifizierten elektronischen Signatur nicht (mehr) geeignet (mindestens ein Teil-Algorithmus war nicht (mehr) geeignet).

Abbildung 36: Ergebnis der Eignungsprüfung des verwendeten Signaturalgorithmus zum Signierzeitpunkt

4.3.7.3 Spalte Einzelprüfergebnis „Durchführung der Prüfung“

In der Spalte „Durchführung der Prüfung“ wird unter der Überschrift das Ergebnis der Eignungsprüfung des zur Signatur der Inhaltsdaten verwendeten Signaturalgorithmus zum Zeitpunkt der Durchführung der Signaturprüfung angezeigt. 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 geeignet (alle Teil-Algorithmen waren 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 (mindestens ein Teil-Algorithmus war nicht (mehr) 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 nicht (mehr) geeignet (mindestens ein Teil-Algorithmus war 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.

4.3.7.4 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 der Zertifikatssignatur	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
Rot (nein)	rot (nein)	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 auf Basis des verwendeten Algorithmenkatalogs in Abhängigkeit vom Verwendungszeck (Anbringung einer Inhaltsdatensignatur, Prüfung einer Inhaltsdatensignatur, Anbringung einer Zertifikatssignatur, Prüfung einer Zertifikatssignatur).

Auszug aus dem Algorithmenkatalog SOG-IS plus (Bundesnetzagentur 2017/SOG-IS Agreed Cryptographic Mechanisms V1.1) veröffentlicht von der Governikus KG am 01.06.2018

Algorithmusname	Typ	geeignet für	bis
PKCS#1 v1.5	Paddingalgorithmus	Anbringung von Zertifikatssignaturen	31.12.2018
PKCS#1 v1.5	Paddingalgorithmus	Anbringung von Inhaltsdatensignaturen	31.12.2017
PKCS#1 v1.5	Paddingalgorithmus	Prüfung von Zertifikats- und Inhaltsdatensignaturen	31.12.2022
RSA (n = 2048)	Schlüsselalgorithmus	Anbringung von Zertifikats- und Inhaltsdatensignaturen	31.12.2022
RSA (n = 2048)	Schlüsselalgorithmus	Prüfung von Zertifikats- und Inhaltsdatensignaturen	31.12.2024
SHA256	Hashalgorithmus	Anbringung/Prüfung von Zertifikats- und Inhaltsdatensignaturen	Ohne Ablaufdatum
SHA256withRSA	Signaturalgorithmus	Anbringung von Zertifikats- und Inhaltsdatensignaturen	31.12.2022
SHA256withRSA	Signaturalgorithmus	Prüfung von Zertifikats- und Inhaltsdatensignaturen	31.12.2024

Abbildung 37: Anzeige der verwendeten Algorithmen für eine qualifizierte elektronische Signatur mit Datum des Ablaufs der Eignung in Abhängigkeit vom Verwendungszeck

4.3.8 Zeile "Erläuterungen"

Unter der Zeile „Erläuterungen“ werden die Ursachen angezeigt, die zu einem unbestimmten Status (Gelbprüfung) der Prüfung des Zertifikats oder zu einem Fehlschlagen der Prüfung (Rotprüfung) geführt haben.

Ursachen für einen unbestimmten Status

- Die Vertrauenswürdigkeit des Ausstellers des Zertifikats konnte nicht ermittelt werden.
- Die mathematische Prüfung der Zertifikatssignaturen konnte nicht durchgeführt werden.
- Der Sperrstatus des Zertifikats konnte nicht ermittelt werden.
- Der Sperrstatusdienst für das angefragte Zertifikat wurde durch das Trustcenter eingestellt.
- Es konnte nicht ermittelt werden, ob der Signaturzeitpunkt innerhalb des Gültigkeitsintervalls des Zertifikats liegt.
- Qualifizierte elektronische Signatur. Es wurde aber ein Algorithmus verwendet, der zum Zeitpunkt der Durchführung der Prüfung nicht mehr für eine qualifizierte elektronische Signatur geeignet war (nur bei einer qualifizierten elektronischen Signatur).
- Die Eignung eines Algorithmus konnte nicht ermittelt werden (nur bei einer qualifizierten elektronischen Signatur).

Ursachen für eine fehlgeschlagene Prüfung

- Das Zertifikat war zum Signaturzeitpunkt ungültig.
- Der Aussteller des Zertifikats ist nicht vertrauenswürdig.
- Die mathematische Prüfung der Zertifikatssignaturen ist fehlgeschlagen. Mindestens ein Zertifikat wurde nach der Signatur verändert.
- Der Signaturzeitpunkt liegt außerhalb des Gültigkeitsintervalls des Zertifikats
- Das Zertifikat war zum Signaturzeitpunkt bereits gesperrt.
- Zum Zeitpunkt der Durchführung der Prüfung war das Zertifikat dem Trustcenter unbekannt.

4.3.9 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 (Vertrauensdiensteanbieter) 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 Bereich befindet sich am Ende des Prüfprotokolls. Die technischen Informationen werden im Kapitel 6 ausführlich erläutert.

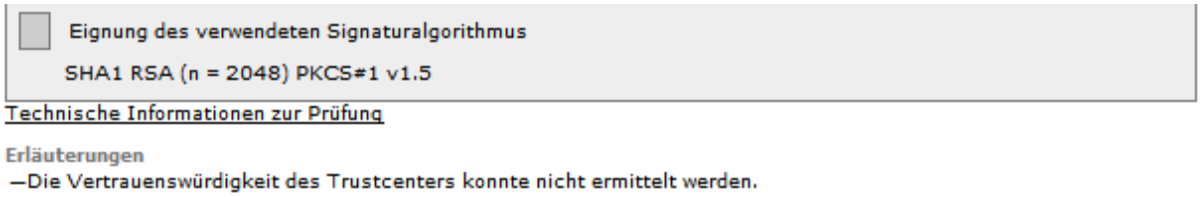


Abbildung 38: Link zu den technischen Informationen zur Prüfung und Erläuterungen

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 elektronischen Signatur beschränkt, erweitert oder präzisiert. Attributzertifikate wurden im SigG-Kontext herausgegeben und sind gemäß CommonPKI-Spezifikation Version 2.0 profiliert. Mit dem Übergang zur eIDAS-Verordnung haben die meisten Vertrauensdiensteanbieter die Ausgabe von Attributzertifikaten aus eIDAS-konformen PKIs eingestellt.

Grundsätzlich wird 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".

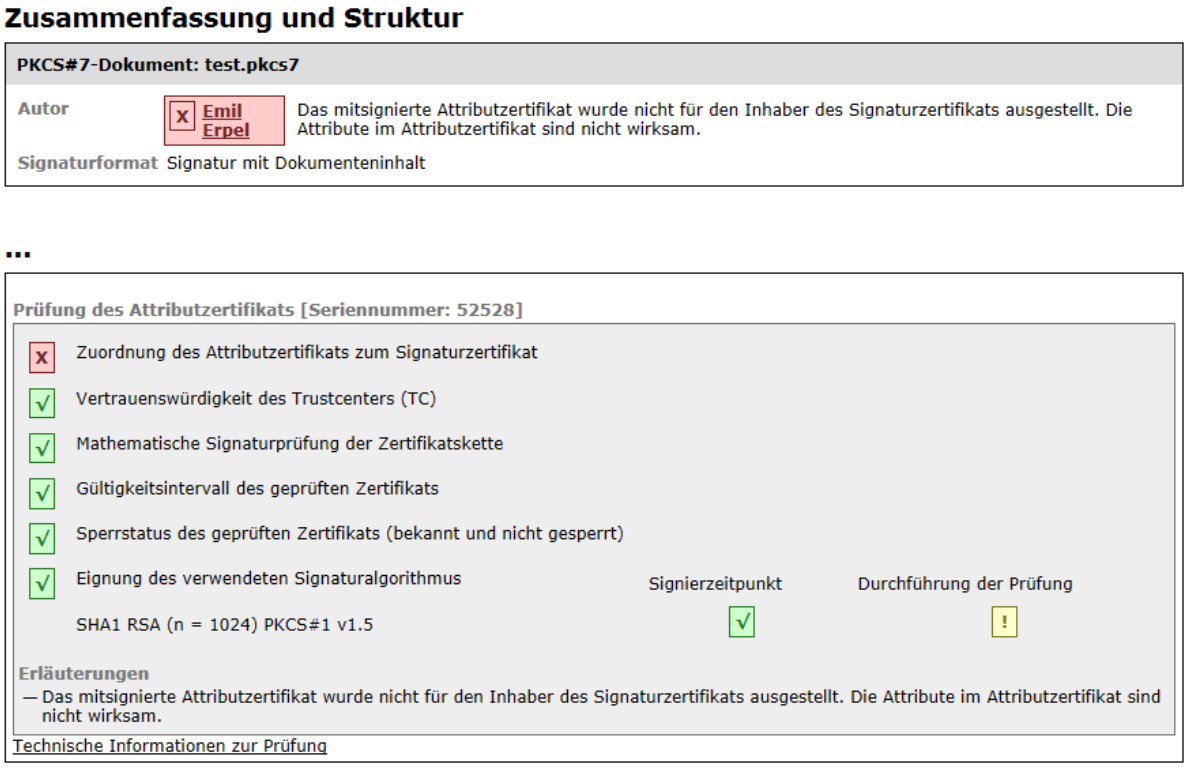


Abbildung 39: Teil 3 "Prüfung eines Attributzertifikats zu einem Signaturzertifikat"

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"

Die Attribute eines Attributzertifikats sind Bestandteil der abgegebenen Willenserklärung und damit auch Bestandteil der Signatur. Es ist daher zu prüfen, ob das qualifizierte Attributzertifikat dem qualifizierten Signaturzertifikat zugeordnet werden kann. In der Zeile "Zuordnung des Attributzertifikats zum Signaturzertifikat" wird das Ergebnis dieser Prüfung 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 fehlgeschlagen. Das Prüfergebnis wirkt sich auf das Ergebnis der Signaturprüfung aus. Es erhält den Status "Signatur ungültig".
  Unter der Überschrift "Erläuterungen" am Ende des Teils "Prüfung des Attributzertifikats" wird der folgende Hinweis angezeigt: "Das mitsignierte Attributzertifikat wurde nicht für den Inhaber des Signaturzertifikats ausgestellt. Die Attribute im Attributzertifikat sind nicht wirksam."
- **Grauer Kasten**: Aus technischen Gründen ist keine Zuordnung möglich.

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

4.4.3 Zeile "Erläuterungen"

Unter der Zeile „Erläuterungen“ werden die Ursachen angezeigt, die zu einem unbestimmten Status (Gelbprüfung) der Prüfung des Attributzertifikats oder zu einem Fehlschlagen der Prüfung (Rotprüfung) geführt haben.

Ursachen für einen unbestimmten Status

- Angezeigt werden alle Meldungen, die bei einer Prüfung des Attributzertifikats zu einem unbestimmten Status führen. Zur Erläuterung siehe Kapitel 4.3.8.

Ursachen für eine fehlgeschlagene Prüfung

- Angezeigt werden alle Meldungen, die bei einer Prüfung des Attributzertifikats zu einem Fehlschlagen der Prüfung führen. Zur Erläuterung siehe Kapitel 4.3.8.
- Das mitsignierte Attributzertifikat wurde nicht für den Inhaber des Signaturzertifikats ausgestellt. Die Attribute im Attributzertifikat sind nicht wirksam. (nur bei einem mitsignierten Attributzertifikat)

4.5 Zusätzliche Prüfungen bei einer *AdES Level-T-Signatur

Bei CAdES-, PAdES- und XAdES-Signaturen kann die Existenz der Signatur zu einem Zeitpunkt durch einen Signaturzeitstempel nachgewiesen werden. Diese sogenannten Level-T-Signaturen wurden in den entsprechenden ETSI-Baseline-Standards definiert.

Im Fall einer Level-T Signatur wird deshalb neben der Signaturprüfung zusätzlich die Signatur des Signaturzeitstempels geprüft und festgestellt, ob sich der Signaturzeitstempel tatsächlich auf die vorliegende (und geprüfte) Inhaltsdatensignatur bezieht. Durch diese zusätzlichen Prüfungen ergibt sich ein erweitertes Prüfprotokoll, das im Bereich 2 "Signaturprüfungen" einen zusätzlichen Teil 4 "Prüfung des Signaturzeitstempels" enthält.

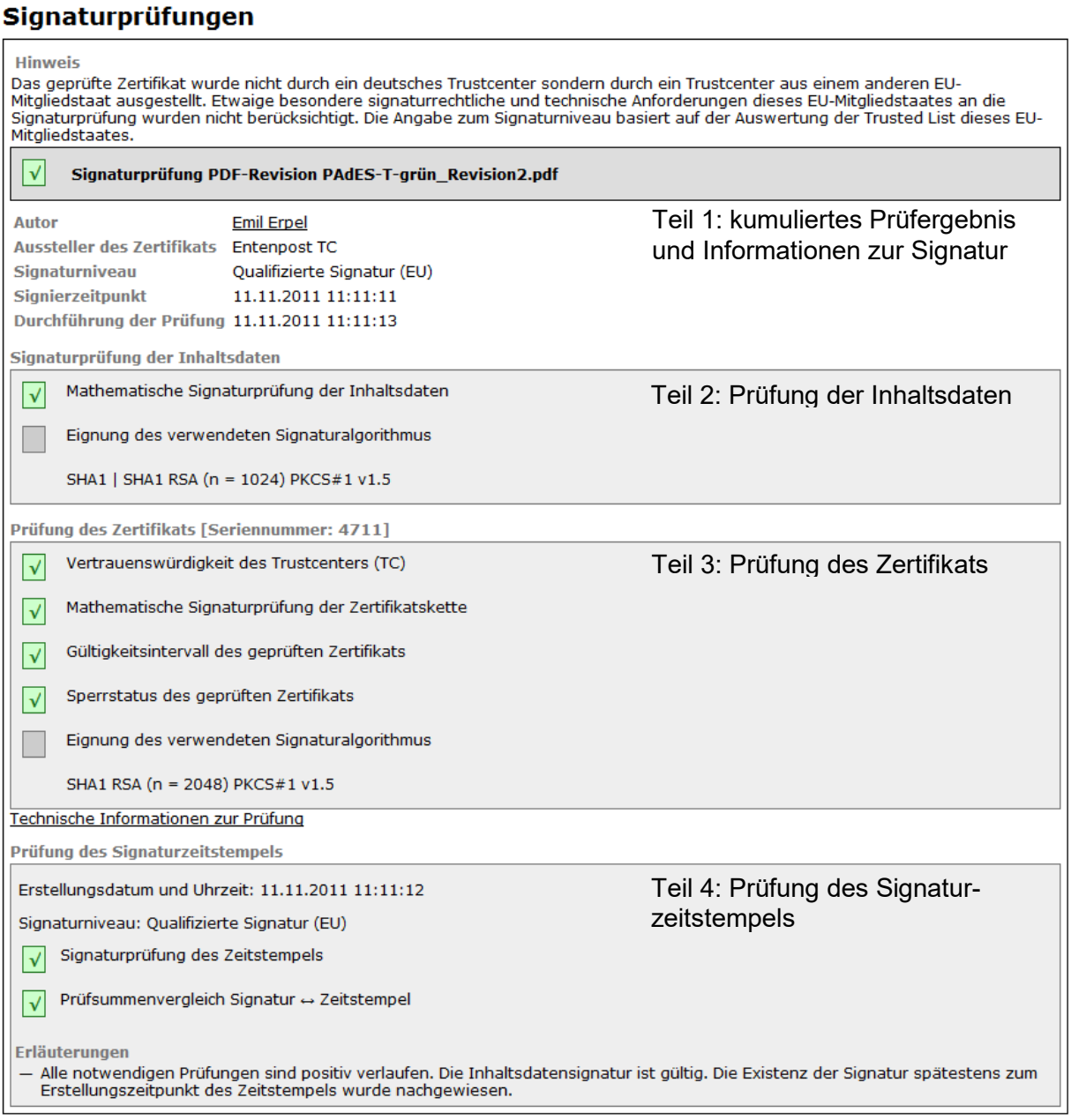


Abbildung 40: Prüfung eines Signaturzeitstempels bei einer *AdES-T-Signatur

4.5.1 Erfolgreicher Nachweis der Existenz einer Signatur zu einem Zeitpunkt

Bei einer CAdES-, PAdES- und XAdES-Level-T-Signatur ist intendiert, dass die Existenz der Inhaltsdatensignatur zu einem Zeitpunkt durch einen Signaturzeitstempel nachgewiesen werden soll. Dafür müssen folgende drei Voraussetzungen gegeben sein:

a) Der Signaturzeitstempel weist das gleiche Signaturniveau wie die Inhaltsdatensignatur auf.

b) Die Prüfung der Signatur des Zeitstempels verläuft erfolgreich.

c) Der Prüfsummenvergleich Signatur – Zeitstempel verläuft erfolgreich (Der neu berechnete Hashwert über die Inhaltsdatensignatur und der zeitgestempelte Hashwert stimmen überein).

Die Prüfschritte a) bis c) und deren mögliche Status werden in den Kapiteln 4.5.3 bis 4.5.5 erläutert. Verlaufen diese Prüfungen erfolgreich, hat die Signatur spätestens zum Erstellungszeitraum des Signaturzeitstempels mit dem angegebenen Prüfergebnis existiert. Bei einer gültigen Inhaltsdatensignatur wird in diesem Fall unter der Überschrift "Erläuterungen" des Teils 4 "Prüfung des Signaturzeitstempels" die folgende Meldung angezeigt:

- Alle notwendigen Prüfungen sind positiv verlaufen. Die Inhaltsdatensignatur ist gültig. Die Existenz der Signatur spätestens zum Erstellungszeitpunkt des Zeitstempels wurde nachgewiesen.

Der erfolgreiche Nachweis der Existenz der Signatur zu einem bestimmten Zeitpunkt kann in einem besonderen Fall das negative Einzelprüfergebnis "Sperrstatus des Zertifikats" aufheben: Wurde das Signaturzertifikat mit dem Sperrgrund "kompromittiert" gesperrt und erfolgte der Widerruf (Sperrung) nach der Erzeugung des Zeitstempels, kann nämlich nachgewiesen werden, dass die Signaturerstellung vor der Kompromittierung des Schlüssels erfolgt sein muss. Ohne den Nachweis der Existenz der Signatur zu einem Zeitpunkt, müssten bei einer Kompromittierung des privaten Schlüssels nämlich alle jemals mit diesem Schlüssel erzeugten Signaturen (unabhängig vom Signierzeitpunkt) als ungültig betrachtet werden.

Als Kompromittierung wird der Umstand bezeichnet, dass der Eigentümer des privaten Schlüssels keine alleinige Kontrolle mehr über den privaten Schlüssel besitzt und daher Signaturen auch rückwirkend manipuliert werden können.

In diesem Fall wird zusätzlich unter der Überschrift "Erläuterungen" des Teils 4 "Prüfung des Signaturzeitstempels" die folgende Meldung angezeigt:

- Das Ergebnis der Sperrstatusprüfung des Zertifikats mit dem Sperrgrund "kompromittiert" wird ignoriert, da der gültige Zeitstempel nachweist, dass die Signatur vor dem Sperrzeitpunkt erfolgte.

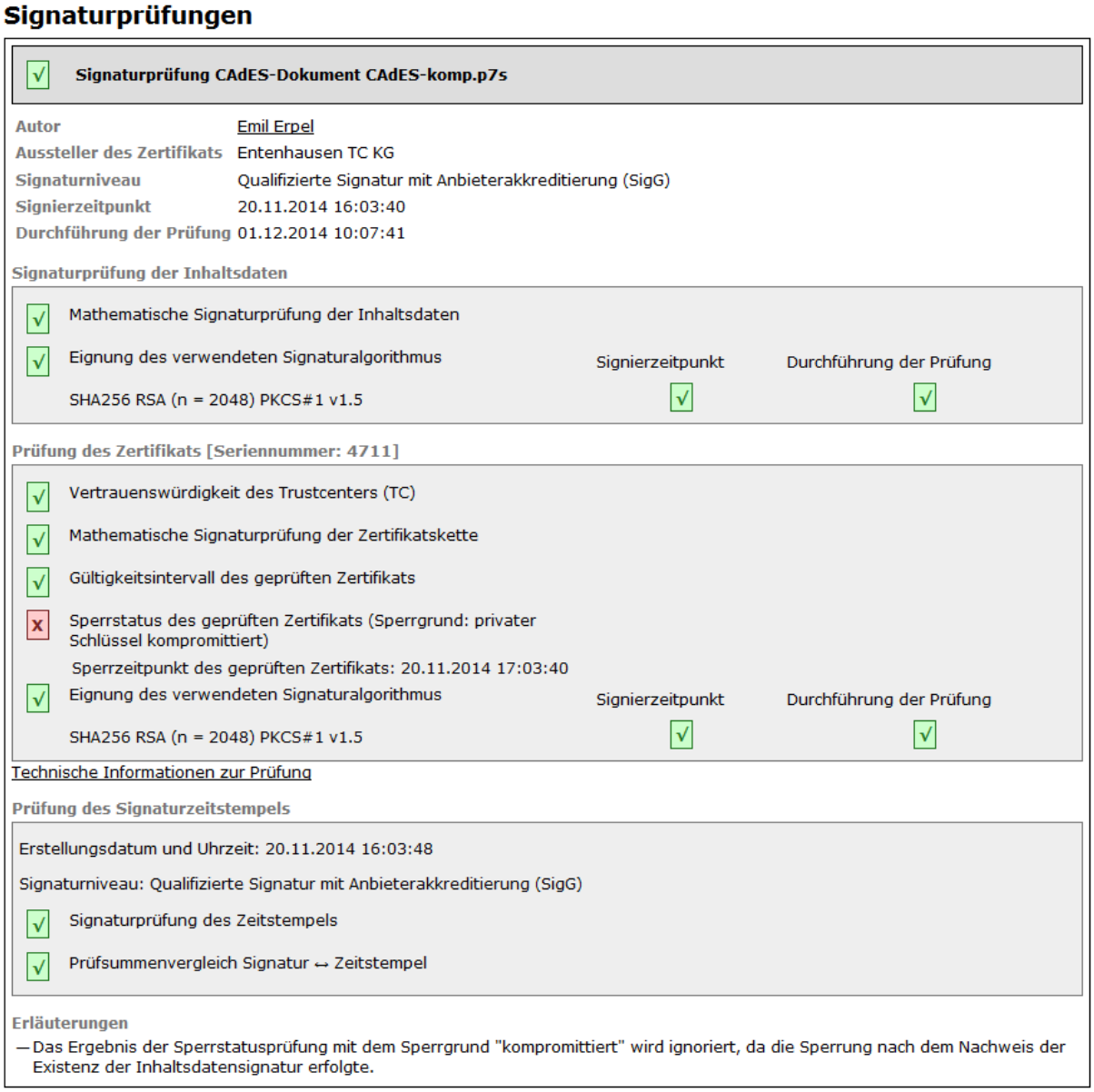


Abbildung 41: Wechsel des Gesamtstatus der Signaturprüfung auf gültig trotz kompromittierendem Sperrgrund bei einer Level-T-Signatur

4.5.2 Zeile "Erstellungsdatum und Uhrzeit"

Angezeigt wird hinter dem Betreff "Erstellungsdatum und Uhrzeit" der Erstellungszeitpunkt (Generation Time) des Zeitstempels in der Form `TT.MM.JJJJ hh:mm:ss`. Der Erstellungszeitpunkt des Zeitstempels wird auch als Zeitpunkt der Signatur des Zeitstempels verwendet.

Sollte der angegebene Signierzeitpunkt der Inhaltsdaten nach dem Zeitpunkt der Erzeugung des Zeitstempels liegen (weil lokale Clientzeit nicht korrekt zeitsynchronisiert war), führt dieses bei einer erfolgreichen Prüfung des Signaturzeitstempels (Prüfungen a bis c erfolgreich) immer zu einem unbestimmten Status der Signaturprüfung. D.h., auch bei einer gültigen Signatur (alle Einzelprüfungen der Inhaltsdatensignatur waren erfolgreich) wechselt der Gesamtstatus der Signaturprüfung auf "unbestimmt". In diesem Fall wird unter der Überschrift "Erläuterungen" des Teils 4 "Prüfung des Signaturzeitstempels" die folgende Meldung angezeigt:

- Der angegebene Signaturzeitpunkt der Inhaltsdatensignatur liegt nach dem Erstellungszeitpunkt des gültigen Signaturzeitstempels.

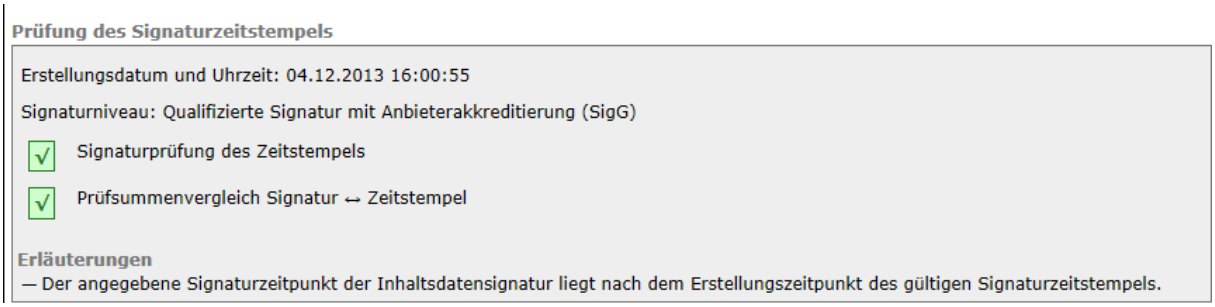


Abbildung 42: Erläuterung bei einem Signaturzeitpunkt nach dem Erstellungszeitpunkt des gültigen Signaturzeitstempels

4.5.3 Zeile "Signaturniveau"

Angezeigt wird das intendierte Niveau der elektronischen Signatur. Dieses ist das Niveau, das erreicht wird, wenn die Signatur des Zeitstempels als "gültig" geprüft wurde. Die Signaturniveaus sind im Kapitel 4.1.4 erläutert. Das gleichwertige Signaturniveau ist eine notwendige Bedingung für den Nachweis der Existenz der Inhaltsdatensignatur zum Erstellungszeitpunkt des Signaturzeitstempels (Prüfung a). Als gleichwertig werden in diesem Zusammenhang alle qualifizierten Signaturen betrachtet, die konform zur EU-Signaturrichtlinie erstellt wurden. Entspricht das Signaturniveau des Zeitstempels nicht dem Signaturniveau der Inhaltsdatensignatur, wird unter der Überschrift "Erläuterungen" des Teils 4 "Prüfung des Signaturzeitstempels" die folgende Meldung angezeigt:

- Der Nachweis, dass die Signatur zum Erstellungszeitpunkt des Zeitstempels existierte, konnte nicht erbracht werden, da das Signaturniveau des Zeitstempels nicht dem Signaturniveau der Inhaltsdatensignatur entspricht.

4.5.4 Zeile "Signaturprüfung"

In der Zeile "Signaturprüfung" wird das Ergebnis der Signaturprüfung des Zeitstempels angezeigt. Das Prüfergebnis umfasst die mathematische Signaturprüfung und die Prüfung des Zeitstempelzertifikats. Bei einem qualifizierten Zeitstempel wird auch die Eignung der verwendeten Signaturalgorithmen/Hashalgorithmen der Zeitstempelsignatur, der Signatur des Zeitstempelzertifikats sowie die Eignung des Hashalgorithmus über die Inhaltsdatensignatur geprüft. Das Prüfergebnis umfasst alle Einzelprüfungen und entspricht vollständig dem kumulierten Ergebnis der Prüfung einer Inhaltsdatensignatur (Gesamtprüfergebnis), wie sie in den Kapiteln 4.1 bis 4.3 beschrieben wird.

Die erfolgreiche Prüfung der Signatur des Zeitstempels ist eine notwendige Bedingung für den Nachweis der Existenz der Inhaltsdatensignatur zum Erstellungszeitpunkt des Signaturzeitstempels (Prüfung b). Folgende Prüfstatus sind möglich:

- Grüner Kasten mit Haken: Die Signatur des Zeitstempels ist gültig.
- Gelber Kasten mit Ausrufungszeichen: Das Prüfergebnis ist unbestimmt.
- Roter Kasten mit Kreuz: Die Signatur des Zeitstempels ist ungültig.

Eine detaillierte Beschreibung des Prüfergebnisses befindet sich im Kapitel 3.1.1. Verläuft die Prüfung nicht erfolgreich werden unter der Überschrift "Erläuterungen" des Teils 4 "Prüfung des Signaturzeitstempels" entsprechende Erläuterungen für den Prüfstatus angezeigt.

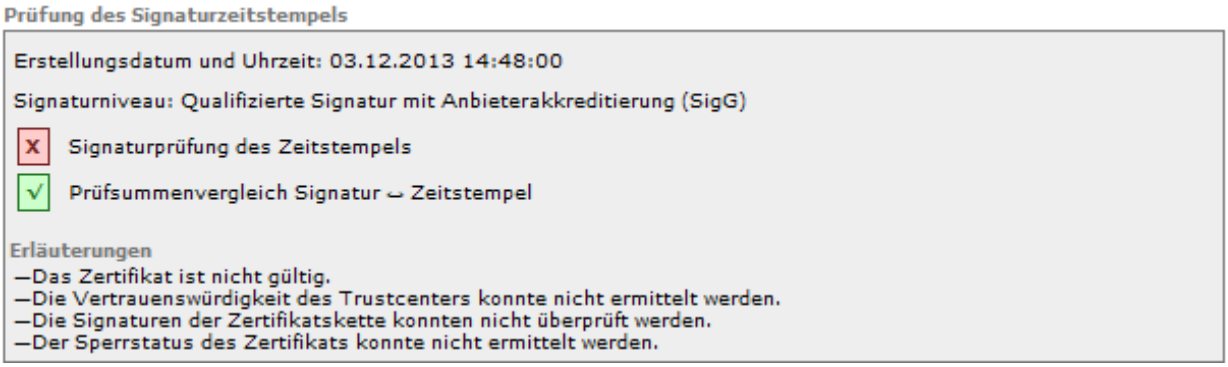


Abbildung 43: Gesamtstatus der Signaturprüfung des Zeitstempels bei einer fehlgeschlagenen Zertifikatsprüfung

4.5.5 Zeile "Prüfsummenvergleich Signatur - Zeitstempel"

Der Prüfsummenvergleich beinhaltet die folgende Prüfung: Der Hashwert über die Inhaltsdatensignatur (genauer SignerInfo) wird mit dem zeitgestempelten Hashwert verglichen. Stimmen beide Hashwerte überein, wird nachgewiesen, dass die vorliegende Inhaltsdatensignatur zeitgestempelt wurde. Der erfolgreiche Prüfsummenvergleich ist eine notwendige Bedingung für den Nachweis der Existenz der Inhaltsdatensignatur zum Erstellungszeitpunkt des Signaturzeitstempels (Prüfung c).

In der Zeile "Prüfsummenvergleich Signatur - Zeitstempel" wird das Ergebnis dieser Prüfung angezeigt. Die folgenden Status sind möglich:

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

Erläuterungen zu Grüner Kasten mit Haken:

Bei einem Grünen Kasten mit Haken war der Prüfsummenvergleich erfolgreich. Der Hashwert über die Signatur (signedInfo) und der zeitgestempelte Hashwert stimmt überein. Die vorliegende Signatur wurde zeitgestempelt.

Erläuterungen zu Gelber Kasten mit Ausrufungszeichen:

Bei einem gelben Kasten mit Ausrufezeichen konnte der Prüfsummenvergleich nicht durchgeführt werden, weil z.B. der verwendete Hashalgorithmus unbekannt ist. In diesem Fall wird unter der Überschrift "Erläuterungen" des Teils 4 "Prüfung des Signaturzeitstempels" der folgende Hinweis angezeigt.

- Der Nachweis, dass die Signatur zum Erstellungszeitpunkt des Zeitstempels existierte, konnte nicht erbracht werden, da der Hashwertvergleich (Hashwert der Signatur und zeitgestempelter Hashwert) nicht durchgeführt werden konnte.

Erläuterungen zu Roter Kasten mit Kreuz:

Bei einem roten Kasten mit Kreuz war der Prüfsummenvergleich nicht erfolgreich. In diesem Fall wird unter der Überschrift "Erläuterungen" des Teils 4 "Prüfung des Signaturzeitstempels" der folgende Hinweis angezeigt.

- Der Nachweis, dass die Signatur zum Erstellungszeitpunkt des Zeitstempels existierte, konnte nicht erbracht werden, da der Hashwertvergleich (Hashwert der Signatur und zeitgestempelter Hashwert) fehlgeschlagen ist.

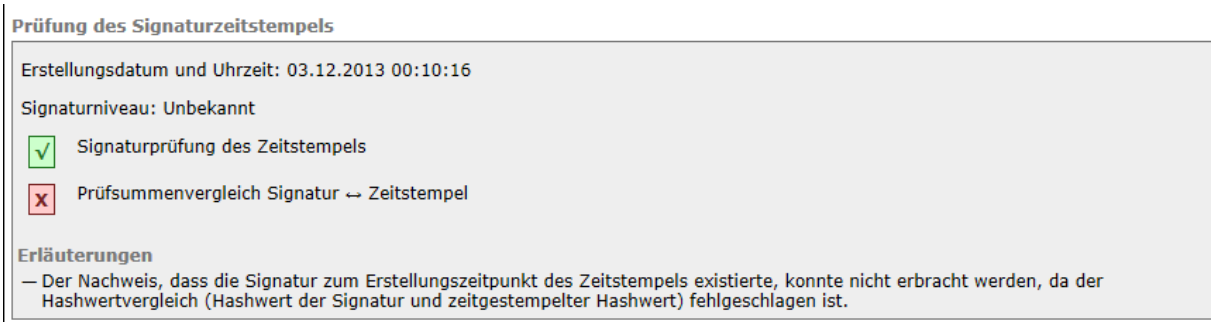


Abbildung 44: Erläuterung bei fehlgeschlagenem Prüfsummenvergleich

4.5.6 Zeile "Erläuterungen"

Unter der Überschrift "Erläuterungen" des Teils 4 "Prüfung des Signaturzeitstempels" werden alle Erläuterungen zum Prüfstatus des Signaturzeitstempels angezeigt.

Erläuterungen bei erfolgreicher Prüfung des Signaturzeitstempels (Prüfungen a bis c erfolgreich)

- Die Signaturprüfung, Zeitstempelprüfung und Prüfsummenvergleich waren erfolgreich. Die Existenz der Inhaltsdatensignatur zum Erstellungszeitpunkt des Zeitstempels wurde nachgewiesen.
- Der angegebene Signaturzeitpunkt der Inhaltsdatensignatur liegt nach dem Erstellungszeitpunkt des gültigen Signaturzeitstempels.
  Hinweis: Zur Erläuterung siehe Kapitel 4.5.2).
- Das Ergebnis der Sperrstatusprüfung des Zertifikats mit dem Sperrgrund "kompromittiert" wird ignoriert, da der gültige Zeitstempel nachweist, dass die Signatur vor dem Sperrzeitpunkt erfolgte.
  Hinweis: Zur Erläuterung siehe Kapitel)

Erläuterungen bei nicht erfolgreicher Prüfung des Signaturzeitstempels

Die Existenz der Inhaltsdatensignatur zum Erstellungszeitpunkt des Zeitstempels kann in diesem Fall nicht nachgewiesen werden.

- Alle Meldungen zur mathematischen Signaturprüfung und Zertifikatsprüfung, die zu einem unbestimmten Status oder zu einem Fehlschlagen der Prüfung führen. Zur Erläuterung siehe Kapitel 4.2.2.5 (Abschnitt a) und 4.3.8.
- Der Nachweis, dass die Signatur zum Erstellungszeitpunkt des Zeitstempels existierte, konnte nicht erbracht werden, da der Hashwertvergleich (Hashwert der Signatur und zeitgestempelter Hashwert) nicht durchgeführt werden konnte.
- Der Nachweis, dass die Signatur zum Erstellungszeitpunkt des Zeitstempels existierte, konnte nicht erbracht werden, da der Hashwertvergleich (Hashwert der Signatur und zeitgestempelter Hashwert) fehlgeschlagen ist.
- Der Nachweis, dass die Signatur zum Erstellungszeitpunkt des Zeitstempels existierte, konnte nicht erbracht werden, da das Signaturniveau des Zeitstempels nicht dem Signaturniveau der Inhaltsdatensignatur entspricht.

4.6 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 enthalten. Im Laufzettel ist nämlich nur das Signaturzertifikat und die Prüfergebnisse enthalten, nicht aber das CA-Zertifikat. Dieses wird aber benötigt, um die Eignung des zur Zertifikatssignatur verwendeten Algorithmus überprüfen zu können.

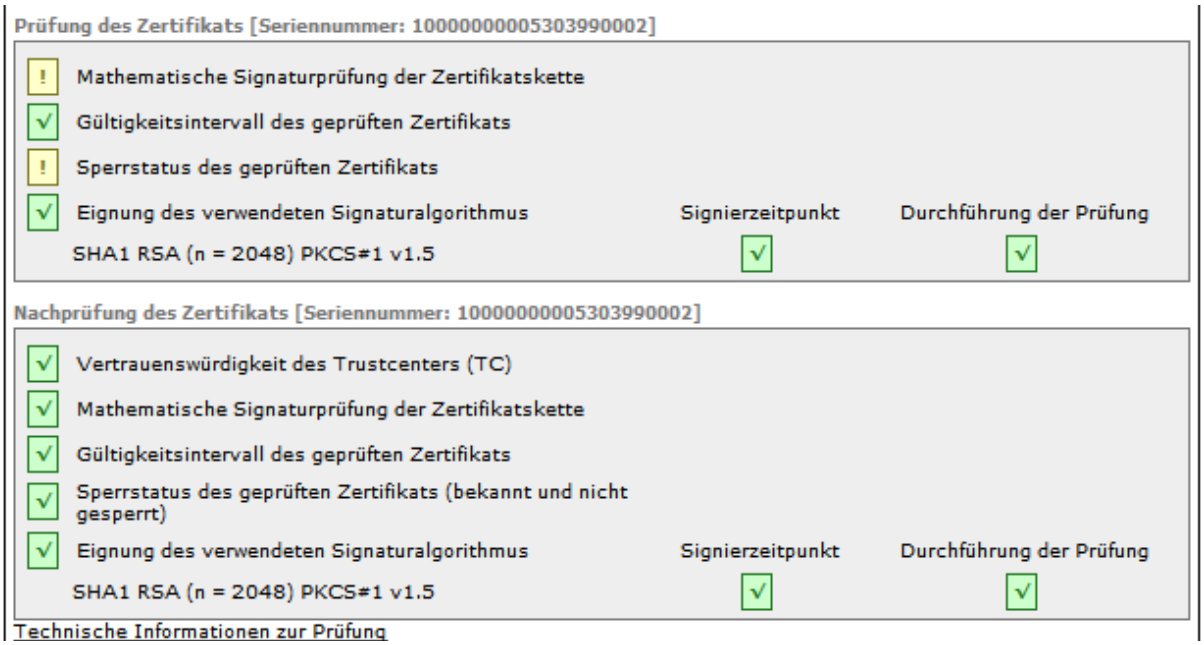


Abbildung 45: Teil 3 "Nachprüfung eines Zertifikats bei OCSI-Nachrichten"

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.

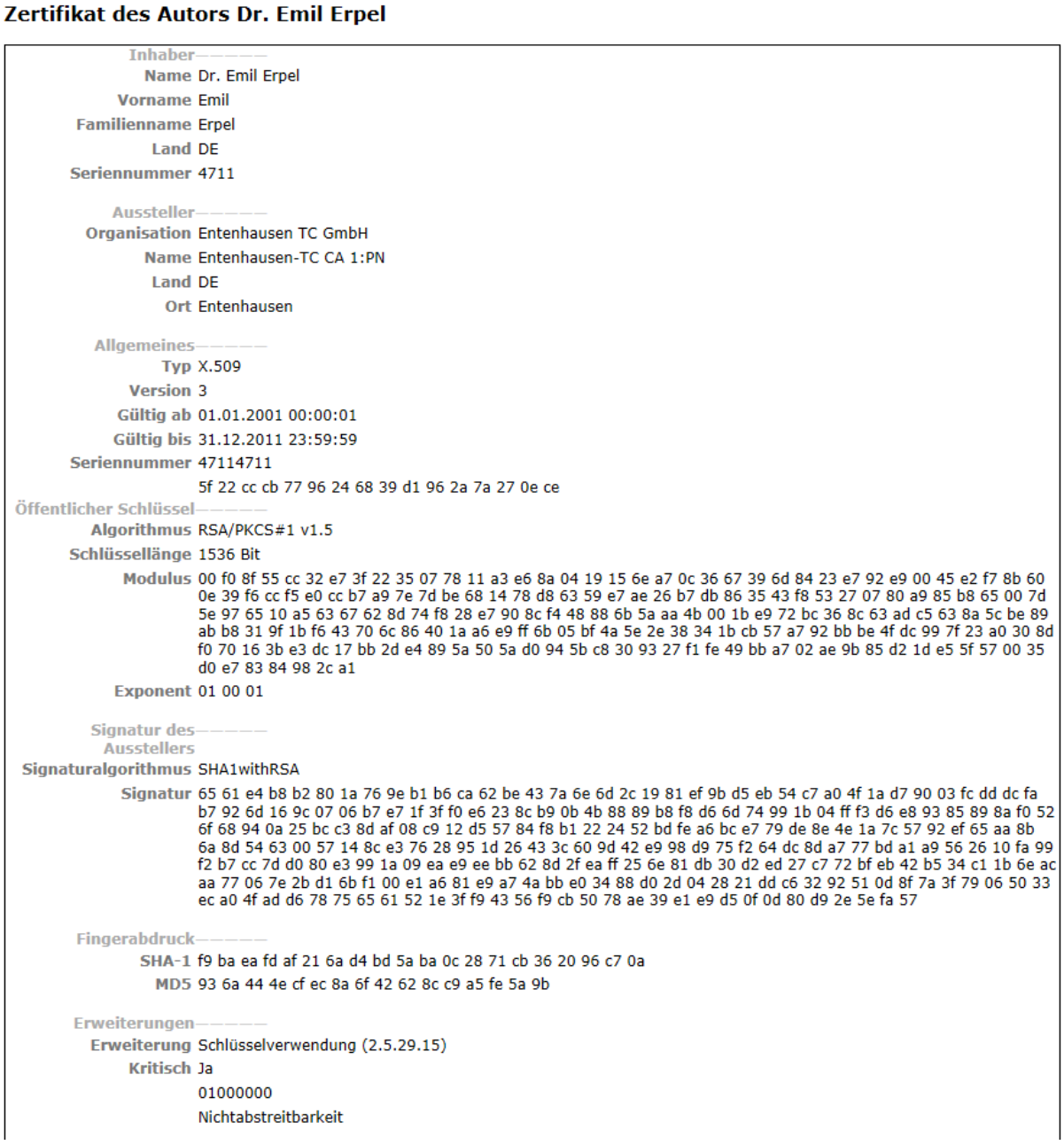


Abbildung 46: Bereich 3 "Zertifikate“ des Prüfprotokolls"

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
- In den ETSI EN 319 412-1 bis 5
- und in der CommonPKI-Spezifikation Version 2.0 (Legacy-Signaturzertifikate nach deutschem Signaturgesetz)

profilierten Zertifikatsfelder und Erweiterungen menschenlesbar übersetzt werden.

Alle in den ETSI EN 319 412 angegebenen Zertifikatsprofile basieren auf dem RFC 5280. Die Inhalte eines Zertifikats werden daher in der Reihenfolge des RFC beschrieben. Dazu gehören auch die optionalen Attribute in qualifizierten Signaturzertifikaten und/oder in qualifizierten Attributzertifikaten (qualifizierte Legacy-Zertifikate gemäß CommonPKI SigG-Profil ausgestellt von deutschen qualifizierten Vertrauensdiensteanbietern), 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 einfach verständliche Anzeige der Zertifikatsinhalte kann zudem 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.

5.2 Inhaber eines Zertifikats

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

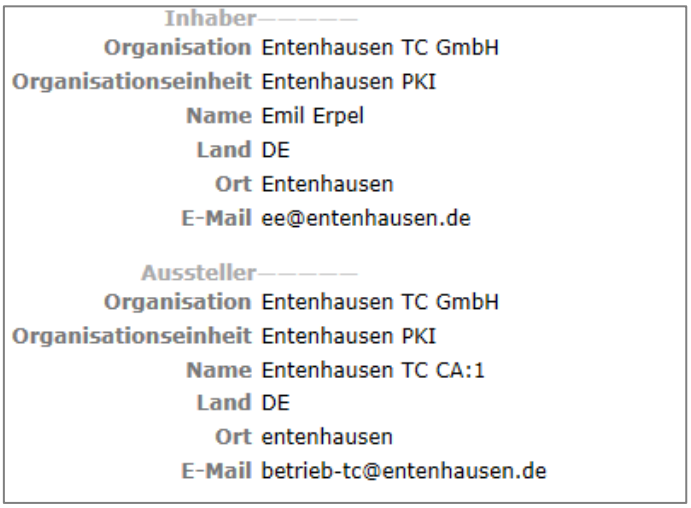


Abbildung 47: Bereich "Inhaber und Aussteller eines Zertifikats"

Folgende Attribute können 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 Qualifizierte Legacy-Zertifikate 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. Im CommonPKI SigG-Profil wird bei einem Pseudonym daher der Suffix ":PN" vorgeschrieben.

Eine vergleichbare Regelung findet sich in den ETSI-EN zu Zertifikatsprofilen nicht.

5.2.2 Qualifiziertes Legacy-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 durften gemäß CommonPKI SigG-Profil nur ausgestellt werden, wenn dazu ein qualifiziertes Basiszertifikat (Signaturzertifikat) existiert. In diesem Fall musste die baseCertificateID-Option verwendet werden.

Abbildung 48: Bereich "Inhaber und Austeller eines Attributzertifikats"

5.3 Aussteller eines Zertifikats

Angezeigt werden alle im Zertifikat vorhandenen Informationen zum Aussteller [Feld `issuer`]. Die folgenden Attribute können 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.

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`].

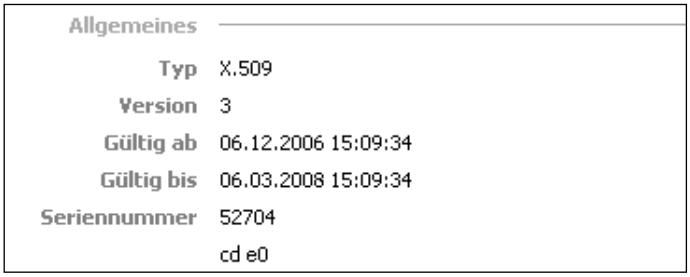


Abbildung 49: Allgemeine Informationen zum Zertifikat

5.4.2 Zeile "Algorithmus"

Angezeigt wird der vom Aussteller (Vertrauensdiensteanbieter, 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.

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 gemäß RFC 5280 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 Signaturprüfschlüssel, 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.

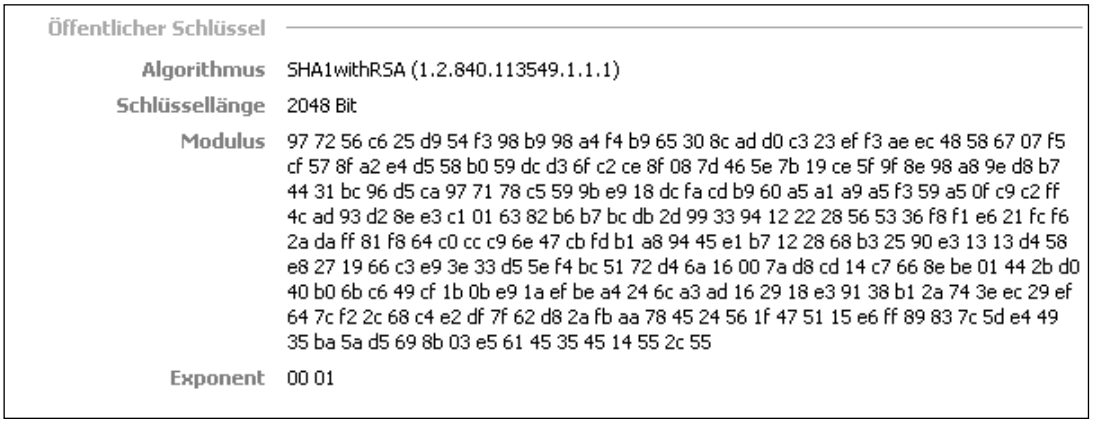


Abbildung 50: Bereich "öffentlicher Schlüssel" (RSA-Schlüssel)

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.

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 51: Bereich "öffentlicher Schlüssel" (ECDSA-Schlüssel)

5.6 Signatur des Ausstellers im Zertifikat

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

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 52: Anzeige "Signatur des Ausstellers"

5.6.1 Zeile "Signaturalgorithmus"

Angezeigt wird der vom Aussteller (Aussteller (Vertrauensdiensteanbieter, 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, Aussteller (Vertrauensdiensteanbieter) [`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`].

5.8 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), ETSI EN 319 412-1 bis 5 und jeweils eine Erweiterung aus dem RFC 2560 und der CommonPKI-Spezifikation beschrieben:

- 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
- Authority Information Access
- Subject Information Access
- Angaben zum qualifizierten Zertifikat
- keine OCSP-Prüfung
- 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 Prüfkomponente in der Regel generisch ist und in der Regel nicht in einen fachlichen Workflow eingebunden ist, wird die Erweiterung nur 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 Aussteller-zertifikats	

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 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)

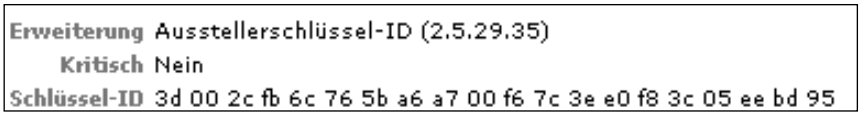


Abbildung 53: Anzeige Erweiterung "Ausstellerschlüssel-ID"

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 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 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).

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 entfaltet diese Signatur eine Rechtswirkung wie eine eigenhändige Unterschrift.

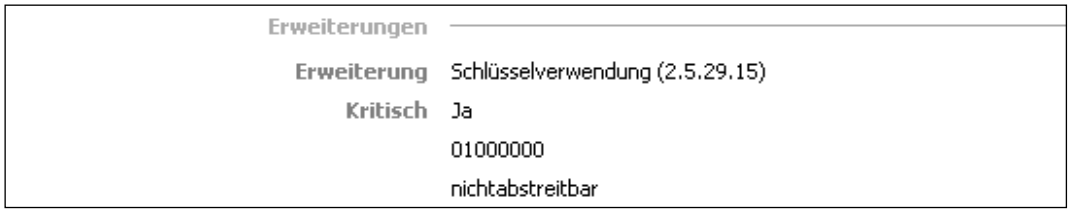


Abbildung 54: Anzeige Erweiterung "Schlüsselverwendung"

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.

5.8.3 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.

5.8.4 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).

5.8.6 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.

5.8.7 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"

5.8.8 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.

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

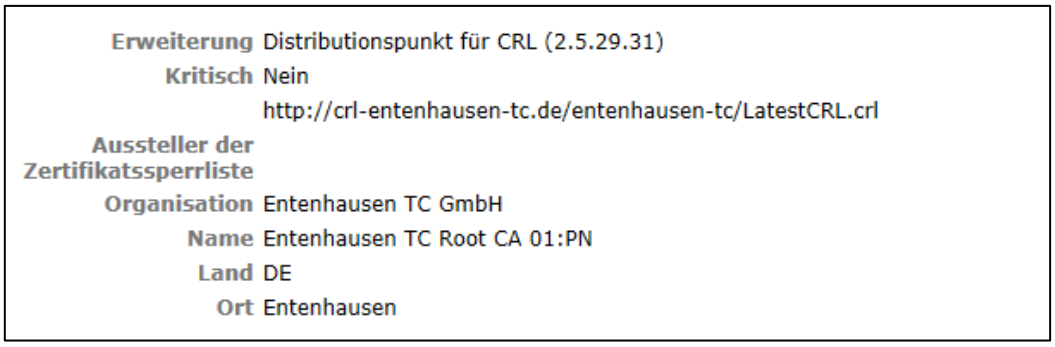


Abbildung 55: Anzeige Erweiterung "Distributionspunkt für CRL"

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`]

5.8.13 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"

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

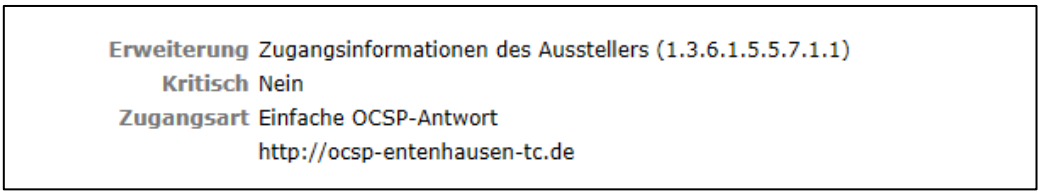


Abbildung 56: Anzeige Erweiterung "Zugangsinformationen des Ausstellers"

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"

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.

5.8.17 Erweiterung "BiometricData" (Legacy-Zertifikate gemäß CommonPKI SigG-Profil)

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"

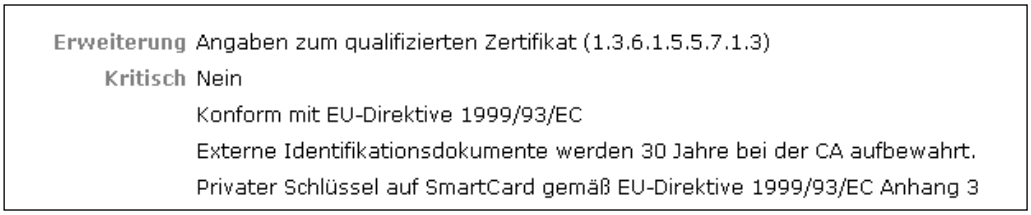


Abbildung 57: Anzeige Erweiterung "Angaben zum qualifizierten Zertifikat"

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" (Legacy-Zertifikate gemäß CommonPKI SigG-Profil)

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.

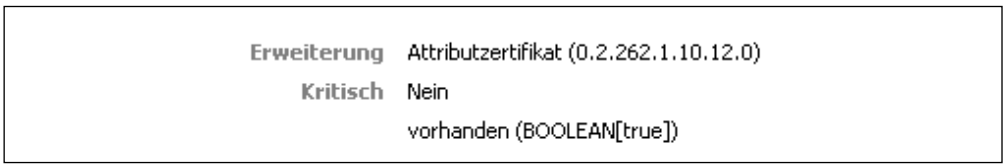


Abbildung 58: Anzeige Erweiterung "Attributzertifikat" vorhanden

Der Wert "nicht vorhanden" oder die nicht vorhandene Erweiterung "Attributzertifikat" darf nicht zu der Annahme verleiten, es würde kein Attributzertifikat existieren. Einige Aussteller (Vertrauensdiensteanbieter haben Attributzertifikate auch nachträglich ausgestellt, sodass diese Information dann im Signaturzertifikat nicht vorhanden sein konnte.

5.8.21 Erweiterung "Datum Zertifikatserzeugung"

Die Erweiterung "Datum Zertifikatserzeugung" [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" (Legacy-Zertifikate gemäß CommonPKI SigG-Profil)

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

5.9 Inhaberattribute (in Legacy-Zertifikaten gemäß CommonPKI 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 wurden u.a. die speziellen Anforderungen umgesetzt, die sich aus dem deutschen Signaturgesetz für qualifizierte Zertifikate ergaben. Diese Attribute können sich in einem qualifizierten Signaturzertifikat (technisch dann als Extension [Erweiterung]) oder in einem separaten qualifizierten Attributzertifikat (technisch dann als Attribut) befinden.

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 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-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]`

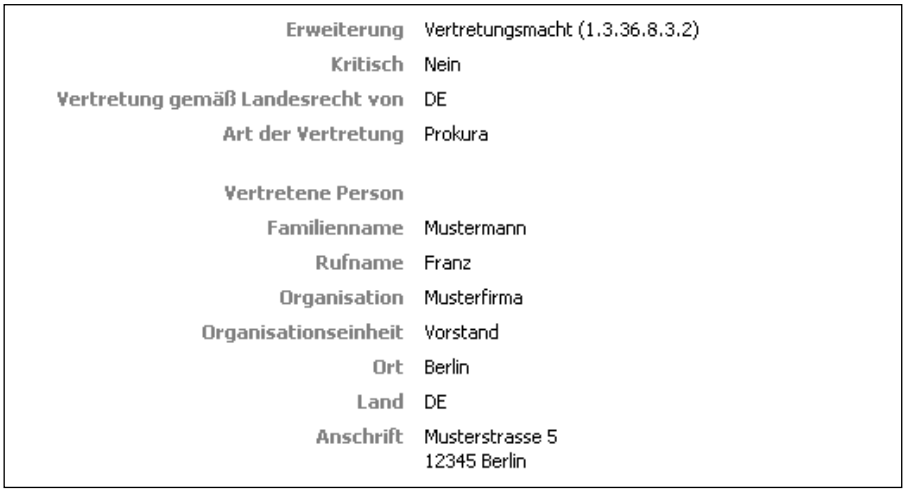


Abbildung 59: Attribut "Vertretungsmacht gemäß CommonPKI SigG-Profil"

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. 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.

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.

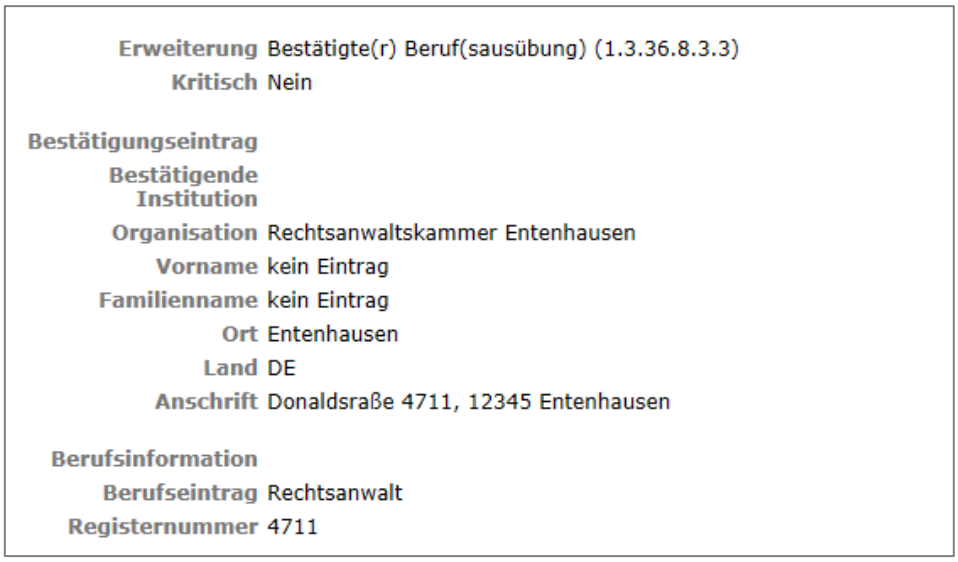


Abbildung 60: Erweiterung bestätigter Beruf (einer namingAuthority) gemäß CommonPKI SigG-Profil

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) [`notYoungerThan`]) 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.

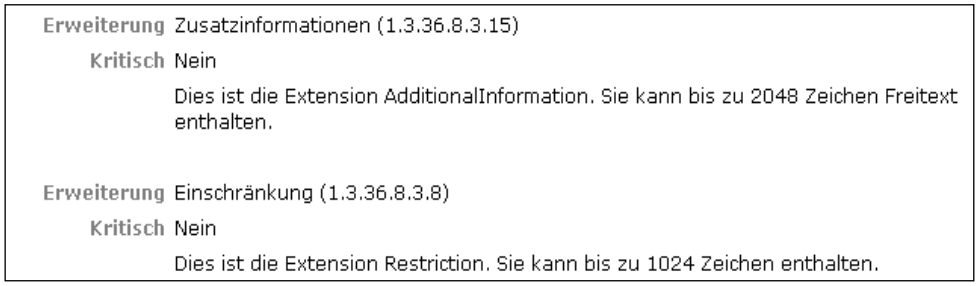


Abbildung 61: Attribute "Einschränkung" und "Zusatzinformationen" gemäß CommonPKI SigG-Profil

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 der Vertrauensdiensteanbieter 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 Emil Erpel zum Zeitpunkt 29.08.2011 10:35:31	
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.entenhausen.de
Konfiguration der Prüfinstanz	individual configuration
Policy der Prüfinstanz	Policy Version 2.0
Vertrauenswürdige Liste der ZDA	DE_10
Status XKMS-Verarbeitung	Erfolgreich beendet

Abbildung 62: 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 Vertrauensdiensteanbieter ansässig ist"

Angezeigt wird in der Zeile das Land aus der europäischen Union, in dem das Trustcenter bzw. der Aussteller (Vertrauensdiensteanbieter), 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 jeden Aussteller (Vertrauensdiensteanbieter oder CA) hinterlegt, in welchem Staat es ansässig ist.

6.1.3 Zeile "Art der Überwachung" des Trustcenters

Angezeigt wird in dieser Zeile die Art der Überwachung des Trustcenters/Vertrauensdiensteanbieters. 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 Vertrauensdiensteanbieter 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 Vertrauensdiensteanbieter wird dabei in Übereinstimmung mit einem entsprechenden Standard zertifiziert.
b) Überwachungsarten für qualifizierte Vertrauensdiensteanbieter, 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 Vertrauensdiensteanbieter 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 Vertrauensdiensteanbieter ist zusätzlich durch eine öffentliche, nationale oder internationale Stelle/ Behörde akkreditiert und wird auf Einhaltung des geltenden Rechts überwacht.

Tabelle 15: Art der Überwachung

6.1.4 Zeile "Zertifikatsniveau gemäß Zertifizierungsrichtlinie des TC"

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

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 Vertrauensdiensteanbieter 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 Vertrauensdiensteanbieter 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/EC zu erfüllen und ohne die Verwendung einer sicheren Signaturerstellungseinheit (SSCD/QSCD, Smartcard die den Anforderungen der EU-Direktive 1999/93/EC oder Verordnung (EU) Nr. 910/2014) für den privaten Schlüssel vorzuschreiben.
Fortgeschrittenes Zertifikat gemäß einer normalisierten Zertifizierungsrichtlinie mit privatem Schlüssel auf Smartcard	Das Zertifikat wurde von einem Vertrauensdiensteanbieter erstellt, dessen Zertifizierungsrichtlinie dem ETSI TS 102 042-Standard für normalisierte Zertifizierungsrichtlinien oder einem vergleichbaren Standard genügt, wobei die Verwendung einer sicheren Signaturerstellungseinheit (SSCD/QSCD) 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 ohne die rechtlichen Anforderungen gemäß EU-Direktive 1999/93/EC oder Verordnung (EU) Nr. 910/2014 zu erfüllen.

Tabelle 16: Zertifikatsniveau gemäß Zertifizierungsrichtlinie des Vertrauensdiensteanbieters (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 Vertrauensdiensteanbieter/jede CA diese Information hinterlegt. Der Eintrag in der Standardkonfiguration wird bei qualifizierten Vertrauensdiensteanbietern der hoheitlichen Trusted List 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 Zertifikatsgenerierungsdienste (Vertrauensdiensteanbieter) Zertifikate ausstellen.

b) Zertifikatsniveau für qualifizierte Vertrauensdiensteanbieter	
Qualifiziertes Zertifikat gemäß Signaturrichtlinie oder eIDAS-Verordnung für eine fortgeschrittene Signatur	Das Zertifikat wurde von einem qualifizierten Vertrauensdiensteanbieter erstellt, dessen Zertifizierungsrichtlinie dem ETSI-Standard für qualifizierte Zertifikate (Qualified Certificate Policy, QCP) oder einem vergleichbaren Standard genügt. Zertifikate nach QCP entsprechen den Anforderungen der EU-Direktive 1999/93/EC oder Verordnung (EU) Nr. 910/2014 und sind von einem qualifizierten Vertrauensdiensteanbieter ausgestellt. Eine SSCD oder QSCD wird für den privaten Schlüssel nicht verwendet. Die Signatur entfaltet daher nicht die rechtliche Wirksamkeit, wie die eigenhändige Unterschrift (siehe EU-Direktive 1999/93/EC oder Verordnung (EU) Nr. 910/2014).
Qualifiziertes Zertifikat gemäß Signaturrichtlinie oder eIDAS-Verordnung mit privatem Schlüssel auf Smartcard für eine qualifizierte elektronische Signatur	Das Zertifikat wurde von einem qualifizierten Vertrauensdiensteanbieter erstellt, dessen Zertifizierungsrichtlinie dem ETSI-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 der er EU-Direktive 1999/93/EC oder Verordnung (EU) Nr. 910/2014 und sind von einem qualifizierten Vertrauensdiensteanbieter ausgestellt. Der private Schlüssel befindet sich auf einer SSCD oder QSCD, die den Anforderungen der EU-Direktive 1999/93/EC oder Verordnung (EU) Nr. 910/2014 erfüllt. In diesem Fall entfaltet die Signatur weitestgehend die gleiche rechtliche Wirksamkeit, wie die eigenhändige Unterschrift (siehe EU-Direktive 1999/93/EC oder Verordnung (EU) Nr. 910/2014).

Tabelle 17: Zertifikatsniveau gemäß Zertifizierungsrichtlinie des Vertrauensdiensteanbieters (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 wurde definiert in der CommonPKI-Spezifikation zur Umsetzung der besonderen Anforderungen an die Prüfung qualifizierter elektronischer Zertifikate gemäß deutschem Signaturgesetz. 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 Vertrauensdiensteanbieter/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 Vertrauensdiensteanbietern 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 durchgeführt. In der durch den OCSP-Dienst des Vertrauensdiensteanbieters signierten Antwort wird neben der Sperrstatusinformation in der Regel auch der Hashwert des Zertifikats zurückgegeben. Das OCSP/CRL-Relay kann so feststellen, ob das Zertifikat dem Vertrauensdiensteanbieter tatsächlich bekannt ist. In Deutschland war dieses Verfahren für die Prüfung qualifizierter Zertifikate gemäß Signaturgesetz quasi vorgeschrieben.
- **OCSP**: OCSP-Anfrage gemäß RFC2560. Dem OCSP-Responder wird eine CertificateID übergeben, die aus der Seriennummer des User-Zertifikats und Teilen des Ausstellers-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 Vertrauensdiensteanbieters tatsächlich durchgeführt hat.

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 "Vertrauensliste"

Bei einem qualifizierten Zertifikat aus einem EU-Staat wird in der Zeile "Vertrauensliste" eine eindeutige Identifizierung der Liste angezeigt, auf deren Basis die Qualitätsinformationen zum Zertifikat bzw. zur Signatur und zum Vertrauensdiensteanbieter beruhen. Diese wird von der Prüfinstanz geliefert und sollte die folgende Form haben: Link zur maschinenlesbaren Vertrauensliste des EU-Staat, in dem der Vertrauensdienste, dessen Zertifikat geprüft wurde, überwacht wird 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 Informati-

onen 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.

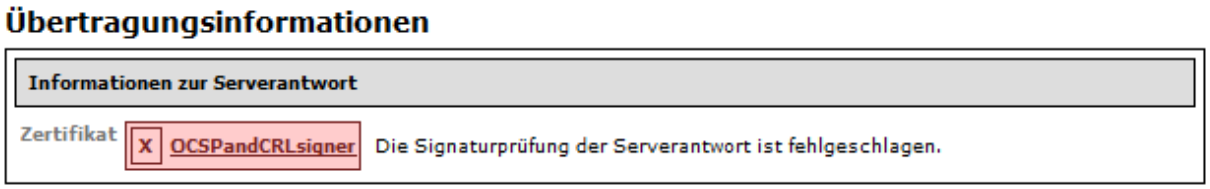


Abbildung 63: Bereich "Übertragungsinformation" bei "Gelb"-Prüfung

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 stimmen 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

Tabellen