

# GOVERNIKUS



GOVERNIKUS  
DATA **VARUNA**<sup>®</sup>

---

## Governikus Prüfprotokoll DATA Varuna

---

## Inhaltsverzeichnis

|        |  |    |
|--------|--|----|
| 1      | Rechtliche Informationen und weitere Hinweise .....  | 8  |
| 2      | Über dieses Handbuch .....   | 9  |
| 2.1    | Bereiche des Governikus Prüfprotokolls .....   | 9  |
| 2.2    | Unterstützte Signaturformate .....   | 13 |
| 3      | Hauptseite des Prüfprotokolls .....  | 14 |
| 3.1    | Bereich A "Dokument- bzw. Containerstruktur" .....   | 14 |
| 3.2    | Bereich B "Signaturprüfung/Zertifikatprüfung" .....  | 14 |
| 3.2.1  | Zeile "Signaturformat und signierte Datei" .....   | 14 |
| 3.2.2  | Zeile "Zeitpunkt der Durchführung der Prüfung" .....   | 15 |
| 3.2.3  | Zeile "Signierte Datei oder Inhalt" .....  | 15 |
| 3.2.4  | Alternative Zeilen "Signatur durch", "Zertifikat von" und "Zeitstempel erzeugt durch" .....  | 15 |
| 3.2.5  | Optionale Zeile "Signaturgrund" .....  | 16 |
| 3.2.6  | Optionale Zeile "Adresse" .....  | 16 |
| 3.2.7  | Optionale Zeile "Mitsigniertes Attributzertifikat mit der Seriennummer" .....  | 16 |
| 3.2.8  | Alternative Zeilen "Niveau und Typ der Signatur", "Niveau des Zeitstempels" oder "Niveau und Typ des Zertifikats" mit Knoten .....   | 16 |
| 3.2.9  | Zeile "Behaupteter Signaturzeitpunkt" .....  | 18 |
| 3.2.10 | Optionale Zeile "Eingangszeitpunkt auf dem Server als Zeitmarke" .....   | 19 |
| 3.2.11 | Optionale Zeile "Zeitpunkt des Signaturzeitstempels" .....   | 19 |
| 3.2.12 | Optionale Zeile "Ergebnis der Prüfung des Signaturzeitstempels" mit Knoten .....   | 19 |
| 3.2.13 | Alternative Zeilen "Prüfzeitpunkt der Signatur", "Prüfzeitpunkt des Zeitstempels" oder "Prüfzeitpunkt des Zertifikats" .....   | 20 |
| 3.2.14 | Alternative Zeilen "Ergebnis der Signaturprüfung", "Ergebnis der Zeitstempelprüfung" oder "Prüfzeitpunkt des Zertifikats" mit Knoten .....   | 21 |
| 3.2.15 | Optionale Zeile "Beweiswertbewahrung durch Archivzeitstempel" mit Knoten .....   | 22 |
| 3.3    | Bereich C "Technischer Anhang" .....   | 23 |
| 4      | Bereich B Knoten "Niveau" aufgeklappt .....  | 24 |
| 4.1    | Alternative Überschrift "Ermittlung des Signaturniveaus und des Typs" oder "Ermittlung des Zertifikatniveaus und des Typs" oder "Ermittlung Zeitstempelniveaus und des Typs" ..... | 26 |
| 4.1.1  | Zeile "Ergebnis" .....   | 26 |
| 4.1.2  | Zeile "Meldungen" .....  | 28 |
| 4.2    | Überschrift "Entscheidungsgrundlagen laut Vertrauensliste" .....   | 28 |
| 4.2.1  | Zeile "Diensteanbieter" .....  | 29 |
| 4.2.2  | Zeile "Dienstetyp" .....   | 29 |
| 4.2.3  | Zeile "Dienstestatus" .....  | 29 |
| 4.2.4  | Zeile "Ermittlungszeitpunkt des Dienstestatus" .....   | 30 |
| 4.2.5  | Zeile "Startdatum des Dienstestatus" .....   | 30 |
| 4.2.6  | Optionale Zeile "zusätzliche Qualifizierungen des Zertifikats" .....   | 30 |
| 4.2.7  | Zeile "Link zu Details der verwendeten Vertrauensliste" .....  | 31 |
| 4.3    | Überschrift "Entscheidungsgrundlagen laut Angaben des VDA im Zertifikat" .....   | 31 |
| 5      | Bereich B Knoten "Ergebnis" aufgeklappt .....  | 33 |
| 5.1    | Zeile "Verwendete Prüfrichtlinie mit Link:" .....  | 34 |
| 5.2    | Optionale Zeile "Verwendeter Algorithmenkatalog mit Link:" .....   | 34 |

|        |   |    |
|--------|---|----|
| 5.3    | Überschrift "Integritätsprüfung" .....  | 35 |
| 5.3.1  | Zeile "Strukturspezifische Prüfung" .....   | 35 |
| 5.3.2  | Zeile "Mathematische Signaturprüfung" .....   | 35 |
| 5.3.3  | Zeile "Signaturalgorithmus" .....   | 36 |
| 5.3.4  | Optionale Zeile "Signaturalgorithmus für QES geeignet bis" .....  | 36 |
| 5.3.5  | Optionale Zeile "Ausgewählter Eignungszeitpunkt" .....  | 36 |
| 5.3.6  | Optionale Zeile "Eignung zu diesem Zeitpunkt" .....   | 37 |
| 5.4    | Überschrift "Zertifikatsprüfungen" .....  | 37 |
| 5.4.1  | Zeile "Gültigkeitsmodell für die Zertifikatskette" .....  | 38 |
| 5.4.2  | Zeile "Gültigkeitsmodell definiert in" .....  | 39 |
| 5.4.3  | Zeilen "Prüfung des Zertifikats von < Name >" mit Knoten .....  | 39 |
| 5.5    | Bereich B Knoten "Prüfung des Zertifikats von < Name >" aufgeklappt .....                                 | 40 |
| 5.5.1  | Überschrift "Angaben aus dem Zertifikat" .....  | 40 |
| 5.5.2  | Zeile "Name des Inhabers" .....   | 41 |
| 5.5.3  | Zeile "Seriennummer" .....  | 41 |
| 5.5.4  | Zeile "Gültigkeitszeitraum" .....   | 41 |
| 5.5.5  | Optionale Zeile "Angaben zur Zertifikatsqualität" .....   | 41 |
| 5.5.6  | Überschrift "Zertifikatsprüfung" .....  | 41 |
| 5.5.7  | Optionale Zeile "Zuordnung des Attributzertifikats zum Signaturzertifikat" ....                           | 42 |
| 5.5.8  | Zeile "Zertifikatsherkunft" .....   | 42 |
| 5.5.9  | Zeile "Mathematische Prüfung der Zertifikatssignatur" .....   | 42 |
| 5.5.10 | Zeile "Signaturalgorithmus" .....   | 43 |
| 5.5.11 | Optionale Zeile "Signaturalgorithmus für QES geeignet bis" .....  | 43 |
| 5.5.12 | Optionale Zeile "Ausgewählter Eignungszeitpunkt" .....  | 43 |
| 5.5.13 | Optionale Zeile "Eignung zu diesem Zeitpunkt" .....   | 44 |
| 5.5.14 | Zeile "Prüfzeitpunkt des Zertifikats" .....   | 44 |
| 5.5.15 | Zeile "Prüfzeitpunkt der Signatur innerhalb Gültigkeitsintervall des<br>Zertifikats" 46                   |    |
| 5.5.16 | Zeile "Sperrstatus des Zertifikats" .....   | 46 |
| 5.5.17 | Optionale Zeile "Sperrzeitpunkt" .....  | 47 |
| 5.5.18 | Optionale Zeile "Sperrgrund" .....  | 47 |
| 5.5.19 | Überschrift "Prüfung der Sperrstatusinformationen" .....  | 48 |
| 5.5.20 | Zeile "Art der Sperrstatusermittlung" .....   | 48 |
| 5.5.21 | Zeile "Herkunft der Sperrstatusinformationen" .....   | 48 |
| 5.5.22 | Zeile "Signatur durch" .....  | 48 |
| 5.5.23 | Zeile "Ermittelter Status mindestens korrekt bis" .....   | 48 |
| 5.5.24 | Zeile "Neuere Statusinformationen spätestens verfügbar ab" .....  | 49 |
| 5.5.25 | Zeile "Signaturzeitpunkt der OCSP-Antwort bzw. CRL" .....   | 49 |
| 5.5.26 | Zeile "Prüfzeitpunkt der Signatur der OCSP-Antwort bzw. CRL" .....  | 49 |
| 5.5.27 | Zeile "Ergebnis der Signaturprüfung der OCSP-Antwort bzw. CRL" mit<br>Knoten 49                           |    |
| 5.6    | Bereich B Knoten "Prüfung des Zertifikats von < Name >" aufgeklappt (Zertifikat<br>Vertrauensanker) ..... | 50 |
| 5.6.1  | Überschrift "Angaben aus dem Zertifikat" .....  | 50 |
| 5.6.2  | Zeile "Name des Inhabers" mit Knoten .....  | 50 |
| 5.6.3  | Zeile "Staat in dem der Aussteller ansässig ist" .....  | 50 |
| 5.6.4  | Zeile "Seriennummer" .....  | 50 |
| 5.6.5  | Zeile "Gültigkeitszeitraum" .....   | 51 |
| 5.6.6  | Überschrift "Prüfung der verwendeten Vertrauensliste" .....   | 51 |
| 5.6.7  | Zeile "Ergebnis der Prüfung der Signatur der verwendeten Vertrauensliste<br>und LOTL" .....               | 51 |
| 5.6.8  | Zeile "Ergebnis der Prüfung der zeitlichen Gültigkeit der Vertrauensliste" ....                           | 51 |
| 5.6.9  | Zeile "Link zu Details zur Vertrauensliste" .....   | 51 |

|        |   |    |
|--------|---|----|
| 6      | Bereich B optionaler Knoten "Ergebnis der Prüfung des Signaturzeitstempels" |    |
|        | aufgeklappt.....  | 52 |
| 6.1    | Zeile "Zeitstempel erzeugt durch" mit Knoten.....                           | 52 |
| 6.2    | Zeile "Niveau und Typ des Zeitstempels" mit Knoten .....                    | 52 |
| 6.3    | Zeile "Ergebnis der Zeitstempelprüfung" mit Knoten .....                    | 53 |
| 7      | Bereich B optionaler Knoten "Beweiswertbewahrung durch Archivzeitstempel"   |    |
|        | aufgeklappt.....  | 54 |
| 7.1    | Überschrift "Archivzeitstempel" .....                                       | 54 |
| 7.1.1  | Optionale Überschrift "Hashwertbaum" .....                                  | 54 |
| 7.1.2  | Zeile "Hashverfahren" .....   | 55 |
| 7.1.3  | Zeile "Verwendeter Algorithmenkatalog" .....                                | 55 |
| 7.1.4  | Zeile "Hashverfahren zur Beweiswertbewahrung geeignet bis" .....            | 55 |
| 7.1.5  | Zeile "Prüfzeitpunkt der Beweiswertbewahrung".....                          | 55 |
| 7.1.6  | Zeile "Beweiswertbewahrung bis zu diesem Zeitpunkt" .....                   | 55 |
| 8      | Bereich A Knoten "Dokument bzw. Containerstruktur" aufgeklappt.....         | 56 |
| 8.1    | Zeile "Signaturformat und Dateiname" .....                                  | 56 |
| 8.2    | Knoten "Dokument- bzw. Containerstruktur" aufgeklappt.....                  | 56 |
| 8.3    | CAdES-Signaturen.....   | 57 |
| 8.3.1  | Zeile "Signaturtyp" .....   | 57 |
| 8.4    | OSCI-Nachrichten.....   | 58 |
| 8.4.1  | Zeile "OSCI-Nachricht: Dateiname" .....                                     | 58 |
| 8.4.2  | Zeile "Betreff" .....   | 58 |
| 8.4.3  | Zeile "Nachrichtenkennzeichen" .....  | 58 |
| 8.4.4  | Zeilen "Absender" und "Empfänger" .....                                     | 58 |
| 8.4.5  | Zeile "Eingang auf dem Server".....   | 59 |
| 8.4.6  | Optionale Zeile "Formatkonformität" .....                                   | 59 |
| 8.4.7  | Zeile "Inhaltsdatencontainer: Name".....                                    | 59 |
| 8.4.8  | Optionale Zeile "Ergebnis der Signaturprüfung" .....                        | 59 |
| 8.4.9  | Zeile "Inhaltsdaten" .....  | 59 |
| 8.4.10 | Zeile "Anhänge".....  | 59 |
| 8.5    | Signierte PDF-Dokumente .....   | 59 |
| 8.5.1  | Zeile "PDF-Dokument: Dateiname" .....                                       | 60 |
| 8.5.2  | Zeile "x. Revision" .....   | 60 |
| 8.5.3  | Optionale Zeile "Signatur durch".....                                       | 60 |
| 8.5.4  | Optionale Zeile "Ergebnis der Signaturprüfung" .....                        | 61 |
| 8.5.5  | Optionale Zeilen "Hinweis" und Zeile "Warnung" .....                        | 61 |
| 8.6    | De-Mail-Nachrichten .....   | 62 |
| 8.6.1  | Zeile "De-Mail-Nachricht: Dateiname" .....                                  | 63 |
| 8.6.2  | Zeile "De-Mail-Nachrichtentyp" .....  | 63 |
| 8.6.3  | Zeile "Betreff" .....   | 64 |
| 8.6.4  | Zeile "Vollständiger Name".....   | 64 |
| 8.6.5  | Zeile "Absenderadresse" .....   | 64 |
| 8.6.6  | Zeile "Empfänger-Adressen" .....  | 65 |
| 8.6.7  | Optionale Zeile "aktuelle Empfänger-Adresse(n)" .....                       | 65 |
| 8.6.8  | Zeile "Versanddatum und Zeitpunkt" .....                                    | 65 |
| 8.6.9  | Zeile "Gewählte Versandoptionen" .....                                      | 65 |
| 8.6.10 | Zeile "Authentisierungsniveau und -mechanismus des Absenders".....          | 66 |
| 8.6.11 | Optionale Zeile "Nachrichten-ID des Absenders".....                         | 67 |
| 8.6.12 | Zeile "Nachrichten-ID des Providers".....                                   | 67 |
| 8.6.13 | Zeile "De-Mail-Provider" .....  | 67 |
| 8.6.14 | Zeile "De-Mail-Header-Version".....   | 67 |
| 8.6.15 | Zeile "Typ der Meldung" .....   | 67 |
| 8.6.16 | Zeile "Signatur durch".....   | 67 |

|         |  |    |
|---------|--|----|
| 8.6.17  | Zeile "Ergebnis der Signaturprüfung".....                                  | 67 |
| 8.7     | De-Mail-Bestätigungsnachrichten .....                                      | 67 |
| 8.7.1   | Teil 1: De-Mail-Bestätigungsnachricht mit DKIM-Signatur .....              | 68 |
| 8.7.2   | Teil 2: XML-Dokument Acknowledge Message .....                             | 69 |
| 8.7.2.1 | Zeile "XML-Dokument: Acknowledge Message" .....                            | 69 |
| 8.7.2.2 | Zeile "Hashwert passt zum Hashwert der bestätigten Nachricht" ...          | 69 |
| 8.7.2.3 | Zeile "Nachrichten-ID passt zur ID der bestätigten Nachricht" .....        | 70 |
| 8.7.2.4 | Zeile "Signatur durch" .....   | 70 |
| 8.7.2.5 | Zeile "Ergebnis der Signaturprüfung" .....                                 | 70 |
| 8.7.3   | Teil 3: Normale De-Mail-Nachricht.....                                     | 70 |
| 8.8     | ASiC-Container mit Signaturen .....  | 70 |
| 8.8.1   | Zeile "ASiC-Container: Dateiname" .....                                    | 70 |
| 8.8.2   | Zeile "ASiC Container Typ" .....   | 71 |
| 8.8.3   | Optionale Zeile "Formatkonformität" .....                                  | 71 |
| 8.9     | Optionaler Bereich "Zusammenfassung Dokumente und Signaturprüfungen" ..... | 71 |
| 9       | Knoten "Name des Inhabers" aufgeklappt.....                                | 73 |
| 9.1     | Überschrift "Inhaber" .....  | 74 |
| 9.2     | Überschrift "Aussteller" .....   | 75 |
| 9.3     | Überschrift "Allgemeines" .....  | 76 |
| 9.3.1   | Zeilen "Typ" und "Version" .....   | 76 |
| 9.3.2   | Zeilen "gültig ab" und "gültig bis" (Gültigkeitszeitraum).....             | 76 |
| 9.3.3   | Zeile "Seriennummer".....  | 76 |
| 9.3.4   | Zeile "Algorithmus" .....  | 76 |
| 9.4     | Überschrift "öffentlicher Schlüssel".....                                  | 76 |
| 9.4.1   | Zeilen "Algorithmus" und Folgezeilen .....                                 | 76 |
| 9.5     | Überschrift "Signatur des Ausstellers" .....                               | 76 |
| 9.5.1   | Zeile "Signaturalgorithmus" .....  | 77 |
| 9.5.2   | Zeile "Signatur" .....   | 77 |
| 9.6     | Überschrift "Fingerabdruck" .....  | 77 |
| 9.6.1   | Zeile "SHA-1" .....  | 77 |
| 9.7     | Überschrift "Zertifikatserweiterungen" .....                               | 77 |
| 9.7.1   | Erweiterung "Aussteller- und Inhaberschlüssel-ID" .....                    | 77 |
| 9.7.2   | Erweiterung "Schlüsselverwendung" .....                                    | 78 |
| 9.7.3   | Erweiterung "Zertifizierungsrichtlinien" .....                             | 78 |
| 9.7.4   | Erweiterung "Richtlinienzuordnungen".....                                  | 79 |
| 9.7.5   | Erweiterung "Alternativer Name des Inhabers" .....                         | 79 |
| 9.7.6   | Erweiterung "Alternativer Name des Ausstellers" .....                      | 79 |
| 9.7.7   | Erweiterung "Allgemeine Einschränkungen" .....                             | 79 |
| 9.7.8   | Erweiterung "Beschränkung des Namensraums" .....                           | 79 |
| 9.7.9   | Erweiterung "Richtlinienbeschränkungen" .....                              | 79 |
| 9.7.10  | Erweiterung "Erweiterte Schlüsselverwendung" .....                         | 80 |
| 9.7.11  | Erweiterung "Distributionspunkt für CRL" .....                             | 80 |
| 9.7.12  | Erweiterung "Unterdrückung jeder Policy" .....                             | 80 |
| 9.7.13  | Erweiterung "neueste CRL" .....  | 80 |
| 9.7.14  | Erweiterung "Zugangsinformationen des Ausstellers" .....                   | 80 |
| 9.7.15  | Erweiterung "Zugangsinformationen des Inhabers" .....                      | 81 |
| 9.7.16  | Erweiterung "Angaben zum qualifizierten Zertifikat" .....                  | 81 |
| 9.7.17  | Erweiterung "keine OCSP-Prüfung".....                                      | 81 |
| 9.7.18  | Erweiterung "Gültigkeit zugesichert".....                                  | 82 |
| 9.7.19  | Erweiterung "Datum Zertifikatserzeugung" .....                             | 82 |
| 9.7.20  | Erweiterung "Open Banking-Attribute (PSD2)" .....                          | 82 |
| 10      | Bereich C Knoten "Technischer Anhang" aufgeklappt.....                     | 83 |
| 10.1    | Knoten "Prüfrichtlinien" aufgeklappt .....                                 | 83 |

|           |   |    |
|-----------|---|----|
| 10.1.1    | Überschrift "Prüfrichtlinie #1" .....   | 83 |
| 10.1.1.1  | Zeile "Herausgeber" .....   | 83 |
| 10.1.1.2  | Zeile "Version" .....   | 83 |
| 10.1.1.3  | Zeile "Name" .....  | 83 |
| 10.1.1.4  | Zeile "Bewertung der Prüfrichtlinie" .....  | 84 |
| 10.1.1.5  | Zeile "Herkunft der Prüfrichtlinie" .....   | 84 |
| 10.1.1.6  | Zeile "Zertifikatsketten-Prüfmethode" .....   | 84 |
| 10.1.1.7  | Zeile "Prüfung der Eignung der Schlüsselverwendung" .....   | 84 |
| 10.1.1.8  | Zeile "Aktualität des Sperrstatuswertes berücksichtigen" .....  | 84 |
| 10.1.1.9  | Zeile "Maximales Alter der Sperrstatusantwort bei Prüfzeitpunkt<br>"Zeitpunkt der Durchführung der Prüfung" ..... | 85 |
| 10.1.1.10 | Zeile "Eignung des Signaturalgorithmus zum behaupteten<br>Signaturzeitpunkt ermitteln" .....                      | 85 |
| 10.1.1.11 | Zeile "Eignung Signaturalgorithmus zum Zeitpunkt der<br>Durchführung der Prüfung ermitteln" .....                 | 85 |
| 10.1.1.12 | Zeile "Wenn möglich, Eignung des Signaturalgorithmus ..." .....   | 85 |
| 10.1.1.13 | Zeile "Verwendung von Vertrauensankern zulässig bei" .....  | 85 |
| 10.1.1.14 | Zeile "Notwendige Prüftiefe der Zertifikatskette" .....   | 86 |
| 10.1.1.15 | Zeile "Maximal zulässige Cache-Zeit von OCSP-Antworten für<br>CA-Zertifikate" .....                               | 86 |
| 10.1.1.16 | Zeile "Maximal zulässige Cache-Zeit von OCSP-Antworten für<br>EE-Zertifikate" .....                               | 86 |
| 10.1.1.17 | Zeile "Alle Signaturprüfungen werden zu den behaupteten<br>Signaturzeitpunkten durchgeführt" .....                | 87 |
| 10.1.1.18 | Zeile "Zertifikat-Hashwert in OCSP-Antwort muss vorhanden<br>sein" .....  | 87 |
| 10.1.1.19 | Zeile "Sperrstatusermittlung nur über OCSP erlaubt" .....   | 87 |
| 10.1.1.20 | Zeile "Minimal notwendiges Vertrauensniveau des<br>Prüfzeitpunktes" .....   | 87 |
| 10.1.1.21 | Zeile "Prüfergebnis bei gesperrten Zertifikaten" .....  | 87 |
| 10.1.1.22 | Zeile "Prüfergebnis außerhalb des Gültigkeitsintervalls" .....  | 88 |
| 10.1.1.23 | Zeile "Prüfung der Vertrauensstellung für Sperrstatus-<br>Antworten" .....  | 88 |
| 10.2      | Knoten "Vertrauenslisten" aufgeklappt .....   | 88 |
| 10.2.1    | Überschrift "Vertrauensliste #1" .....  | 88 |
| 10.2.1.1  | Zeile "Staat" .....   | 88 |
| 10.2.1.2  | Zeile "Ausstellende Aufsichtsbehörde oder Stelle" .....   | 88 |
| 10.2.1.3  | Zeile "Version" .....   | 88 |
| 10.2.1.4  | Zeile "Download-URL" .....  | 89 |
| 10.2.1.5  | Zeile "Ausgegeben am" .....   | 89 |
| 10.2.1.6  | Zeile "Nächste Aktualisierung am" .....   | 89 |
| 10.2.2    | Überschrift "Erweiterung der Vertrauensliste #1" .....  | 89 |
| 10.2.2.1  | Zeile "Staat" .....   | 89 |
| 10.2.2.2  | Zeile "Ausstellende Aufsichtsbehörde oder Stelle" .....   | 89 |
| 10.2.2.3  | Zeile "Version" .....   | 89 |
| 10.2.2.4  | Zeile "Download-URL" .....  | 89 |
| 10.2.2.5  | Zeile "Ausgegeben am" .....   | 89 |
| 10.2.2.6  | Zeile "Nächste Aktualisierung am" .....   | 90 |
| 10.3      | Knoten "Algorithmenkataloge" aufgeklappt .....  | 90 |
| 10.3.1    | Zeile "Name" .....  | 90 |
| 10.3.2    | Zeile "Version" .....   | 90 |
| 10.3.3    | Zeile "Land" .....  | 90 |
| 10.3.4    | Zeile "Veröffentlicht von" .....  | 90 |
| 10.3.5    | Zeile "Veröffentlicht am" .....   | 90 |

|        |   |    |
|--------|---|----|
| 10.3.6 | Zeile "URL des Herausgebers" .....  | 90 |
| 10.4   | Knoten "Prüfinstanz" aufgeklappt.....                                       | 90 |
| 10.4.1 | Zeile "URL des Certificate Validation Servers" .....                        | 90 |
| 10.4.2 | Zeile "Kumulierte Wartezeit auf externe Antworten (in ms) " .....           | 91 |
| 10.4.3 | Zeile "Version des CVS" .....   | 91 |
| 10.4.4 | Zeile "Version der CSL" .....   | 91 |
| 11     | Signaturformate, Prüftiefe, Abkürzungsverzeichnis .....                     | 92 |
| 11.1   | Signaturformate, Nachrichtentypen mit Signaturen und Containerformate ..... | 92 |
| 11.2   | Prüftiefe .....   | 94 |
| 12     | Abkürzungsverzeichnis .....   | 95 |
| 13     | Abbildungsverzeichnis .....   | 98 |

## **1 Rechtliche Informationen und weitere Hinweise**

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

Diese Produktinformation sowie sämtliche urheberrechtsfähigen Materialien, die mit dem Produkt vertrieben werden, sind urheberrechtlich geschützt. Alle Rechte sind der Governikus GmbH & Co. KG, im folgenden Governikus KG, vorbehalten. Alle urheberrechtsfähigen Materialien dürfen ohne vorherige Einwilligung der Governikus KG weder ganz noch teilweise kopiert oder auf sonstige Art und Weise reproduziert werden. Für rechtmäßig Nutzende des Produkts gilt diese Einwilligung im Rahmen der vertraglichen Vereinbarungen als erteilt. Jegliche Kopien dieser Produktinformation, bzw. von Teilen daraus, müssen den gleichen Hinweis auf das Urheberrecht enthalten wie das Original.

Governikus und DATA Varuna sind eingetragene Marken der Governikus KG, Bremen. Andere in diesem Produkt aufgeführte Produkt- und/oder Firmennamen sind möglicherweise Marken weiterer Eigentümer, deren Rechte ebenfalls zu wahren sind.



## 2 Über dieses Handbuch

Das folgende Dokument erläutert das Governikus-Prüfprotokoll so wie es durch die Produkte DATA Boreum, COM Vibilia, den Validation Service von DATA Varuna und weitere Governikus-Produkte erstellt wird.

Das Prüfprotokoll stellt die Ergebnisse der technischen Prüfung der digitalen Signatur eines Dokuments in Verbindung mit der Ermittlung des rechtlichen Niveaus und des Typs der Signatur menschenlesbar dar. Die technische Prüfung der digitalen Signatur bzw. technische Ermittlung des rechtlichen Niveaus in den oben benannten Produkten erfolgt auf Basis der Europäischen Normen (EN) und technischen Standards (TS), die durch ETSI im Rahmen des Normierungsmandats M/460 erstellt wurden. Diese EN und TS beanspruchen (Eigenaussage ETSI), den rechtlichen Anforderungen aus der eIDAS-VO zu genügen. Die Prüfung von digitalen Signaturen, die unter den rechtlichen und technischen Anforderungen des deutschen Signaturgesetzes erstellt wurden, ist natürlich auch weiterhin möglich.

In diesem Dokument werden ausschließlich die signaturtechnischen Prüfergebnisse beschrieben. Mögliche weitere Prüfungen, die aus fachlichen Erwägungen erfolgen können, sind nicht Gegenstand des Signaturprüfprotokolls.

+ -
**Prüfprotokoll: 12.04.2021, 09:47:25**

Dokument bzw. Containerstruktur:

+ CAdES-Dokument: QES\_BNotK\_gruen.p7s

Signaturprüfung:

| CAdES-Signatur B: QES_BNotK_gruen.p7s   |   |
|---|---|
| Zeitpunkt der Durchführung der Prüfung: | 12.04.2021, 09:47:25                              |
| Signierte Datei oder Inhalt:            | QES_BNotK_gruen.p7s                               |
| Signatur durch:                         | Gustav Gans                                       |
| + Niveau und Typ der Signatur:          | EU-qualifizierte elektronische Signatur (EUMS-TL) |
| Behaupteter Signaturzeitpunkt:          | 05.02.2019, 17:24:01                              |
| Prüfzeitpunkt der Signatur:             | Behaupteter Signaturzeitpunkt                     |
| + Ergebnis der Signaturprüfung:         | <b>gültig</b>                                     |

| Technischer Anhang                     |  |
|--|--|
| + Prüfrichtlinien                      |  |
| + Vertrauenslisten (mit Erweiterungen) |  |
| + Algorithmenkataloge                  |  |
| + Prüfinstanz                          |  |

Abbildung 1: Hauptseite Governikus Prüfprotokoll

### 2.1 Bereiche des Governikus Prüfprotokolls

Das Governikus Prüfprotokoll gliedert sich in drei inhaltliche Bereiche:

- Bereich A "Dokument bzw. Containerstruktur"
- Bereich B "Signaturprüfung" oder "Zertifikatsprüfung"
- Bereich C "Technischer Anhang"

Alle drei Bereiche werden auf einer Übersichtsseite dargestellt und verfügen über eine Baumstruktur.

Beim HTML-Prüfprotokoll kann die Baumstruktur aufgeklappt werden. Das Pluszeichen im linken senkrechten Balken zeigt an, dass nach dem Aufklappen des Knotens detaillierte Informationen, zum Beispiel zu einem Prüfergebnis, zur Verfügung stehen. Durch einen Klick auf das Minuszeichen werden die Detailinformationen wieder geschlossen.

Das PDF-Prüfprotokoll hat eine identische Baumstruktur. Da es sich um ein PDF im Format UA handelt, sind alle Knoten bereits aufgeklappt. Zur besseren Übersicht wird der Bereich B deshalb vor der aufgeklappten Anzeige (Überschrift "Prüfung der Signaturen im Detail") nicht aufgeklappt (Überschrift "Übersicht Prüfung der Signaturen") angezeigt.

Die Bereiche des Prüfprotokolls werden im Folgenden kurz vorgestellt.

### Bereich A "Dokument bzw. Containerstruktur"

Im Bereich A "Dokument bzw. Containerstruktur" werden in der blau unterlegten Überschrift des Knotens das Signatur- oder Containerformat und danach der Dateiname des signierten Dokuments bzw. des Containers angezeigt. Die Beschreibung der Hauptseite des Prüfprotokolls für den Bereich A befindet sich im Kapitel 3.1.

Nach dem Aufklappen des Knotens wird der Name der signierenden Person und das Ergebnis der Signaturprüfung in Ampelform ausgegeben und ggf. weitere wichtige Kontextinformationen angezeigt. Bei einer signierten OSCI-Nachricht mit signierten Attachments, einem ZIP-Container mit signierten Dateien, einem PDF-Portfolio mit signierten PDF-Dateien, oder bei mehreren \*AdES-Signaturen in einer Datei wird auch deren Struktur dargestellt. Somit kann auch optisch nachvollzogen werden, mit welcher Signatur welcher Inhalt signiert wurde.

### Bereich B "Signaturprüfung" oder "Zertifikatprüfung"

Im Bereich B "Signaturprüfung" wird auf einer Übersichtsseite das Ergebnis der technischen Signaturprüfung angezeigt. Das Ergebnis einer separaten Zertifikatsprüfung wird unter dem Bezeichner "Zertifikatprüfung" angezeigt.

Hinweis: Wird eine Datei mit einem (detached) Inhaltsdatenzeitstempel übergeben, befindet sich das Ergebnis der Prüfung auch vollständig auf der Hauptseite des Prüfprotokolls unter dem Bezeichner "Signaturprüfung".

#### Signaturprüfung:

| CAAdES-Signatur B: eIDAS-QES_B.p7s      |   |
|---|---|
| Zeitpunkt der Durchführung der Prüfung: | 01.04.2021, 14:31:49                              |
| Signierte Datei oder Inhalt:            | eIDAS-QES_B.p7s                                   |
| Signatur durch:                         | Emil Erpel  |
| + Niveau und Typ der Signatur:          | EU-qualifizierte elektronische Signatur (EUMS-TL) |
| Behaupteter Signaturzeitpunkt:          | 09.05.2017, 13:18:43                              |
| Prüfzeitpunkt der Signatur:             | Behaupteter Signaturzeitpunkt                     |
| + Ergebnis der Signaturprüfung:         | <b>gültig</b>                                     |

Abbildung 2: Hauptseite Governikus Prüfprotokoll Bereich B bei der Prüfung einer Signatur ohne optionale Zeilen

Das Protokoll hat im Bereich B immer den folgenden Aufbau. Die Reihenfolge der Aufzählung entspricht der Reihenfolge im Prüfprotokoll; optionale Zeilen sind *kursiv* gesetzt.

- In der Zeile "Zeitpunkt der Durchführung der Prüfung" (time of validation) wird angezeigt, wann die Prüfung durchgeführt wurde.
- In der Zeile "Signierte Datei oder Inhalt" wird angezeigt, welche Datei oder welcher Inhalt (ggf. mehre Dateien in einem Container) geprüft wurde.
- Alternative Zeilen "Signatur durch", "Zertifikat von" und "Zeitstempel erzeugt durch":

- Wird eine Inhaltsdatensignatur geprüft, wird in der Zeile "Signatur durch" angezeigt, welche Person oder Organisation die Inhaltsdatensignatur erzeugt hat.
- Wird ein Zertifikat separat geprüft, wird dies in der Zeile "Zertifikat von" angezeigt.
- Wird ein detached Inhaltsdatenzeitstempel geprüft, wird die Zeile "Zeitstempel erzeugt durch" angezeigt.
- In den optionalen Zeilen "Signaturgrund" und "Adresse" wird - soweit in der Signatur vorhanden - der angegebene Grund der Signatur und die "Adresse" der Signaturerstellung angezeigt. In der optionalen Zeile "mitsigniertes Attributzertifikat" wird - sollte ein Attributzertifikat vorhanden sein - die Referenz auf das Attributzertifikat angezeigt.
- Alternative Zeilen "Niveau und Typ der Signatur", "Niveau und Typ des Zertifikats" oder "Niveau des Zeitstempels":
  - Wird eine Inhaltsdatensignatur geprüft, wird in der Zeile "Niveau und Typ der Signatur" das auf der Basis von Vertrauenslisten ermittelte Niveau und – soweit möglich – auch der Typ der Inhaltsdatensignatur (Signatur/Siegel) angezeigt.
  - Wird ein Zertifikat separat geprüft, wird in der Zeile "Niveau und der Typ des Zertifikats" das auf der Basis von Vertrauenslisten ermittelte Niveau und – soweit möglich – auch der Typ des Zertifikats (Zertifikat für Signatur/Siegel/Website-Authentisierung) angezeigt.
  - Wird ein detached Inhaltsdatenzeitstempel geprüft, wird in der Zeile "Niveau des Zeitstempels" das auf der Basis von Vertrauenslisten ermittelte Niveau des Zeitstempels angezeigt.

Nach dem Aufklappen des Knotens werden das Ergebnis der Ermittlung sowie die Entscheidungsgrundlagen angezeigt, die für die Ermittlung des Niveaus und gegebenenfalls des Typs herangezogen wurden.

### Zertifikatprüfung:

| X509-Zertifikat: QES_SigG_EE.cer        |  |
|---|--|
| Zeitpunkt der Durchführung der Prüfung: | 10.08.2021, 07:59:13   |
| + Zertifikat von:                       | Wilhelm Tell   |
| + Niveau und Typ des Zertifikats:       | EU-qualifiziertes Zertifikat für Signaturen (EUMS-TL)            |
| Behaupteter Signaturzeitpunkt:          | 20.10.2014, 17:35:04   |
| Prüfzeitpunkt des Zertifikats:          | Zeitpunkt der Durchführung der Prüfung                           |
| Ergebnis der Zertifikatprüfung          | <b>ungültig</b>  |
| + Meldungen:                            | Zum Prüfzeitpunkt war das Signaturzertifikat bereits abgelaufen. |

Abbildung 3: Hauptseite Governikus Prüfprotokoll Bereich B bei der Prüfung eines separaten Zertifikats

- In der Zeile "Behaupteter Signaturzeitpunkt" wird angezeigt, zu welchem Zeitpunkt die Inhaltsdatensignatur nach Angabe der signierenden Instanz erstellt wurde. Wurde ein detached Inhaltsdatenzeitstempel geprüft, ist dies der Zeitpunkt der Erstellung des Zeitstempeltokens (`genTime`). Bei einem separat geprüften Zertifikat ist dies der Erstellungszeitpunkt des Zertifikats (`notBefore`).
- In der optionalen Zeile "Übergebener Zeitpunkt" wird bei einer separaten Prüfung eines Zertifikats der in der Anfrage übergebene Zeitpunkt angezeigt zu dem die Gültigkeit des Zertifikats geprüft wurde.
- In der optionalen Zeile "Eingangszeitpunkt auf dem Server als Zeitmarke" wird - sollte eine Zeitmarke vorhanden sein - angezeigt, zu welchem Zeitpunkt z.B. eine OSCNachricht auf dem OSCN-Server eingegangen ist.

- In der optionalen Zeile "Zeitpunkt des Signaturzeitstempels" wird - sollte ein Signaturzeitstempel vorhanden sein - angezeigt, zu welchem Zeitpunkt die Signatur mit einem Zeitstempel abgesichert wurde.
- In der optionalen Zeile "Ergebnis der Prüfung des Signaturzeitstempels" mit Knoten wird - sollte ein Signaturzeitstempel vorhanden sein - das Ergebnis der Prüfung des Signaturzeitstempels angezeigt. Nach dem Aufklappen des Knotens werden die einzelnen Prüfergebnisse angezeigt.
- In der Zeile "Prüfzeitpunkt" (validation time) wird angezeigt, zu welchem Datum die Gültigkeit der Inhaltsdatensignatur, des Zeitstempel oder des einzelnen Zertifikats geprüft wurde.
- Alternative Zeilen "Ergebnis der Signaturprüfung", "Ergebnis der Zertifikatprüfung" oder "Ergebnis der Zeitstempelprüfung" mit Knoten:
  - Wird eine Inhaltsdatensignatur geprüft, wird in der Zeile "Ergebnis der Signaturprüfung" das Gesamtergebnis der Signaturprüfung angezeigt.
  - Wird ein Zertifikat separat geprüft, wird in der Zeile "Ergebnis der Zertifikatprüfung" das Ergebnis der Gültigkeitsprüfung des Zertifikats angezeigt.
  - Wird ein detached Inhaltsdatenzeitstempel geprüft, wird in der Zeile "Ergebnis der Zeitstempelprüfung" das Gesamtprüfergebnis der Prüfung des Zeitstempels angezeigt.

Nach Aufklappen des Knotens in der entsprechenden Zeile werden die Einzelprüfergebnisse detailliert dargestellt.

- In der optionalen Zeile "Beweiswertbewahrung durch Archivzeitstempel" mit Knoten wird - sollte ein Archivzeitstempel vorhanden sein - das Gesamtergebnis der Archivzeitstempelprüfung angezeigt. Nach Aufklappen des Knotens werden Ergebnisse der Prüfung des Archivzeitstempels bzw. des ERS mit Archivzeitstempel angezeigt.

Die Beschreibung der einzelnen Zeilen der Hauptseite des Prüfprotokolls für den Bereich B befindet sich im Kapitel 3.2.

**Signaturprüfung:**

| CAdES-Signatur LTA: eIDAS-QES-Test.p7s           |   |
|--|---|
| Zeitpunkt der Durchführung der Prüfung:          | 01.04.2021, 08:16:52                              |
| Signierte Datei oder Inhalt:                     | eIDAS-QES-Test.p7s                                |
| Signatur durch:                                  | Donald Duck                                       |
| + Niveau und Typ der Signatur:                   | EU-qualifizierte elektronische Signatur (EUMS-TL) |
| Behaupteter Signaturzeitpunkt:                   | 09.05.2017, 13:18:43                              |
| Zeitpunkt des Signaturzeitstempels:              | 18.06.2019, 15:13:38                              |
| + Signaturzeitstempel                            | <b>gültig</b>                                     |
| Prüfzeitpunkt der Signatur:                      | Behaupteter Signaturzeitpunkt                     |
| + Ergebnis der Signaturprüfung:                  | <b>gültig</b>                                     |
| + Beweiswertbewahrung durch Archivzeitstempel #1 | <b>gültig</b>                                     |

Abbildung 4: Hauptseite Prüfprotokoll Bereich B bei der Prüfung einer Signatur mit optionalen Zeilen

Wurde mehr als eine Signatur geprüft, wird der Bereich B entsprechend häufig wiederholt.

**Bereich C "Technischer Anhang"**

Im Bereich C "Technischer Anhang" werden nach dem Aufklappen der Knoten technische Kontextinformationen zur Signaturprüfung angezeigt.

| Technischer Anhang |                                      |
|--------------------|--------------------------------------|
| +                  | Prüfrichtlinien                      |
| +                  | Vertrauenslisten (mit Erweiterungen) |
| +                  | Algorithmenkataloge                  |
| +                  | Prüfinstanz                          |

Abbildung 5: Hauptseite Prüfprotokoll Bereich C "Technischer Anhang"

Nach dem Aufklappen des Knotens "Prüfrichtlinien" werden die Prüfrichtlinien, die im Kontext der Signaturprüfung verwendet wurden, vollständig angezeigt (siehe Kapitel 10.1). Im aufgeklappten Knoten "Vertrauenslisten" Detailinformationen zu den verwendeten Vertrauenslisten (siehe Kapitel 10.2). Im aufgeklappten Knoten "Algorithmenkataloge" folgen die Detailinformationen zu den verwendeten Algorithmenkatalogen (siehe Kapitel 10.3). Im aufgeklappten Knoten "Prüfinstanz" (Kapitel 10.4) wird schließlich angezeigt, welche Prüfinstanz (URL) auf der Basis welcher Produktversion und CSL die Prüfung durchgeführt hat.

## 2.2 Unterstützte Signaturformate

Das Governikus-Prüfprotokoll in der HTML- oder PDF-Version wird von Governikus Produkten erzeugt, die Signaturen validieren. Dazu gehören der Validation Service von DATA Varuna, aber auch die Governikus-Produkte (Governikus Clients) DATA Boreum, DATA Pavonis oder COM Vibilia.

Validiert werden:

- Dokumente mit PAdES-, CAdES, XAdES- und JAdES-Baseline-Signaturen in allen Levels (B, T, LT und LTA) gemäß ETSI-Vorgaben,
- signierte Dokumente in OSCI-, ASiC- und ZIP-Containern,
- signierte OSCI-Nachrichten (Containersignaturen), De-Mailnachrichten mit DKIM-Signaturen und signierte E-Mails sowie
- End-Entity-Zertifikate des Typs Signatur, Siegel oder Website-Authentisierung (separat übergeben).

Detaillierte Informationen zu den unterstützten Signaturformaten, ggf. notwendige Einschränkungen sowie die Benennung der unterstützten technischen ETSI-Standards und Europäischen Normen finden Sie im Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** dieses Dokuments.

Bitte beachten Sie außerdem, dass Governikus Produkte den Umfang der unterstützten Signaturformate, Nachrichtentypen und Containerformate einschränken können.

### 3 Hauptseite des Prüfprotokolls

In diesem Kapitel werden die drei Bereiche der Hauptseite des Prüfprotokolls beschrieben. Im Kapitel 3.1 folgt die Beschreibung des Bereichs A "Dokument- bzw. Containerstruktur" des Prüfprotokolls. Die auf der Hauptseite angezeigten Prüfergebnisse des Bereich B "Prüfung der Signaturen" werden im Kapitel 3.2 erläutert. Im Kapitel 3.3 wird anschließend der auf der Hauptseite angezeigte Bereich C "Technischer Anhang beschrieben."

#### 3.1 Bereich A "Dokument- bzw. Containerstruktur"

Auf der Hauptseite des Prüfprotokolls werden im Bereich A "Dokument bzw. Containerstruktur" in der blau unterlegten Überschrift des Knotens das Signatur- oder Containerformat und danach der Dateiname des signierten Dokuments bzw. des Containers angezeigt.



Abbildung 6: Hauptseite Bereich A des Prüfprotokolls

#### 3.2 Bereich B "Signaturprüfung/Zertifikatprüfung "

Im Bereich B wird auf der Hauptseite das Ergebnis der technischen Signatur- oder Zertifikatsprüfung (letzteres nur bei der Gültigkeitsprüfung eines einzelnen Zertifikats) sowie das Ergebnis der Ermittlung des rechtlichen Niveaus der Signatur oder des Zertifikats angezeigt. Sind in einer Datei mehrere Signaturen vorhanden, wird im Bereich B die Anzeige für jede Signatur wiederholt.

In den folgenden Unterkapiteln wird jede Zeile der Übersichtsseite des Prüfprotokolls erläutert. Das Prüfprotokoll besitzt auch in diesem Bereich eine Baumstruktur. Das Pluszeichen im linken senkrechten Balken zeigt an, dass nach dem Aufklappen eines Knotens detaillierte Informationen angezeigt werden.

##### Signaturprüfung:

| CAdES-Signatur LTA: eIDAS-QES-Test.p7s           |   |
|--|---|
| Zeitpunkt der Durchführung der Prüfung:          | 01.04.2021, 08:16:52                              |
| Signierte Datei oder Inhalt:                     | eIDAS-QES-Test.p7s                                |
| Signatur durch:                                  | Donald Duck                                       |
| + Niveau und Typ der Signatur:                   | EU-qualifizierte elektronische Signatur (EUMS-TL) |
| Behaupteter Signaturzeitpunkt:                   | 09.05.2017, 13:18:43                              |
| Zeitpunkt des Signaturzeitstempels:              | 18.06.2019, 15:13:38                              |
| + Signaturzeitstempel                            | <b>gültig</b>                                     |
| Prüfzeitpunkt der Signatur:                      | Behaupteter Signaturzeitpunkt                     |
| + Ergebnis der Signaturprüfung:                  | <b>gültig</b>                                     |
| + Beweiswertbewahrung durch Archivzeitstempel #1 | <b>gültig</b>                                     |

Abbildung 7: Hauptseite Bereich B des Prüfprotokolls mit optionalen Zeilen

##### 3.2.1 Zeile "Signaturformat und signierte Datei"

In der ersten blau unterlegten Zeile "Signaturformat und signierte Datei" des Bereichs B wird zunächst angezeigt, auf welches Signaturformat (mit Nachrichtentyp oder Dateiformat) sich

das Prüfergebnis und, nach dem Doppelpunkt, auf welches Datenobjekt sich die Prüfung bezieht. Folgende Informationen können angezeigt werden:

- CAdES-Signatur mit Angabe des Baseline-Levels
- PAdES-Signatur mit Angabe des Baseline-Levels
- XAdES-Signatur mit Angabe des Baseline-Levels
- JAdES-Signatur mit Angabe des Baseline-Levels
- OSCI-Containersignatur
- DKIM-Signatur (in einer De-Mail-Nachricht)
- S/MIME-Signatur
- X509-Zertifikat-Signatur
- Zeitstempel-Signatur

Detailliertere Informationen zu den unterstützten Signaturformaten, Nachrichtentypen mit Signaturen und Containerformaten befinden sich im Kapitel 2.2.

### 3.2.2 Zeile "Zeitpunkt der Durchführung der Prüfung"

In der Zeile "Zeitpunkt der Durchführung der Prüfung" (time of validation) werden das Datum und die Uhrzeit in der Form `TT.MM.JJJJ` und `hh:mm:ss` angezeigt, zu dem die Prüfung von der Validierungsanwendung durchgeführt wurde.

### 3.2.3 Zeile "Signierte Datei oder Inhalt"

In der Zeile "Signierte Datei oder Inhalt" wird der Name der signierten Datei oder des signierten Inhalts angezeigt.

Folgende Sonderfälle sind zu beachten:

- Bei einem signierten OSCI-Container werden die Namen aller signierten Dateien aufgezählt.
- Bei einer signierten PDF-Datei wird der Dateiname und zusätzlich die Revision der Signatur angezeigt (`Dateiname.pdf_Revision x`, `x` = Revisionsnummer).
- Wird eine Signatur durch eine andere Signatur gegengezeichnet (Countersignatur), wird statt der Zeile "Signierte Datei oder signierter Inhalt" die Zeile "Gegenzeichnung für" angezeigt.
- Bei einer zeitgestempelten Datei (Inhaltsdatenzeitstempel) wird hinter dem Bezeichner der Name der zeitgestempelten Datei angezeigt.

Wird ein einzelnes Zertifikat geprüft, entfällt diese Zeile.

### 3.2.4 Alternative Zeilen "Signatur durch", "Zertifikat von" und "Zeitstempel erzeugt durch"

Wird eine Inhaltsdatensignatur geprüft, wird in der Zeile "Signatur durch" der Common Name der signierenden Person oder Organisation angezeigt. Bei Organisationszertifikaten (z.B. Siegelzertifikaten) wird der Name der Organisation angezeigt, der in der Regel verwendet wird, um sich selbst zu vertreten. Dieser Name muss nicht exakt der vollständige, registrierte Organisationsname sein.

Wird ein detached Inhaltsdatenzeitstempel geprüft, wird in Zeile "Zeitstempel erzeugt durch" der Name des Vertrauensdiensteanbieters angezeigt, der das Zeitstempel-Token erstellt hat. Häufig enthält der Name den Zusatz TSA (Time Stamp Authority) angezeigt.

Wird ein Zertifikat separat geprüft, wird in der Zeile "Zertifikat von" bei Personenzertifikaten in der Regel der Vor- und Nachname des Zertifikatsinhabers oder ein Pseudonym angezeigt. Bei Organisationszertifikaten (z.B. Siegelzertifikaten) wird der Name der Organisation angezeigt, der in der Regel verwendet wird, um sich selbst zu vertreten. Dieser Name muss nicht exakt der vollständige, registrierte Organisationsname sein.

### **3.2.5 Optionale Zeile "Signaturgrund"**

In der optionalen Zeile "Signaturgrund" wird der durch die signierende Person angegebene Grund der Signatur - soweit in \*AdES-Formatprofilierung als signiertes Attribut vorgesehen und in der Signatur angegeben - angezeigt.

### **3.2.6 Optionale Zeile "Adresse"**

In der optionalen Zeile "Adresse" wird der durch die signierende Person angegebene Adresse der Signaturerstellung - soweit im \*AdES-Formatprofilierung als signiertes Attribut vorgesehen und in der Signatur angegeben - angezeigt. Folgende Angaben sind möglich: Land [`countryName`], Ort [`localityName`], Postadresse [`postaladdress`].

### **3.2.7 Optionale Zeile "Mitsigniertes Attributzertifikat mit der Seriennummer"**

Sollte neben dem Signaturzertifikat auch ein Attributzertifikat (gemäß Common-PKI-Spezifikation zur Umsetzung der Anforderungen aus dem SigG) mitsigniert worden sein wird in dieser Zeile die Referenz auf das Attributzertifikat angezeigt. Das ist in diesem Fall die Seriennummer des Attributzertifikats. Das Ergebnis der Prüfung des Attributzertifikats wird in diesem Fall unter der Überschrift "Zertifikatsprüfungen" (siehe Kapitel 5.4 ff) in einem eigenen Knoten angezeigt.

### **3.2.8 Alternative Zeilen "Niveau und Typ der Signatur", "Niveau des Zeitstempels" oder "Niveau und Typ des Zertifikats" mit Knoten**

Wird eine Inhaltsdatensignatur geprüft, wird in der Zeile "Niveau und Typ der Signatur" das auf der Basis von Vertrauenslisten ermittelte Niveau und – soweit möglich – auch der Typ der Inhaltsdatensignatur (Signatur/Siegel) angezeigt.

Wird ein Zertifikat separat geprüft, wird in der Zeile "Niveau und der Typ des Zertifikats" das auf der Basis von Vertrauenslisten ermittelte Niveau und – soweit möglich – auch der Typ des End-Entity-Zertifikats angezeigt.

Wird ein detached Inhaltsdatenzeitstempel geprüft, wird in der Zeile "Niveau des Zeitstempels" das auf der Basis von Vertrauenslisten ermittelte Niveau des Zeitstempels angezeigt.

In den folgenden Abschnitten werden die möglichen Werte der Anzeige erläutert.

#### **Niveaus elektronischer Signaturen/Siegel**

Folgende Signaturniveaus mit Typ sind für elektronische Signaturen gemäß eIDAS-VO bzw. der zugehörigen Normierung definiert worden:

- EU-qualifizierte elektronische Signatur
- Fortgeschrittene elektronische Signatur unterstützt durch ein EU-qualifiziertes Zertifikat für die elektronische Signatur



- Fortgeschrittene elektronische Signatur
- Digitale Signatur

Die Ermittlung des Niveaus "EU-qualifizierte elektronische Signatur" oder "fortgeschrittene elektronische Signatur unterstützt durch ein EU-qualifiziertes Zertifikat" erfolgt ausschließlich auf Basis der Angaben in einer European Union Member State Trusted List (EUMS-TL). Die Angabe EUMS-TL wird in Klammern hinter dem angezeigten Niveau aufgeführt.

Die Ermittlung des Niveaus "fortgeschrittene elektronische Signatur" erfolgt entweder auf Basis von Angaben in einer EUMS-TL oder über eine Governikus-TL oder Kunden-TL (Custom-TL). Die Angabe, welche Vertrauensliste verwendet wurde, wird in Klammern hinter dem angezeigten Niveau aufgeführt. Kann als Typ "Siegel" ermittelt werden, wird statt Typ "Signatur" Typ "Siegel" angezeigt.

Kann zwar ein zertifikatsausstellender Dienst in der EUMS-TL ermittelt werden, der Dienst wurde aber zum Zeitpunkt der Ausstellung des Zertifikats nicht mehr durch die Aufsichtsbehörde überwacht oder die dortige Konfiguration genügt nicht den Anforderungen, so wird dem ermittelten Niveau ein "Kein/Keine" vorangestellt. Erfolgt die Niveauermittlung auf Basis der Angaben in der Governikus-TL oder einer Custom-TL, kann keine Negativaussage erfolgen, da die in diesen Vertrauenslisten konfigurierten Dienste den Status "nicht überwacht" besitzen.

Kann das Niveau einer Signatur oder eines Siegels nicht auf Basis einer der drei Typen von Vertrauenslisten bestimmt werden, wird "Digitale Signatur" angezeigt. Diese digitale Signatur kann gleichwohl trotzdem technisch gültig geprüft werden. Die Signatur ist allerdings technisch nicht geeignet, um eine fortgeschrittene oder eine qualifizierte elektronische Signatur im Sinne der zum Zeitpunkt der Signaturerstellung geltenden europäischen Rechtsvorschriften (EU-Signaturrichtlinie oder eIDAS-Verordnung) darzustellen.

Nach Aufklappen des Knotens werden das Ergebnis der Ermittlung sowie die Entscheidungsgrundlagen angezeigt, die für die Ermittlung des Niveaus und des Typs herangezogen wurden. Eine Beschreibung der einzelnen Entscheidungsgrundlagen befindet sich in Kapitel 4.

### Niveaus elektronischer Zeitstempel

Folgende Niveaus eines Zeitstempels können ermittelt und angezeigt werden:

- EU-qualifizierter elektronischer Zeitstempel (EUMS-TL)
- Nicht-qualifizierter elektronischer Zeitstempel eines qVDA zur Augmentierung von QES
- Nicht-qualifizierter elektronischer Zeitstempel eines VDA zur Augmentierung von QES
- Nicht-qualifizierter elektronischer Zeitstempel
- Digitaler Zeitstempel

Die Ermittlung des Niveaus "EU-qualifizierter elektronischer Zeitstempel" erfolgt ausschließlich auf Basis der Angaben in einer European Union Member State Trusted List (EUMS-TL). Die Angabe EUMS-TL wird in Klammern hinter dem angezeigten Niveau aufgeführt.

Die Ermittlung des Niveaus von nicht qualifizierten elektronischen Zeitstempeln erfolgt entweder auf Basis von Angaben in einer EUMS-TL oder über eine Governikus-TL oder Kunden-TL (Custom-TL). Die Angabe, welche Vertrauensliste verwendet wurde, wird in Klammern hinter dem angezeigten Niveau aufgeführt.

Kann zwar ein Zeitstempeldienst in der EUMS-TL ermittelt werden, der Dienst wurde aber zum Zeitpunkt der Ausstellung des Zeitstempeltokens nicht mehr durch die Aufsichtsbehörde überwacht oder die dortige Konfiguration genügt nicht den Anforderungen, so wird dem ermittelten Niveau ein "Kein/Keine" vorangestellt. Erfolgt die Niveauermittlung auf Basis der Angaben in der Governikus-TL oder einer Custom-TL, kann keine Negativaussage erfolgen, da die in diesen Vertrauenslisten konfigurierten Dienste den Status "nicht überwacht" besitzen.

Kann das Niveau eines Zeitstempels nicht auf Basis einer der drei Typen von Vertrauenslisten bestimmt werden wird "Digitaler Zeitstempel" angezeigt.

Hinweis: Neben den oben benannten Niveaus gibt es noch den Sonderfall "qualifizierter Zeitstempel gemäß Signaturgesetz". Die Ermittlung erfolgt ausschließlich auf Basis der Angaben in einer EUMS-TL. Die Angabe EUMS-TL wird in Klammern hinter dem angezeigten Niveau aufgeführt. Dieser Wert wird nur zur Kennzeichnung eines qualifizierten Zeitstempeldienstes verwendet, der in Deutschland von einem qVDA gemäß den Anforderungen des deutschen Signaturgesetzes vor Inkrafttreten der eIDAS-Verordnung erstellt wurde. In der eIDAS-Verordnung werden diese Zeitstempel rechtlich nicht EU-qualifizierten Zeitstempeln gleichgestellt.

Nach Aufklappen des Knotens werden das Ergebnis der Ermittlung sowie die Entscheidungsgrundlagen angezeigt, die für die Ermittlung des Niveaus des Zeitstempels herangezogen wurden. Eine Beschreibung der einzelnen Entscheidungsgrundlagen befindet sich im Kapitel 4.

### Zertifikatniveaus

Folgende Niveaus eines Zertifikats können ermittelt und angezeigt werden:

- EU-qualifiziertes elektronisches Zertifikat für Signaturen
- Fortgeschrittenes elektronisches Zertifikat für Signaturen
- Digitales Zertifikat für Signaturen

Die Ermittlung eines EU-qualifizierten elektronischen Zertifikats erfolgt ausschließlich auf Basis der Angaben in einer European Union Member State Trusted List (EUMS-TL). Die Angabe EUMS-TL wird in Klammern hinter dem angezeigten Niveau aufgeführt.

Die Ermittlung des Niveaus "Fortgeschrittenes elektronisches Zertifikat" erfolgt entweder auf Basis von Angaben in einer EUMS-TL oder über eine Governikus-TL oder Kunden-TL (Custom-TL). Die Angabe, welche Vertrauensliste verwendet wurde, wird in Klammern hinter dem angezeigten Niveau aufgeführt. Kann als Typ "Siegel" oder "Website-Authentisierung" ermittelt werden, wird der entsprechende Typ angezeigt.

Kann zwar ein zertifikatsausstellender Dienst in der EUMS-TL ermittelt werden, der Dienst wurde aber zum Zeitpunkt der Ausstellung des Zertifikats nicht mehr durch die Aufsichtsbehörde überwacht oder die dortige Konfiguration genügt nicht den Anforderungen wird dem ermittelten Niveau ein "Kein/Keine" vorangestellt. Erfolgt die Niveauermittlung auf Basis der Angaben in der Governikus-TL oder einer Custom-TL, kann keine Negativaussage erfolgen, da die in diesen Vertrauenslisten konfigurierten Dienste den Status "nicht überwacht" besitzen.

Kann das Niveau des Zertifikats nicht auf Basis einer der drei Typen von Vertrauenslisten bestimmt werden, wird "Digitales Zertifikat" angezeigt.

Nach Aufklappen des Knotens werden das Ergebnis der Ermittlung sowie die Entscheidungsgrundlagen angezeigt, die für die Ermittlung des Niveaus herangezogen wurden. Eine Beschreibung der einzelnen Entscheidungsgrundlagen befindet sich in Kapitel 4.

### 3.2.9 Zeile "Behaupteter Signaturzeitpunkt"

In der Zeile "Behaupteter Signaturzeitpunkt" wird das Datum und die Uhrzeit (in der Form TT.MM.JJJJ hh:mm:ss) angezeigt, zu dem die signierende Person oder Organisation behauptet, die Signatur bzw. das Siegel erstellt zu haben. Dieses ist in der Regel die lokale Zeit des Rechners, an dem signiert wurde. Gemäß aktueller ETSI-Normierung ist der behauptete Signaturzeitpunkt immer anzuzeigen, unabhängig davon, ob dieser Zeitpunkt tatsächlich auch als Prüfzeitpunkt (validation time) verwendet wurde.

Bei der Prüfung eines Dokuments mit einem Zeitstempel ist der "Behauptete Signaturzeitpunkt" immer der Erstellungszeitpunkt des Zeitstempels (`genTime`). Bei einer separaten Zertifikatsprüfung ist der "Behauptete Signaturzeitpunkt" immer der Erstellungszeitpunkt des End-Entity-Zertifikats (Beginn der Gültigkeit `notBefore`).

### 3.2.10 Optionale Zeile "Eingangszeitpunkt auf dem Server als Zeitmarke"

Die optionale Zeile "Eingangszeitpunkt auf dem Server als Zeitmarke" ist nur vorhanden, wenn eine OSCI-Nachricht mit einer Containersignatur validiert wurde. In diesem Fall wird das Datum und die Uhrzeit (in der Form `TT.MM.JJJJ hh:mm:ss`) angezeigt, zu dem die OSCI-Nachricht auf dem OSCI-Server eingegangen ist. Dieses ist in der Regel eine synchronisierte Serverzeit. Da OSCI-Containersignaturen keinen lokalen Erstellungszeitpunkt besitzen ist diese Zeitmarke der Prüfzeitpunkt der Containersignatur. Wird eine der Governikus Prüfrichtlinien verwendet ist dieses immer der Fall. Andere Prüfrichtlinien, die ein anderes Vertrauensniveau des Prüfzeitpunkts verlangen, können den Zeitpunkt der Gültigkeitsprüfung verschieben.

### 3.2.11 Optionale Zeile "Zeitpunkt des Signaturzeitstempels"

Die optionale Zeile "Zeitpunkt des Signaturzeitstempels" ist nur vorhanden, wenn in der Signatur ein Signaturzeitstempel ermittelt werden konnte. In diesem Fall werden das Datum und die Uhrzeit (in der Form `TT.MM.JJJJ hh:mm:ss`) angezeigt, zu dem die Inhaltsdatensignatur mit einem Zeitstempel versehen wurde. Gemäß der aktuellen ETSI-Normierung ist der Zeitpunkt der Zeitstempelung immer anzuzeigen, unabhängig davon ob die Prüfung des Zeitstempels erfolgreich gewesen ist oder ob dieser Zeitpunkt tatsächlich auch als Prüfzeitpunkt verwendet wurde.

### 3.2.12 Optionale Zeile "Ergebnis der Prüfung des Signaturzeitstempels" mit Knoten

Die optionale Zeile "Ergebnis der Prüfung des Signaturzeitstempels" ist nur vorhanden, wenn ein Signaturzeitstempel ermittelt werden konnte. In diesem Fall wird das Ergebnis der Signaturprüfung des Zeitstempels angezeigt. Folgende Werte sind möglich:

- **gültig** (grün gültig): Alle gemäß Prüfrichtlinie notwendigen Einzelprüfungen sind erfolgreich verlaufen. Es handelt sich gemäß den Vorgaben in der Prüfrichtlinie zum angezeigten Prüfzeitpunkt mit dem angegebenen Vertrauensniveau des Prüfzeitpunkts um einen gültigen Signaturzeitstempel.
- **unbestimmt** (gelb unbestimmt): Mindestens eine, gemäß Prüfrichtlinie notwendige, Einzelprüfung konnte nicht durchgeführt werden oder lieferte ein unbestimmtes Ergebnis zurück. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.
- **ungültig** (rot ungültig): Mindestens eine gemäß Prüfrichtlinie notwendige Einzelprüfung ist endgültig fehlgeschlagen. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.

Die Anzeige des Prüfergebnisses des Zeitstempels ist - wenn eine der Governikus Prüfrichtlinien verwendet wird - rein informativ und hat keinen Einfluss auf das Ergebnis der Inhaltsdatensignaturprüfung. Auch verschiebt ein gültiger Signaturzeitstempel nicht den Prüfzeitpunkt der Signatur, da in allen Governikus Prüfrichtlinien als ausreichendes Vertrauensniveau des Prüfzeitpunktes der behauptete Signaturzeitpunkt konfiguriert ist.

Nach dem Aufklappen des Knotens werden die einzelnen Prüfergebnisse angezeigt. Eine Beschreibung findet sich im Kapitel 6.

### 3.2.13 Alternative Zeilen "Prüfzeitpunkt der Signatur", "Prüfzeitpunkt des Zeitstempels" oder "Prüfzeitpunkt des Zertifikats"

#### Zeile "Prüfzeitpunkt der Signatur"

Bei der Validierung einer Inhaltsdatensignatur wird in der Zeile "Prüfzeitpunkt der Signatur" das Vertrauensniveau angezeigt, zu dem die Gültigkeit der Signatur ermittelt wurde. Folgende Niveaus wurden in Rahmen der ETSI-Normierung festgelegt:

- Behaupteter Signaturzeitpunkt,
- Zeitmarke,
- Signaturzeitstempel (Nicht-qualifizierter Zeitstempel oder Nicht-qualifizierter Zeitstempel eines VDA zur Augmentierung von QES oder Nicht-qualifizierter Zeitstempel eines qVDA zur Augmentierung von QES oder EU-qualifizierter elektronischer Zeitstempel oder qualifizierter Zeitstempel gemäß SigG)
- Zeitpunkt der Durchführung der Prüfung.

Das konkrete Datum und die Zeit für den Prüfzeitpunkt beim angegebenen Vertrauensniveau ist der Datums- und Zeitangabe in der entsprechenden Zeile des Prüfprotokolls zu entnehmen (Zeile "Behaupteter Signaturzeitpunkt", Zeile "Zeitmarke", Zeile "Signaturzeitstempel" oder Zeile "Zeitpunkt der Durchführung der Prüfung" im Prüfprotokoll). Wird eine Governikus Prüfrichtlinie verwendet, dann ist das verwendete Vertrauensniveau der behauptete Signaturzeitpunkt (claimed signing time), bei OSCI-Containersignaturen ist das Vertrauensniveau die Zeitmarke „Eingang auf dem Server“.

Das hier angegebene Vertrauensniveau des Prüfzeitpunktes der Signaturprüfung bezieht sich immer auf den Prüfzeitpunkt der Inhaltsdatensignatur. Wurde als Gültigkeitsmodell der Signaturzertifikatskette das Schalenmodell ausgewählt, dann wird der angegebene Prüfzeitpunkt der Inhaltsdatensignatur auch als Prüfzeitpunkt der Zertifikate der Signaturzertifikatskette verwendet. Beim Kettenmodell wird der angegebene Zeitpunkt nur für die Prüfung des Signaturzertifikats verwendet. Bei CA- und Root-Zertifikaten erfolgt die Prüfung zum Erstellungszeitpunkt des jeweils ausgestellten Zertifikats (*notBefore*). Eine detaillierte Erläuterung befindet sich im Kapitel 5.5.14.

#### Zeile "Prüfzeitpunkt des Zeitstempels"

Die Validierung eines Zeitstempels erfolgt immer zum Anbringungszeitpunkt des Zeitstempels (*genTime*). Als Vertrauensniveau wird "behaupteter Signaturzeitpunkt" angezeigt.

#### Zeile "Prüfung des Zertifikats"

Bei der Prüfung der Gültigkeit eines einzelnen End-Entity-Zertifikats vom Typ Signatur- oder Siegelzertifikat oder Zertifikat für Website-Authentisierung können in der Zeile "Prüfzeitpunkt des Zertifikats" folgende Niveaus angezeigt werden:

- **Übergebener Zeitpunkt:** Die Gültigkeitsprüfung wurde zu einem übergebenen Prüfzeitpunkt durchgeführt. Ein Vertrauensniveau ist mit dem Prüfzeitpunkt nicht verbunden.
- **Zeitpunkt der Durchführung der Prüfung:** Wird kein Prüfzeitpunkt übergeben, wird automatisch als Prüfzeitpunkt der Zeitpunkt der Durchführung der Prüfung ausgewählt und angezeigt.

Wurde als Gültigkeitsmodell das Schalenmodell ausgewählt, dann wird der übergebene Prüfzeitpunkt auch als Prüfzeitpunkt der Zertifikate der Signaturzertifikatskette verwendet. Beim

Kettenmodell wird der angegebene Zeitpunkt nur für die Prüfung des Signaturzertifikats verwendet. Bei CA- und Root-Zertifikaten erfolgt die Prüfung zum Erstellungszeitpunkt des jeweils ausgestellten Zertifikats (notBefore).

### 3.2.14 Alternative Zeilen "Ergebnis der Signaturprüfung", "Ergebnis der Zeitstempelprüfung" oder "Prüfzeitpunkt des Zertifikats" mit Knoten

Wird eine Inhaltsdatensignatur geprüft, wird in der Zeile "Ergebnis der Signaturprüfung" das Gesamtergebnis der Signaturprüfung angezeigt. Wird ein Zertifikat separat geprüft, wird in der Zeile "Ergebnis der Zertifikatsprüfung" das Ergebnis der Gültigkeitsprüfung des Zertifikats angezeigt. Wird ein detached Inhaltsdatenzeitstempel geprüft, wird in der Zeile "Ergebnis der Zeitstempelprüfung" das Gesamtprüfergebnis Prüfung des Zeitstempels angezeigt.

In den folgenden Abschnitten werden die möglichen Werte der Anzeige erläutert.

#### Zeile "Ergebnis der Signaturprüfung"

In der Zeile "Ergebnis der Signaturprüfung" wird das Gesamtergebnis der Prüfung einer Inhaltsdatensignatur angezeigt. Folgende Werte sind für den Gesamtstatus möglich:

- **gültig** (grün gültig): Alle gemäß Prüfrichtlinie notwendigen Einzelprüfungen sind erfolgreich verlaufen. Es handelt sich um eine technisch gültige Signatur mit dem angegebenen Niveau und dem angezeigten Typ gemäß den Vorgaben in der Prüfrichtlinie zum angezeigten Prüfzeitpunkt mit dem angegebenen Vertrauensniveau des Prüfzeitpunkts.
- **unbestimmt** (gelb unbestimmt): Mindestens eine gemäß Prüfrichtlinie notwendige Einzelprüfung konnte nicht durchgeführt werden oder lieferte ein unbestimmtes Ergebnis zurück. Keine durchgeführte Einzelprüfung ist endgültig fehlgeschlagen (Prüfergebnis rot ungültig). In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.
- **ungültig** (rot ungültig): Mindestens eine gemäß Prüfrichtlinie notwendige Einzelprüfung ist endgültig fehlgeschlagen. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.

Das Gesamtprüfergebnis kumuliert alle durchgeführten Einzelprüfergebnisse, die durch die Anwendung des Validierungsalgorithmus ermittelt wurden. Der Validierungsalgorithmus ist in der ETSI-Norm EN 319 102-1 (Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation) beschrieben. Er wird zutreffend angewendet, wenn eine der durch die Governikus KG erstellten Prüfrichtlinien verwendet wurde.

Nach Aufklappen des Knotens der Zeile "Ergebnis der Signaturprüfung" werden die Einzelprüfergebnisse der Integritätsprüfung und die Zertifikatsprüfungen angezeigt, die zum Gesamtstatus der Signatur geführt haben. Eine Beschreibung der Einzelprüfergebnisse finden Sie in Kapitel 5.

#### Zeile "Ergebnis der Zeitstempelprüfung"

Bei der Prüfung eines detached Inhaltsdatenzeitstempels wird statt der Zeile "Ergebnis der Signaturprüfung" die Zeile "Ergebnis der Zeitstempelprüfung" mit Knoten angezeigt. Folgende Werte sind für das Gesamtprüfergebnis möglich:

- **gültig** (grün gültig): Alle gemäß Prüfrichtlinie notwendigen Einzelprüfungen sind erfolgreich verlaufen. Es handelt sich um einen technisch gültigen Zeitstempel mit dem angegebenen Niveau zum angezeigten Prüfzeitpunkt.
- **unbestimmt** (gelb unbestimmt): Mindestens eine gemäß Prüfrichtlinie notwendige Einzelprüfung konnte nicht durchgeführt werden oder lieferte ein unbestimmtes Ergebnis

zurück. Keine durchgeführte Einzelprüfung ist endgültig fehlgeschlagen (Prüfergebnis rot ungültig). In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.

- **ungültig** (rot ungültig): Mindestens eine gemäß Prüfrichtlinie notwendige Einzelprüfung ist endgültig fehlgeschlagen. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.

Nach Aufklappen des Knotens der Zeile "Ergebnis der Zeitstempelprüfung" werden die Einzelprüfergebnisse der Integritätsprüfung und die Zertifikatsprüfungen angezeigt, die zum Gesamtstatus der Signatur geführt haben. Eine Beschreibung der Einzelprüfergebnisse finden Sie in Kapitel 5.

### Zeile "Ergebnis der Zertifikatsprüfung"

In der Zeile "Ergebnis der Zertifikatsprüfung" wird das Gesamtergebnis der Gültigkeitsprüfung eines einzelnen Zertifikats angezeigt. Folgende Werte sind für den Gesamtstatus möglich:

- **gültig** (grün gültig): Alle gemäß Prüfrichtlinie notwendigen Einzelprüfungen sind erfolgreich verlaufen. Es handelt sich um ein technisch gültiges Zertifikat mit dem angegebenen Niveau zum angezeigten Prüfzeitpunkt.
- **unbestimmt** (gelb unbestimmt): Mindestens eine gemäß Prüfrichtlinie notwendige Einzelprüfung konnte nicht durchgeführt werden oder lieferte ein unbestimmtes Ergebnis zurück. Keine durchgeführte Einzelprüfung ist endgültig fehlgeschlagen (Prüfergebnis rot ungültig). In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.
- **ungültig** (rot ungültig): Mindestens eine gemäß Prüfrichtlinie notwendige Einzelprüfung ist endgültig fehlgeschlagen. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.

Nach Aufklappen des Knotens der Zeile "Ergebnis der Zertifikatsprüfung" werden die Einzelprüfergebnisse der einzelnen Zertifikatsprüfungen angezeigt, die zum Gesamtstatus geführt haben. Eine Beschreibung der Einzelprüfergebnisse finden Sie in Kapitel 5.4.

### 3.2.15 Optionale Zeile "Beweiswertbewahrung durch Archivzeitstempel" mit Knoten

Die optionale Zeile "Beweiswertbewahrung durch Archivzeitstempel" mit Knoten ist nur vorhanden, wenn ein Archivzeitstempel ermittelt werden konnte. Die Anzeige des kumulierten Ergebnisses der Prüfung des Archivzeitstempels erfolgt unabhängig davon, ob der Zeitstempel den Beweiswert tatsächlich sichern konnte.

In der Zeile "Ergebnis der Zeitstempelprüfung" wird im Ergebnis der Prüfung angezeigt, ob der Archivzeitstempel zum Zeitpunkt der Durchführung der Prüfung technisch noch geeignet ist, den Beweiswert einer EU-qualifizierten Signatur zu bewahren. Damit ist keine Aussage verbunden, ob die Anbringung des EU-qualifizierten Archivzeitstempels rechtzeitig vor dem Schwachwerden des für die Inhaltsdatensignatur verwendeten Signaturalgorithmus erfolgt ist.

Folgende Werte sind möglich:

- **gültig** (grün gültig): Alle gemäß Prüfrichtlinie notwendigen Einzelprüfungen sind erfolgreich verlaufen. Es handelt sich gemäß den Vorgaben in der Prüfrichtlinie um einen gültigen EU-qualifizierten Archivzeitstempel, der technisch geeignet ist, den Beweiswert einer EU-qualifizierten Signatur zu bewahren.
- **unbestimmt** (gelb unbestimmt): Mindestens eine gemäß Prüfrichtlinie notwendige Einzelprüfung konnte nicht durchgeführt werden oder lieferte ein unbestimmtes Ergebnis

zurück. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.

- **ungültig** (rot ungültig): Mindestens eine gemäß Prüfrichtlinie notwendige Einzelprüfung ist endgültig fehlgeschlagen. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.

Mit einem gültigen EU-qualifizierten Archivzeitstempel ist es technisch möglich, einen noch zum Zeitpunkt der Zeitstempelung vorhandenen Beweiswert einer EU-qualifizierten Signatur zu bewahren. Ob dieses tatsächlich gelungen ist, kann dem Ergebnis der Signaturprüfung (siehe Zeile "Ergebnis der Signaturprüfung") entnommen werden. Ist das kumulierte Prüfergebnis "gültig", dann wird bei der Ermittlung der Eignung des Signaturalgorithmus für eine QES berücksichtigt, dass die Eignung nur zum Zeitpunkt der Erstellung des EU-qualifizierten Archivzeitstempels noch gegeben gewesen sein muss und nicht mehr zum Zeitpunkt der Durchführung der Signaturprüfung.

Ein EU-qualifizierter Archivzeitstempel gemäß der EU-Normierung sichert nicht nur den Beweiswert der Inhaltsdatensignatur, sondern auch den Beweiswert aller in der Signatur vorhandenen Zertifikatssignaturen und signierten OCSP-Antworten/CRLs. Dies bedeutet, dass auch für diese Signaturen die Eignung der verwendeten Signaturalgorithmen zum Erstellungszeitpunkt des EU-qualifizierten Archivzeitstempels ermittelt wird. Das kumulierte Ergebnis der Signaturprüfung der Inhaltsdaten umfasst auch diese Prüfergebnisse.

Nach Aufklappen des Knotens "Beweiswertbewahrung durch Archivzeitstempel" werden Ergebnisse der Prüfung des Archivzeitstempels bzw. des ERS mit Archivzeitstempel angezeigt. Eine detaillierte Beschreibung des aufgeklappten Knotens befindet sich in Kapitel 7.

Sollten mehrere Archivzeitstempel oder mehrere Hashwertbäume mit einem Archivzeitstempel oder mehreren Archivzeitstempeln die Signatur absichern, wird die in den folgenden Unterkapiteln erläuterte Anzeige im Prüfprotokoll untereinander wiederholt. Eine detaillierte Beschreibung des aufgeklappten Knotens befindet sich in Kapitel 7.

### 3.3 Bereich C "Technischer Anhang"

Im Anhang Bereich C "Technischer Anhang" werden im aufgeklappten Knoten "Prüfrichtlinien" die im Kontext der Signaturprüfung verwendeten Prüfrichtlinien vollständig angezeigt (siehe Kapitel 10.1). Es folgen im aufgeklappten Knoten "Vertrauenslisten" Detailinformationen zu den verwendeten Vertrauenslisten (siehe Kapitel 10.2). Im aufgeklappten Knoten "Algorithmenkataloge" folgen Detailinformationen zu den verwendeten Algorithmenkatalogen (siehe Kapitel 10.3). Im aufgeklappten Knoten "Prüfinstanz" (Kapitel 10.4) wird schließlich angezeigt, welche Prüfinstanz (URL) auf der Basis welcher Produktversion und CSL die Prüfung durchgeführt hat.

| Technischer Anhang |                                      |
|--------------------|--------------------------------------|
| +                  | Prüfrichtlinien                      |
| +                  | Vertrauenslisten (mit Erweiterungen) |
| +                  | Algorithmenkataloge                  |
| +                  | Prüfinstanz                          |

Abbildung 8: Hauptseite Prüfprotokoll Bereich C "Technischer Anhang"

## 4 Bereich B Knoten "Niveau" aufgeklappt

In diesem Kapitel wird der Teil des Prüfprotokolls beschrieben, der nach dem Aufklappen des Knotens in der alternativen Zeile "Niveau und Typ der Signatur" oder "Niveau und Typ des Zertifikats" oder "Niveau des Zeitstempels" im Bereich B der Hauptseite des Prüfprotokolls angezeigt wird.

Zu dem Ergebnis der Ermittlung des Niveaus und des Typs der Signatur, des separat geprüften Zertifikats oder des Zeitstempels, werden im aufgeklappten Knoten ergänzende Erläuterungen als Meldungstexte sowie die einzelnen Entscheidungsgrundlagen angezeigt, die für die Ermittlung des Niveaus und ggf. des Typs herangezogen wurden.

| Niveau und Typ der Signatur:   | EU-qualifizierte elektronische Signatur (EUMS-TL)  |
|--|--|
| <b>Ermittlung des Signaturniveaus und des Typs</b>   |  |
| Ergebnis:  | EU-qualifizierte elektronische Signatur (EUMS-TL)  |
| Meldungen:   | Es wurde ermittelt, ob das digitale Zertifikat als ein EU-qualifiziertes Zertifikat für elektronische Signaturen, Siegel oder Website Authentifizierung ausgestellt wurde. Bei Signaturen und Siegeln wurde zusätzlich ermittelt, ob sich die Signaturerstellungsdaten auf einer QSCD befinden. Die Ermittlung erfolgte auf Basis einer hoheitlichen Vertrauensliste (EUMS-TL).<br>EU-qualifiziertes Zertifikat bestätigt durch Angaben im Zertifikat und in der verwendeten EUMS-TL. Die Signaturerstellungsdaten befinden sich auf einer QSCD. |
| <b>Entscheidungsgrundlagen laut Vertrauensliste</b>  |  |
| Diensteanbieter:   | Bundesnotarkammer  |
| Dienstetyp:  | Qualifizierter Vertrauensdienst zur Generierung von qualifizierten Zertifikaten ( <a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a> )  |
| Dienststatus:  | Gewährt ( <a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</a> )  |
| Ermittlungszeitpunkt des Dienststatus:   | 29.01.2019, 14:13:21   |
| Startdatum des Dienststatus:   | 13.06.2018, 15:30:00   |
| Zusätzliche Qualifizierungen des Zertifikats:  | Zertifikat für elektronische Signaturen ( <a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a> )  |
| Link zu Details der verwendeten Vertrauensliste:   | <a href="#">Vertrauensliste #1</a>   |
| <b>Entscheidungsgrundlagen laut Angaben des VDA im Zertifikat</b>  |  |
| <ul style="list-style-type: none"> <li>• Zertifikat für elektronische Signaturen gemäß eIDAS-Verordnung</li> <li>• Qualifiziertes Zertifikat gemäß Signatordirektive oder eIDAS-Verordnung</li> <li>• Privater Schlüssel und öffentlicher Schlüssel im qualifizierten Zertifikat auf SSCD gemäß EU-Signatordirektive oder auf QSCD gemäß eIDAS-Verordnung</li> </ul> |  |

Abbildung 9: Knoten "Niveau und Typ der Signatur" aufgeklappt (EU-qualifizierte Signatur)

Die Ermittlung des Niveaus und des Typs basiert immer auf der Auswertung der Angaben aus einer Vertrauensliste. Drei Typen von Vertrauenslisten können für die der Ermittlung herangezogen werden:

- Die EUMS-TL (**E**uropean **U**nion **M**ember **S**tate **T**rusted **L**ist) ist die von der nationalen Aufsichtsbehörde eines EU-Mitgliedstaates herausgegebene Vertrauensliste. In ihr sind mindestens alle von qualifizierten Vertrauensanbietern angebotenen Dienste, die Signaturzertifikate herausgeben oder Zeitstempeltoken erstellen konfiguriert.
- Die Governikus-TL ist die von Governikus KG herausgegebene Vertrauensliste. Sie enthält ausschließlich konfigurierte Dienste deutscher Vertrauensdiensteanbieter, die fortgeschrittene Signaturzertifikate ausstellen, die nicht in der EUMS-TL aus Deutschland konfiguriert sind.

Hinweis: In die Governikus-TL wird ein zertifikatsausstellender Dienst nur dann aufgenommen, wenn der Dienst nachweislich (laut Selbstaussage des VDA z.B. im CP-Dokument oder über einen CP-Identifizierer im Zertifikat) einer Zertifikatsrichtlinie der Niveaus LCP, NCP oder NCP+ genügt. Zur genauen inhaltlichen Beschreibung der Richtlinien siehe EN 319 411-1.



- Die Custom-TL ist eine Vertrauensliste, die Betreiber eines Certificate Validation Servers optional herausgeben können, um die Vertrauensstellung von eigenen PKIs zu konfigurieren. Sie darf ausschließlich zertifikatsausstellende Dienste deutscher Vertrauensdiensteanbieter enthalten, die nicht schon in der EUMS-TL aus Deutschland oder in der Governikus TL konfiguriert sind.

Notwendige Bedingungen für die zutreffende und vertrauenswürdige Ermittlung des Niveaus und des Typs einer Signatur, sind die Gültigkeit der Signatur der Vertrauensliste und die positive Prüfung der zeitlichen Gültigkeit der Vertrauensliste. Die Prüfergebnisse zu beiden Prüfungen werden im aufgeklappten Knoten 5.6 angezeigt. Ist mindestens eine der beiden Prüfungen negativ, wird daher als Niveau nur "Digitale Signatur", "Digitaler Zeitstempel" oder "Digitales Zertifikat" angezeigt. Ein Meldungstext erläutert die Ursache des Prüfergebnisses. Den in den folgenden Zeilen aufgeführten Entscheidungsgrundlagen zur Niveau- und Typbestimmung darf in diesem Fall nicht vertraut werden.

Sind beide Prüfungen positiv verlaufen und kann für das Signaturzertifikat oder den Zeitstempeltoken ein Service Digital Identifier (SDI) ermittelt werden, wird auch das in der Vertrauensliste konfigurierte Niveau des zertifikats- oder zeitstempelausstellenden Dienstes angezeigt. In Abhängigkeit vom Typ der verwendeten Vertrauensliste sind in diesem Fall folgende Unterschiede zu beachten:

Für in der EUMS-TL konfigurierte Dienste werden Negativ-Aussagen zum Niveau angezeigt (Beispiel: "EU-qualifizierte elektronische Signatur (EUMS-TL)" oder "Keine EU-qualifizierte elektronische Signatur (EUMS-TL)"),

- a) wenn zwar ein Dienst in der EUMS-TL über den SDI-Eintrag ermittelt werden konnte,
- b) der Dienst aber zum Zeitpunkt der Zertifikatsausstellung oder Erzeugung des Zeitstempeltokens nicht mehr oder noch nicht durch die Aufsichtsbehörde überwacht wurde und/oder
- c) die Konfiguration des Dienstes in der EUMS-TL nicht den technischen Anforderungen (siehe EU-Beschluss EU 2015/1505 und ETSI TS 119 612, 119 615 und 119 172-4) genügte und/oder
- d) die Niveauangaben im Zertifikat (QCStatement, Zertifizierungsrichtlinie, Trade Name, etc.) nicht widerspruchsfrei zu den Angaben in der EUMS-TL waren.

Erfolgt die Niveauermittlung demgegenüber auf Basis der Angaben in der Governikus-TL oder einer Custom-TL, kann keine Negativaussage erfolgen, da die in diesen Vertrauenslisten konfigurierten Dienste den Status "nicht überwacht" besitzen und keine zusätzlichen konfigurativen Anforderungen durch ETSI definiert wurden.

Auch ohne Überwachungsstatus lässt sich für fortgeschrittene Signaturen das Signaturniveau zuverlässig bestimmen, da das als Dienste-Identifizier (SDI) konfigurierte CA-Zertifikat durch den Vertrauensdiensteanbieter gesperrt wird, wenn die Voraussetzungen für die Dienststeuerbringung (hier: Ausstellung von Signaturzertifikaten) nicht mehr gegeben sind. Da die hier konfigurierten SDIs nicht als Trusted Anchor (TA) verwendet werden (wenn als Prüfrichtlinie die Governikus Prüfrichtlinie für fortgeschrittene Signaturen verwendet wurde), kann bei der Ermittlung des Sperrstatus des CA-Zertifikats festgestellt werden, ab wann die Voraussetzungen für die Dienststeuerbringung nicht mehr gegeben sind.

Eine weitere Besonderheit gibt es bei der Ermittlung des Niveaus von EU-qualifizierten Signaturen, die zweistufig durchgeführt wird. Zunächst wird das Niveau des Signaturzertifikats ermittelt. Wird im Positivfall (siehe Aufzählung oben: a) zutreffend und b) bis d) nichtzutreffend) als Niveau "EU-qualifiziertes Zertifikat" ermittelt, handelt es sich bei der Signatur mindestens um eine "Fortgeschrittene elektronische Signatur, unterstützt durch ein EU-qualifiziertes Zertifikat (EUMS-TL)". Ist im Zertifikat im QCStatement zusätzlich der Eintrag "SSCD" oder "QSCD"

vorhanden, ist der Nachweis erbracht, dass sich der private Signaturschlüssel und das Signaturzertifikat mit Signaturprüf Schlüssel auf einer notifizierten qualifizierten sicheren Signaturerstellungseinheit befinden und deshalb die technischen Voraussetzungen für eine "EU-qualifizierte elektronische Signatur (EUMS-TL)" gegeben sind. Ist im QCStatement explizit der Typ "Siegel" angegeben, handelt es sich um ein "EU-qualifiziertes elektronisches Siegel (EUMS-TL)".

Kann das Niveau einer Signatur nicht auf Basis der vorliegenden gültigen Vertrauenslisten bestimmt werden, weil kein konfigurierter SDI ermittelt werden kann, wird als Wert "Digitale Signatur" und ein erläuternder Meldungstext angezeigt. Die digitale Signatur kann gleichwohl trotzdem technisch gültig geprüft werden. Die digitale Signatur ist allerdings technisch nicht geeignet, eine elektronische Signatur im Sinne der zum Zeitpunkt der Signaturerstellung geltenden europäischen Rechtsvorschriften (EU-Signaturrichtlinie oder eIDAS-Verordnung) darzustellen. Sinngemäß gilt dieses dann auch für digitale Zeitstempel oder Zertifikate.

Hinweis: Der Knoten ist generisch aufgebaut und wird sinngemäß auch für die Anzeige der Ergebnisse der Ermittlung des Niveaus von Zeitstempeln und des Niveaus und Typs von separat geprüften Zertifikaten verwendet.

### **Exkurs: Vertrauensanker aus EUMS-TL**

Zertifikate, die in der EUMS-TL als Dienste Identifier (SDI) verwendet werden, dürfen als Vertrauensanker (Trusted Anchor) verwendet werden, falls den Angaben in der EUMS-TL vertraut werden kann und der in einer EUMS-TL konfigurierte Dienst zum übergebenen Ermittlungszeitpunkt den Status "überwacht" besitzt. In diesem Fall muss z.B. der Sperrstatus vom konfigurierten Zertifikaten nicht mehr ermittelt oder die Signatur dieses Zertifikats nicht mehr geprüft werden.

Wird über die automatische Prüfrichtlinienauswahl eine der Governikus-Prüfrichtlinien für EU-qualifizierte Signaturen ausgewählt, werden folgende Service Digital Identifier (SDI) aus EUMS-TL als Vertrauensanker verwendet:

- SDI für zertifikatsausstellende Dienste (CA-Zertifikate), unabhängig vom in der EUMS-TL konfigurierten Niveau des Dienstes.
- SDI für Zeitstempeldienste (meist EE-Zertifikate) unabhängig vom in der EUMS-TL konfigurierten Niveau des ausgestellten Zeitstempeltokens.
- SDI für Sperrstatusdienste (meist EE-Zertifikate) unabhängig vom in der EUMS-TL konfigurierten Niveau des Sperrdienstes.

Konfigurierte SDI in der Governikus-TL oder Custom-TL fungieren demgegenüber nie als Vertrauensanker, da den Schema-Verantwortlichen der Governikus KG oder einer Custom-TL keine Informationen zum Status der Dienste vorliegen.

## **4.1 Alternative Überschrift "Ermittlung des Signaturniveaus und des Typs" oder "Ermittlung des Zertifikatniveaus und des Typs" oder "Ermittlung Zeitstempelniveaus und des Typs"**

Unter der alternativen Überschrift "Ermittlung des Signaturniveaus und des Typs" oder "Ermittlung des Zertifikatniveaus und des Typs" oder "Ermittlung Zeitstempelniveaus und des Typs" werden das Ermittlungsergebnis und erläuternde Meldungstexte angezeigt.

### **4.1.1 Zeile "Ergebnis"**

Je nach Prüfgegenstand werden in der Zeile "Ergebnis" das ermittelte Niveau und der Typ der Signatur, das Niveau und der Typ des Zertifikats oder das Niveau des Zeitstempels angezeigt.

|   |  |
|---|--|
| Niveau und Typ des Zeitstempels:  | EU-qualifizierter Zeitstempel (EUMS-TL)  |
| <b>Ermittlung des Zeitstempelniveaus und des Typs</b>                   |  |
| Ergebnis:   | EU-qualifizierter Zeitstempel (EUMS-TL)  |
| Meldungen:  | Prüfung, ob der Zeitstempel als ein qualifizierter europäischer Zeitstempel erstellt und signiert wurde im Sinne der geltenden europäischen Rechtsvorschriften. Die Prüfung erfolgt in Anlehnung an ETSI TS 119172-4 unter der Verwendung einer Vertrauensliste (EUMS-TL). |
| <b>Entscheidungsgrundlagen laut Vertrauensliste</b>                     |  |
| Diensteanbieter:  | exceet Secure Solutions GmbH   |
| Dienstetyp:   | Qualifizierter Zeitstempeldienst zur Erstellung und Signatur von EU-qualifizierten Zeitstempeln ( <a href="http://uri.etsi.org/TrstSvc/SvcType/TSA/QTST">http://uri.etsi.org/TrstSvc/SvcType/TSA/QTST</a> )  |
| Dienststatus:   | Gewährt ( <a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</a> )  |
| Ermittlungszeitpunkt des Dienststatus:                                  | 18.06.2019, 15:13:38   |
| Startdatum des Dienststatus:  | 26.10.2016, 12:00:00   |
| Link zu Details der verwendeten Vertrauensliste:                        | <a href="#">Vertrauensliste #1</a>   |
| <b>Entscheidungsgrundlagen laut Angaben des VDA im Zeitstempeltoken</b> |  |
| nicht vorhanden   |  |

Abbildung 10: Knoten "Niveau und Typ der Signatur" aufgeklappt (EU-qualifizierter Zeitstempel)

### Angezeigte Niveaus von Signaturen und Siegeln

Folgende Niveaus mit Typ sind für Signaturen gemäß eIDAS-VO bzw. der zugehörigen Normierung definiert oder abgeleitet worden und werden angezeigt:

- Positivfälle:
  - EU-qualifizierte elektronische Signatur (EUMS-TL)
  - Fortgeschrittene elektronische Signatur unterstützt durch ein EU-qualifiziertes Zertifikat für die elektronische Signatur (EUMS-TL)
  - Fortgeschrittene elektronische Signatur (EUMS-TL oder Governikus-TL oder Custom-TL)
- Negativfälle
  - Keine EU-qualifizierte elektronische Signatur (EUMS-TL)
  - Keine fortgeschrittene elektronische Signatur unterstützt durch ein EU-qualifiziertes Zertifikat für die elektronische Signatur (EUMS-TL)
  - Keine fortgeschrittene elektronische Signatur (EUMS-TL)
- Digitale Signatur

Kann als Typ "Siegel" ermittelt werden, wird entsprechend Siegel statt Signatur angezeigt. Eine detaillierte Beschreibung der Niveaus und Typen befindet sich in Kapitel 3.2.8.

### Angezeigte Niveaus von Zeitstempeln

Folgende Niveaus und Typen von Zeitstempeln wurden gemäß eIDAS-VO bzw. der zugehörigen Normierung definiert oder abgeleitet und werden angezeigt:

- Positivfälle:
  - EU-qualifizierter elektronischer Zeitstempel (EUMS-TL)
  - Qualifizierter elektronischer Zeitstempel gemäß SigG (EUMS-TL) (geplant)
  - Nicht-qualifizierter elektronischer Zeitstempel eines qVDA zur Augmentierung von QES (EUMS-TL oder Governikus-TL oder Custom-TL)
  - Nicht-qualifizierter elektronischer Zeitstempel eines VDA zur Augmentierung von QES (EUMS-TL oder Governikus-TL oder Custom-TL)

- Nicht-qualifizierter elektronischer Zeitstempel (EUMS-TL oder Governikus-TL oder Custom-TL)
- Negativfälle
  - Kein EU-qualifizierter elektronischer Zeitstempel (EUMS-TL)
  - Kein nicht-qualifizierter elektronischer Zeitstempel eines VDA zur Augmentierung von QES (EUMS-TL)
  - Kein nicht-qualifizierter elektronischer Zeitstempel eines qVDA zur Augmentierung von QES (EUMS-TL)
  - Kein nicht-qualifizierter elektronischer Zeitstempel (EUMS-TL)
- Digitaler Zeitstempel

Eine detaillierte Beschreibung der Niveaus befindet sich in Kapitel 3.2.8.

### Angezeigte Niveaus von End-Entity-Zertifikaten

Folgende Niveaus sind für Zertifikate gemäß eIDAS-VO bzw. der zugehörigen Normierung definiert oder abgeleitet worden und werden angezeigt:

- Positivfälle
  - EU-qualifiziertes elektronisches Zertifikat für Signaturen (EUMS-TL)
  - Fortgeschrittenes elektronisches Zertifikat für Signaturen (EUMS-TL oder Governikus-TL oder Custom-TL)
- Negativfälle
  - Kein EU-qualifiziertes elektronisches Zertifikat für Signaturen (EUMS-TL)
  - Kein fortgeschrittenes elektronisches Zertifikat für Signaturen (EUMS-TL)
- Digitales Zertifikat für Signaturen

Kann statt Typ "Signatur" der Typ "Siegel" oder "Website-Authentisierung" ermittelt werden, wird dieser Typ angezeigt. Eine detaillierte Beschreibung der Niveaus und Typen befindet sich in Kapitel 3.2.8.

#### 4.1.2 Zeile "Meldungen"

Angezeigt werden bei EU-qualifizierten elektronischen Signaturen, bei fortgeschrittenen elektronischen Signaturen basierend auf einem EU-qualifizierten Zertifikat sowie bei EU-qualifizierten Zeitstempeln die in der Normierung vorgesehenen Meldungstexte und eigene Erläuterungen für den Fehlerfall. Für fortgeschrittene elektronische Signaturen oder Zeitstempel werden an die Normierung angelehnte Meldungstexte und Erläuterungen angezeigt.

## 4.2 Überschrift "Entscheidungsgrundlagen laut Vertrauensliste"

Unter der Überschrift "Entscheidungsgrundlagen laut Vertrauensliste" folgen Angaben zum Namen des Diensteanbieters, dem Status des Dienstes und den Diensteeigenschaften aus der verwendeten gültigen Vertrauensliste soweit ein SDI ermittelt werden konnte.

Hinweis: Die Ermittlungsgrundlagen werden immer angezeigt, wenn sie in der Vertrauensliste vorhanden sind. Ihnen dar jedoch nur getraut werden, wenn es sich im Ergebnis (siehe Zeile "Ergebnis", Erläuterung siehe Kapitel 4.1.1) im Niveau um eine Positivaussage handelt (fortgeschrittene Signatur, fortgeschrittene Signatur basierend auf einem EU-qualifizierten Zertifikat oder EU-qualifizierte Signatur).

#### 4.2.1 Zeile "Diensteanbieter"

In der Zeile "Diensteanbieter" wird der Name des Vertrauensdiensteanbieters (VDA), unter dem dieser den Dienst betreibt, angezeigt.

#### 4.2.2 Zeile "Dienstetyp"

In der Zeile "Dienstetyp" wird der Typ des Dienstes angezeigt. Es handelt sich um die in der ermittelten Vertrauensliste für diesen Dienst angegebenen Uniform Resource Identifier (URI), die in Klammern nach der Dienstbeschreibung angegeben wird. Folgende URIs sind im Kontext Zeitstempel und- Signaturprüfung relevant und wurden durch die ETSI-Normierung definiert (Auswahl):

- Nicht qualifizierter Dienst für die Generierung nicht qualifizierter Zertifikate (<http://uri.etsi.org/TrstSvc/Svctype/CA/PKC>)
- Qualifizierter Vertrauensdienst zur Generierung von EU-qualifizierten Zertifikaten (<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>)
- Nicht qualifizierter CRL-Informationdienst (<http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL>)
- Qualifizierter CRL-Informationdienst als Teil eines qualifizierten Vertrauensdienstes zur Generierung von EU-qualifizierten Zertifikaten (<http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC>)
- Qualifizierter OCSP-Informationdienst als Teil eines qualifizierten Vertrauensdienstes zur Generierung von EU-qualifizierten Zertifikaten (<http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC>)
- Nationale Root-CA (<http://uri.etsi.org/TrstSvc/Svctype/NationalRootCA-QC>)
- Nicht qualifizierter Zeitstempeldienst zur Erstellung und Signatur von Zeitstempeln (<http://uri.etsi.org/TrstSvc/Svctype/TSA>)
- Qualifizierter Zeitstempeldienst zur Erstellung und Signatur von EU-qualifizierten Zeitstempeln (<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>)
- Zeitstempeldienst als Teil eines VDA zur Verlängerung der Gültigkeit EU-qualifizierter Signaturen/Siegel (<http://uri.etsi.org/TrstSvc/Svctype/TSA/TSS-AdESQCandQES>)
- Zeitstempeldienst als Teil eines qVDA zur Verlängerung der Gültigkeit EU-qualifizierter Signaturen/Siegel (<http://uri.etsi.org/TrstSvc/Svctype/TSA/TSS-QC>)

Durch einen Klick auf die URI wird die offizielle ETSI-Beschreibung des Dienstes angezeigt.

#### 4.2.3 Zeile "Dienstestatus"

In der Zeile "Dienstestatus" wird der Status des oben angegebenen Dienstes zum Ermittlungszeitpunkt (siehe Zeile Ermittlungszeitpunkt, Erläuterung siehe Kapitel 4.2.4) angezeigt. Dieses ist bei Signaturzertifikaten der Gültigkeitsbeginn des Zertifikats, bei Zeitstempeltoken derstellungszeitpunkt des Tokens.

Der Status wird durch für den in der Zeile "Diensteanbieter" angegebenen VDA und dort für den in der Zeile "Dienstearart" angegebenen Dienst in Abhängigkeit von der Dienstearart gewährt oder anerkannt oder festgelegt. Folgende Bezeichner sind für den Status des Dienstes in Abhängigkeit vom Typ definiert (Auswahl):

- Gewährt (*Granted*) zeigt an, dass der qualifizierte Status des Dienstes gewährt wurde (<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>)

- **Widerrufen (`Withdrawn`)** zeigt an, dass der qualifizierte Status des Dienstes initial nicht gewährt wurde oder zum angegebenen Datum widerrufen wurde (<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>)
- **Anerkannt auf nationaler Ebene (`Recognized at national level`)** zeigt an, dass der nicht qualifizierte Dienst auf nationaler Ebene anerkannt wurde (<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/recognisedatnationallevel>)
- **Veraltet auf nationaler Ebene (`Deprecated at national level`)** zeigt an, dass der Status des nicht qualifizierten Dienstes auf nationaler Ebene zum angegebenen Datum zurückgezogen wurde (<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/deprecatedatnationallevel>)
- **Festgelegt durch nationales Recht (`Set by national law`)** zeigt an, dass der Status des Dienstes durch nationales Recht in Übereinstimmung mit den geltenden europäischen Gesetzen festgelegt und von der zuständigen nationalen Stelle betrieben wird, die die qualifizierten Zertifikate an akkreditierte Vertrauensdienstleister ausstellt (nur für Dienstetyp `.../NationalRootCA-QC`) (<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/setbynationallaw>)
- **Veraltet nach nationalem Recht (`Deprecated at national law`)** zeigt an, dass der Status des Dienstes durch nationales Recht in Übereinstimmung mit den geltenden europäischen Gesetzen seit dem angegebenen Datum veraltet ist (<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/deprecatedbynationallaw>)

Durch einen Klick auf die URI wird die offizielle ETSI-Beschreibung des Status angezeigt.

- **nicht überwacht:** Dienste, die in der Governikus-TL oder der Custom-TL konfiguriert sind, besitzen den Status "nicht überwacht". Dies bedeutet, dass der Status des Dienstes nicht durch den Schema-Verantwortlichen überwacht wird.

#### **4.2.4 Zeile "Ermittlungszeitpunkt des Dienstestatus"**

In der Zeile "Ermittlungszeitpunkt des Dienstestatus" werden das Datum und die Uhrzeit (in der Form `TT.MM.JJJJ hh:mm:ss`) angezeigt zu dem der angezeigte Dienstestatus ermittelt worden ist. Dies ist bei Signaturzertifikaten der Gültigkeitsbeginn des Zertifikats, bei Zeitstempeltoken der Erstellungszeitpunkt des Tokens.

#### **4.2.5 Zeile "Startdatum des Dienstestatus"**

In der Zeile "Startdatum des Dienstestatus" werden das Startdatum und die Uhrzeit (in der Form `TT.MM.JJJJ hh:mm:ss`) des ermittelten Dienstestatus aus der Vertrauensliste angezeigt.

#### **4.2.6 Optionale Zeile "zusätzliche Qualifizierungen des Zertifikats"**

Bei Signaturen oder Siegeln werden hier - soweit vorhanden - die in der EUMS-TL vorhandenen zusätzlichen Qualifizierungen des Dienstes oder der durch den Dienst ausgestellten Zertifikate aufgeführt. Diese Erweiterungen können durch die Aufsichtsbehörde gesetzt werden um z.B.

- anzuzeigen, wie lange ein Dienst Sperrinformationen bereitstellt, nachdem die Zertifikate abgelaufen sind,
- besondere Eigenschaften von EU-qualifizierten Zertifikaten (Typ des Zertifikats, Zertifikat auf QSCD, etc.) zu setzen (die nicht im Zertifikat stehen) oder zu überschreiben,

- Informationen über die Übernahme eines gelisteten Vertrauensdienstes durch einen anderen Vertrauensdiensteanbieter zu geben.

Angezeigt werden Kurzbeschreibungen und die URIs in Klammern. Durch einen Klick auf die URI wird die offizielle ETSI-Beschreibung der Service Information Extension angezeigt. In Governikus TLs oder Custom TLs können Service Information Extensions nicht gesetzt werden.

#### **4.2.7 Zeile "Link zu Details der verwendeten Vertrauensliste"**

In der Zeile "Link zu Details der verwendeten Vertrauensliste" wird der Link zur Detailangabe der verwendeten Vertrauensliste angezeigt. Durch einen Klick auf den Link gelangt man zu den Detailinformationen der Vertrauensliste, die im technischen Anhang stehen. Dort befindet sich auch ein Downloadlink, der es ermöglicht, die maschinenlesbare Vertrauensliste herunterzuladen.

### **4.3 Überschrift "Entscheidungsgrundlagen laut Angaben des VDA im Zertifikat"**

Unter der Überschrift "Entscheidungsgrundlagen laut Angaben des VDA im Zertifikat" folgen Angaben aus dem Signaturzertifikat. Es handelt sich um eine Aufzählung der in den Extensions "QC-Statement" und "Zertifizierungsrichtlinien" des Zertifikats angegebenen Eigenschaften des Dienstes, der Qualität des Zertifikats bzw. der Signatur mit der OID des Merkmals in Klammern. Folgende Angaben sind möglich:

- Zertifikat für elektronische Signaturen eIDAS-Verordnung (OID 0.4.0.1862.1.6.1)
- Qualifiziertes Zertifikat gemäß Signaturdirektive oder eIDAS-Verordnung (OID 0.4.0.1862.1.1),
- Qualifizierte Zertifikatsrichtlinie (OID 0.4.0.194112.1)
- Qualifizierte Zertifikatsrichtlinie für juristische Personen gemäß eIDAS-Verordnung (OID 0.4.0.194112.1.1),
- Qualifizierte Zertifikatsrichtlinie für juristische Personen mit Schlüssel auf QSCD gemäß eIDAS-Verordnung (OID 0.4.0.194112.1.3),
- Qualifizierte Zertifikatsrichtlinie für natürliche Personen gemäß eIDAS-Verordnung (OID 0.4.0.194112.1.0),
- Qualifizierte Zertifikatsrichtlinie für natürliche Personen mit Schlüssel auf QSCD gemäß eIDAS-Verordnung (OID 0.4.0.194112.1.2),
- Qualifizierte Zertifikatsrichtlinie für die Öffentlichkeit gemäß Signaturdirektive (OID 0.4.0.1456.1.2),
- Qualifizierte Zertifikatsrichtlinie für die Öffentlichkeit mit Schlüssel auf SSCD gemäß Signaturdirektive (OID 0.4.0.1456.1.1),
- Qualifizierte Zertifikatsrichtlinie für qualifizierte Website-Zertifikate gemäß eIDAS-Verordnung (OID 0.4.0.194112.1.4),
- Privater Schlüssel und öffentlicher Schlüssel im qualifizierten Zertifikat auf SSCD gemäß Signaturdirektive oder auf QSCD gemäß eIDAS-Verordnung (OID 0.4.0.1862.1.4).

Es handelt sich immer um Selbstaussagen des Dienstes, der das Zertifikat ausgestellt hat.

Wird das Ergebnis der Ermittlung des Niveaus und des Typs eines Zeitstempels angezeigt, wird bei einem EU-qualifizierten Zeitstempel unter der Überschrift "Entscheidungsgrundlagen

laut Angaben des VDA aus dem Zeitstempeltoken" die in der Extension "QC-Statement" des Tokens die folgende angegebene Eigenschaft des Dienstes angezeigt:

- Qualifizierter elektronischer Zeitstempel gemäß ETSI EN 319 422 oder eIDAS-Verordnung (OID 0.4.0.19422.1.1).




## 5 Bereich B Knoten "Ergebnis" aufgeklappt

In diesem Kapitel wird der Teil des Prüfprotokolls beschrieben, der nach dem Aufklappen des Knotens in den alternativen Zeilen "Ergebnis der Signaturprüfung" oder "Ergebnis der Zertifikatsprüfung" oder "Ergebnis der Zeitstempelprüfung" der Hauptseite des Prüfprotokolls angezeigt wird.

Nach dem Aufklappen des Knotens folgt, bei einer Signaturprüfung und bei einer Zeitstempelprüfung", die Darstellung immer dem folgenden Aufbau:

- Zunächst folgen technische Angaben zur verwendeten Prüfrichtlinie und zum verwendeten Algorithmenkatalog für diese Signaturprüfung
- Anschließend werden unter der Überschrift "Integritätsprüfung" die einzelnen Prüfergebnisse zur Integritätsprüfung angezeigt. Eine detaillierte Beschreibung der einzelnen Prüfergebnisse befindet sich im Kapitel 5.3.
- Anschließend folgenden unter der Überschrift "Zertifikatsprüfungen" die Ergebnisse der Prüfungen der Zertifikate der Kette vom Signaturzertifikat bis zu einem Vertrauensanker. Eine detaillierte Beschreibung der einzelnen Prüfergebnisse befindet sich im Kapitel 5.4.

Nach dem Aufklappen des Knotens "Ergebnis der Zertifikatsprüfung" folgt die Darstellung der Prüfergebnisse bei einer separaten Zertifikatsprüfung. Die Darstellung entspricht der Darstellung der Ergebnisse der Prüfungen der Zertifikate der Kette bei einer Signaturprüfung. Eine detaillierte Beschreibung befindet sich im Kapitel 5.4.



**Hinweis:** Die Anzeige der Prüfung einer Signatur im Prüfprotokoll ist generisch und daher im Wesentlichen unabhängig davon, ob eine Inhaltsdatensignatur, eine Zertifikatssignatur, die Signatur einer OCSP-Antwort/einer CRL oder eine Zeitstempelsignatur geprüft wurde. Der implementierte Validierungsalgorithmus und die Anzeige unterscheiden nicht zwischen den unterschiedlichen Kontexten von Signaturen.

|  |  |
|--|--|
| Ergebnis der Signaturprüfung:                      | <b>gültig</b>  |
| Verwendete Prüfrichtlinie:                         | <a href="#">Qualifizierte elektronische Signatur (qVDA aus DE eIDAS-VO) #1</a>   |
| Verwendeter Algorithmenkatalog:                    | <a href="#">Katalog Anwendung Governikus (SOG-IS Agreed Cryptographic Mechanisms v1.2 / BNetzA 2017)</a>   |
| <b>Integritätsprüfung</b>                          |  |
| Strukturspezifische Prüfung:                       | <b>gültig</b>  |
| Mathematische Signaturprüfung:                     | <b>gültig</b>  |
| Signaturalgorithmus:                               | SHA256 RSA (n = 2048) (e = -1712693453) PKCS#1 v1.5  |
| Signaturalgorithmus für QES geeignet bis:          | 31.12.2025, 23:59:59   |
| Ausgewählter Eignungszeitpunkt:                    | EU-qualifizierter elektronischer Zeitstempel   |
| Eignung zu diesem Zeitpunkt:                       | <b>gültig</b>  |
| <b>Zertifikatprüfungen</b>                         |  |
| Gültigkeitsmodell für die Zertifikatskette:        | Schale   |
| Gültigkeitsmodell definiert in:                    | Verwendete Prüfrichtlinie  |
| + Prüfung des Zertifikats von Donald Duck:         | <b>gültig</b>  |
| + Prüfung des Zertifikats von D-TRUST CA 3-1 2016: | <b>nicht geprüft</b>   |
| + Meldungen:                                       | Das Zertifikat ist ein Dienste-Identifizier aus einer gültigen hoheitlichen Vertrauensliste (EUMS-TL). Gemäß verwendeter Prüfrichtlinie ist es damit ein Vertrauensanker und wird nicht geprüft. |

Abbildung 11: Bereich B Knoten "Ergebnis der Signaturprüfung" aufgeklappt (EU-qualifizierte Signatur mit optionalen Knoten)

## 5.1 Zeile "Verwendete Prüfrichtlinie mit Link:"

In der Zeile "Verwendete Prüfrichtlinie mit Link" wird der Name der für die Prüfung der Signatur verwendeten Prüfrichtlinie angezeigt. Der angezeigte Name ist auch gleichzeitig der Link zur Prüfrichtlinie, die sich im technischen Anhang befindet.

Die Prüfrichtlinie wird entweder automatisch ausgewählt oder manuell von der anfragenden Instanz mitgegeben. In diesem Fall kann auch eine selbst erstellte Prüfrichtlinie übergeben werden. Folgende Prüfrichtlinien wurden von der Governikus KG definiert und werden, sollte keine Prüfrichtlinie von der anfragenden Instanz mitgegeben werden, automatisch ausgewählt:

- I. Qualifizierte elektronische Signatur (qVDA aus DE SigG): Technische Validierungsrichtlinie für EU-qualifizierte elektronische Signaturen. Der qualifizierte Vertrauensdiensteanbieter (qVDA) kommt aus Deutschland und das Zertifikat wurde noch gemäß den technischen Anforderungen des deutschen Signaturgesetzes erstellt (Common-PKI-Spezifikation).
- II. Qualifizierte elektronische Signatur (qVDA aus DE eIDAS-VO): Technische Validierungsrichtlinie für EU-qualifizierte elektronische Signaturen. Der qualifizierte Vertrauensdiensteanbieter kommt aus Deutschland und das Zertifikat wurde aus einer eIDAS-konformen PKI heraus erzeugt. Diese Differenzierung ist erforderlich, da einige der qVDA aus Deutschland in der Übergangsphase noch Signaturalgorithmen verwendet haben, die im Algorithmenkatalog der Bundesnetzagentur als geeignet angesehen wurden.
- III. Qualifizierte elektronische Signatur (qVDA nicht DE eIDAS-VO): Technische Validierungsrichtlinie für EU-qualifizierte elektronische Signaturen. Der qVDA kommt nicht aus Deutschland, sondern aus einem anderen EU-Mitgliedsstaat und das Zertifikat wurde aus einer eIDAS-konformen PKI heraus erzeugt.
- IV. Fortgeschrittene elektronische Signatur (VDA eIDAS-VO oder SigG): Technische Validierungsrichtlinie für fortgeschrittene elektronische Signaturen eines EU-Mitgliedsstaats sowohl für alte fortgeschrittene SigG-konforme Signaturen als auch aktuelle Signaturen.

Die automatische Auswahl der Prüfrichtlinie erfolgt über einen Algorithmus, der auf Basis der Angaben im Signaturzertifikat und ggf. unter Zuhilfenahme der Angaben aus einem Keystore (in dem alle qualifizierten CA-Zertifikate aus SigG-konformen PKIs enthalten sind) die für die Prüfung zutreffende Prüfrichtlinie ermittelt. Es ist damit keine Entscheidung verbunden, welche Qualität die Signatur tatsächlich erreicht.

Hinweis: Der Name einer benutzerdefinierten Prüfrichtlinie (Custom Policy) kann frei gewählt werden. Ob eine Prüfrichtlinie tatsächlich von der Governikus KG herausgegeben wurde, wird an dieser Stelle nicht angezeigt. Durch einen Klick auf den Link mit dem Namen der Prüfrichtlinie wird zum technischen Anhang gesprungen, in der die Prüfrichtlinie vollständig angezeigt wird. Dort wird auch angezeigt, ob die verwendete Prüfrichtlinie einer Governikus Prüfrichtlinie entspricht und ob die Auswahl automatisch oder manuell erfolgt ist.

## 5.2 Optionale Zeile "Verwendeter Algorithmenkatalog mit Link:"

Die optionale Zeile "verwendeter Algorithmenkatalog mit Link" ist nur vorhanden, wenn eine EU-qualifizierte Signatur validiert wurde. Der angezeigte Name ist auch gleichzeitig der Link zu Detailinformationen zum Algorithmenkatalog, die sich im technischen Anhang befindet. Der Algorithmenkatalog ist die Grundlage sowohl für die Prüfung der Inhaltsdatensignatur als auch für die Prüfung der Signaturen der Zertifikate. Für die Ermittlung der Eignung wird - wenn über eine durch die Governikus KG erstellte Prüfrichtlinie ausgewählt - der Algorithmenkatalog der Anwendung Governikus des IT-PLR verwendet. Diesen gibt es in zwei Varianten:

- SOG-IS Agreed Cryptographic Mechanisms/BNetzA 2017:  
Der Katalog wird für die Eignungsprüfung einer EU-qualifizierten elektronischen Signatur, deren Signaturzertifikat von einem in Deutschland ansässigen qualifizierten Vertrauensdiensteanbieter herausgegeben wurde, verwendet. Aus Vertrauensschutzwägungen werden für unter dem Signaturgesetz erzeugte qualifizierte Signaturen die Eignungsangaben aus dem letzten Algorithmenkatalog der Bundesnetzagentur von 2017 verwendet. Dabei wird für jeden Algorithmus immer das hinsichtlich der Eignung günstigste Ablaufdatum aus beiden Katalogen verwendet.
- SOG-IS Agreed Cryptographic Mechanisms/ETSI Cryptographic Suites:  
Für alle anderen EU-qualifizierte elektronischen Signaturen wird diese Variante gewählt. Der Katalog wurde um historische Angaben aus der TS ETSI Cryptographic Suites ergänzt. Hinweis: Im Geltungszeitraum der EU-Signaturrichtlinie gab es zum Teil nationale Kataloge. Diese liegen nicht vor und konnten nicht berücksichtigt werden.

Die konkret verwendete Version des Algorithmenkatalogs ist der Angabe im Link zu entnehmen. Durch einen Klick auf den Link gelangt man zu Detailangaben zum verwendeten Algorithmenkatalog, die im technischen Anhang stehen. Dort befindet sich auch ein Downloadlink, der es ermöglicht die maschinenlesbare Version des Algorithmenkatalogs herunterzuladen.

Hinweis: Die Verwendung des Kataloges SOG-IS Agreed Cryptographic Mechanisms wurde durch die EU-Kommission und die BNetzA empfohlen, ist aber nicht verpflichtend.

### 5.3 Überschrift "Integritätsprüfung"

Unter der Überschrift "Integritätsprüfung" werden die Ergebnisse aller durchgeführten Einzelprüfungen und relevante Kontextinformationen zu den Prüfungen angezeigt.

#### 5.3.1 Zeile "Strukturspezifische Prüfung"

In der Zeile "Strukturspezifische Prüfung" wird das Ergebnis der Prüfung der Struktur der Signatur (`SignerInfo`) angezeigt. Diese wird durchgeführt, um sicherheitskritische Mängel in der Signatur zu erkennen, die das Prüfergebnis verfälschen können. Folgende Prüfergebnisse sind möglich:

- **gültig** (grün gültig): Bei der Prüfung konnten keine sicherheitskritischen Mängel festgestellt werden oder
- **gültig** (grün gültig) mit Meldungstext: Bei der Prüfung konnten keine sicherheitskritischen Mängel festgestellt werden. Gleichwohl gibt es mindestens einen nicht sicherheitskritischen Mangel, der in einem Meldungstext erläutert wird. Nichtsicherheitskritische Mängel beeinflussen nicht das Signaturprüfergebnis.
- **unbestimmt** (gelb unbestimmt): Bei der Prüfung wurden sicherheitskritische Mängel festgestellt. Sicherheitskritische Mängel führen immer zu einem unbestimmten Signaturprüfergebnis, da sie das Vertrauen in die Signatur erschüttern. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für das Prüfergebnis erläutert.

#### 5.3.2 Zeile "Mathematische Signaturprüfung"

In der Zeile "Mathematische Prüfung" wird das Ergebnis der kryptographischen Signaturprüfung einer Inhaltsdatensignatur angezeigt. Folgende Prüfergebnisse sind möglich:

- **gültig** (grün gültig): Die Prüfung ist erfolgreich verlaufen. Die Signatur konnte erfolgreich mathematisch mit dem Signaturprüfchlüssel aus dem Signaturzertifikat mit

dem in der Zeile Signaturalgorithmus angegebenen Signaturalgorithmus geprüft werden. Der signierte Inhalt des Dokumentes wurde nach der Signatur nicht verändert.

- **unbestimmt** (gelb unbestimmt): Die Prüfung lieferte ein unbestimmtes Ergebnis zurück. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.
- **ungültig** (rot ungültig): Die Prüfung ist fehlgeschlagen. Der Inhalt des Dokumentes wurde nach der Signatur verändert. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.



**Hinweis:** Auch Zertifikate, OCSP-Antworten, CRLs oder Zeitstempeltoken besitzen Inhalte. Diese Inhalte sind auch alle signiert. Auch in diesem Zusammenhang werden daher Inhaltsdatensignaturen validiert.

### 5.3.3 Zeile "Signaturalgorithmus"

In der Zeile „Verwendeter Signaturalgorithmus“ wird der Name des für die Signatur verwendeten Signaturalgorithmus angezeigt.

Der angezeigte Name des verwendeten Signaturalgorithmus setzt sich aus mehreren Teilalgorithmen zusammen, die zusammen den verwendeten Signaturalgorithmus bilden. Dies sind in der Regel:

- der Hashalgorithmus, der für das Hashen der Inhaltsdaten und des `SignerInfo` verwendet wird,
- der Schlüsselalgorithmus mit Bitlängen von Parametern. Es ist das eigentliche kryptographische Verfahren zum Signieren,
- das Padding-Verfahren bei RSA-Signaturen, um den berechneten Hashwert aufzufüllen.

Das Padding-Verfahren wird nur angezeigt, wenn eine RSA-Signatur erzeugt wurde, da ECDSA-Signaturen nicht formatiert werden.

### 5.3.4 Optionale Zeile "Signaturalgorithmus für QES geeignet bis"

In der optionalen Zeile "Signaturalgorithmus für QES geeignet bis" werden das Datum und die Uhrzeit angezeigt, bis zu der der Signaturalgorithmus für eine EU-qualifizierte Signatur oder ein EU-qualifiziertes Siegel geeignet ist. Die Form ist `TT.MM.JJJJ hh:mm:ss`.

Die optionale Zeile ist zuverlässig nur dann vorhanden, wenn eine durch die Governikus KG erstellte Prüfrichtlinie für EU-qualifizierte Signaturen ausgewählt wurde.

Es werden Datum und Uhrzeit des Ablaufs der Eignung von dem Teilalgorithmus angezeigt, dessen Eignung am frühesten abläuft. Wird statt eines Datums "ohne Ablaufdatum" angezeigt, handelt es sich um einen Signaturalgorithmus, für den in dem verwendeten Algorithmenkatalog kein Ablaufdatum festgelegt wurde.

### 5.3.5 Optionale Zeile "Ausgewählter Eignungszeitpunkt"

In der optionalen Zeile "Ausgewählter Eignungszeitpunkt" wird der Zeitpunkt angezeigt, zu dem ermittelt wird, ob der für die EU-qualifizierte Signatur verwendete Signaturalgorithmus, angezeigt in der Zeile "Signaturalgorithmus", gemäß der Angaben im verwendeten Algorithmenkatalog (siehe Zeile "Verwendeter Algorithmenkatalog mit Link:") für eine EU-qualifizierte Signatur noch geeignet ist. Die optionale Zeile wird zuverlässig nur dann angezeigt, wenn eine durch die Governikus KG erstellte Prüfrichtlinie für EU-qualifizierte Signaturen ausgewählt wurde.

Folgende Zeitpunkte können für die Eignungsprüfung angewendet werden.

- Zeitpunkt der Durchführung der Prüfung
- EU-qualifizierter elektronischer Zeitstempel

Wird eine EU-qualifizierte elektronische Signatur unter der Verwendung einer der Governikus Prüfrichtlinien für EU-qualifizierte Signaturen geprüft, dann ist der ausgewählte Zeitpunkt der Eignungsprüfung in der Regel der Zeitpunkt der Durchführung der Prüfung (time at validation).

Wird als ausgewählter Eignungszeitpunkt "EU-qualifizierter elektronischer Zeitstempel" angezeigt, dann wurde eine EU-qualifizierte elektronische Signatur durch einem gültigen EU-qualifizierten Archivzeitstempel abgesichert. Der Zeitpunkt der Algorithmeneignung der Inhaltsdatensignatur ist in diesem Fall nicht mehr der Zeitpunkt der Durchführung der Prüfung verwendet, sondern das Datum der Erstellung des Archivzeitstempels.

Hinweis: Ein gültiger EU-qualifizierter Archivzeitstempel sichert nicht nur den Beweiswert der Inhaltsdatensignatur, sondern auch den Beweiswert - soweit vorhanden - aller in der Signatur (als unsignierte Attribute) vorhandenen signierten Objekte, wie Zertifikate und OCSP-Antworten/CRLs. Dies bedeutet, dass auch für diese Signaturen die Eignung der verwendeten Signaturalgorithmen zum Datum der Erstellung des Archivzeitstempels ermittelt wird. Ist das Ergebnis der Signaturprüfung "gültig", kann davon ausgegangen werden, dass die Eignung aller verwendeten Signaturalgorithmen zum Zeitpunkt der Zeitstempelung noch gegeben war. Fehlen zum Beispiel für die Ermittlung des Sperrstatus in die Signatur eingebettete OCSP-Antworten, werden diese neu angefordert. In diesem Fall wird die Eignung der für die Signatur der OCSP-Antworten verwendeten Algorithmen dann wieder zum Zeitpunkt der Durchführung der Prüfung bestimmt.

### 5.3.6 Optionale Zeile "Eignung zu diesem Zeitpunkt"

In der optionalen Zeile "Eignung zu diesem Zeitpunkt" wird das Ergebnis der Prüfung der Eignung des Signaturalgorithmus zum in der vorherigen Zeile angegebenen Zeitpunkt angezeigt. Die optionale Zeile wird zuverlässig nur dann angezeigt, wenn eine durch die Governikus KG erstellte Prüfrichtlinie für EU-qualifizierte Signaturen ausgewählt wurde. Folgende Prüfergebnisse sind möglich:

- **gültig** (grün gültig): Der Signaturalgorithmus war zum in der vorherigen Zeile angegebenen Zeitpunkt für EU-qualifizierte Signaturen geeignet.
- **ungültig** (rot ungültig): Der Signaturalgorithmus war zum in der vorherigen Zeile angegebenen Zeitpunkt für EU-qualifizierte Signaturen nicht oder nicht mehr geeignet.

## 5.4 Überschrift "Zertifikatsprüfungen"

Unter der Überschrift "Zertifikatsprüfungen" werden untereinander die Ergebnisse der kumulierten Prüfungen jedes Zertifikats einer Zertifikatskette und relevante Kontextinformationen zu den Prüfungen angezeigt. Die in diesem Kapitel beschriebenen Ergebnisse entsprechen auch der Anzeige nach dem Aufklappen des Knotens "Ergebnis der Zertifikatsprüfung" auf der Hauptseite des Prüfprotokolls bei der separaten Prüfung eines End-Entity-Zertifikats.

Die Anzeige des kumulierten Ergebnisses einer Zertifikatsprüfung und auch die Einzelprüfergebnisse nach Aufklappen des Knotens im Prüfprotokoll sind generisch und weitestgehend unabhängig davon, ob ein

- (1) Signaturzertifikat oder Siegelzertifikat,
- (2) Zeitstempelzertifikat,
- (3) OCSP-Signer-Zertifikat oder CRL-Signer-Zertifikat,

- (4) CA-Zertifikat oder
- (5) Root-Zertifikat

geprüft wird.

Die im Kapitel 5.4.3 erläuterten Prüfergebnisse gelten für alle diese Zertifikatstypen.

Relevante Unterschiede bei der Prüfung und damit bei der Anzeige von Prüfergebnissen ergeben sich dann, wenn Zertifikate validiert werden, die Vertrauensanker sind und daher selbst nicht mehr geprüft werden müssen. Signaturzertifikate selbst können nicht als ein Vertrauensanker fungieren, sondern nur die Zertifikatstypen (2), (3) und (4). Bedingung ist, dass Zertifikatstyp (4) als gültiger Service Digital Identifier (SDI) eines zertifikatsausstellenden Dienstes, Typ (3) als SDI eines OCSP-Antworten ausstellender Dienst oder Typ (2) als Zeitstempel generierender Dienst in einer gültigen EUMS-TL (zeitliche Gültigkeit und gültige Signaturprüfung) konfiguriert ist und die automatische Auswahl einer Prüfrichtlinie durchgeführt wurde.

Fungieren diese Zertifikatstypen als Vertrauensanker, werden in der Kette darüber liegende Zertifikate (ausstellende Zertifikate) nicht mehr betrachtet.

In den beiden Kapiteln 5.5 und 5.6 wird somit auch der Standardfall einer Zertifikatsprüfung für eine EU-qualifizierte elektronischen Signatur beschrieben: Die Prüfung des qualifizierten Signaturzertifikats und der Nachweis, dass das CA-Zertifikat als Vertrauensanker verwendet werden darf.

#### **5.4.1 Zeile "Gültigkeitsmodell für die Zertifikatskette"**

In der Zeile "Gültigkeitsmodell für die Zertifikatskette" wird das der Prüfung der Zertifikate zugrunde gelegte Gültigkeitsmodell angezeigt. Das Modell ist für die Bestimmung der Zeitpunkte, zu dem die Gültigkeit der Zertifikate ermittelt wird, von Bedeutung. Das betrifft alle Zertifikate der Kette vom Signaturzertifikat bis zum Zertifikat, das als Vertrauensanker fungiert. Folgende Modelle können angewendet werden:

- Schale
- Kettenprüfung
- Escape-Route (gemäß Common-PKI-Spezifikation SigG)

Das Modell "Schale" bedeutet, dass die Inhaltsdatensignatur und alle Zertifikatssignaturen zum konfigurierten Vertrauensniveau des Prüfzeitpunktes validiert werden. Der Prüfzeitpunkt kann der Zeile "ausgewählter Prüfzeitpunkt" (Beschreibung siehe Kapitel 3.2.13) entnommen werden. Beim "Kettenmodell" wird die Inhaltsdatensignatur und das Signaturzertifikat zum ausgewählten Vertrauensniveau des Prüfzeitpunktes geprüft. Das CA- und Rootzertifikat muss jeweils zum Erstellungszeitpunkt (notBefore) des ausgestellten Zertifikats gültig gewesen sein.

Wird eine Governikus Prüfrichtlinie verwendet, dann wird als Vertrauensniveau des Prüfzeitpunktes immer der behauptete Signaturzeitpunkt (claimed signing time) als minimales Vertrauensniveau verwendet.

Die "Escape-Route" gemäß Common-PKI-Spezifikation wird bei Auswahl der entsprechenden Governikus Prüfrichtlinie "Qualifizierte elektronische Signatur (qVDA aus DE SigG)" nur bei qualifizierten SigG-konformen Signaturen angewendet. Escape-Route bedeutet, dass als Prüfzeitpunkt der Inhaltsdatensignatur immer der behauptete Signaturzeitpunkt ausgewählt wird und versucht wird, zu diesem Prüfzeitpunkt auch die Gültigkeit der Zertifikate der Signaturzertifikatskette nach dem Schalenmodell zu prüfen. Schlägt die Prüfung bei einem ausstellenden Zertifikat (z.B. beim CA-Zertifikat) fehl, wird als Fallback für dieses Zertifikat nach dem Kettenmodell geprüft und der Erstellungszeitpunkt des ausgestellten Zertifikats verwendet.

Hinweis: Auch für OCSP-Signer-Zertifikate, CRL-Signer-Zertifikate oder Zeitstempel-Zertifikate werden Zertifikatsketten bis zu einem Rootzertifikat oder einem Vertrauensanker gebildet.

Als Gültigkeitsmodell wird hier immer das in der Prüfrichtlinie festgelegte Modell verwendet. Inhaltsdatensignatur bezeichnet in diesem Zusammenhang auch die Signatur einer OCSP-Antwort, einer CRL oder eines Zeitstempeltokens.

#### 5.4.2 Zeile "Gültigkeitsmodell definiert in"

In der Zeile "Gültigkeitsmodell definiert in" wird die Quelle für die Auswahl des Gültigkeitsmodells angezeigt. Folgende Quellen können ausgewertet und bezeichnet werden:

- **Verwendete Prüfrichtlinie:**  
Die Angabe zeigt an, dass das in der Prüfrichtlinie konfigurierte Modell verwendet wurde.
- **Signaturzertifikat Erweiterung Gültigkeitsmodell:**  
Die Angabe bedeutet, dass im Zertifikat vorgeschrieben wurde, welches Gültigkeitsmodell zu verwenden ist.
- **Erweiterung der Vertrauensliste:**  
Die Angabe bedeutet, dass in der durch die Governikus KG bereitgestellte Erweiterung der Vertrauensliste das Modell vorgegeben wurde.
- **Standardwert:**  
Keine der oben benannten Quellen waren verfügbar. In diesem Fall wird das Schalenmodell verwendet.

Folgende Modelle sind in den Governikus-Prüfrichtlinien konfiguriert: Es wird immer das Schalenmodell verwendet bis auf eine Ausnahme: Wird eine qualifizierte Signatur aus einer SigG-konformen PKI validiert, wird gemäß der Common-PKI-Spezifikation als Gültigkeitsmodell die Escape-Route verwendet. Eine etwaige Angabe in der Prüfrichtlinie wird durch eine individuelle Angabe im Zertifikat oder eine CA-spezifische Angabe in der Erweiterung der Vertrauensliste überschrieben. Eine individuelle Angabe im Zertifikat zählt dabei mehr als eine etwaige Angabe in der Erweiterung einer Vertrauensliste.

#### 5.4.3 Zeilen "Prüfung des Zertifikats von < Name >" mit Knoten

Die Zeile "Prüfung des Zertifikats von <Name>" mit Knoten wird für jede durchgeführte Zertifikatsprüfung wiederholt. Die Anzahl der angezeigten Zeilen mit kumuliertem Prüfergebnis ist abhängig von der Anzahl der Zertifikate in der Zertifikatskette und endet beim ersten Vertrauensanker. Dieses kann z.B. ein CA-Zertifikat als Vertrauensanker aus einer EUMS-TL sein oder das Rootzertifikat der Zertifikatskette.

In der Zeile "Prüfung des Zertifikats von < Name >" wird das kumulierte Ergebnis einer durchgeführten Zertifikatsprüfung angezeigt. Folgende Ergebnisse sind möglich:

- **gültig** (grün gültig): Alle gemäß Prüfrichtlinie notwendigen Einzelprüfungen bezüglich des Zertifikats sind erfolgreich verlaufen.
- **unbestimmt** (gelb unbestimmt): Mindestens eine gemäß der verwendeten Prüfrichtlinie notwendige Einzelprüfung bezüglich des Zertifikats lieferte ein unbestimmtes Ergebnis zurück. Keine durchgeführte Einzelprüfung ist endgültig fehlgeschlagen (Prüfergebnis rot ungültig). Je nach Ursache kann eine Nachprüfung sinnvoll sein. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.
- **ungültig** (rot ungültig): Mindestens eine gemäß Prüfrichtlinie notwendige Einzelprüfung bezüglich des Zertifikats ist endgültig fehlgeschlagen. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.
- **nicht geprüft** (schwarz nicht geprüft): Das angegebene Zertifikat wurde nicht geprüft. Gemäß verwendeter Prüfrichtlinie handelt es sich um einen Vertrauensanker aus einer

gültigen Vertrauensliste. In einem Meldungstext unter dem Prüfergebnis wird dieses Ergebnis erläutert.

Hinweis Das Prüfergebnis "nicht geprüft" ist nur bei der Prüfung eines CA-Zertifikats, eines OCSP-Signer-Zertifikats oder eines Zeitstempel-Zertifikats möglich, wenn es als Service Digital Identifier (SDI) in einer gültigen EUMS-TL konfiguriert ist und daher – bei Auswahl einer Governikus-Prüfrichtlinie - als Vertrauensanker fungiert.

Nach dem Aufklappen des Knoten werden wichtige Zertifikatsinhalte und die Ergebnisse aller durchgeführten Einzelprüfungen sowie relevante Kontextinformationen angezeigt.

## 5.5 Bereich B Knoten "Prüfung des Zertifikats von < Name >" aufgeklappt

In diesem Kapitel werden die Einzelprüfergebnisse einer Zertifikatsprüfung beschrieben, die nach Aufklappen des Knotens der Zeile "Prüfung des Zertifikats von < Name >" angezeigt werden.

| Prüfung des Zertifikats von Donald Duck:    |                                  | gültig   |
|---|----------------------------------|--|
| <b>Angaben aus dem geprüften Zertifikat</b> |                                  |  |
| +   | Name des Inhabers:               | Donald Duck  |
|   | Seriennummer:                    | 88400119455509264629949541749585847694   |
|   | Gültigkeitszeitraum:             | 03.05.2017, 06:18:39 bis 03.05.2020, 06:18:39  |
|   | Angaben zur Zertifikatsqualität: | EU-qualifiziertes Zertifikat<br>Signatur Schlüssel auf qualifizierter sicherer Signaturerstellungseinheit (QSCD)<br>Zertifikat für elektronische Signaturen gemäß eIDAS-Verordnung |

Abbildung 12: Bereich B Knoten "Prüfung des Zertifikats von <Name>" aufgeklappt, Angaben aus dem Zertifikat

Zunächst werden unter der Überschrift "Angaben aus dem geprüften Zertifikat" ausgewählte Zertifikatsinhalte angezeigt (siehe Kapitel 5.5.1 und folgende Unterkapitel).

Danach folgen unter der Überschrift "Zertifikatsprüfung" die Ergebnisse der durchgeführten Einzelprüfungen (ab Kapitel 5.5.6). Dazu gehört auch die Ermittlung des Sperrstatus des geprüften Zertifikats. Sperrstatusinformationen erhält man entweder vom Vertrauensdiensteanbieter (VDA) über eine OCSP-Anfrage oder den Download einer CRL. Sowohl die CRL als auch die OCSP-Antwort sind durch den VDA signiert. Diese Signaturen sind - wie auch Zertifikatssignaturen - in der Regel wiederum zu prüfen.

Nach der Überschrift "Prüfung der Sperrstatusinformationen" werden ab Kapitel 5.5.19 zunächst wichtige Kontextinformationen zur Sperrstatus-Ermittlung angezeigt bevor dann das Ergebnis der Signaturprüfung der Sperrstatusprüfung selbst angezeigt wird.

### 5.5.1 Überschrift "Angaben aus dem Zertifikat"

Unter der Überschrift "Angaben aus dem geprüften Zertifikat" werden ausgewählte Zertifikatsinhalte angezeigt.

Handelt es sich bei dem geprüften Zertifikat um ein Attributzertifikat gemäß Common-PKI-Spezifikation wird als Überschrift angezeigt: "Angaben aus dem Attributzertifikat".



### 5.5.2 Zeile "Name des Inhabers"

In der Zeile "Name des Inhabers" wird der Name des Inhabers des geprüften Zertifikats angezeigt. Es handelt sich um den Common-Name des Inhabers aus dem Zertifikat.

Nach dem Aufklappen des Knotens wird je nach Anforderung entweder der gesamte Inhalt des Zertifikats angezeigt oder eine Kurzansicht. Diese Kurzansicht umfasst die Bereiche Inhaber, Aussteller, die Erweiterung QC-Statement und die wichtigsten Felder aus dem Bereich allgemeine Angaben. Bei Common-PKI-konformen Zertifikaten werden auch die beschränkten Attribute aufgeführt.

Zur Beschreibung der Zertifikatsinhalte siehe Kapitel 9.

Handelt es sich bei dem angezeigten Zertifikat um ein Attributzertifikat zu dem geprüften Signaturzertifikat gemäß Common-PKI-Spezifikation, wird in der Zeile entweder die Seriennummer des Signaturzertifikats (dem das Attributzertifikat zugeordnet ist) oder der Aussteller des Attributzertifikats angezeigt.

### 5.5.3 Zeile "Seriennummer"

In der Zeile "Seriennummer" wird die Seriennummer aus dem geprüften Zertifikat angezeigt.

### 5.5.4 Zeile "Gültigkeitszeitraum"

In der Zeile "Gültigkeitszeitraum" wird der Gültigkeitszeitraum des geprüften Zertifikats angezeigt. Die Form ist `TT.MM.JJJJ, hh:mm:ss` bis `TT.MM.JJJJ, hh:mm:ss`.

### 5.5.5 Optionale Zeile "Angaben zur Zertifikatsqualität"

Handelt es sich um ein EU-qualifiziertes Zertifikat, werden in der optionalen Zeile "Angaben zur Zertifikatsqualität" die Angaben zur Zertifikatsqualität aus dem Zertifikat angezeigt. Diese Angaben stammen aus der Erweiterung QCStatement im Zertifikat.

### 5.5.6 Überschrift "Zertifikatsprüfung"

Unter der Überschrift "Zertifikatsprüfung" werden die Ergebnisse der durchgeführten Einzelprüfungen angezeigt.

| Zertifikatsprüfung   |   |
|--|---|
| Zertifikatsherkunft:   | Aus der Inhaltsdatensignatur  |
| Mathematische Prüfung der Zertifikatssignatur:                             | <b>gültig</b>   |
| Signaturalgorithmus:   | SHA512 RSA (n = 4096) (e = 65537) PSS   |
| Signaturalgorithmus für QES geeignet bis:                                  | ohne Ablaufdatum  |
| Ausgewählter Eignungszeitpunkt:  | Zeitpunkt der Durchführung der Prüfung  |
| Eignung zu diesem Zeitpunkt:   | <b>gültig</b>   |
| Prüfzeitpunkt des Zertifikats:   | Behaupteter Signaturzeitpunkt   |
| Prüfzeitpunkt der Signatur innerhalb Gültigkeitsintervall des Zertifikats: | <b>gültig</b>   |
| Sperrstatus des Zertifikats:   | <b>gültig</b>   |
| Meldungen:   | Die Sperrstatusanfrage wurde nach dem Ablauf des Zertifikats ausgeführt. Der Dienst speichert aber Sperrinformationen für einen Zeitraum über den Ablauf eines Zertifikats hinaus und die Abfrage war innerhalb dieses Zeitraums. |
| <b>Prüfung der Sperrstatusinformationen</b>                                |   |

Abbildung 13: Bereich B Knoten "Prüfung des Zertifikats von <Name>", Zertifikatsprüfung

### 5.5.7 Optionale Zeile "Zuordnung des Attributzertifikats zum Signaturzertifikat"

In der optionalen Zeile "Zuordnung des Attributzertifikats zum Signaturzertifikat" wird angezeigt, ob ein mitsigniertes Attributzertifikat (gemäß Common-PKI-Spezifikation) für das Signaturzertifikat ausgestellt wurde.

Folgende Prüfergebnisse sind möglich:

- **gültig** (grün gültig): Die Prüfung ist erfolgreich verlaufen. Das mitsignierte Attributzertifikat wurde für das Signaturzertifikat und damit für den Inhaber des Signaturzertifikats ausgestellt.
- **unbestimmt** (gelb unbestimmt): Die Prüfung lieferte ein unbestimmtes Ergebnis zurück. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.
- **ungültig** (rot ungültig): Die Prüfung ist fehlgeschlagen. Das mitsignierte Attributzertifikat wurde nicht für das Signaturzertifikat und damit nicht für den Inhaber des Signaturzertifikats ausgestellt. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.

### 5.5.8 Zeile "Zertifikatsherkunft"

In der Zeile "Zertifikatsherkunft" wird angezeigt, aus welcher Quelle das Zertifikat stammt. Folgende Werte sind möglich:

- **Mit der Prüfanfrage übermittelt** bedeutet, dass das Zertifikat mit der Validierungsanfrage von der anfragenden Instanz übermittelt wurde.
- **Aus der Inhaltsdatensignatur** bedeutet, dass das Zertifikat aus der Signatur entnommen wurde. Das ist der Regelfall, da die Normierung vorschreibt, dass das Zertifikat als mitsigniertes Attribut in der Signatur vorliegen muss.
- **Aus dem Zwischenspeicher des CVS** bedeutet, dass das Zertifikat durch den Certificate Validation Server (CVS) kurzzeitig gepuffert vorlag.
- **Aus der verwendeten Vertrauensliste** bedeutet, dass das Zertifikat der verwendeten Vertrauensliste entnommen wurde. Dieses ist in der Regel bei CA-Zertifikaten der Fall.
- **Online bezogen vom Vertrauensdiensteanbieter** bedeutet, dass das Zertifikat online vom Vertrauensdiensteanbieter heruntergeladen wurde. Der Downloadlink stammt aus dem in der Zertifikatskette unter dem geprüften Zertifikat liegenden Zertifikat. Der Link befindet sich in der Extension `AuthorityInfoAccess`.

### 5.5.9 Zeile "Mathematische Prüfung der Zertifikatssignatur"

In der Zeile "Mathematische Prüfung der Zertifikatssignatur" wird das Ergebnis der kryptographischen Prüfung der Zertifikatssignatur angezeigt. Folgende Prüfergebnisse sind möglich:

- **gültig** (grün gültig): Die Prüfung ist erfolgreich verlaufen. Die Signatur konnte erfolgreich mathematisch mit dem Signaturprüf Schlüssel aus dem ausstellenden Zertifikat mit dem in der Zeile Signaturalgorithmus angegebenen Signaturalgorithmus geprüft werden. Das Zertifikat wurde nach der Signatur nicht verändert.
- **unbestimmt** (gelb unbestimmt): Die Prüfung lieferte ein unbestimmtes Ergebnis zurück. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.

- **ungültig** (rot ungültig): Die Prüfung ist fehlgeschlagen. Das Zertifikat wurde nach der Signatur verändert. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.

### 5.5.10 Zeile "Signaturalgorithmus"

In der Zeile verwendeter Signaturalgorithmus" wird der Name des für die Signatur des Zertifikats verwendeten Signaturalgorithmus angezeigt.

Der angezeigte Name des verwendeten Signaturalgorithmus setzt sich aus mehreren Teil-Algorithmen zusammen, die zusammen den verwendeten Signaturalgorithmus bilden. Dieses ist in der Regel:

- der Hashalgorithmus, der für das Hashen der Inhaltsdaten und `SignerInfo` verwendet wird.
- der Schlüsselalgorithmus mit Bitlängen von Parametern. Es ist das eigentliche kryptographische Verfahren zum Signieren.
- das Padding-Verfahren bei RSA-Signaturen, um den berechneten Hashwert aufzufüllen.

Das Padding-Verfahren wird nur angezeigt, wenn eine RSA-Signatur erzeugt wurde, da ECDSA-Signaturen nicht formatiert werden.

### 5.5.11 Optionale Zeile "Signaturalgorithmus für QES geeignet bis"

In der optionalen Zeile "Signaturalgorithmus für QES geeignet bis" werden das Datum und die Uhrzeit angezeigt, bis zu der der Signaturalgorithmus für eine EU-qualifizierte Signatur oder ein EU-qualifiziertes Siegel geeignet ist. Die Form ist `TT.MM.JJJJ hh:mm:ss`.

Die optionale Zeile ist zuverlässig nur dann vorhanden, wenn eine durch die Governikus KG erstellte Prüfrichtlinie für EU-qualifizierte Signaturen ausgewählt wurde.

Es werden Datum und Uhrzeit des Ablaufs der Eignung von dem Teilalgorithmus angezeigt, dessen Eignung am frühesten abläuft. Wird statt eines Datums "ohne Ablaufdatum" angezeigt, handelt es sich um einen Signaturalgorithmus, für den in dem verwendeten Algorithmenkatalog kein Ablaufdatum festgelegt wurde.

### 5.5.12 Optionale Zeile "Ausgewählter Eignungszeitpunkt"

In der optionalen Zeile "Ausgewählter Eignungszeitpunkt" wird der Zeitpunkt angezeigt, zu dem ermittelt wird, ob der für die EU-qualifizierte Signatur verwendete Signaturalgorithmus, angezeigt in der Zeile "Signaturalgorithmus", gemäß der Angaben im verwendeten Algorithmenkatalog (siehe Zeile "Verwendeter Algorithmenkatalog mit Link:") für eine EU-qualifizierte Signatur noch geeignet ist. Die optionale Zeile wird zuverlässig nur dann angezeigt, wenn eine durch die Governikus KG erstellte Prüfrichtlinie für EU-qualifizierte Signaturen ausgewählt wurde.

Folgende Zeitpunkte können für die Eignungsprüfung angewendet werden.

- Zeitpunkt der Durchführung der Prüfung
- EU-qualifizierter elektronischer Zeitstempel

Wird eine EU-qualifizierte elektronische Signatur unter der Verwendung einer der Governikus Prüfrichtlinien für EU-qualifizierte Signaturen geprüft, dann ist der ausgewählte Zeitpunkt der Eignungsprüfung in der Regel der Zeitpunkt der Durchführung der Prüfung (time at validation).

Wird als ausgewählter Eignungszeitpunkt "EU-qualifizierter elektronischer Zeitstempel" angezeigt, dann wurde eine EU-qualifizierte elektronische Signatur durch einem gültigen EU-

qualifizierten Archivzeitstempel abgesichert. Der Zeitpunkt der Algorithmeignung der Inhaltsdatensignatur ist in diesem Fall nicht mehr der Zeitpunkt der Durchführung der Prüfung, sondern das Datum der Erstellung des Archivzeitstempels.

Hinweis: Ein gültiger EU-qualifizierter Archivzeitstempel sichert nicht nur den Beweiswert der Inhaltsdatensignatur, sondern auch den Beweiswert - soweit vorhanden - aller in der Signatur (als unsignierte Attribute) vorhandenen signierten Objekte, wie Zertifikate und OCSP-Antworten/CRLs. Dies bedeutet, dass auch für diese Signaturen die Eignung der verwendeten Signaturalgorithmen zum Datum der Erstellung des Archivzeitstempels ermittelt wird. Ist das Ergebnis der Signaturprüfung "gültig", kann davon ausgegangen werden, dass die Eignung aller verwendeten Signaturalgorithmen zum Zeitpunkt der Zeitstempelung noch gegeben war. Fehlen zum Beispiel für die Ermittlung des Sperrstatus in die Signatur eingebettete OCSP-Antworten, werden diese neu angefordert. In diesem Fall wird die Eignung der für die Signatur der OCSP-Antworten verwendeten Algorithmen dann wieder zum Zeitpunkt der Durchführung der Prüfung bestimmt.

### 5.5.13 Optionale Zeile "Eignung zu diesem Zeitpunkt"

In der optionalen Zeile "Eignung zu diesem Zeitpunkt" wird das Ergebnis der Prüfung der Eignung des Signaturalgorithmus zum in der vorherigen Zeile angegebenen Zeitpunkt angezeigt. Die optionale Zeile wird zuverlässig nur dann angezeigt, wenn eine durch die Governikus KG erstellte Prüfrichtlinie für EU-qualifizierte Signaturen ausgewählt wurde. Folgende Prüfergebnisse sind möglich:

- **gültig** (grün gültig): Der Signaturalgorithmus war zum in der vorherigen Zeile angegebenen Zeitpunkt für EU-qualifizierte Signaturen geeignet.
- **ungültig** (rot ungültig): Der Signaturalgorithmus war zum in der vorherigen Zeile angegebenen Zeitpunkt für EU qualifizierte Signaturen nicht oder nicht mehr geeignet.

### 5.5.14 Zeile "Prüfzeitpunkt des Zertifikats"

In der Zeile "Prüfzeitpunkt des Zertifikats" wird das Vertrauensniveau des Prüfzeitpunktes des Zertifikats angezeigt. Bezogen auf den Prüfzeitpunkt wird ermittelt ob:

- das geprüfte Zertifikat zeitlich gültig war (Prüfzeitpunkt innerhalb des Gültigkeitsintervalls des Zertifikats. Das Intervall wird in der Zeile "Gültigkeitszeitraum" angezeigt),
- das Zertifikat gültig und nicht gesperrt war (Ermittlung des Sperrstatus zum Prüfzeitpunkt).

Die Prüfergebnisse werden in den beiden folgenden Zeilen des Prüfprotokolls angezeigt. Der in der Prüfrichtlinie konfigurierte Prüfzeitpunkt bezieht sich zunächst immer auf den Prüfzeitpunkt der Inhaltsdatensignatur (Content Signatur).

Folgende Vertrauensniveaus wurden von ETSI definiert, können ausgewählt und grundsätzlich angezeigt werden:

- (1) Behaupteter Signaturzeitpunkt,
- (2) Zeitmarke,
- (3) Signaturzeitstempel,
- (4) Zeitpunkt der Durchführung der Prüfung,
- (5) Übergabener Zeitpunkt (nur bei separater Zertifikatsprüfung).

### Prüfung einer Inhaltsdatensignatur

In Abhängigkeit vom verwendeten Gültigkeitsmodell werden bei der Gültigkeitsprüfung der einzelnen Zertifikate der Signaturzertifikatskette unterschiedliche Prüfzeitpunkte ausgewählt. Dabei hat das angezeigte Vertrauensniveau "Behaupteter Signaturzeitpunkt" verschiedene Bedeutungen. Details sind der folgenden Tabelle 1 zu entnehmen:

| Signaturzertifikatskette   |                   | Vertrauensniveaus des Prüfzeitpunkts bei der Prüfung der Zertifikatsgültigkeit |  |  |
|--|-------------------|--|--|--|
|  |                   | Schalenmodell  | Kettenmodell   | Escape Route (SigG)  |
| Signaturzertifikat (EE)  | Angezeigter Wert: | (1) (2) (3) oder (4)   |  | Nur (1)  |
|  | Bedeutung:        | Prüfzeitpunkt der Inhaltsdatensignatur (Content Signatur)                      |  |  |
| CA-Zertifikat  | Angezeigter Wert: | (1) (2) (3) oder (4)   | Nur (1) behaupteter Signaturzeitpunkt  |  |
|  | Bedeutung:        | Prüfzeitpunkt der Inhaltsdatensignatur   | Prüfzeitpunkt ist der Erstellungszeitpunkt (Signatur) des ausgestellten Zertifikats (also notBefore EE-Zertifikat) | Zweistufig: Zunächst Prüfzeitpunkt der Inhaltsdatensignatur, im Fehlerfall dann Erstellungszeitpunkt des ausgestellten Zertifikats |
| Root-Zertifikat  | Angezeigter Wert: | (1) (2) (3) oder (4)   | Nur (1) behaupteter Signaturzeitpunkt  |  |
|  | Bedeutung:        | Prüfzeitpunkt der Inhaltsdatensignatur   | Prüfzeitpunkt ist der Erstellungszeitpunkt (Signatur) des ausgestellten Zertifikats (also notBefore CA-Zertifikat) | Zweistufig: Zunächst Prüfzeitpunkt der Inhaltsdatensignatur, im Fehlerfall dann Erstellungszeitpunkt des ausgestellten Zertifikats |
| Legende: (1) Behaupteter Signaturzeitpunkt, (2) Zeitmarke, (3) Signaturzeitstempel, (4) Zeitpunkt der Durchführung der Prüfung |                   |  |  |  |

Tabelle 1: Bedeutung der Vertrauensniveaus der Prüfzeitpunkte in Abhängigkeit vom Kontext

### Signaturprüfung von OCSP-Antworten, CRL oder Zeitstempeltoken

Die Signaturprüfung von OCSP-Antworten, CRL oder Zeitstempeltoken erfolgt immer und ausschließlich zu deren Erstellungszeitpunkten. Bei der OCSP-Antwort ist das die Zeitangabe `producedAt`, bei der CRL die Zeitangabe `thisUpdate` und bei Zeitstempeltoken die `genTime`. Dieses sind dann auch immer die Zeitpunkte, zu dem die Gültigkeit des OCSP-Signer-Zertifikats, CRL-Signer-Zertifikats oder Zeitstempelzertifikats geprüft wird. Angezeigt wird dieser Zeitpunkt immer als "Behaupteter Signaturzeitpunkt". Als Gültigkeitsmodell für die jeweiligen Zertifikatsketten wird das für die Signaturzertifikatskette ausgewählte Modell verwendet. Die Prüfzeitpunkte der CA- und Root-Zertifikate entsprechen sinngemäß den Angaben in der obigen Tabelle. Der Begriff "Inhaltsdatensignatur" ist durch "Signatur der OCSP-Antwort", "Signatur der CRL" bzw. "Signatur des Zeitstempel-Tokens" zu ersetzen.

### Prüfung eines einzelnen Signaturzertifikats

Wird nur ein separat übergebenes Signaturzertifikat (End-Entity-Zertifikat) validiert, dann wird entweder der mit der Anfrage übergebene Zeitpunkt verwendet (angezeigt als (5) "übergebener Zeitpunkt") oder, sollte kein Prüfzeitpunkt übergeben worden sein, der Zeitpunkt der Durchführung der Prüfung ().

### 5.5.15 Zeile "Prüfzeitpunkt der Signatur innerhalb Gültigkeitsintervall des Zertifikats"

In der Zeile "Prüfzeitpunkt der Signatur (Inhaltsdatensignatur bzw. Zertifikatssignatur) innerhalb Gültigkeitsintervall des Zertifikats" wird angezeigt, ob der Prüfzeitpunkt der Inhaltsdatensignatur innerhalb des Gültigkeitsintervalls des Signaturzertifikats bzw. ob der Prüfzeitpunkt der Zertifikatssignatur innerhalb des Gültigkeitsintervalls des ausstellenden Zertifikats lag. Folgende Prüfergebnisse sind möglich:

- **gültig** (grün gültig): Die Prüfung ist erfolgreich verlaufen. Der Prüfzeitpunkt liegt innerhalb des Gültigkeitsintervalls des Zertifikats.
- **unbestimmt** (gelb unbestimmt): Die Prüfung lieferte ein unbestimmtes Ergebnis zurück. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.
- **ungültig** (rot ungültig): Die Prüfung ist fehlgeschlagen. Der Prüfzeitpunkt liegt außerhalb des Gültigkeitsintervalls des Zertifikats. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.

### 5.5.16 Zeile "Sperrstatus des Zertifikats"

In der Zeile "Sperrstatus des Zertifikats" wird der Sperrstatus des Zertifikats zum angegebenen Prüfzeitpunkt (siehe Zeile "Prüfzeitpunkt des Zertifikats") angezeigt. Folgende Prüfergebnisse sind möglich:

- **gültig** (grün gültig): Das Zertifikat war zum Zeitpunkt, zu dem die Gültigkeit ermittelt werden sollte (Prüfzeitpunkt der Signatur), nicht gesperrt.
- **unbestimmt** (gelb unbestimmt): Die Prüfung lieferte ein unbestimmtes Ergebnis zurück. Der Grund wird in einem Meldungstext erläutert.
- **gesperrt** (rot gesperrt): Das Zertifikat war zum Zeitpunkt, zu dem die Gültigkeit geprüft werden sollte (Prüfzeitpunkt der Signatur), gesperrt. Ist das Zertifikat gesperrt, werden in den nächsten beiden Zeilen das Sperrdatum und der Sperrgrund angegeben.
- **nicht geprüft** (schwarz nicht geprüft): Dieses Ergebnis wird angezeigt, wenn der Sperrstatus nicht geprüft wurde, weil eine Prüfung aufgrund der verwendeten Prüfrichtlinie oder aufgrund von Angaben im Zertifikat nicht erforderlich war. Der Grund wird unter diesem Status im Prüfprotokoll in einem Meldungstext erläutert.

Der Status "nicht geprüft" wird angezeigt bei der Ermittlung des Sperrstatus

- eines Root-Zertifikats, wenn die Governikus-Prüfrichtlinie für fortgeschrittene Signaturen verwendet wird,
- eines OCSP-Signer-Zertifikats, falls in dem Zertifikat der Eintrag OCSPNoCheck enthalten ist und die verwendete Prüfrichtlinie den Verzicht auf die Sperrstatusermittlung erlaubt oder
- eines Signaturzertifikats, wenn es sich um ein Short-Term-Zertifikat handelt, welches die Erweiterung „Validity Assured“ enthält (die Erweiterung besagt, dass es während seiner Laufzeit nicht gesperrt wird) und die verwendete Prüfrichtlinie den Verzicht auf die Sperrstatusermittlung erlaubt.

In diesen Fällen fehlt auch die Überschrift "Prüfung der Sperrstatusinformationen" und die folgenden Zeilen (beschrieben in den Kapiteln ab 5.5.19).

### Vertrauensstellung der Sperrstatusantwort

Gemäß RFC 6960 muss die OCSP-Antwort/CRL über das OCSP-Signer-Zertifikat oder das CRL-Signer-Zertifikat in einer Vertrauensstellung zu der CA oder dem Vertrauensdiensteanbieter stehen, der das Signaturzertifikat (dessen Sperrstatus ermittelt werden sollte) ausgestellt hat. Wird eine Governikus Prüfrichtlinie verwendet, wird überprüft, ob dem Dienst (der die OCSP-Antwort oder die CSL signiert) vertraut werden kann. Dies ist der Fall,

- wenn eine Kette vom OCSP-Signer-Zertifikat oder CRL-Signer-Zertifikat zu einem in einer Vertrauensliste zum konfigurierten Dienst oder Vertrauensdiensteanbieter, der auch das Signaturzertifikat ausgestellt hat, hergestellt werden kann und
- der Status des Dienstes zum Zeitpunkt der Erstellung der OCSP-Antwort/CRL "gewährt", "anerkannt" oder "festgelegt" ist.

Kann die Kette nur zu einem anderen qualifizierten Vertrauensdiensteanbieter hergestellt werden, muss in der verwendeten hoheitlichen Vertrauensliste (EUMS-TL) der durch die Aufsichtsbehörde konfigurierte Nachweis vorhanden sein, dass dieser Vertrauensdiensteanbieter autorisiert ist, Sperrstatusinformationen für einen in der Vertrauensliste konfigurierten Dienst eines anderen Vertrauensdiensteanbieter anzubieten. Hat ein qualifizierter Vertrauensdiensteanbieter seinen Betrieb vollständig eingestellt, kann auch die nationale Aufsichtsbehörde diese Aufgabe übernehmen. Auch in diesem Fall ist in der hoheitlichen Vertrauensliste (EUMS-TL) der Nachweis vorhanden, dass die Aufsichtsbehörde für diesen qualifizierten Vertrauensdiensteanbieter den Sperrstatusdienst übernommen hat.

Der RFC 6960 erlaubt es auch, die Vertrauenswürdigkeit einer Sperrstatusantwort durch die Konfiguration der URL des zu vertrauenden OCSP-Responders in einer separaten Konfiguration vorzuhalten. Dieses Verfahren wird auch akzeptiert, wenn die Konfiguration in der Erweiterung der Governikus-TL vorgenommen wurde. Diese Prüfung erfolgt immer und führt im Negativfall zu einem unbestimmten Sperrstatus und einem Meldungstext, dass eine Vertrauensstellung nicht ermittelt werden konnte.

#### 5.5.17 Optionale Zeile "Sperrzeitpunkt"

In der optionalen Zeile "Sperrzeitpunkt" wird, sollte das Zertifikat zum Prüfzeitpunkt gesperrt sein, das Datum und die Uhrzeit des Zeitpunktes des Sperrzeitpunktes angezeigt. Die Form ist `TT.MM.JJJJ hh:mm:ss`.

#### 5.5.18 Optionale Zeile "Sperrgrund"

In der optionalen Zeile "Sperrgrund" wird, sollte das Zertifikat zum Prüfzeitpunkt gesperrt sein, der Sperrgrund angezeigt. Die Angabe wurde der OCSP-Antwort oder der CRL entnommen. Folgende Sperrgründe sind möglich und werden 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

### 5.5.19 Überschrift "Prüfung der Sperrstatusinformationen"

Unter der Überschrift "Prüfung der Sperrstatusinformationen" werden die Ergebnisse der Signaturprüfung der OCSP-Antwort oder CRL sowie notwendige Kontextinformationen angezeigt.

| Prüfung der Sperrstatusinformationen                    |  |
|---|--|
| Art der Sperrstatusermittlung:                          | OCSP-Antwort                                 |
| Herkunft der Sperrstatusinformationen:                  | Online bezogen vom Vertrauensdiensteanbieter |
| Signatur durch:   | D-TRUST OCSP 3 3-1 2016                      |
| Ermittelter Status mindestens korrekt bis:              | 05.10.2021, 10:47:25                         |
| Neuere Statusinformationen spätestens verfügbar ab:     | nicht vorhanden                              |
| Signaturzeitpunkt der OCSP-Antwort bzw. CRL:            | 05.10.2021, 10:47:25                         |
| Prüfzeitpunkt der Signatur der OCSP-Antwort bzw. CRL:   | Behaupteter Signaturzeitpunkt                |
| Ergebnis der Signaturprüfung der OCSP-Antwort bzw. CRL: | <b>gültig</b>                                |

Abbildung 14: Bereich B Knoten "Prüfung des Zertifikats von <Name>", Prüfung der Sperrstatusinformation

### 5.5.20 Zeile "Art der Sperrstatusermittlung"

In der Zeile "Art der Sperrstatusermittlung" wird angezeigt ob eine OCSP-Antwort eingeholt wurde oder die Ermittlung auf Basis einer CRL erfolgte. Folgende Werte sind möglich:

- Zertifikatsperrliste (CRL)
- OCSP-Antwort

### 5.5.21 Zeile "Herkunft der Sperrstatusinformationen"

In der Zeile "Herkunft der Sperrstatusinformationen" wird die Quelle der Sperrstatusinformation angezeigt. Folgende Werte sind möglich:

- **Aus der Inhaltsdatensignatur:** bedeutet, dass die Sperrstatusinformation bereits der Signatur (als unsigniertes Attribut) beigefügt und diese Quelle verwendet wurde.
- **Aus dem Zwischenspeicher des CVS:** bedeutet, dass die Sperrstatusinformation durch den Certificate Validation Server gepuffert vorlag. D.h., der Sperrstatus des geprüften Zertifikats wurde bereits einmal kurz vor der Durchführung dieser Prüfung schon einmal über OCSP ermittelt.
- **Online bezogen vom Vertrauensdiensteanbieter:** bedeutet, dass eine Sperrstatusanfrage (OCSP-Anfrage) online an den (in der Regel) im Zertifikat konfigurierten Dienst des Vertrauensdiensteanbieters gerichtet, die Anfrage vom Dienst beantwortet oder über die im Zertifikat konfigurierte URL eine CRL heruntergeladen wurde.

### 5.5.22 Zeile "Signatur durch"

In der Zeile "Signatur durch" wird der Name der Organisation angezeigt, für die das OCSP-Signer-Zertifikat oder das CRL-Signer-Zertifikat ausgestellt wurde. Es handelt sich um den Common Name des Inhabers aus dem Zertifikat. Das ist in der Regel der Name des Vertrauensdiensteanbieters mit dem Zusatz OCSP bzw. CRL.

### 5.5.23 Zeile "Ermittelter Status mindestens korrekt bis"

In der Zeile "Ermittelter Status mindestens korrekt bis" werden das Datum und Uhrzeit angezeigt, zu der in der Sperrinformation kommunizierte Status aktuell war. Die Form ist



TT.MM.JJJJ hh:mm:ss. Die Angabe wurde der OCSP-Antwort oder der CRL entnommen (Feld `thisUpdate`).

#### 5.5.24 Zeile "Neuere Statusinformationen spätestens verfügbar ab"

In der Zeile "Neuere Statusinformationen spätestens verfügbar ab:" werden das Datum und Uhrzeit angezeigt, zu der spätestens eine aktualisierte Sperrinformation beim Dienst angefordert werden kann. Die Form ist TT.MM.JJJJ hh:mm:ss. Bei OCSP-Antworten wird in der Regel hier "nicht vorhanden" angegeben sein. Dies bedeutet, dass jede neue OCSP-Anfrage zu einem aktualisierten Status führt.

#### 5.5.25 Zeile "Signaturzeitpunkt der OCSP-Antwort bzw. CRL"

In der Zeile "Signaturzeitpunkt der OCSP-Antwort bzw. CRL" wird das Datum und die Uhrzeit des Signaturzeitpunktes der OCSP-Antwort oder CRL angezeigt. Die Form ist TT.MM.JJJJ hh:mm:ss.

#### 5.5.26 Zeile "Prüfzeitpunkt der Signatur der OCSP-Antwort bzw. CRL"

Die Signaturprüfung von OCSP-Antworten und CRLs erfolgt ausschließlich zu deren Erstellungszeitpunkten. Bei der OCSP-Antwort ist das die Zeitangabe `producedAt`; bei der CRL die Zeitangabe `thisUpdate`. Angezeigt wird dieser Zeitpunkt als "Behaupteter Signaturzeitpunkt", obwohl es sich in der Regel um einen Zeitpunkt handelt, der auf Basis einer technisch synchronisierten Serverzeit erstellt wurde. Eine Konfiguration des Vertrauensniveaus über eine Prüfrichtlinie ist nicht möglich.

#### 5.5.27 Zeile "Ergebnis der Signaturprüfung der OCSP-Antwort bzw. CRL" mit Knoten

In der Zeile "Ergebnis der Signaturprüfung der OCSP-Antwort bzw. CRL" mit Knoten wird das kumulierte Ergebnis der Prüfung der Signatur der Sperrstatusantwort angezeigt. Folgende Werte sind möglich:

- **gültig** (grün gültig): Alle gemäß verwendeter Prüfrichtlinie notwendigen Einzelprüfungen sind erfolgreich verlaufen.
- **unbestimmt** (gelb unbestimmt): Mindestens eine gemäß Prüfrichtlinie notwendige Einzelprüfung konnte nicht durchgeführt werden oder lieferte ein unbestimmtes Ergebnis zurück.
- **ungültig** (rot ungültig): Mindestens eine gemäß Prüfrichtlinie notwendige Einzelprüfung ist endgültig fehlgeschlagen.
- **nicht geprüft** (schwarz nicht geprüft): Ist es aufgrund der verwendeten Prüfrichtlinie oder aufgrund von Angaben des Vertrauensdiensteanbieters im OCSP-Signer-Zertifikat (`ocsp_no_check`) nicht notwendig, den Sperrstatus zu ermitteln, wird dieser Wert angezeigt mit einer erläuternden Meldung.

Nach Aufklappen dieses Knotens werden die einzelnen Prüfergebnisse zur Integritätsprüfung und die kumulierten Prüfergebnisse zur Prüfung der Zertifikate vom Signaturzertifikat bis zu einem Vertrauensanker angezeigt. Die Anzeige der Prüfung einer Signatur im Prüfprotokoll ist generisch und daher auch für die Prüfung der Signatur einer OCSP-Antwort/einer CRL zutreffend. Die Beschreibung der Einzelprüfergebnisse folgt daher auch der Beschreibung in diesem Kapitel beginnend mit Kapitel 5.1 Zeile "Verwendete Prüfrichtlinie mit Link:".

## 5.6 Bereich B Knoten "Prüfung des Zertifikats von < Name >" aufgeklappt (Zertifikat Vertrauensanker)

In diesem Kapitel werden die Einzelprüfergebnisse einer Zertifikatsprüfung beschrieben die nach Aufklappen des Knotens der Zeile "Prüfung des Zertifikats von < Name >" im Prüfprotokoll des Bereichs B "Prüfung der Signaturen" angezeigt werden für den Fall, dass das Zertifikat als Vertrauensanker genutzt werden darf. Da in diesem Fall das Zertifikat selbst nicht mehr geprüft wird, sind diese ausgewählte Zertifikatsinhalte und der Nachweis, dass das CA-Zertifikat als Vertrauensanker verwendet werden darf.

|  |  |
|--|--|
| Prüfung des Zertifikats von D-TRUST CA 3-1 2016:<br>Meldungen:   | <div style="background-color: #444; color: white; padding: 2px; text-align: center; font-weight: bold;">nicht geprüft</div> Das Zertifikat ist ein Dienste-Identifizier aus einer gültigen hoheitlichen Vertrauensliste (EUMS-TL). Gemäß verwendeter Prüfrichtlinie ist es damit ein Vertrauensanker und wird nicht geprüft. |
| <b>Angaben aus dem geprüften Zertifikat</b>  |  |
| + Name des Inhabers:<br>Staat in dem der Aussteller ansässig ist:<br>Seriennummer:<br>Gültigkeitszeitraum:   | D-TRUST CA 3-1 2016<br>Deutschland<br>1041526<br>26.10.2016, 10:36:38 bis 26.10.2031, 09:36:50   |
| <b>Prüfung der verwendeten Vertrauensliste</b>   |  |
| Ergebnis der Prüfung der Signatur der verwendeten Vertrauensliste und LOTL:<br>Ergebnis der Prüfung der zeitlichen Gültigkeit der Vertrauensliste: | <div style="background-color: #008000; color: white; padding: 2px; text-align: center; font-weight: bold;">gültig</div><br><div style="background-color: #008000; color: white; padding: 2px; text-align: center; font-weight: bold;">gültig</div>   |
| Link zu Details zur Vertrauensliste:   | <a href="#">Vertrauensliste #1</a>   |

Abbildung 15: Bereich B Knoten "Prüfung des Zertifikats von < Name >" aufgeklappt, wenn Zertifikat Vertrauensanker (EU-qualifizierte Signatur)

### 5.6.1 Überschrift "Angaben aus dem Zertifikat"

Unter der Überschrift "Angaben aus dem Zertifikat" werden ausgewählte Zertifikatsinhalte angezeigt.

### 5.6.2 Zeile "Name des Inhabers" mit Knoten

In der Zeile "Name des Inhabers" wird der Name des Inhabers des geprüften Zertifikats angezeigt. Es handelt sich um den Common-Name des Inhabers aus dem Zertifikat.

Nach dem Aufklappen des Knotens wird je nach Anforderung entweder der gesamte Inhalt des Zertifikats angezeigt oder eine Kurzansicht. Diese Kurzansicht umfasst die Bereiche Inhaber, Aussteller, die Erweiterung QC-Statement und die wichtigsten Felder aus dem Bereich allgemeine Angaben. Bei Common-PKI-konformen Zertifikaten werden auch die beschränkenden Attribute aufgeführt. Zur Beschreibung der Zertifikatsinhalte, siehe Kapitel 9.

### 5.6.3 Zeile "Staat in dem der Aussteller ansässig ist"

In der Zeile "Staat in dem der Aussteller ansässig ist" wird der EU-Mitgliedsstaat angezeigt, in dem der Aussteller des CA-Zertifikats (also der Vertrauensdiensteanbieter) seinen Geschäftssitz beisitzt.

### 5.6.4 Zeile "Seriennummer"

In der Zeile "Seriennummer" wird die Seriennummer aus dem geprüften Zertifikat angezeigt.

### 5.6.5 Zeile "Gültigkeitszeitraum"

In der Zeile "Gültigkeitszeitraum" wird der Gültigkeitszeitraum des geprüften Zertifikats angezeigt. Die Form ist `TT.MM.JJJJ, hh:mm:ss` bis `TT.MM.JJJJ, hh:mm:ss`.

### 5.6.6 Überschrift "Prüfung der verwendeten Vertrauensliste"

Unter der Überschrift "Prüfung der verwendeten Vertrauensliste" werden die Einzelprüfergebnisse angezeigt, die eine notwendige Bedingung sind, damit das Zertifikat als Vertrauensanker genutzt werden darf.

### 5.6.7 Zeile "Ergebnis der Prüfung der Signatur der verwendeten Vertrauensliste und LOTL"

In der Zeile "Ergebnis der Prüfung der Signatur der verwendeten Vertrauensliste und LOTL" wird das Ergebnis der Signaturprüfung der verwendeten Vertrauensliste (aus dem das Zertifikat als SDI stammt, welches als Vertrauensanker fungiert) und die Prüfung der Signatur der List of Trusted Lists der EU-Kommission (LOTL) angezeigt.

- **gültig** (grün gültig): Die Prüfung ist erfolgreich verlaufen. Die Vertrauensliste ist gültig und kann verwendet werden.
- **unbestimmt** (gelb unbestimmt): Die Prüfung lieferte ein unbestimmtes Ergebnis zurück. Mindestens eine der beiden Signaturprüfungen lieferte ein unbestimmtes Ergebnis zurück, so dass den Konfigurationen in der Vertrauensliste nicht vertraut werden darf. Sie werden nicht genutzt.

Ist das Prüfergebnis "unbestimmt", haben alle Einzelprüfungen, die auf Informationen der Vertrauensliste zurückgreifen, einen unbestimmten Status. Der SDI darf z.B. nicht als Vertrauensanker verwendet werden.

### 5.6.8 Zeile "Ergebnis der Prüfung der zeitlichen Gültigkeit der Vertrauensliste"

In der Zeile "Ergebnis der Prüfung der zeitlichen Gültigkeit der Vertrauensliste" wird angezeigt, ob zum Zeitpunkt der Verwendung der Vertrauensliste gültig war (`NextUpdate` in der Zukunft). Folgende Prüfergebnisse sind möglich:

- **gültig** (grün gültig): Die Prüfung ist erfolgreich verlaufen. Der Prüfzeitpunkt liegt innerhalb des Gültigkeitsintervalls der Vertrauensliste.
- **ungültig** (rot ungültig): Die Prüfung ist fehlgeschlagen. Der Prüfzeitpunkt liegt außerhalb des Gültigkeitsintervalls der Vertrauensliste. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.

Hinweis: Über die durch die Governikus KG betriebene Infrastruktur zur Verteilung von Vertrauenslisten ist sichergestellt, dass immer die aktuellsten Listen zur Verfügung gestellt werden.

### 5.6.9 Zeile "Link zu Details zur Vertrauensliste"

Durch einen Klick auf den Link in der Zeile "Link zu Details zur Vertrauensliste" wird zu dem technischen Bereich im Prüfprotokoll gesprungen, an dem relevante Metainformationen zur verwendeten Vertrauensliste angezeigt werden. Über einen Link dort kann auch die verwendete Vertrauensliste (im XML-Format) vom lokalen Filemanager heruntergeladen werden. Der lokale Filemanager ist der Service beim Betreiber, der dem Certificate Validation Server die Vertrauenslisten zur Verfügung stellt.

## 6 Bereich B optionaler Knoten "Ergebnis der Prüfung des Signaturzeitstempels" aufgeklappt

Der optionale Knoten "Ergebnis der Prüfung des Signaturzeitstempels" des Bereichs B "Prüfung der Signaturen" ist nur dann vorhanden, wenn ein Signaturzeitstempel und/oder ein Inhaltsdatenzeitstempel ermittelt werden konnte. Inhaltsdaten- und Signaturzeitstempel haben unterschiedliche Funktionen:

- Ein Inhaltsdatenzeitstempel kann bei positiver Prüfung die unveränderte Existenz von Inhaltsdaten zu einem bestimmten Zeitpunkt nachweisen.
- Ein Signaturzeitstempel kann bei positiver Prüfung nachweisen, dass eine elektronische Signatur spätestens zum Zeitpunkt der Erzeugung des Zeitstempels existiert hat.

Nach dem Aufklappen des Knotens folgt eine weitere Baumstruktur - analog zur Signaturprüfung -, die in den folgenden Unterkapiteln beschrieben wird.

|   |                                  |   |
|---|----------------------------------|---|
| - | Signaturzeitstempel              | <b>gültig</b>                           |
| + | Zeitstempel erzeugt durch:       | exceet TSA 05                           |
| + | Niveau und Typ des Zeitstempels: | EU-qualifizierter Zeitstempel (EUMS-TL) |
| + | Ergebnis der Zeitstempelprüfung: | <b>gültig</b>                           |

Abbildung 16: Bereich B optionaler Knoten "Ergebnis der Prüfung des Signaturzeitstempels" aufgeklappt (EU-qualifizierter Zeitstempel)

### 6.1 Zeile "Zeitstempel erzeugt durch" mit Knoten

In der Zeile "Zeitstempel erzeugt durch" wird der Common Name des Inhabers aus dem Zertifikat angezeigt. Dies ist in der Regel der Name des Anbieters, ggf. ein Namensunterscheider.

Nach dem Aufklappen des Knotens in der Zeile "Zeitstempel erzeugt durch" wird der vollständige Inhalt des geprüften Zertifikats angezeigt. Zur Beschreibung der Zertifikatsinhalte siehe Kapitel 6.

### 6.2 Zeile "Niveau und Typ des Zeitstempels" mit Knoten

In der Zeile "Niveau und Typ des Zeitstempels" wird das Niveau des Zeitstempels angezeigt. Mögliche Werte sind:

- Nicht-qualifizierter Zeitstempel
- Nicht-qualifizierter Zeitstempel eines VDA zur Augmentierung von QES
- Nicht-qualifizierter Zeitstempel eines qVDA zur Augmentierung von QES
- EU-qualifizierter elektronischer Zeitstempel
- Qualifizierter elektronischer Zeitstempel gemäß SigG

#### Erläuterung der Niveaus und Typen

- Ein nicht-qualifizierter Zeitstempel:  
wird von einem nicht qualifizierten Zeitstempeldienst herausgegeben, der Zeitstempel erzeugt und signiert.
- Ein nicht-qualifizierter Zeitstempel eines VDA zur Augmentierung von QES:  
wird von einem nicht qualifizierten Zeitstempeldienst herausgegeben, der Zeitstempel-Token erstellt. Er wird von einem Vertrauensdiensteanbieter betrieben, der einen nicht-

qualifizierten Zeitstempeldienst betreibt. Die Zeitstempel-Token können bei der Validierung von EU-qualifizierten Signaturen (auch Siegel sowie fortgeschrittene Signaturen oder Siegel unterstützt durch EU-qualifizierte Zertifikate) verwendet werden, um die Signaturgültigkeit zu ermitteln oder zu verlängern, wenn das EU-qualifizierte Zertifikat widerrufen oder auslaufen wird.

- Ein nicht-qualifizierter Zeitstempel eines qVDA zur Augmentierung von QES: wird von einem nicht qualifizierten Zeitstempeldienst, der Zeitstempel-Token erstellt, herausgegeben. Er wird betrieben von einem qualifizierten Vertrauensdiensteanbieter, der EU-qualifizierte Zertifikate ausstellt. Die Zeitstempel-Token können bei der Validierung von EU-qualifizierten Signaturen (auch Siegel sowie fortgeschrittene Signaturen oder Siegel unterstützt durch EU-qualifizierte Zertifikate) verwendet werden, um die Signaturgültigkeit zu ermitteln oder zu verlängern, wenn das qualifizierte Zertifikat widerrufen oder auslaufen wird.
- Ein EU-qualifizierter elektronischer Zeitstempel: wird von einem EU-qualifizierten Zeitstempeldienst herausgegeben, der EU-qualifizierte Zeitstempel erzeugt und qualifiziert signiert (qualifizierte Zeitstempel-Token). Dieses geschieht in Übereinstimmung mit nationalen Rechtsvorschriften gemäß dem in der Trusted List benannten EU-Mitgliedsstaat oder gemäß der Verordnung (EU) Nr. 910/2014.
- Ein qualifizierter elektronischer Zeitstempel gemäß SigG: wurde von einem nicht EU-qualifizierten Zeitstempeldienst sondern einem Zeitstempeldienst herausgegeben, der gemäß den Anforderungen des deutschen Signaturgesetzes vor Inkrafttreten der eIDAS-Verordnung betrieben wurde. In der eIDAS-Verordnung (EU) Nr. 910/2014 werden diese Zeitstempel nicht EU-qualifizierten Zeitstempeln rechtlich gleichgestellt.

Nach Aufklappen des Knotens werden das Ermittlungsergebnis und die Entscheidungsgrundlagen angezeigt, die für die Ermittlung des Niveaus herangezogen wurden. Der aufgeklappte Knoten ist vom Aufbau her identisch mit dem aufgeklappten Knoten 4 "Niveau und Typ der Signatur".

### 6.3 Zeile "Ergebnis der Zeitstempelprüfung" mit Knoten

In der Zeile "Ergebnis der Zeitstempelprüfung" wird das Ergebnis der Prüfung der Signatur des Zeitstempels angezeigt. Folgende Werte sind möglich:

- **gültig** (grün gültig): Alle gemäß Prüfrichtlinie notwendigen Einzelprüfungen sind erfolgreich verlaufen. Es handelt sich gemäß den Vorgaben in der Prüfrichtlinie zum angezeigten Prüfzeitpunkt und mit dem angegebenen Vertrauensniveau des Prüfzeitpunkts um eine gültige Zeitstempel-Signatur.
- **unbestimmt** (gelb unbestimmt): Mindestens eine gemäß Prüfrichtlinie notwendige Einzelprüfung konnte nicht durchgeführt werden oder lieferte ein unbestimmtes Ergebnis zurück. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.
- **ungültig** (rot ungültig): Mindestens eine gemäß Prüfrichtlinie notwendige Einzelprüfung ist endgültig fehlgeschlagen. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.

Nach Aufklappen des Knotens der Zeile "Ergebnis der Zeitstempel" werden die Einzelprüfergebnisse der Integritäts- und Zertifikatsprüfungen angezeigt, die zum Gesamtstatus der Zeitstempelsignatur geführt haben. Eine Beschreibung der Einzelprüfergebnisse befindet sich in Kapitel 5 "Knoten Ergebnis der Signaturprüfung aufgeklappt".

## 7 Bereich B optionaler Knoten "Beweiswertbewahrung durch Archivzeitstempel" aufgeklappt

Wird in einer EU-qualifizierten Signatur ein EU-qualifizierter Archivzeitstempel gefunden, dann wird im Prüfprotokoll des Bereichs B "Prüfung der Signaturen" die optionale Zeile "Beweiswertbewahrung durch Archivzeitstempel" mit Knoten angezeigt.

| Archivzeitstempel #1.1             |  |
|------------------------------------|--|
| Zeitpunkt des Archivzeitstempels:  | 18.06.2019, 15:14:16   |
| + Zeitstempel erzeugt durch:       | exceet TSA 05  |
| + Verwendete Prüfrichtlinie:       | <a href="#">Qualifizierte elektronische Signatur (qVDA aus DE eIDAS-VO) #1</a> |
| + Niveau und Typ des Zeitstempels: | EU-qualifizierter Zeitstempel (EUMS-TL)  |
| + Ergebnis der Zeitstempelprüfung: | <b>gültig</b>  |

Abbildung 17: Bereich B optionaler Knoten "Beweiswertbewahrung durch Archivzeitstempel" aufgeklappt

Im folgenden Kapitel werden Ergebnisse der Prüfung des Archivzeitstempels bzw. des ERS mit reduziertem Hashwertbaum und Archivzeitstempel beschrieben.

Sollten mehrere Archivzeitstempel oder mehrere reduzierte Hashwertbäume mit einem oder mehreren Archivzeitstempeln die Signatur absichern, wird die in den folgenden Unterkapiteln erläuterte Anzeige im Prüfprotokoll untereinander wiederholt.

Die Zeile wird immer angezeigt, unabhängig davon, ob der EU-qualifizierte Archivzeitstempel gültig ist und der Beweiswert einer EU-qualifizierten Signatur gesichert werden konnte.

### 7.1 Überschrift "Archivzeitstempel"

Unter der Überschrift "Archivzeitstempel" werden Kontextinformationen zum Zeitstempel und das Ergebnis der Zeitstempelprüfung angezeigt.

Die Anzeige ist identisch mit der Anzeige für einen Signatur- oder Inhaltsdatenzeitstempel und wird in den Unterkapiteln des Kapitels 6 erläutert.

#### 7.1.1 Optionale Überschrift "Hashwertbaum"

Neben \*AdES-Signaturen des Levels LTA können auch CAdES E ERS Signaturen oder Signaturen in exportierten XAIP-Containern, beide mit eingebetteter `EvidenceRecordSyntax` (mit Archivzeitstempel), validiert werden. In diesem Fall werden über einen Hashwertbaum die Signatur und die Kontextinformationen, wie OCSP-Antworten, referenziert und abgesichert.

Die Prüfergebnisse, ob das für den Hashwertbaum verwendete Hashwertverfahren für eine EU-qualifizierte elektronische Signatur zum Zeitpunkt der Durchführung der Prüfung noch geeignet war, werden unter der Überschrift "Hashwertbaum" angezeigt.

| Hashwertbaum #1.1                                   |   |
|---|---|
| Hashverfahren                                       | SHA256  |
| Verwendeter Algorithmenkatalog:                     | <a href="#">ETSI Cryptographic Suites TS 119 312 V1.2.1</a> |
| Hashverfahren zur Beweiswertbewahrung geeignet bis: | 31.12.2023, 23:59:59  |
| Prüfzeitpunkt der Beweiswertbewahrung:              | 07.08.2019, 13:51:19  |
| Beweiswertbewahrung bis zu diesem Zeitpunkt:        | <b>gültig</b>   |

Abbildung 18: Überschrift "Hashwertbaum" bei CAdES E ERS Signaturen

### 7.1.2 Zeile "Hashverfahren"

In der Zeile "Hashverfahren" wird der Name des für den Hashwertbaum verwendeten Hashverfahrens angezeigt.

### 7.1.3 Zeile "Verwendeter Algorithmenkatalog"

In der Zeile "Verwendeter Algorithmenkatalog" wird der Name und die Version des für die Eignungsprüfung des Hashverfahrens verwendeten Algorithmenkatalogs angezeigt.

### 7.1.4 Zeile "Hashverfahren zur Beweiswertbewahrung geeignet bis"

In der Zeile "Hashverfahren zur Beweiswertbewahrung geeignet bis" wird das Datum und die Uhrzeit angezeigt, bis zu dem das Hashverfahren für qualifizierte elektronische Signaturen verwendet werden darf. Die Form ist `TT.MM.JJJJ hh:mm:ss`.

Wird statt eines Datums "ohne Ablaufdatum" angezeigt, handelt es sich um einen Signaturalgorithmus, für den in dem verwendeten Algorithmenkatalog kein Ablaufdatum festgelegt wurde.

### 7.1.5 Zeile "Prüfzeitpunkt der Beweiswertbewahrung"

In der Zeile "Prüfzeitpunkt der Beweiswertbewahrung" werden das Datum und Uhrzeit angezeigt, zu dem die Eignung des Hashverfahrens ermittelt wird. Die Form ist `TT.MM.JJJJ hh:mm:ss`. Wird eine Governikus Prüfrichtlinie für qualifizierte elektronische Signaturen verwendet, dann ist das in der Regel der Zeitpunkt der Durchführung der Prüfung.

Nur wenn es einen jüngeren reduzierten Hashwertbaum gibt, der rechtzeitig vor Ablauf der Eignung des verwendeten Hashverfahrens für den ersten Hashwertbaum den Beweiswert bewahrt hat und durch einen neuen Archivzeitstempel abgesichert wurde, wird als Prüfzeitpunkt die Zeitstempelung des jüngeren Archivzeitstempels verwendet.

### 7.1.6 Zeile "Beweiswertbewahrung bis zu diesem Zeitpunkt"

In der Zeile "Beweiswertbewahrung bis zu diesem Zeitpunkt" wird das Prüfergebnis der Eignung des Hashverfahrens zum in der vorherigen Zeile angegebenen Zeitpunktes angezeigt. Folgende Prüfergebnisse sind möglich:

- **gültig** (grün gültig): Das Hashverfahren war zum in der vorherigen Zeile angegebenen Zeitpunkt für eine EU-qualifizierte elektronische Signatur (und damit zur Beweiswertbewahrung) geeignet.
- **ungültig** (rot ungültig): Das Hashverfahren war zum in der vorherigen Zeile angegebenen Zeitpunkt für eine EU-qualifizierte elektronische Signatur (und damit zur Beweiswertbewahrung) nicht oder nicht mehr geeignet.

Die Eignung des verwendeten Hashverfahrens ist eine notwendige, aber nicht hinreichende Bedingung für eine erfolgreiche Beweiswertbewahrung einer qualifizierten elektronischen Signatur. Zusätzlich zu dem positiven Prüfergebnis muss auch die Prüfung des EU-qualifizierten elektronischen Archivzeitstempels und der EU-qualifizierten elektronischen Signatur positiv verlaufen sein.

## 8 Bereich A Knoten "Dokument bzw. Containerstruktur" aufgeklappt

Im Bereich A "Dokument bzw. Containerstruktur" werden nach dem Aufklappen des Knotens das Signaturformat, der Name des Signierenden und das Signaturprüfergebnis in Ampelform angezeigt. Sind in dem geprüften Dokument/Container mehrere Signaturen vorhanden, werden für jede Signatur der Name des Signierenden und das Prüfergebnis in Ampelform angezeigt. Wurden mehrere Signaturen geprüft, werden diese grafisch in ihrer Zuordnung zum signierten Inhalt angezeigt.

Im Unterkapitel 8.2 wird zunächst grundsätzlich der aufgeklappte Knoten "Dokument-/Containerstruktur" vorgestellt, bevor in den folgenden Kapiteln die Besonderheiten der einzelnen Dokumenten-/Containerformate mit Strukturinformationen beschrieben werden:

- CAdES-Signaturen (Kapitel 8.3)
- OSCI-Nachrichten (Kapitel 8.4)
- Signierte PDF-Dokumente (PAdES-Signaturen) (Kapitel 8.5)
- De-Mail-Nachrichten (Kapitel 8.6)
- De-Mail-Bestätigungsnachrichten (Kapitel 8.7)
- ASiC-Container mit signierten Dokumenten (Kapitel 8.8).

### 8.1 Zeile "Signaturformat und Dateiname"

In der ersten Zeile des Knotens werden blau unterlegt das Signaturformat gefolgt durch den Dateinamen des signierten Dokuments angezeigt.

### 8.2 Knoten "Dokument- bzw. Containerstruktur" aufgeklappt

Nach Aufklappen des Knotens werden das Signaturformat, der Name des Signierenden und das Signaturprüfergebnis in Ampelform angezeigt.

Dokument-/Containerstruktur:

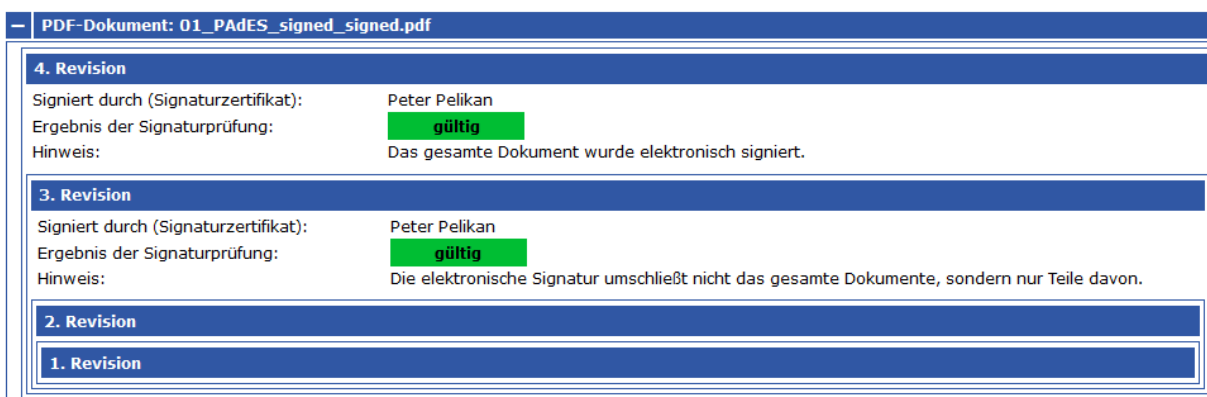


Abbildung 19: Bereich A " Dokument-/Containerstruktur" (aufgeklappt) bei einem signierten PDF-Dokument mit zwei Signaturen

Nach Aufklappen des Knotens hat dieser Bereich immer den folgenden Aufbau:



- In der Zeile "Signatur durch" wird immer der Name des Signierenden angezeigt.
- In der Zeile "Ergebnis der Signaturprüfung" wird das Gesamtprüfergebnis der digitalen Einzelsignatur in Ampelform angezeigt. Folgende Werte sind möglich:
  - **gültig** (grün gültig): Alle gemäß Prüfrichtlinie notwendigen Einzelprüfungen sind erfolgreich verlaufen.
  - **unbestimmt** (gelb unbestimmt): Mindestens eine gemäß Prüfrichtlinie notwendige Einzelprüfung konnte nicht durchgeführt werden oder lieferte ein unbestimmtes Ergebnis zurück. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.
  - **ungültig** (rot ungültig): Mindestens eine gemäß Prüfrichtlinie notwendige Einzelprüfung ist endgültig fehlgeschlagen. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.
- In weiteren Zeilen werden ggf. formatspezifische Kontextinformationen oder Hinweise angezeigt.

Wird ein Dokument mit einer Signatur geprüft, bei dem Strukturinformationen notwendig sind, um zu erkennen, welche Teile des Dokuments signiert wurden, werden nach Aufklappen des Knotens entsprechende Strukturinformationen angezeigt. Dies geschieht auch, wenn das Dokument mehrere Signaturen enthält oder signierte Dokumente in einem Container (OSCI-Nachricht, ZIP, ASiC, PDF-Portfolio) geprüft wurden.

Eine Beschreibung der möglichen Inhalte der Strukturinformationen findet sich im folgenden Kapitel.

## 8.3 CAdES-Signaturen

In diesem Kapitel wird die Dokumentenstruktur von CAdES-Signaturen beschrieben.

### 8.3.1 Zeile "Signaturtyp"

In der Zeile "Signaturtyp" wird im Bereich der Strukturinformationen in der Zeile „Signaturtyp“ zusätzlich angezeigt, um welchen Typ der Signatur es sich handelt.

Dokument bzw. Containerstruktur:

| - CAdES-Dokument: CAdES_enveloped_gruen.p7s                             |               |
|---|---------------|
| Signatur durch:   | Emil Erpel    |
| Signaturtyp:  | Enveloped     |
| Ergebnis der Signaturprüfung:   | <b>gültig</b> |
| Unbekanntes Dokumentformat: CAdES_enveloped_gruen.p7s_enveloped_content |               |

Abbildung 20: Bereich A "Dokument- bzw. Containerstruktur" bei CAdES-Signaturen

Folgende Werte sind möglich:

- Enveloped
- Detached

Bei einer enveloped Signatur liegen die Signatur und die Inhaltsdaten in einer Datei vor. Bei einer detached Signatur befinden sich Signatur und Inhaltsdaten in zwei getrennten Dateien.

## 8.4 OSCI-Nachrichten

In diesem Kapitel wird der Bereich A "Dokument-/Containerstruktur" für OSCI-Nachrichten der 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 OSCI-Nachricht. Ein Datencontainer wird dabei immer durch einen blau umrahmten Kasten symbolisiert.

Dokument bzw. Containerstruktur:

| - OSCI-Nachricht: OSCI_Nachricht_QES_TEST.osci |  |
|--|--|
| Betreff:                                       | Testnachricht  |
| Nachrichtenkennezeichen:                       | OSCI_3_125552554545  |
| Absender:                                      | Gans, Gustav   |
| Empfänger:                                     | Dagobert Duck  |
| Eingang auf dem Server:                        | 22.08.2017, 13:01:04   |
| Inhaltsdatencontainer: project_coco            |  |
| Signatur durch (Autor):                        | Gans, Gustav   |
| Ergebnis der Signaturprüfung:                  | <b>gültig</b>  |
| Inhaltsdaten:                                  | Nachrichteninhalt.xml, Nachrichtenvisualisierung.xml, Visitenkartenvisualisierung.xml, Nachrichteninformationen.properties |
| Inhaltsdatencontainer: govello_coco            |  |
| Inhaltsdaten:                                  | additional_infos, local_timestamps   |

Abbildung 21: Bereich A "Dokument-/Containerstruktur" OSCI-Nachricht (aufgeklappt)

Im Beispiel (siehe Abbildung 21) gibt es zwei Container (`project_coco` und `govello_coco`), der erste Inhaltsdatencontainer wurde signiert.

### 8.4.1 Zeile "OSCI-Nachricht: Dateiname"

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

### 8.4.2 Zeile "Betreff"

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

### 8.4.3 Zeile "Nachrichtenkennezeichen"

In der Zeile "Nachrichtenkennezeichen" wird das Nachrichtenkennezeichen der OSCI-Nachricht angezeigt. Das Nachrichtenkennezeichen selbst wird vom OSCI-Manager vergeben und dient auch im Nachhinein zur eindeutigen Bezugnahme auf die betreffende Nachricht. Jedes Nachrichtenkennezeichen ist eindeutig, da es nur einmal vergeben wird.

### 8.4.4 Zeilen "Absender" und "Empfänger"

In der Zeile "Absender" bzw. "Empfänger" wird der Name des Absenders bzw. Empfängers der OSCI-Nachricht angezeigt. Ist kein Empfänger vorhanden, wird die Meldung "k. A." für "keine Angabe" ausgegeben.

#### 8.4.5 Zeile "Eingang auf dem Server"

In der Zeile "Eingang auf dem Server" wird der Zeitpunkt angegeben, zu dem der Empfang der Nachricht auf dem OSCI-Server abgeschlossen wurde. Die Zeit wird in der Form `TT.MM.JJJJ hh:mm:ss` angezeigt. Ist kein Eingangszeitpunkt vorhanden, wird die Meldung "k. A." für "keine Angabe" ausgegeben.

#### 8.4.6 Optionale Zeile "Formatkonformität"

Die Zeile "Formatkonformität" wird nur angezeigt, wenn das Format der OSCI-Nachricht nicht spezifikationskonform ist. Folgende Werte sind möglich:

- **Unbestimmt** (gelb unbestimmt): Die Formatprüfung (gemäß OSCI-Spezifikation 1.2) lieferte ein unbestimmtes Ergebnis zurück. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert. Dieses unbestimmte Ergebnis wird z.B. angezeigt, wenn der Inhaltsdatencontainer der OSCI-Nachricht noch verschlüsselt ist.
- **ungültig** (rot ungültig): Die Formatprüfung lieferte ein endgültig ungültiges Ergebnis zurück. In einem Meldungstext unter dem Prüfergebnis werden die Gründe für dieses Prüfergebnis erläutert.

Die Formatprüfung hat keinen Einfluss auf das Prüfergebnis der Signatur.

#### 8.4.7 Zeile "Inhaltsdatencontainer: Name"

In der ersten Zeile hinter der Bezeichnung "Inhaltsdatencontainer" wird blau unterlegt der Name des Containers angezeigt, auf den sich das Ergebnis der Signaturprüfung und die in den folgenden Zeilen angezeigten Kontextinformationen beziehen. Ist der Datencontainer verschlüsselt, können keine Aussagen über den Inhalt gemacht werden. In diesem Fall wird hinter der Bezeichnung "Inhaltsdatencontainer" "(verschlüsselt)" angezeigt.

#### 8.4.8 Optionale Zeile "Ergebnis der Signaturprüfung"

Konnte eine Signatur ermittelt werden, wird in der optionalen Zeile "Ergebnis der Signaturprüfung" das kumulierte Signaturprüfergebnis angezeigt. Zur Erläuterung siehe Kapitel 8.2.

#### 8.4.9 Zeile "Inhaltsdaten"

In der Zeile "Inhaltsdaten" werden hinter dem Eintrag "Inhaltsdaten" die Dateinamen der Inhaltsdaten angezeigt.

#### 8.4.10 Zeile "Anhänge"

In der Zeile "Anhänge" werden hinter dem Eintrag "Anhänge" die Dateinamen der Anhänge angezeigt.

### 8.5 Signierte PDF-Dokumente

In diesem Kapitel wird die Dokumentenstruktur bei signierten PDF-Dokumenten beschrieben. Das PDF-Dateiformat unterstützt die inkrementelle Dokumentenaktualisierung. Jedes Mal, wenn das PDF-Dokument nach einer Veränderung (z.B. einer Anmerkung) gespeichert wird,

wird eine sogenannte neue "Revision" der PDF-Datei erstellt. Eine Signatur erzeugt auch immer eine neue Revision, die die vorherigen Revisionen miteinschließt. Enthält ein PDF-Dokument mehrere Signaturen, sind sie daher auch ineinander verschachtelt. Die Anzeige stellt diese Struktur graphisch dar.

Dokument-/Containerstruktur:

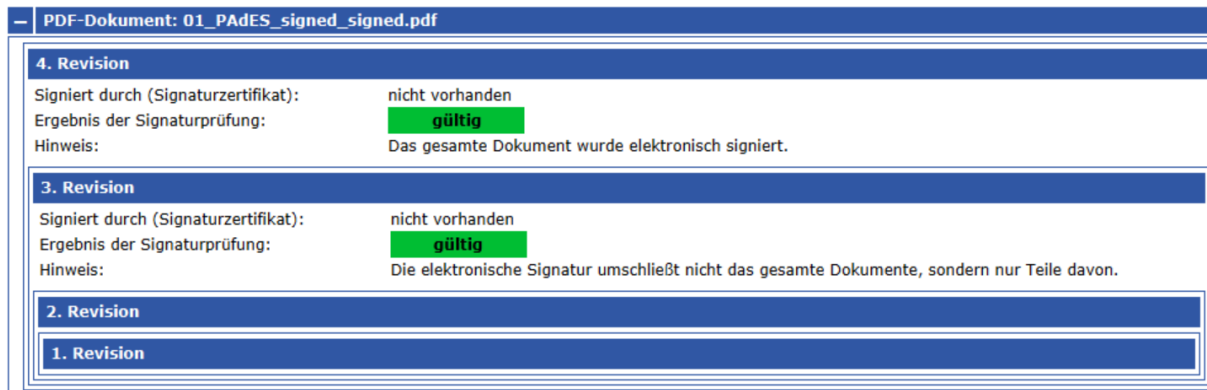


Abbildung 22: Struktur eines PDF-Dokuments mit zwei Signaturen (aufgeklappt)

Im Beispiel (siehe Abbildung 22) enthält die geprüfte Datei zwei Signaturen, wobei die äußere Signatur (erzeugt die 4. Revision) alle weiteren inneren Revisionen umfasst sowie eine Signatur (3. Revision), die Dokumenteninhalte von zwei Revisionen (2. und 1. Revision) umschließt.

Die Prüfung von PDF-Portfolios wird auch unterstützt, wenn diese ausschließlich PDF-Dokumente enthalten. Die Anzeige der Strukturinformationen kann dann eine sehr hohe Komplexität aufweisen.

### 8.5.1 Zeile "PDF-Dokument: Dateiname"

In der Zeile "PDF-Dokument: Dateiname" wird in der ersten Zeile blau unterlegt der Dateiname hinter der Bezeichnung des Signaturformats "PDF-Dokument" angezeigt.

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

### 8.5.2 Zeile "x. Revision"

In der Zeile "x. Revision" wird blau unterlegt die Revisionsnummer angezeigt. Ist in der Revision keine Signatur ermittelt worden, wird in der Folgezeile die nächste Revision angezeigt bis zur 1. Revision.

### 8.5.3 Optionale Zeile "Signatur durch"

Konnte eine Signatur ermittelt werden, wird in der optionalen Zeile "Signatur durch" der Name des Signierenden angezeigt. Der Name besteht bei Personenzertifikaten in der Regel aus dem Vor- und Nachnamen des Zertifikatsinhabers oder einem Pseudonym. Bei Organisationszertifikaten (z.B. Siegelzertifikaten) wird der Name der Organisation angezeigt, der in der Regel verwendet wird, um sich selbst zu vertreten.

### 8.5.4 Optionale Zeile "Ergebnis der Signaturprüfung"

Konnte eine Signatur ermittelt werden, wird in der optionalen Zeile "Ergebnis der Signaturprüfung" das kumulierte Signaturprüfergebnis angezeigt. Zur Erläuterung siehe Kapitel 8.2.

### 8.5.5 Optionale Zeilen "Hinweis" und Zeile "Warnung"

Konnte eine Signatur ermittelt werden, werden in dieser Zeile Informationen zur PAdES-Signatur angezeigt. Es gibt Hinweise und Warnungen.

Hinweise beziehen sich auf Eigenschaften der Signatur, die, betrachtet man nur die einzelne Signatur, nicht sicherheitskritisch sind. Sie beziehen sich z.B. auf Verletzungen der Standardkonformität und beeinflussen das Signaturprüfergebnis nicht.

Zusätzliche Warnmeldungen sind demgegenüber sicherheitskritisch. Es gibt zwar keinen technisch-mathematischen Angriff auf die Einzelsignatur, in der Gesamtbetrachtung des signierten PDF-Dokuments kann eine Manipulation des Inhalts durch nicht-signierte Revisionen jedoch nicht ausgeschlossen werden. Es wird dringend geraten, sich den Inhalt des signierten PDFs durch einen sicheren Viewer anzeigen zu lassen, um eine mögliche Manipulation entdecken zu können. Folgende Hinweise mit Warnung werden bei Manipulationsgefahr angezeigt:

- **Hinweis:** Die elektronische Signatur umschließt nicht das gesamte Dokument, sondern nur Teile davon.
- **Warnung:** Eine nach der digitalen Signatur erstellte Revision kann den signierten Inhalt in der Ansicht überlagern und manipulieren.
- **Hinweis:** Das gesamte Dokument wurde elektronisch signiert.
- **Warnung:** Es gibt mindestens eine weitere digitale Signatur und dazwischen mindestens eine unsignierte Revision. Nur wenn nach der ersten digitalen Signatur alle weiteren Revisionen auch digital signiert wurden, kann eine Manipulation ausgeschlossen werden.

Dokument-/Containerstruktur:

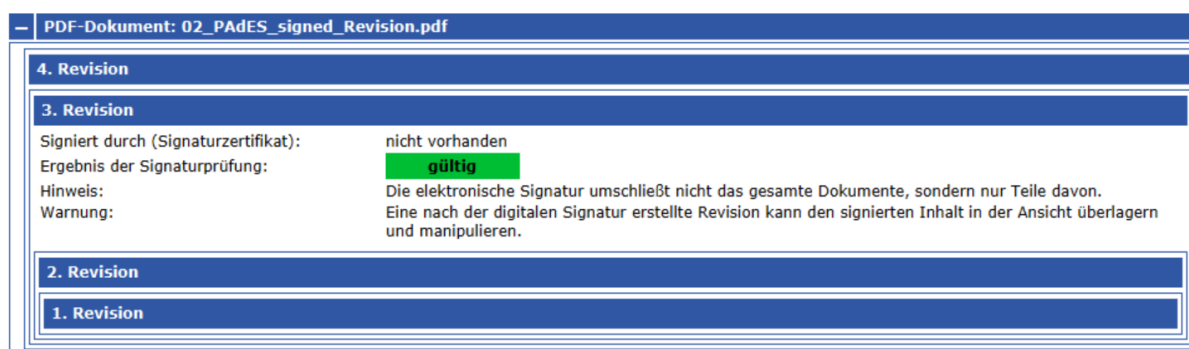


Abbildung 23: Bereich 1 "Zusammenfassung und Struktur" bei einem signierten, manipulationsgefährdeten PDF-Dokument (Teilsignatur)

Die digitale Signatur umschließt im ersten Fall nur Teile des PDFs. Es wurde nach der Signaturanbringung mindestens eine weitere nicht signierte Revision erzeugt. Eine nach der digitalen Signatur erstellte Revision kann den signierten Inhalt in der Ansicht überlagern und manipulieren. 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 (siehe Abbildung 23).

Umschließt die zuletzt erstellte digitale Signatur zwar das gesamte PDF, es gibt jedoch mindestens eine weitere davor erzeugte digitale Signatur und dazwischen mindestens eine unsignierte Revision, kann die unsignierte Revision den signierten Inhalt dieser digitalen Signatur manipulieren. Nur wenn nach der ersten digitalen Signatur alle weiteren Revisionen auch digital signiert wurden, kann eine Manipulation ausgeschlossen werden (siehe Abbildung 24).

Dokument-/Containerstruktur:

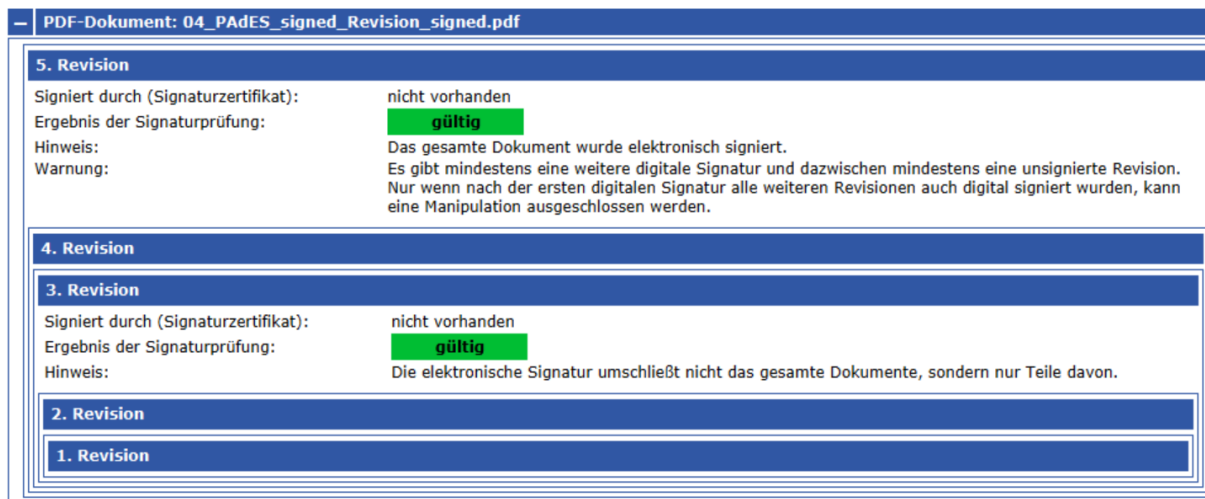


Abbildung 24: Bereich 1 "Zusammenfassung und Struktur" bei einem signierten, manipulationsgefährdeten PDF-Dokument (unsignierte Revision zwischen Signaturen)

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. Es gibt daher die dringende Empfehlung, sich die einzelnen Revisionen des PDFs in einem geeigneten PDF-Reader genau anzuschauen.

### 8.6 De-Mail-Nachrichten

In diesem Kapitel wird der Aufbau des Bereichs A "Dokument-/Containerstruktur" für normale De-Mail-Nachrichten beschrieben. Bei De-Mail-Nachrichten wird hinsichtlich ihrer Funktion insbesondere zwischen "normalen De-Mail-Nachrichten", "Bestätigungsnachrichten" und "Meldungsnachrichten" differenziert.

Dokument bzw. Containerstruktur:

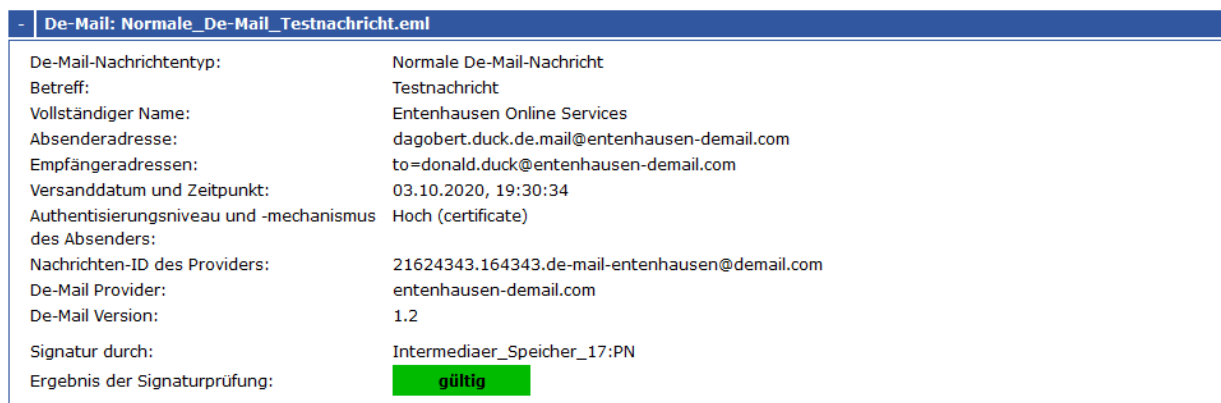


Abbildung 25: Bereich A Normale De-Mail-Nachricht (aufgeklappt)

In der Strukturansicht werden die in der De-Mail-Nachricht vorhandenen Metainformationen und das Signaturprüfergebnis angezeigt. Die einzelnen Nachrichtentypen unterscheiden hinsichtlich der angezeigten Metainformationen nur im Detail. Bei Bedarf ist kenntlich gemacht, auf welchen Nachrichtentyp sich die Erläuterungen beziehen. In den folgenden Kapiteln werden Metainformationen im Bereich "Dokument-/Containerstruktur" erläutert. Nicht alle Metainformationen müssen in jeder De-Mail-Nachricht vorhanden sein. Angezeigt werden aber immer alle vorhandenen Metainformationen.

### **8.6.1 Zeile "De-Mail-Nachricht: Dateiname"**

In der ersten Zeile "De-Mail-Nachricht: Dateiname" wird blau unterlegt bei allen Nachrichtentypen hinter der Bezeichnung des Signaturformats "De-Mail-Nachricht:" der Dateiname der De-Mail-Nachricht angezeigt mit der Endung `.eml`.

### **8.6.2 Zeile "De-Mail-Nachrichtentyp"**

In der Zeile "De-Mail-Nachrichtentyp" wird bei allen De-Mail-Nachrichtentypen der Typ der De-Mail-Nachricht angezeigt. Folgende Nachrichtentypen werden erkannt und angezeigt:

- Normale De-Mail-Nachricht (mit und ohne Absenderbestätigung)
- Versandbestätigung
- Eingangsbestätigung
- Abholbestätigung
- Bestätigungsnachricht im Falle von gefundener Schadsoftware
- Meldungsnachricht im Falle von gefundener Schadsoftware
- Meldungsnachricht
- Ident-Bestätigungsnachricht
- Unbekannter Typ

#### **Erläuterungen zu normalen De-Mail-Nachrichten**

Die normale De-Mail-Nachricht enthält den Nachrichteninhalte des Absenders. Sie kann durch den De-Mail-Provider qualifiziert elektronisch signiert sein (sogenannte DKIM-Signatur). Ist die Versandoption "Absenderbestätigt" durch den Absender gewählt worden (siehe Zeile Versandoptionen), muss die Nachricht vom De-Mail-Provider des Absenders mit einer qualifizierten elektronischen Signatur versehen werden (DKIM-Signatur). Der De-Mail-Provider des De-Mail-Absenders bestätigt damit, dass er den angegebenen Nachrichteninhalte der De-Mail-Nachricht entgegengenommen hat und dass der De-Mail-Absender sich mindestens mit "hoch" authentisiert hat.

#### **Erläuterungen zu Versandbestätigung, Eingangsbestätigung und Abholbestätigung**

Die Bestätigungsnachricht ist eine Nachricht, die von den De-Mail-Providern erstellte Bestätigungen über den Zustand einer De-Mail-Nachricht enthält. Die Versand- und Eingangsbestätigung muss folgende Daten enthalten: Adresse des Absenders, Adresse des Empfängers, Datum und Zeit des Versands oder des Eingangs, Name des De-Mail-Providers, Hashwert (Prüfsumme) der versendeten Nachricht. Die Abholbestätigung muss folgende Daten enthalten: Adresse des Absenders, Adresse des Empfängers, Datum und Zeit des Eingangs (Zeitpunkt, an dem die Nachricht im Postfach eingegangen ist), Datum und Zeit der Anmeldung (Zeitpunkt, zu dem die Abholbestätigung erzeugt wird), Name des De-Mail-Providers, Hashwert (Prüfsumme) der versendeten Nachricht.

Bestätigungsnachrichten müssen durch den De-Mail-Provider qualifiziert elektronisch signiert sein (sogenannte DKIM-Signatur). Eine besondere Bestätigungsnachricht wird bei gefundener Schadsoftware versendet.

### Erläuterungen zu Meldungsnachrichten

Meldungsnachrichten sind Nachrichten, die vom De-Mail-Provider erstellt werden, um den Nutzern Informationen über bestimmte Ereignisse zukommen zu lassen. Die zu übermittelnde Meldung ist im Nachrichten-Body der Nachricht enthalten. Eine besondere Meldungsnachricht wird bei gefundener Schadsoftware versendet.

### Erläuterung zu Ident-Bestätigungsnachrichten

Die Ident-Bestätigungsnachricht dient der Identitätsfeststellung. Auf Anforderung des Nutzers erstellt der De-Mail-Provider eine Ident-Bestätigung, die anschließend per De-Mail an die De-Mail-Adresse des Empfängers gesendet wird. Damit soll z.B. die Registrierung bei Online-Shops möglich sein oder der Nachweis, dass der De-Mail-Postfachinhaber älter als 18 Jahre ist. Die Nachricht muss vom De-Mail-Provider qualifiziert signiert (DKIM-Signatur) werden.

## 8.6.3 Zeile "Betreff"

In der Zeile "Betreff" wird bei allen Nachrichtentypen der Betreff der De-Mail-Nachricht aus dem E-Mail-Header angezeigt, bei Bestätigungsnachrichten auch die vom De-Mail-Provider ergänzten Bestandteile.

### Normale De-Mail-Nachrichten

Bei einer normalen De-Mail-Nachricht wird der Betreff aus dem E-Mail-Header angezeigt.

### Bestätigungsnachrichten

Bei Bestätigungsnachrichten gibt es zusätzlich folgende Konventionen für die Betreff-Zeile. Bei einer Versandbestätigung lautet der Betreff der Nachricht `"*Versandbestätigung* [Betreff der Nachricht]"`, bei einer Eingangsbestätigung: `"*Eingangsbestätigung* [Betreff der Nachricht]"` und bei einer Abholbestätigung `"*Abholbestätigung* [Betreff der Nachricht]"`.

### Meldungsnachrichten

Eine Meldungsnachricht, die darüber informiert, dass eine eingegangene Nachricht eine Anmeldung des De-Mail-Empfängers mit dem Authentifizierungsniveau "hoch" erforderlich macht, kann im Betreff den folgenden Hinweis enthalten: `"*Hinweis* Eine Nachricht erfordert vertrauliche Anmeldung"`.

## 8.6.4 Zeile "Vollständiger Name"

In der Zeile "Vollständiger Name" wird bei natürlichen Personen den Namen und die Vornamen des De-Mail-Kontoinhabers (`x-de-mail-account-holder`) angezeigt. Bei Pseudonym-Adressen wird nur das Pseudonym angegeben. Bei Institutionen wird der Name oder die Bezeichnung des Kontoinhabers angezeigt. Das Feld ist bei allen normalen De-Mails gemäß De-Mail-Spezifikation eine Pflichtangabe.

## 8.6.5 Zeile "Absenderadresse"

In der Zeile "Absenderadresse" wird bei allen Nachrichtentypen die Absenderadresse aus dem E-Mail-Header angezeigt. Dieses Feld ist eine Pflichtangabe durch den De-Mail-Provider für



alle Nachrichtentypen. Bei einer normalen De-Mail-Nachricht ist dieses die vom Absender gewählte De-Mail-Adresse; bei einer Bestätigungsnachricht oder Meldungsnachricht ist dieses die De-Mail-Adresse des De-Mail-Providers, von dem die Bestätigungsnachricht oder die Meldungsnachricht versendet wurde.

### 8.6.6 Zeile "Empfänger-Adressen"

In der Zeile "Empfänger-Adresse" wird bei allen Nachrichtentypen die vom Absender gewählte Empfänger-Adresse angegeben, an die die Nachricht versendet wurde. Bei normalen De-Mail-Nachrichten können auch mehrere Adressen angezeigt werden. Diese Angabe muss für alle Nachrichtentypen vorhanden sein.

### 8.6.7 Optionale Zeile "aktuelle Empfänger-Adresse(n)"

In der Zeile "aktuelle Empfänger-Adresse" wird bei allen Nachrichtentypen durch den De-Mail-Provider die tatsächliche Empfänger-Adresse angegeben, an die die Nachricht im Fall einer Weiterleitung oder Nachsendung versendet wurde. Initial entspricht diese Adresse der durch den Absender gewählten Empfängeradresse.

### 8.6.8 Zeile "Versanddatum und Zeitpunkt"

In der Zeile "Versanddatum und Zeitpunkt" werden bei allen Nachrichtentypen das Versanddatum und die Versandzeit der Nachricht durch den De-Mail-Provider in der Form `TT.MM.JJJJ hh:mm:ss` angezeigt. Dieses Feld ist eine Pflichtangabe durch den De-Mail-Provider für alle Nachrichtentypen.

### 8.6.9 Zeile "Gewählte Versandoptionen"

In der Zeile "Gewählte Versandoptionen" wird angezeigt, ob und ggf. welche Versandoptionen durch den Absender gesetzt wurden. Die Versandoptionen führen zu verschiedenen Aktionen beim absendenden und/oder empfangenden De-Mail-Provider (erzeugen beim De-Mail-Provider Bestätigungsnachrichten und/oder Meldungsnachrichten). Meldungsnachrichten können keine Versandoptionen beinhalten, Bestätigungsnachrichten bis auf eine Ausnahme ebenfalls nicht.

## Normale De-Mail-Nachricht

Eine normale De-Mail-Nachricht kann folgende, durch den Absender gewählte Versandoptionen enthalten: Versandbestätigung, Eingangsbestätigung, Abholbestätigung, Absenderbestätigt oder Persönlich.

Mit der Option "**Versandbestätigung**" fordert der De-Mail-Absender eine Versandbestätigung von seinem De-Mail-Provider an. Diese Bestätigung bekommt er, wenn seine De-Mail-Nachricht von seinem De-Mail-Provider versendet wurde. Die Bestätigungsnachricht muss vom De-Mail-Provider des Empfängers qualifiziert signiert werden (DKIM-Signatur). Die Bestätigung bekommt der Absender auch dann, wenn die Mail in der Ziel-Domain nicht zugestellt werden konnte. Natürlich muss die Ziel-Domain eine existierende De-Mail-Domain sein, sonst kann die Nachricht vom Provider nicht versendet werden.

Mit der Option "**Eingangsbestätigung**" fordert der Absender eine Eingangsbestätigung vom De-Mail-Provider des Empfängers an. Der De-Mail-Provider des Empfängers bestätigt in diesem Fall nach Ablage der Original-De-Mail-Nachricht im De-Mail-Postfach des Empfängers, dass er die De-Mail-Nachricht zu einem bestimmten Zeitpunkt in das Postfach des De-Mail-Empfängers eingestellt hat. Die Bestätigungsnachricht muss vom De-Mail-Provider des Empfängers qualifiziert signiert werden (DKIM-Signatur).

Mit der Option "**Abholbestätigung**" fordert der Absender der De-Mail eine Abholbestätigung vom De-Mail-Provider des De-Mail-Empfängers an. Der De-Mail-Provider des Empfängers versendet die Abholbestätigung nach Anmeldung des De-Mail-Empfängers mit Authentisierungsniveau "hoch". Die Bestätigungsnachricht muss vom De-Mail-Provider des Empfängers qualifiziert signiert werden (DKIM-Signatur).

Mit der Option "**Absenderbestätigt**" fordert der Absender der De-Mail vom De-Mail-Provider eine Bestätigung für den De-Mail-Empfänger an, in der der De-Mail-Provider des De-Mail-Absenders bestätigt, dass er den angegebenen Nachrichteninhalt der De-Mail-Nachricht entgegengenommen hat und dass der De-Mail-Absender sich mindestens mit "hoch" authentisiert hat. Dieses muss der De-Mail-Provider des Absenders mit einer qualifizierten elektronischen Signatur bestätigen (sogenannte DKIM-Signatur). Der De-Mail-Empfänger erhält dadurch einen starken Nachweis zur Authentizität des Absenders und zur Integrität der Nachricht.

Mit der Option "**Persönlich**" fordert der Absender der De-Mail vom De-Mail-Provider des Empfängers, dass der De-Mail-Empfänger sich bei seinem De-Mail-Provider mit mindestens "hoch" authentisiert, um die De-Mail-Nachricht lesen zu können. Dieses Authentisierungsniveau gilt in diesem Fall auch für den Absender der De-Mail-Nachricht, d.h. um diese Versandoption setzen zu können, muss sich der Sender auch mit dem Authentisierungsniveau "hoch" an seinem De-Mail-Postfach anmelden.

### Ident-Bestätigungsnachricht

Bei einer Ident-Bestätigungsnachricht muss die Versandoption "Persönlich" gesetzt werden. Mit der Option fordert der De-Mail-Provider des Empfängers an, dass der Empfänger der Ident-Bestätigungsnachricht sich bei seinem De-Mail-Provider mit mindestens "hoch" authentisiert, um diese Nachricht lesen zu können. Dieses geschieht durch eine entsprechende Meldungsnachricht mit dem folgenden Hinweis im Betreff "`*Hinweis* Eine Nachricht erfordert vertrauliche Anmeldung`".

### 8.6.10 Zeile "Authentisierungsniveau und -mechanismus des Absenders"

In der Zeile "Authentisierungsniveau und -mechanismus des Absenders" muss bei einer normalen De-Mail-Nachricht durch den De-Mail-Provider angegeben werden, mit welchem Authentisierungsniveau sich der Absender der De-Mail-Nachricht angemeldet und welchen Authentisierungsmechanismus er verwendet hat. Bei allen anderen Nachrichtentypen sind die Angaben optional.

Mögliche Werte für das Authentisierungsniveau sind:

- normal
- hoch

Für das "normale" Authentisierungsniveau reicht die Anmeldung mit Benutzernamen und Passwort aus. Für die Anmeldung mit dem Niveau "hoch" sind zwei voneinander unabhängige Sicherungsmittel notwendig. Typischerweise setzen solche Verfahren die zwei Elemente "Besitz" (z.B. eine Smartcard) und "Wissen" (z.B. PIN) voraus. Jeder De-Mail-Provider bietet hierzu mindestens zwei verschiedene Verfahren an, von denen eines die Nutzung des elektronischen Identitätsnachweises mit dem Online-Ausweis ist.

In Klammern wird in dieser Zeile zusätzlich angegeben, mit welchem Authentisierungsmechanismus sich der Absender der De-Mail-Nachricht zum Zeitpunkt des Versendens am De-Mail-Konto angemeldet hat. Es handelt sich um eine Freitextangabe des De-Mail-Providers.

### **8.6.11 Optionale Zeile "Nachrichten-ID des Absenders"**

In der Zeile "Nachrichten-ID des Absenders" wird – wenn vorhanden - eine ID angezeigt, die dem Absender dazu dient, eine Zuordnung einer versendeten De-Mail-Nachricht zu einer Bestätigungsnachricht durchführen zu können. Die ID ist für alle Nachrichtentypen bis auf die Ident-Bestätigungsnachricht optional. Bei der Ident-Bestätigungsnachricht darf sie nicht vorhanden sein.

### **8.6.12 Zeile "Nachrichten-ID des Providers"**

In der Zeile "Nachrichten-ID des Providers" wird bei allen Nachrichtentypen die Nachrichten-ID, vergeben vom De-Mail-Provider, angezeigt. Der De-Mail-Provider muss sicherstellen, dass die Nachrichten-ID eine Nachricht eindeutig identifizierbar macht. Dies ist eine Pflichtangabe durch den De-Mail-Provider für alle Nachrichtentypen.

### **8.6.13 Zeile "De-Mail-Provider"**

In der Zeile "De-Mail-Provider" wird bei allen Nachrichtentypen die Bezeichnung des De-Mail-Providers angezeigt, der die angezeigten Metadaten der De-Mail-Nachricht erstellt hat. Dies ist eine Pflichtangabe durch den De-Mail-Provider für alle Nachrichtentypen.

### **8.6.14 Zeile "De-Mail-Header-Version"**

In der Zeile "De-Mail-Version" wird bei allen Nachrichtentypen die Version des De-Mail-Headers angezeigt. Dies ist eine Pflichtangabe durch den De-Mail-Provider für alle Nachrichtentypen.

### **8.6.15 Zeile "Typ der Meldung"**

In der Zeile "Typ der Meldung" wird der Meldungstyp der De-Mail-Spezifikationen angezeigt.

### **8.6.16 Zeile "Signatur durch"**

In der Zeile "Signatur durch" wird der Name des signierenden De-Mail-Providers angezeigt. Dieser Name muss nicht exakt der vollständige registrierte Organisationsname sein.

### **8.6.17 Zeile "Ergebnis der Signaturprüfung"**

In der Zeile "Ergebnis der Signaturprüfung" wird das kumulierte Signaturprüfergebnis angezeigt. Zur Erläuterung siehe Kapitel 8.2.

## **8.7 De-Mail-Bestätigungsnachrichten**

In diesem Kapitel wird der Aufbau des Bereichs A "Dokument-/Containerstruktur" für De-Mail-Bestätigungsnachrichten beschrieben. Eine De-Mail-Bestätigungsnachricht ist eine De-Mail-Nachricht, die eine vom De-Mail-Provider erstellte Bestätigung über den Zustand einer De-Mail-Nachricht enthält. Sollte die bestätigte normale De-Mail-Nachricht auch vorliegen, wird eine komplexe Nachrichtenstruktur angezeigt und geprüft, ob die Bestätigungsnachricht tatsächlich die vorliegende normale De-Mailnachricht bestätigt.

| De-Mail: De-Mail_Eingangsbestätigung_zu_Normale_De-Mail_gruen.eml  |  |
|--|--|
| De-Mail-Nachrichtentyp:  | Eingangsbestätigung  |
| Betreff:   | *Eingangsbestätigung* TEST   |
| Absenderadresse:   | eingangsbestaetigung@entenhausen.de-mail.de  |
| Empfängeradressen:   | to=emil.erpel@Duck-Online.entenhausen.de-mail.de;cc=dagobert.duck@governikus-abnahme1-a.entenhausen.de-mail.de |
| Versanddatum und Zeitpunkt:  | 18.09.2018, 15:31:58   |
| Nachrichten-ID des Providers:                                      | ad6a58e0-a2ef-4476-a169-fdd1db96c559@entenhausen.de-mail.de  |
| De-Mail Provider:  | entenhausen.de-mail.de   |
| De-Mail Version:   | 1.2  |
| Signatur durch:  | De-Mail DKIM:PN  |
| Ergebnis der Signaturprüfung:                                      | <b>gültig</b>  |
| <b>Teil 1</b>  |  |
| XML-Dokument: Acknowledge message                                  |  |
| Hashwert passt zum Hashwert der bestätigten Nachricht:             | <b>ok</b>  |
| Nachrichten-ID passt zur Nachrichten-ID der bestätigten Nachricht: | <b>ok</b>  |
| Signatur durch:  | De-Mail DKIM:PN  |
| Ergebnis der Signaturprüfung:                                      | <b>gültig</b>  |
| <b>Teil 2</b>  |  |
| De-Mail: Normale_De-Mail_T-Systems-Header_1_2-gruen.eml            |  |
| De-Mail-Nachrichtentyp:  | Normale De-Mail-Nachricht  |
| Betreff:   | TEST   |
| Vollständiger Name:  | Duck-Online GmbH   |
| Absenderadresse:   | emil.erpel@Duck-Online.entenhausen.de-mail.de  |
| Empfängeradressen:   | to=dagobert.duck@governikus-abnahme1-a.entenhausen.de-mail.de  |
| Versanddatum und Zeitpunkt:  | 18.09.2018, 15:31:50   |
| Gewählte Versandoptionen:  | Absenderbestätigt<br>Versandbestätigung<br>Eingangsbestätigung   |
| Authentisierungsniveau und -mechanismus des Absenders:             | Hoch (sms-token)   |
| Nachrichten-ID des Providers:                                      | 4711-wert-16@entenhausen.de-mail.de  |
| De-Mail Provider:  | entenhausen.de-mail.de   |
| De-Mail Version:   | 1.2  |
| Signatur durch:  | De-Mail DKIM:PN  |
| Ergebnis der Signaturprüfung:                                      | <b>gültig</b>  |
| <b>Teil 3</b>  |  |

Abbildung 26: Bereich A bei einer De-Mail-Bestätigungsnachricht (aufgeklappt)

### 8.7.1 Teil 1: De-Mail-Bestätigungsnachricht mit DKIM-Signatur

Eine Bestätigungsnachricht ist eine De-Mail-Nachricht, die eine vom De-Mail-Provider erstellte Bestätigung über den Zustand einer De-Mail-Nachricht enthält. Diese Informationen befinden sich in sogenannten De-Mail-Header-Feldern und zusätzlich noch einmal (maschinenlesbar) auch in einem XML-Bereich der Bestätigungsnachricht (Name: signierte De-Mail-Bestätigungsnachricht), der separat zusätzlich vom De-Mail-Provider signiert wurde (XML-Signatur).

Die qualifizierte DKIM-Signatur der Bestätigungsnachricht umfasst auch den separat qualifiziert signierten XML-Nachrichteninhalt (immer durch eine CAdES-Signatur). Die Prüfung der einzelnen Signaturen erfolgt unabhängig voneinander.

Die Anzeige der Meta-Informationen einer Bestätigungsnachricht ist weitestgehend identisch mit den Metainformationen einer normalen De-Mailnachricht. Die Erläuterungen zu den Metainformationen entnehmen Sie bitte den Kapiteln 8.6.1 bis 8.6.15.

In den beiden auf die Metainformationen folgenden Zeilen wird in der Zeile "signiert durch (Signaturzertifikat)" der Name des signierenden De-Mail-Providers angezeigt und anschließend das Ergebnis der Signaturprüfung.

## 8.7.2 Teil 2: XML-Dokument Acknowledge Message

Im Teil 2 der Dokumentenstruktur wird das Prüfergebnis der Signatur der XML-Acknowledge Message der Bestätigungsnachricht angezeigt. Außerdem wird das Prüfergebnis angezeigt, ob die Bestätigungsnachricht tatsächlich die vorliegende normale De-Mailnachricht bestätigt.

### 8.7.2.1 Zeile "XML-Dokument: Acknowledge Message"

In der ersten, blau unterlegten Zeile "XML-Dokument: Acknowledge Message" wird hinter dem Signaturformat XML der interne Name der Nachricht angezeigt (immer Acknowledge Message).

### 8.7.2.2 Zeile "Hashwert passt zum Hashwert der bestätigten Nachricht"

In der Zeile " Hashwert passt zum Hashwert der bestätigten Nachricht" wird das Ergebnis der Prüfung angezeigt, ob die angezeigte De-Mail-Nachricht zur angezeigten Bestätigungsnachricht passt oder nicht übereinstimmt.

Technisch erfolgt diese Prüfung über den Vergleich des neu berechneten Hashwertes über Teile der De-Mail-Nachricht mit dem Hashwert über die Original-De-Mail-Nachricht, welcher im XML-Nachrichteninhalt der Bestätigungsnachricht enthalten ist. Folgende Prüfergebnisse sind möglich:

- **gültig** (grün ok): Es ist sichergestellt, dass die in der angezeigten De-Mail-Bestätigungsnachricht aufgeführten Informationen über den Zustand einer De-Mail-Nachricht sich tatsächlich auf die angezeigte normale De-Mail-Nachricht beziehen.
- **ungültig** (rot ungültig): Die Prüfung ist fehlgeschlagen. Die De-Mail-Nachricht passt nicht zur Bestätigungsnachricht. Die in der angezeigten De-Mail-Bestätigungsnachricht aufgeführten Informationen beziehen sich nicht auf die angezeigte De-Mail-Nachricht. Die Prüfung der Signaturen ist unabhängig von diesem Prüfergebnis. D.h., obwohl beide Nachrichten nicht zusammengehören, können die Signaturprüfungen positiv verlaufen.
- **nicht geprüft** (schwarz nicht geprüft): Die Prüfung konnte nicht durchgeführt werden, da die zur Bestätigungsnachricht korrespondierende De-Mail-Nachricht nicht vorlag oder nicht gefunden werden konnte.

In einem Meldungstext unter dem Prüfergebnis werden die Gründe für die Prüfergebnisse erläutert.

| XML-Dokument: Acknowledge message                                  |   |
|--|---|
| Hashwert passt zum Hashwert der bestätigten Nachricht:             | <b>nicht geprüft</b>                    |
| Meldungen:   | Die bestätigte De-Mail liegt nicht vor. |
| Nachrichten-ID passt zur Nachrichten-ID der bestätigten Nachricht: | <b>nicht geprüft</b>                    |
| Meldungen:   | Die bestätigte De-Mail liegt nicht vor. |
| Signiert durch (Signaturzertifikat):                               | De-Mail DKIM 93:PN                      |
| Ergebnis der Signaturprüfung:                                      | <b>gültig</b>                           |

Abbildung 27: Bereich A De-Mail-Bestätigungsnachricht ohne vorliegende normale De-Mailnachricht (aufgeklappt)

### 8.7.2.3 Zeile "Nachrichten-ID passt zur ID der bestätigten Nachricht"

In der Zeile "Nachrichten-ID passt zur Nachrichten-ID der bestätigten Nachricht" wird das Ergebnis der Prüfung angezeigt, ob die Nachrichten-ID in der Bestätigungsnachricht zur Nachrichten-ID der vorliegenden bestätigten De-Mailnachricht passt oder nicht übereinstimmt. Folgende Prüfergebnisse sind möglich:

- **gültig** (grün ok): Die Nachrichten-ID in der Bestätigungsnachricht passt zur Nachrichten-ID der bestätigten vorliegenden normalen De-Mailnachricht.
- **ungültig** (rot ungültig): Die Prüfung ist fehlgeschlagen. Die Nachrichten-ID in der Bestätigungsnachricht passt nicht zur Nachrichten-ID der bestätigten vorliegenden normalen De-Mailnachricht
- **nicht geprüft** (schwarz nicht geprüft): Die Prüfung konnte nicht durchgeführt werden, da die zur Bestätigungsnachricht korrespondierende De-Mail-Nachricht nicht vorlag oder nicht gefunden werden konnte.

In einem Meldungstext unter dem Prüfergebnis werden die Gründe für die Prüfergebnisse erläutert.

### 8.7.2.4 Zeile "Signatur durch"

In der Zeile "Signatur durch" wird der Name des signierenden De-Mail-Providers angezeigt, der den XML-Nachrichteninhalt signiert hat. Dieser Name muss nicht exakt der vollständige registrierte Organisationsname sein.

### 8.7.2.5 Zeile "Ergebnis der Signaturprüfung"

In der Zeile "Ergebnis der Signaturprüfung" wird das kumulierte Signaturprüfergebnis angezeigt. Zur Erläuterung siehe Kapitel 8.2.

## 8.7.3 Teil 3: Normale De-Mail-Nachricht

Zur Erläuterung der angezeigten Informationen aus der normalen De-Mailnachricht siehe Kapitel 8.6. Liegt die bestätigte normale De-Mailnachricht nicht vor, fehlt dieser Teil der Anzeige.

## 8.8 ASiC-Container mit Signaturen

In diesem Kapitel wird die Dokumentenstruktur von Signaturen in ASiC-Containern beschrieben.

### 8.8.1 Zeile "ASiC-Container: Dateiname"

In der ersten Zeile "ASiC-Container: Dateiname" wird blau unterlegt hinter der Bezeichnung des Containerformats "ASiC-Container" der Name des Containers angezeigt.

Dokument bzw. Containerstruktur:

| - ASiC-Container: ASiC_S_CAdES.scs     |  |
|--|--|
| ASiC Container Typ:                    | ASiC Simple                                |
| Formatkonformität:                     | <b>gültig</b>                              |
| CAdES-Dokument: META-INF/signature.p7s |  |
| Signierte Datei oder Inhalt:           | HalloWelt.txt                              |
| Signatur durch:                        | Tick_Trick_und_Track                       |
| Signaturtyp:                           | Detached                                   |
| Ergebnis der Signaturprüfung:          | <b>unbestimmt</b>                          |
| Meldungen:                             | Es ist ein allgemeiner Fehler aufgetreten. |

Abbildung 7: Signatur in ASiC-Container (simple)

### 8.8.2 Zeile "ASiC Container Typ"

In der Zeile "ASiC Container Typ" wird der Containertyp angezeigt. Folgende Typen werden unterstützt:

- ASiC Simple
- ASiC Extended

Im Simple-Typ ist eine einzelne Datendatei mit einer Signaturdatei (XAdES- oder CAdES-Format) oder einem Zeitstempel verknüpft. Im Typ ASiC Extended wird einer Datendatei oder werden mehrere Dateidateien einer Signatur (XAdES-oder CAdES-Format) oder mehreren Signaturen/Zeitstempel zugeordnet.

### 8.8.3 Optionale Zeile "Formatkonformität"

In der Zeile "Formatkonformität" wird das Ergebnis der Prüfung auf Formatkonformität angezeigt, wenn die Prüfung Mängel festgestellt hat. Folgende Ergebnisse sind möglich:

- **gültig** (grün gültig): Das Format des Containers entspricht den Anforderungen des technischen Standards gemäß Beschluss 2015/1506 der EU-Kommission zur Festlegung des ASiC-Standards oder der aktuellen ETSI-EN.
- **unbestimmt** (gelb unbestimmt): Das Format des Containers entspricht nicht den Anforderungen des technischen Standards gemäß Beschluss 2015/1506 der EU-Kommission zur Festlegung des ASiC-Standards oder der aktuellen ETSI-EN. In einem Meldungstext werden die Gründe für dieses Prüfergebnis erläutert. Das Prüfergebnis beeinflusst nicht das Ergebnis der Signaturprüfung selbst.

## 8.9 Optionaler Bereich "Zusammenfassung Dokumente und Signaturprüfungen"

Werden mehrere elektronische Signaturen geprüft, kann optional eine Zusammenfassung der Prüfergebnisse der Einzelsignaturen angefordert werden. In diesem Fall wird vor dem Bereich "Dokument- bzw. Containerstruktur" eine tabellarische Zusammenfassung "Zusammenfassung Dokumente und Signaturprüfungen" angezeigt. Diese gibt einen Überblick (Spalten von links nach rechts), welches Dokument (Dateiname), von wem (signiert durch), mit welcher Qualität (Signaturniveau) und mit welchem Ergebnis signiert wurde (Signaturprüfung). Werden mehrere Dokumente durch eine Signatur erfasst, werden diese alle untereinander aufgeführt.

## Zusammenfassung Dokumente und Signaturprüfungen:


| Nr. Dokument  | Signiert durch    | Signaturniveau                                    | Signaturprüfung |
|---|-------------------|---|-----------------|
| 1. <a href="#">PAdES_signed_Revision3.pdf</a>                 | Emil Erpel        | EU-qualifizierte elektronische Signatur (EUMS-TL) | <b>gültig</b>   |
| 2. <a href="#">PAdES_signed_Revision_Revision3.pdf</a>        | Emil Erpel        | EU-qualifizierte elektronische Signatur (EUMS-TL) | <b>gültig</b>   |
| 3. <a href="#">PAdES_signed_Revision_signed_Revision5.pdf</a> | Donald Duck       | EU-qualifizierte elektronische Signatur (EUMS-TL) | <b>gültig</b>   |
| 4. <a href="#">PAdES_signed_Revision_signed_Revision3.pdf</a> | Emil Erpel        | EU-qualifizierte elektronische Signatur (EUMS-TL) | <b>gültig</b>   |
| 5. <a href="#">PAdES_signed_signed_Revision4.pdf</a>          | Daniel Düsentrieb | EU-qualifizierte elektronische Signatur (EUMS-TL) | <b>gültig</b>   |
| 6. <a href="#">PAdES_signed_signed_Revision3.pdf</a>          | Gustav Gans       | EU-qualifizierte elektronische Signatur (EUMS-TL) | <b>gültig</b>   |

Abbildung 28: Hauptseite Governikus Prüfprotokoll mit optionaler Zusammenfassung der Prüfergebnisse mehrerer Signaturen



## 9 Knoten "Name des Inhabers" aufgeklappt

Nach dem Aufklappen des Knotens in der Zeile "Name des Inhabers" oder in der Zeile "Zeitstempel erzeugt durch" im Bereich B "Prüfung der Signaturen" wird der vollständige Inhalt des Zertifikats angezeigt. Es handelt sich um eine "Übersetzung" der in einer abstrakten Beschreibungssprache verfassten Struktur und Inhalte.

|   |   |
|---|---|
|  | <p><b>Hinweis:</b> Die Anzeige aller Zertifikatsinhalte ist die Voreinstellung. Eine verkürzte Ansicht der wichtigsten Zertifikatsinhalte kann von der vorgelegerten Instanz angefordert werden. In diesem Fall werden im aufgeklappten Knoten nur noch die Bereiche Inhaber, Aussteller, die Erweiterung QC-Statement und die wichtigsten Felder aus dem Bereich allgemeine Angaben angezeigt. Bei Common-PKI-konformen Zertifikaten werden auch die - wenn vorhanden - beschränkenden Attribute aufgeführt.</p> |
|---|---|

Die Struktur eines Zertifikats basiert auf ASN.1. Das ist eine abstrakte Beschreibungssprache zur eindeutigen Definition von Datenstrukturen und Inhalten, ohne auf die rechnerinterne Darstellung einzugehen. Die Datenstrukturen und Inhalte sind auf Bit-Ebene völlig eindeutig und damit für Zertifikate geeignet, die elektronisch signiert sind und plattformübergreifend ausgetauscht werden sollen. Sie sind aber auch kaum lesbar, selbst mit einem ASN.1-Viewer. Wo immer uns bekannt, wurden daher alle Identifier und Feldbezeichner übersetzt und in eine lesbare Struktur überführt. Damit sollten sich fast alle im RFC 5280, in der Common-PKI-Spezifikation Version 2.0 (profiliert die Anforderungen aus dem Signaturgesetz) und in den relevanten EU-Normen im Kontext der eIDAS-VO durch ETSI definierten bzw. profilierten Inhalte (in den EN 319 412-1 bis 5) eines Signaturzertifikats menschenlesbar und verständlich anzeigen lassen. Es kann allerdings nicht ausgeschlossen werden, dass in Zertifikaten auch unbekannte Erweiterungen (sogenannte private Extensions, die jeder Vertrauensdiensteanbieter für jede CA selber definieren kann) enthalten sind. Diese werden, wenn sie eine formal korrekte ASN-1-Struktur aufweisen, zwar technisch angezeigt, können aber nicht übersetzt werden. In diesem Fall werden nur die abstrakten Identifier und Feldbezeichner angezeigt.

In den folgenden Unterkapiteln werden die möglichen Zertifikatsinhalte beschrieben. Die Reihenfolge muss dabei nicht immer mit der Reihenfolge im Zertifikat übereinstimmen, da im Bereich der Zertifikatserweiterungen die Reihenfolge durch das ausstellende Trustcenter festgelegt wird.

## 9.1 Überschrift "Inhaber"

|                      |                          |
|----------------------|--------------------------|
| Name des Inhabers:   | Emil Erpel               |
| <b>Inhaber</b>       |                          |
| Titel                | Dr.                      |
| Name                 | Emil Erpel               |
| Vorname              | Emil                     |
| Seriennummer         | 1019715                  |
| Familienname         | Erpel                    |
| <b>Aussteller</b>    |                          |
| Organisation         | Entenhausen Post Service |
| Organisationseinheit | Zertifizierungsstelle    |
| Name                 | EntHaus CA 5 1:PN        |
| Land                 | DE                       |
| <b>Allgemeines</b>   |                          |
| Typ                  | X.509                    |
| Version              | 3                        |
| Gültig ab            | 20.10.2014, 17:25:04     |
| Gültig bis           | 01.02.2019, 00:00:00     |
| Seriennummer         | 2881058629070599248      |
|                      | 27 fb 93 8f 02 d3 b4 50  |

Abbildung 29: Anzeige Inhaber und Aussteller eines Zertifikats

Es werden alle im Zertifikat vorhandenen Informationen zum Inhaber [Feld `subject`] des Zertifikats (Inhaberattribute) angezeigt. Eine Untermenge der folgenden Attribute wird in der Regel verwendet:

- 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]

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.

Wird ein Pseudonym verwendet, ist im QES-SigG-Kontext beim Attribut Namen das Suffix ":PN" vorgeschrieben. Im Kontext der eIDAS-Verordnung gibt es noch keine Festlegung.

## 9.2 Überschrift "Aussteller"

Es werden alle im Zertifikat vorhandenen Informationen zum Aussteller [Feld issuer] angezeigt. Eine Untermenge der folgenden Attribute wird in der Regel verwendet:

- 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]
- Organisationskennung [organizationIdentifier]

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

## 9.3 Überschrift "Allgemeines"

Unter der Überschrift "Allgemeines" werden der Typ und die Version des Zertifikats, der Gültigkeitszeitraum sowie der Name des Signaturalgorithmus angezeigt, mit dem das Zertifikat signiert wurde.

### 9.3.1 Zeilen "Typ" und "Version"

Es werden der Typ (Immer X509) und die Version angezeigt [Feld `version`], immer 3.

### 9.3.2 Zeilen "gültig ab" und "gültig bis" (Gültigkeitszeitraum)

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

- 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]` angezeigt. Bei "gültig bis" wird das Datum `[notAfter]` entsprechend angezeigt.

### 9.3.3 Zeile "Seriennummer"

Es wird die Seriennummer des Zertifikats angezeigt [Feld `serialNumber`] in dezimal und hexadezimal.

### 9.3.4 Zeile "Algorithmus"

Es wird der vom Aussteller (des Zertifikats) verwendete Signaturalgorithmus zur Signatur des Zertifikats angezeigt [Feld `signature`].

## 9.4 Überschrift "öffentlicher Schlüssel"

Unter der Überschrift "öffentlicher Schlüssel" werden alle im Zertifikat vorhandenen Informationen zum öffentlichen Schlüssel angezeigt.

### 9.4.1 Zeilen "Algorithmus" und Folgezeilen

Es wird der technische Name des Signaturalgorithmus, auf dem der öffentliche Schlüssel des Zertifikatsinhabers basiert angezeigt. In der Regel RSA oder EC für elliptische Kurven. Die angezeigten Folgezeilen sind abhängig von der Art des Signaturalgorithmus. Dieses sind bei RSA die Schlüssellänge, das Modulo und der Exponent. Bei elliptischen Kurven ist dies die Kurven-OID (nur wenn `named curve`) sowie Kurvenparameter.

## 9.5 Überschrift "Signatur des Ausstellers"

Angezeigt werden unter der Überschrift "Signatur des Ausstellers" der Name des Signaturalgorithmus, der vom Aussteller des Zertifikats zur Signatur des Zertifikats (TBS-Bereich des Zertifikats) verwendet wurde, und die Signatur.

### 9.5.1 Zeile "Signaturalgorithmus"

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

### 9.5.2 Zeile "Signatur"

Es wird die Signatur des Ausstellers [`signatureValue`] als hexadezimaler Ausdruck angezeigt.

## 9.6 Überschrift "Fingerabdruck"

Der Fingerabdruck (Fingerprint) ist der berechnete Hashwert einer auf das angezeigte Zertifikat (TBS-Teil des Zertifikats) angewendeten Hash-Funktion. Der Hashwert ist nicht Bestandteil des Zertifikats, sondern wird berechnet.

### 9.6.1 Zeile "SHA-1"

Es wird der SHA-1-Hashwert angezeigt.

## 9.7 Überschrift "Zertifikatserweiterungen"

Unter der Überschrift "Zertifikatserweiterungen" werden alle im Zertifikat vorhandenen Zertifikatserweiterungen angezeigt. Bei qualifizierten Signaturzertifikaten aus eIDAS-konformen PKIs, herausgegeben von qualifizierten Vertrauensdiensteanbietern, sind mindestens folgende Erweiterungen vorhanden.

- Zugangsinformationen des Ausstellers: URL für OCSP-Anfragen, URL zum Download des ausstellenden Zertifikats (CA-Zertifikat),
- Angaben zum qualifizierten Zertifikat: Qualität und Typ des Zertifikats,
- Distributionspunkt für CRL: URL für den Download der CRL,
- Zertifizierungsrichtlinien: Angabe der Zertifizierungsrichtlinie unter der das Zertifikat ausgestellt wurde,
- Ausstellerschlüssel-ID: Eindeutige Kennung des Ausstellerschlüssels,
- Inhaberschlüssel-ID: Eindeutige Kennung des Inhaberschlüssels,
- Schlüsselverwendung: bei QES "Nichtabstreitbarkeit".

Es werden grundsätzlich alle im Zertifikat vorhandenen Erweiterungen angezeigt. Kann eine Erweiterung nicht interpretiert werden, werden nur die OID der Erweiterung und der Wert "nicht interpretiert" angezeigt. In den folgenden Unterkapiteln werden alle wichtigen Erweiterungen detailliert beschrieben.

### 9.7.1 Erweiterung "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 Schlüssel-ID der Erweiterung "Inhaberschlüssel-ID" des Ausstellerzertifikats muss identisch sein mit der Schlüssel-ID der Erweiterung "Ausstellerschlüssel-ID" aus dem Signaturzertifikat (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.

### 9.7.2 Erweiterung "Schlüsselverwendung"

In dieser Erweiterung wird der Zweck, für den der öffentliche Schlüssel des Zertifikats verwendet werden darf [Extension `keyUsage`], angezeigt. Sie muss als kritisch markiert sein und muss demnach von der Anwendung verarbeitet werden können. Da eine Prüfkomponente allerdings generisch ist und in der Regel nicht direkt in einen fachlichen Workflow eingebunden ist, wird der Inhalt der Erweiterung nur vollständig angezeigt. 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)

Angezeigt werden alle im Zertifikat vorhandenen Werte.

### 9.7.3 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. Wird diese Erweiterung in einem CA-Zertifikat verwendet, wird durch diese 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. Häufig finden sich nach der OID für die Qualität der Richtlinie weitere OIDs:

- Die OID für die konkrete Richtlinie des Trustcenters (nicht übersetzt),
- Die übersetzte OID für das Certificate Practice Statement des Trustcenters,
- Die URI zum Download des CPS.

Die im eIDAS-Kontext definierten OIDs für Richtlinien sind:

- Qualifizierte Zertifikatsrichtlinie für juristische Personen gemäß Verordnung EU 910/2014 (QCP-I) (OID 0.4.0.194112.1.1)
- Qualifizierte Zertifikatsrichtlinie für juristische Personen mit Schlüssel auf QSCD gemäß Verordnung EU 910/2014 (QCP-I-qscd) (OID 0.4.0.194112.1.3)
- Qualifizierte Zertifikatsrichtlinie für natürliche Personen gemäß Verordnung EU 910/2014 (QCP-n) (OID 0.4d.0.194112.1.0)

- Qualifizierte Zertifikatsrichtlinie für natürliche Personen mit Schlüssel auf QSCD gemäß Verordnung EU 910/2014 (QCP-n-qscd) (OID 0.4.0.194112.1.2)
- Qualifizierte Zertifikatsrichtlinie für die Öffentlichkeit gemäß Signaturdirektive 1999/93/EC (QCP public) (OID 0.4.0.1456.1.2)
- Qualifizierte Zertifikatsrichtlinie für die Öffentlichkeit mit Schlüssel auf SSCD gemäß Signaturdirektive 1999/93/EC (QCP public +) (OID 0.4.0.1456.1.1)
- Qualifizierte Zertifikatsrichtlinie für qualifizierte Website-Zertifikate gemäß Verordnung EU 910/2014 (QCP-w) (OID 0.4.0.194112.1.4)

#### **9.7.4 Erweiterung "Richtlinienzuordnungen"**

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

#### **9.7.5 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. Häufig wird hier nur die E-Mail-Adresse des Zertifikatsinhabers als RFC 822-Name eingetragen.

#### **9.7.6 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. 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.

#### **9.7.7 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.

In diesem Fall wird angezeigt, dass es sich um ein CA-Zertifikat handelt und zusätzlich wird die Pfadlängenbegrenzung (0) angegeben.

#### **9.7.8 Erweiterung "Beschränkung des Namensraums"**

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

#### **9.7.9 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-Identifizierer (OIDs) definiert werden müssen und/oder verbietet das Policy Mapping in untergeordneten Zertifikaten.

### 9.7.10 Erweiterung "Erweiterte Schlüsselverwendung"

Die Erweiterung "Erweiterte Schlüsselverwendung" [Extension `extendedKeyUsage`] kann zusätzlich die Verwendungsmöglichkeiten des öffentlichen Schlüssels des Zertifikats einschränken oder erweitern. 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 auch, dass die Erweiterung `ExtendedKeyUsage` bei dieser erweiterten Schlüsselverwendung als kritisch markiert werden muss.

### 9.7.11 Erweiterung "Distributionspunkt für CRL"

Die Erweiterung "Distributionspunkt für CRL" [Extension `CRLDistributionPoint`] liefert Informationen darüber, wie Sperrlisteninformationen zu dem Zertifikat bezogen werden können. Der Name des Distributionspunkts für die CRL kann der volle "Distinguished Name" (Eindeutiger Gesamtname eines LDAP-Objekts) sein oder auch die URL zum Download der CRL (LDAP und/oder HTTP). In der Regel werden hier die URL für den Zugriff der CRL über LDAP und HTTP angegeben. Die Erweiterung hat dann typischerweise die folgende Form.

Erweiterung Distributionspunkt für CRL:

```
Ldap://directory.entenhausen.net/CN=entenhausen-TC%20Root%20CA,O=Entenhausen-TC%20GmbH,C=DE?certificaterevocationlist  
http://CRL-entenhausen.net/crl/entenhausen-TC.crl
```

### 9.7.12 Erweiterung "Unterdrückung jeder Policy"

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

### 9.7.13 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".

### 9.7.14 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. In Regel werden hier die URL für den OCSP-Responder und der Downloadlink für das Ausstellerzertifikat angegeben. Die Erweiterung hat dann die folgende Form:

- Erweiterung



- Zugangsinformationen des Ausstellers
- Onlinestatusprotokoll des Zertifikats
- Zugriff auf
  - `http://entenhausen-ocsp.net`
  - Ausstellerzertifikat
- Zugriff auf
  - `http://www.entenhausen/Zertifikatname.crt`

### 9.7.15 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.

### 9.7.16 Erweiterung "Angaben zum qualifizierten Zertifikat"

In der Erweiterung "Angaben zum qualifizierten Zertifikat" [`qcStatements`] werden qualifizierte Zertifikatsstatements aufgelistet. Die Erweiterung hat typischerweise die folgende Form:

- Erweiterung
  - Angaben zum qualifizierten Zertifikat
  - Übersetzte OID(s) für das qualifizierte Statement
- Typ des qualifizierten Zertifikats
  - Übersetzte OID für den Zertifikatstyp
- PKI-Offenlegungserklärung
  - Downloadlink für PKI-Nutzerinformation

Angezeigte qualifizierte Statements sind:

- Qualifiziertes Zertifikat gemäß Signatordirektive 1999/93/EC oder Verordnung EU 910/2014
- Privater Schlüssel und öffentlicher Schlüssel im qualifizierten Zertifikat auf SSCD gemäß Signatordirektive 1999/93/EC oder auf QSCD gemäß Verordnung EU 910/2014

Angezeigte Zertifikatstypen sind:

- Zertifikat für elektronische Siegel gemäß Verordnung EU 910/2014
- Zertifikat für elektronische Signaturen gemäß Verordnung EU 910/2014
- Zertifikat für elektronische Website Authentifizierung gemäß Verordnung EU 910/2014

### 9.7.17 Erweiterung "keine OCSP-Prüfung"

Die Erweiterung "keine OCSP-Prüfung" [private qc Extension gemäß RFC 2560 `OCSPNoCheck`] wird nur bei OCSP-Responder-Zertifikaten verwendet und besagt, dass keine OCSP-Prüfung für diese Zertifikate durchgeführt werden muss, da es während seiner Laufzeit nicht gesperrt wird.

### 9.7.18 Erweiterung "Gültigkeit zugesichert"

Die Erweiterung "Gültigkeit zugesichert" (validity assured) kann in Short-Term-Signaturzertifikaten verwendet werden. Diese besagt, dass der VDA zusichert, das Zertifikat während seines Gültigkeitszeitraums nicht zu sperren. Der Sperrstatus braucht daher nicht ermittelt zu werden.

### 9.7.19 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).

### 9.7.20 Erweiterung "Open Banking-Attribute (PSD2)"

Die Erweiterung "Open Banking-Attribute (PSD2)" zeigt an, dass das Zertifikat auf einen Zahlungsdienstleister gemäß Richtlinie (EU) 2015/2366 (Payment Service Directive 2) ausgestellt wurde. Angegeben sind die Rollen, die der Zahlungsdienstleister gemäß Richtlinie (EU) 2015/2366 innehat. Die möglichen Rollen sind:

| Rolle (Deutsch)  | Rolle (Englisch)  | Rollen OID      |
|--|---|-----------------|
| Nicht spezifiziert   | Unspecified   | 0.4.0.19495.1.0 |
| Kontoführender Zahlungsdienstleister                                   | Account Servicing Payment Service Provider                      | 0.4.0.19495.1.1 |
| Zahlungsauslösedienstleister   | Payment Initiation Service Provider                             | 0.4.0.19495.1.2 |
| Kontoinformationsdienstleister   | Account Information Service Provider                            | 0.4.0.19495.1.3 |
| Zahlungsdienstleister, der kartengebundene Zahlungsinstrumente ausgibt | Payment Service Provider issuing card-based payment instruments | 0.4.0.19495.1.4 |

Tabelle 2: OIDs von Rollen bei Open Banking Attributen

## 10 Bereich C Knoten "Technischer Anhang" aufgeklappt

Im Anhang Bereich C "Technischer Anhang" werden im aufgeklappten Knoten "Prüfrichtlinien" die im Kontext der Signaturprüfung verwendeten Prüfrichtlinien vollständig angezeigt (siehe Kapitel 10.1). Es folgen im aufgeklappten Knoten "Vertrauenslisten" Detailinformationen zu den verwendeten Vertrauenslisten (siehe Kapitel 10.2). Im aufgeklappten Knoten "Algorithmenkataloge" folgen Detailinformationen zu den verwendeten Algorithmenkatalogen (siehe Kapitel 10.3). Im aufgeklappten Knoten "Prüfinstanz" (Kapitel 10.4) wird schließlich angezeigt, welche Prüfinstanz (URL) auf der Basis welcher Produktversion und CSL die Prüfung durchgeführt hat.

| Technischer Anhang |                                      |
|--------------------|--------------------------------------|
| +                  | Prüfrichtlinien                      |
| +                  | Vertrauenslisten (mit Erweiterungen) |
| +                  | Algorithmenkataloge                  |
| +                  | Prüfinstanz                          |

Abbildung 30: Anhang mit Referenzen

### 10.1 Knoten "Prüfrichtlinien" aufgeklappt

Nach Aufklappen des Knotens "Prüfrichtlinien" werden alle in der Prüfrichtlinie vorhandenen Anforderungen an die Prüfung angezeigt.

#### 10.1.1 Überschrift "Prüfrichtlinie #1"

Unter der Überschrift Prüfrichtlinie #1 werden alle in der Prüfrichtlinie vorhandenen Anforderungen an die Prüfung angezeigt. Werden mehrere Prüfrichtlinien angewendet, wird die Überschrift und die Angaben wiederholt.

##### 10.1.1.1 Zeile "Herausgeber"

Es wird der Herausgeber der Prüfrichtlinie nach Angaben des Herausgebers angezeigt. Ist der Herausgeber die Governikus KG und wurde die Prüfrichtlinie als "entspricht Governikus Prüfrichtlinie" bewertet, handelt es sich um eine der Standard-Prüfrichtlinien.

##### 10.1.1.2 Zeile "Version"

Es wird die Versionsnummer der Prüfrichtlinie nach Angaben des Herausgebers angezeigt.

##### 10.1.1.3 Zeile "Name"

Es wird der Name der Prüfrichtlinie nach Angaben des Herausgebers angezeigt. Wenn kein Name angegeben wird, wird "benutzerdefinierte Prüfrichtlinie" angezeigt.

Folgende Prüfrichtlinien wurden von der Governikus KG definiert und werden, sollte keine Prüfrichtlinie von der anfragenden Instanz mitgegeben werden, automatisch ausgewählt:

- Qualifizierte elektronische Signatur (qVDA aus DE SigG)
- Qualifizierte elektronische Signatur (qVDA aus DE eIDAS-VO)
- Qualifizierte elektronische Signatur (qVDA nicht DE eIDAS-VO)
- Fortgeschrittene elektronische Signatur (VDA eIDAS-VO oder SigG).

#### 10.1.1.4 Zeile "Bewertung der Prüfrichtlinie"

Es wird angezeigt, ob die verwendete Prüfrichtlinie einer der durch die Governikus KG herausgegebenen Standardprüfrichtlinien entspricht. Mögliche Werte sind:

- entspricht Governikus Prüfrichtlinie
- benutzerdefinierte Prüfrichtlinie

#### 10.1.1.5 Zeile "Herkunft der Prüfrichtlinie"

Die zu verwendende Prüfrichtlinie kann durch die anfragende Instanz oder den Certificate Validation Server automatisch bestimmt werden. Mögliche Werte sind:

- automatisch bestimmt
- in Anfrage übermittelt

#### 10.1.1.6 Zeile "Zertifikatsketten-Prüfmethode"

Es wird das in der Prüfrichtlinie hinterlegte Gültigkeitsmodell angezeigt. Mögliche Werte sind:

- Kette
- Schale
- Escape Route

#### 10.1.1.7 Zeile "Prüfung der Eignung der Schlüsselverwendung"

Es werden die Zertifikatstypen angezeigt, für die geprüft wird, ob die angegebene Schlüsselverwendung den Anforderungen für den Zertifikatstyp entspricht. Folgende Zertifikatstypen können überprüft werden:

- Signaturzertifikat (Prüfung ob Schlüsselverwendung `nonRepudiation`)
- Zwischenzertifikat (Prüfung ob Schlüsselverwendung `keyCertSign`)
- Zeitstempelzertifikat (Prüfung ob erweiterte Schlüsselverwendung `timeStamping`)
- OCSP/CRL-Zertifikate (Prüfung ob `OCSPSign` oder `CRLSign`)

#### 10.1.1.8 Zeile "Aktualität des Sperrstatuswertes berücksichtigen"

Es wird angezeigt, ob die Aktualität des Sperrstatuswertes berücksichtigt werden soll oder nicht. Mögliche Werte sind:

- Zum in der Prüfrichtlinie festgelegten Vertrauensniveau des Prüfzeitpunktes (POE)
- Nein

Beim Wert "Zum in der Prüfrichtlinie festgelegten Vertrauensniveau des Prüfzeitpunktes (POE)" wird das in der Prüfrichtlinie maximal zulässige Alter des Sperrstatuswertes berücksichtigt. Für die unterschiedlichen Vertrauensniveaus des Prüfzeitpunkts gilt:

- Bei den Vertrauensniveaus des Prüfzeitpunktes "behaupteter Signaturzeitpunkt", "Zeitmarke" und "Zeitstempel" ist das maximale Alter des Sperrstatusantwort 0,0 Sekunden.
- Beim Prüfzeitpunkt "Zeitpunkt der Durchführung der Prüfung" kann das maximal zulässige Alter der Sperrstatusantwort konfiguriert werden (siehe Kapitel 10.1.1.9).

#### **10.1.1.9 Zeile "Maximales Alter der Sperrstatusantwort bei Prüfzeitpunkt "Zeitpunkt der Durchführung der Prüfung""**

Es wird das maximal zulässige Alter in Sekunden des zurückgegebenen Sperrstatuswertes im Vergleich zum Prüfzeitpunkt bei Prüfzeitpunkt "Zeitpunkt der Durchführung der Prüfung" angezeigt. Die Konfiguration wirkt nicht auf die Vertrauensniveaus des Prüfzeitpunkts "behaupteter Signaturzeitpunkt", "Zeitmarke" und "Zeitstempel". Hier ist der Wert 0,0 Sekunden vorge-schrieben.

#### **10.1.1.10 Zeile "Eignung des Signaturalgorithmus zum behaupteten Signaturzeitpunkt ermitteln"**

Es wird angezeigt, ob die Eignung des verwendeten Signaturalgorithmus zum behaupteten Signaturzeitpunkt ermittelt werden soll. Mögliche Werte sind:

- Ja
- Nein

#### **10.1.1.11 Zeile "Eignung Signaturalgorithmus zum Zeitpunkt der Durchführung der Prüfung ermitteln"**

Es wird angezeigt, ob die Eignung des verwendeten Signaturalgorithmus zum Zeitpunkt der Durchführung der Prüfung ermittelt werden soll. Mögliche Werte sind:

- Ja
- Nein

#### **10.1.1.12 Zeile "Wenn möglich, Eignung des Signaturalgorithmus ..."**

##### **Zeile "Wenn möglich, Eignung des Signaturalgorithmus zum abgesicherten Zeitpunkt in der Vergangenheit ermitteln"**

Es wird angezeigt, ob die Eignung des verwendeten Signaturalgorithmus zum einem durch den Validierungsalgorithmus bestimmten Zeitpunkt in der Vergangenheit ermittelt werden darf, wenn sichergestellt ist, dass zu dem bestimmten Zeitpunkt die Eignung des Algorithmus durch eine Übersignatur (mit gültigen Archivzeitstempel, LTA-Signatur) bewahrt worden ist. Mögliche Werte sind:

- Ja
- Nein

Wird keine LTA-Signatur mit gültigem Archivzeitstempel validiert, ist der angegebene Zeitpunkt der Zeitpunkt der Durchführung der Prüfung. Dieses ist zurzeit immer der Fall, da Archiv-Signaturen erst mit einem Folgerelease unterstützt werden.

#### **10.1.1.13 Zeile "Verwendung von Vertrauensankern zulässig bei"**

Es wird angegeben, ob Dienste-Identifizierer aus hoheitlichen Vertrauenslisten (EUMS-TL) als Vertrauensanker (trusted anchor) verwendet werden. Mögliche Werte sind:

- Keine Verwendung
- bestimmte Zertifikate (CA-Zertifikate, OCSP-Signer-Zertifikate, CRL-Signer-Zertifikate, Zeitstempel-Zertifikate) die als SDI aus EUMS-TL fungieren mit den URIs `//uri.etsi.org/TrstSvc/Svctype..`

- ../CA/QC,
  - ../CA/PKC,
  - ../Certstatus/OCSP/QC,
  - ../Certstatus/CRL/QC,
  - ../Certstatus/OCSP,
  - ../Certstatus/CRL,
  - ../NationalRootCA-QC,
  - ../TSA/QTST,
  - ../TSA,
  - ../TSA/TSS-QC und
  - ../TSA/TSS-AdESQCandQES.
- Alle Dienste-Identifizierer aus EUMS-TL

#### 10.1.1.14 Zeile "Notwendige Prüftiefe der Zertifikatskette"

Es wird die Prüftiefe der Zertifikatsketten angegeben. Mögliche Werte sind

- **Minimal:** Dies bedeutet, dass bei der Prüfung der Signatur der OCSP-Antwort (auf die Prüfung eines Zertifikats aus der Signaturzertifikatskette) alle Prüfungen durchgeführt werden, bis auf die Ermittlung des Sperrstatus des OCSP-Signer-Zertifikats.
- **Normal:** Dies bedeutet, dass bei der Prüfung der Signatur der OCSP-Antwort (auf die Prüfung eines Zertifikats aus der Signaturzertifikatskette) alle Prüfungen durchgeführt werden. Dazu gehört auch die Ermittlung des Sperrstatus des OCSP-Signer-Zertifikats. Die OCSP-Antwort auf diese Prüfanfrage wird wieder geprüft, allerdings wird der Sperrstatus des OCSP-Signer-Zertifikats nicht mehr ermittelt. Bei Prüfrichtlinien, herausgegeben von der Governikus KG, ist dies die Voreinstellung.
- **Maximal:** Dies bedeutet, dass bei der Prüfung der Signatur der OCSP-Antwort (auf die Prüfung eines Zertifikats aus der Signaturzertifikatskette) alle Prüfungen durchgeführt werden. Dazu gehört auch die Ermittlung des Sperrstatus des OCSP-Signer-Zertifikats. Alle folgenden OCSP-Antworten werden solange weiter vollständig geprüft, bis ein OCSP-Signer-Zertifikat in einer OCSP-Antwort vorhanden ist, das schon einmal geprüft wurde (Meldung: Der Sperrstatus für dieses Zertifikat wurde bereits an anderer Stelle ermittelt und muss deshalb nicht erneut ermittelt werden). Dies entspricht der Anforderung aus der Common-PKI-Spezifikation zur Prüfung von qualifizierten Signaturen.

#### 10.1.1.15 Zeile "Maximal zulässige Cache-Zeit von OCSP-Antworten für CA-Zertifikate"

Es wird die maximal zulässige Cache-Zeit von OCSP-Antworten für CA-Zertifikate in Sekunden angezeigt.

#### 10.1.1.16 Zeile "Maximal zulässige Cache-Zeit von OCSP-Antworten für EE-Zertifikate"

Es wird die maximal zulässige Cache-Zeit von OCSP-Antworten für EE-Zertifikate in Sekunden angezeigt.

#### **10.1.1.17 Zeile "Alle Signaturprüfungen werden zu den behaupteten Signaturzeitpunkten durchgeführt"**

Es wird angezeigt, ob alle Signaturprüfungen zum behaupteten Signaturzeitpunkt durchgeführt werden sollen. Mögliche Werte sind:

- Ja
- Nein

#### **10.1.1.18 Zeile "Zertifikat-Hashwert in OCSP-Antwort muss vorhanden sein"**

Es wird angezeigt, ob der Zertifikat-Hashwert in OCSP-Antwort vorhanden sein und mit dem geprüften Zertifikat übereinstimmen muss. Dies ist die Anforderung aus dem deutschen Signaturgesetz für die Prüfung qualifizierter elektronischer Signaturen. Mögliche Werte sind:

- Ja
- Nein

#### **10.1.1.19 Zeile "Sperrstatermittlung nur über OCSP erlaubt"**

Es wird angezeigt, ob die Sperrstatermittlung nur über OCSP erfolgen darf. Im anderen Fall sind OCSP oder CRL erlaubt sind. Mögliche Werte sind:

- Ja
- Nein

#### **10.1.1.20 Zeile "Minimal notwendiges Vertrauensniveau des Prüfzeitpunktes"**

Es wird das minimal erforderliche Vertrauensniveau des Prüfzeitpunktes angezeigt. Mögliche Werte sind:

- Behaupteter Signaturzeitpunkt (claimed signing time)
- Zeitmarke (OSCI: Eingangszeitpunkt auf Server)
- Nicht qualifizierter Zeitstempel
- Nicht qualifizierter Zeitstempel für VDA-TSS
- Nicht qualifizierter Zeitstempel für qVDA-QC
- Qualifizierter elektronischer Zeitstempel
- Zeitpunkt der Durchführung der Prüfung (existence)

#### **10.1.1.21 Zeile "Prüfergebnis bei gesperrten Zertifikaten"**

Es wird angezeigt, ob bei einem gesperrten Zertifikat das Einzelprüfergebnis den Status ungültig "rot" oder unbestimmt "gelb" erhalten soll. Ungültig entspricht der Anforderung aus dem deutschen Signaturgesetz. Unbestimmt wird von der EN zur Validierung von Signaturen gefordert. Mögliche Werte sind:

- unbestimmt
- ungültig

### **10.1.1.22 Zeile "Prüfergebnis außerhalb des Gültigkeitsintervalls"**

Es wird angezeigt, ob das Prüfergebnis bei einem Prüfzeitpunkt außerhalb des Gültigkeitsintervalls des Zertifikats liegt, als Einzelprüfergebnis den Status ungültig "rot" oder unbestimmt "gelb" erhalten soll. Ungültig entspricht der Anforderung aus dem deutschen Signaturgesetz. Unbestimmt wird von der EN zur Validierung von Signaturen gefordert. Mögliche Werte sind:

- unbestimmt
- ungültig

### **10.1.1.23 Zeile "Prüfung der Vertrauensstellung für Sperrstatus-Antworten"**

Anzeigt wird, ob die Vertrauensstellung für Sperrstatus-Antworten geprüft werden soll.

Mögliche Werte sind:

- ja
- nein

## **10.2 Knoten "Vertrauenslisten" aufgeklappt**

Nach Aufklappen des Knotens "Vertrauenslisten" werden Detailinformationen zu jeder verwendeten Vertrauensliste und, wenn vorhanden, zur Erweiterung der Vertrauenslisten angezeigt. Außerdem wird eine Download-URL angeboten, um die Vertrauensliste und die Erweiterung der Vertrauensliste herunterladen zu können.

### **10.2.1 Überschrift "Vertrauensliste #1"**

Unter der Überschrift Vertrauensliste #1 werden Detailinformationen zu der im Rahmen der Signaturprüfung verwendeten Vertrauensliste angezeigt. Wurden im Kontext der Signaturprüfung mehrere Vertrauenslisten angewendet, werden die Überschrift und die Angaben wiederholt.

#### **10.2.1.1 Zeile "Staat"**

Es wird der EU-Mitgliedsstaat angezeigt, für den die Vertrauensliste herausgegeben wurde. Die Angabe stammt aus der Vertrauensliste.

#### **10.2.1.2 Zeile "Ausstellende Aufsichtsbehörde oder Stelle"**

Es wird die für den EU-Mitgliedsstaat zuständige Behörde oder Stelle angezeigt, die die Vertrauensliste erstellt hat. Die Angabe stammt aus der Vertrauensliste. Handelt es sich um die von der Governikus KG bereitgestellte Liste für nicht qualifizierte Vertrauensdiensteanbieter, ist die herausgebende Stelle immer die Governikus KG. Die Angabe stammt immer aus der Vertrauensliste.

#### **10.2.1.3 Zeile "Version"**

Es wird die Versionsnummer der Vertrauensliste angezeigt. Die Angabe stammt aus der Vertrauensliste. Bei hoheitlichen Vertrauenslisten oder Governikus Vertrauenslisten wird die Versionsnummer fortlaufend hochgezählt.



#### **10.2.1.4 Zeile "Download-URL"**

Es wird die Download-URL angezeigt, von der die Vertrauensliste heruntergeladen werden kann.

#### **10.2.1.5 Zeile "Ausgegeben am"**

Es werden Datum und Uhrzeit angezeigt, an der die Vertrauensliste durch die ausstellende Behörde ausgegeben wurde: Die Form ist `TT.MM.JJJJ hh:mm:ss`.

#### **10.2.1.6 Zeile "Nächste Aktualisierung am"**

Es werden Datum und Uhrzeit angezeigt, an der die Vertrauensliste durch die ausstellende Behörde spätestens aktualisiert wird. Die Form ist `TT.MM.JJJJ hh:mm:ss`.

### **10.2.2 Überschrift "Erweiterung der Vertrauensliste #1"**

Unter der Überschrift Erweiterung der Vertrauensliste #1 werden Detailinformationen zu der, im Rahmen der Signaturprüfung verwendeten, Erweiterung der Vertrauensliste #1 angezeigt. Die Überschrift und die Detailinformationen werden nur angezeigt, wenn eine Erweiterung zur Vertrauensliste vorhanden ist. Wurden im Kontext der Signaturprüfung mehrere Vertrauenslisten angewendet, werden die Überschrift und die Angaben wiederholt.

#### **10.2.2.1 Zeile "Staat"**

Es wird der EU-Mitgliedsstaat angezeigt, für den die Erweiterung der Vertrauensliste herausgegeben wurde. Die Angabe stammt aus der Vertrauensliste.

#### **10.2.2.2 Zeile "Ausstellende Aufsichtsbehörde oder Stelle"**

Es wird die ausstellende Stelle angezeigt, die die Erweiterung der Vertrauensliste erstellt hat. Die Angabe stammt aus der Erweiterung der Vertrauensliste. Handelt es sich um eine Erweiterung der deutschen hoheitlichen Vertrauensliste, herausgegeben von der Bundesnetzagentur, wird die Erweiterung ausschließlich durch die Governikus KG zur Verfügung gestellt. Der Name der Stelle ist immer Governikus KG.

#### **10.2.2.3 Zeile "Version"**

Es wird die Versionsnummer der Erweiterung der Vertrauensliste angezeigt. Die Angabe stammt aus der Vertrauensliste. Sie wird fortlaufend hochgezählt.

#### **10.2.2.4 Zeile "Download-URL"**

Es wird die Download-URL angezeigt, von der die Erweiterung der Vertrauensliste heruntergeladen werden kann.

#### **10.2.2.5 Zeile "Ausgegeben am"**

Es werden Datum und Uhrzeit angezeigt, zu der die Erweiterung der Vertrauensliste ausgegeben wurde. Die Form ist `TT.MM.JJJJ hh:mm:ss`.

### **10.2.2.6 Zeile "Nächste Aktualisierung am"**

Es werden Datum und Uhrzeit angezeigt, zu der die Erweiterung der Vertrauensliste spätestens aktualisiert wird. Die Form ist `TT.MM.JJJJ hh:mm:ss`.

## **10.3 Knoten "Algorithmenkataloge" aufgeklappt**

Nach dem Aufklappen des Knotens "Algorithmenkataloge" werden Detailinformationen zu den im Rahmen der Signaturprüfung verwendeten Algorithmenkataloge angezeigt.

### **10.3.1 Zeile "Name"**

Es wird der im Algorithmenkatalog angegebene Name des Algorithmenkatalogs angezeigt.

### **10.3.2 Zeile "Version"**

Es wird die im Algorithmenkatalog angegebene Versionsnummer angezeigt.

### **10.3.3 Zeile "Land"**

Es wird das im Algorithmenkatalog angegebene Land angezeigt.

### **10.3.4 Zeile "Veröffentlicht von"**

Es wird der im Algorithmenkatalog angegebene Name des Ausstellers angezeigt.

### **10.3.5 Zeile "Veröffentlicht am"**

Es werden Datum und Uhrzeit angezeigt, zu dem der Algorithmenkatalog veröffentlicht wurde. Die Form ist `TT.MM.JJJJ hh:mm:ss`. Die Angabe wurde aus dem Algorithmenkatalog entnommen.

### **10.3.6 Zeile "URL des Herausgebers"**

Es wird die Download-URL angezeigt, von der der verwendete maschinenlesbare Algorithmenkatalog heruntergeladen werden kann.

## **10.4 Knoten "Prüfinstanz" aufgeklappt**

Nach Aufklappen des Knotens "Prüfinstanz" wird angezeigt, welche Prüfinstanz auf der Basis welcher Produktversion die Prüfung durchgeführt hat.

### **10.4.1 Zeile "URL des Certificate Validation Servers"**

Es wird die URL des Betreibers des Certificate Validation Servers angezeigt, der die Zertifikatsprüfungen durchgeführt hat.

#### **10.4.2 Zeile "Kumulierte Wartezeit auf externe Antworten (in ms) "**

Es wird die kumulierte Wartezeit auf externe Antworten in Millisekunden auf gestellte OCSP-Anfragen/CRL-Downloads angezeigt. Diese Anfragen werden zum Teil parallel gestellt.

#### **10.4.3 Zeile "Version des CVS"**

Es wird die Versionsnummer des Certificate Validation Servers angezeigt, der die Zertifikatsprüfungen durchgeführt hat.

#### **10.4.4 Zeile "Version der CSL"**

Es wird die Versionsnummer der Crypto Service Library angezeigt, die lokal die mathematische Signaturprüfung durchgeführt und das Prüfprotokoll erstellt hat.

## 11 Signaturformate, Prüftiefe, Abkürzungsverzeichnis

### 11.1 Signaturformate, Nachrichtentypen mit Signaturen und Containerformate

Der Validation Service von DATA Varuna validiert

- Dokumente mit PAdES-, CAdES, XAdES- und JAdES-Baseline-Signaturen in allen Levels (B, T, LT und LTA) gemäß ETSI-Vorgaben,
- signierte Dokumente in OSCI-, ASiC- und ZIP-Containern,
- signierte OSCI-Nachrichten (Containersignaturen), De-Mailnachrichten mit DKIM-Signaturen und signierte E-Mails sowie
- End-Entity-Zertifikate des Typs Signatur, Siegel oder Website-Authentisierung (separat übergeben).

Detaillierte Informationen zu den unterstützten Signaturformaten, ggf. notwendige Einschränkungen sowie die Benennung der unterstützten technischen ETSI-Standards und Europäischen Normen finden Sie in der folgenden Tabelle.

Generell werden signierte Dateien und Container bis zu einer Dateigröße von 300 MB unterstützt. Darüber gelten für einzelne Signaturformate, Nachrichtentypen und Container noch weitere Beschränkungen, die in der folgenden Übersicht mit aufgelistet werden.

| Signatur-format                | Unterstützte Standards  | Bemerkungen   |
|--------------------------------|---|---|
| CAdES-Signatur                 | Baseline-Level B, T und LT gemäß ETSI TS 103173 v.2.2.1 *<br>Baseline-Level B-B, B-T, B-LT und B-LTA gemäß ETSI EN 319 122-2 V1.1.1<br>CAdES Baseline Profile BES/EPES gemäß ETSI TS 101 733 v.1.8.1 **<br>CAdES E ERS gemäß ETSI TS 119 122-3 V1.1.1 | <ul style="list-style-type: none"> <li>• attached und detached</li> <li>• detached CAdES-Signaturen können nur dann validiert werden, wenn Inhaltsdatei und Signaturdatei den selben Dateinamen besitzen (Beispiel: dateiname.docx und dateiname.docx.p7s)</li> <li>• die Datendatei muss Validierungsprozess übergeben werden</li> </ul> |
| PAdES-Signatur im PDF-Dokument | Baseline-Level B, T und LT gemäß ETSI TS 103173 v.2.2.2 *<br>Baseline-Level B-B, B-T, B-LT und B-LTA gemäß ETSI EN 319 142-1 V1.1.1<br>PAdES Baseline Profile BES/EPES gemäß ETSI TS 102778-3 v1.2.1 **   | <ul style="list-style-type: none"> <li>• maximal 10 (ggf. PAdES-signierte) Revisionen in einem PDF</li> <li>• signierte Dokumente als PDF-Anlage können nicht validiert werden</li> </ul>   |
| XAdES-Signatur in XMLs         | Baseline-Level B, T und LT gemäß ETSI TS 103171 v.2.1.1 *<br>Baseline-Level B-B, B-T, B-LT und B-LTA gemäß ETSI EN 319 132-1 V1.1.1<br>XAdES Baseline Profile gemäß BES/EPES ETSI TS 101 903 v1.4.1 **  | <ul style="list-style-type: none"> <li>• enveloped, enveloping und detached</li> <li>• detached-Signaturen können nur validiert werden, wenn die URI-Referenz auf ein lokales Datenobjekt verweist, Das Datenobjekt muss Validierungsprozess übergeben werden</li> </ul>  |
| JAdES-Signatur in JSON-Datei   | Baseline-Level B-B, B-T, B-LT und B-LTA gemäß TS 119 182-1 V1.1.1   |   |

| Nachrichtentypen  | Unterstützte Standards   | Bemerkungen   |
|---|--|---|
| De-Mail-Nachricht (mit einer DKIM Signatur)   | BSI Technische Richtlinie TR 01201 bis Version 1.6, Header-Version 1.0, 1.1 und 1.2<br>DKIM-Signaturen (DomainKeys Identified Mail) gemäß RFC 6376     | <ul style="list-style-type: none"> <li>in Bestätigungsnachrichten können auch die inneren XML-Signaturen (XAdES) validiert werden</li> </ul>  |
| Signierte Email (mit einer S/MIME-Signatur)   | S/MIME-Signaturen (Secure/Multipurpose Internet Mail Extensions) Version 3.1 gemäß RFC 3851, Version 3.2 gemäß RFC 5751 und Version 4.0 gemäß RFC 8551 | <ul style="list-style-type: none"> <li>Emails im Plain-Text-Format (Endung eml)</li> <li>Emails im Export-Format (Endung msg), Export aus den Outlook-Versionen 2007, 2010, 2013, 2016 oder 2019</li> </ul>   |
| OSCI-Nachricht mit XML-Containersignatur  | OSCI-Spezifikation 1.2 bis Korrigenda 1-7  | <ul style="list-style-type: none"> <li>validiert werden können nur vom OSCI-Manager abgeholte OSCI-Nachrichten</li> </ul>   |
| Containerformate  | Unterstützte Standards   | Bemerkungen   |
| OSCI-Nachricht mit signierten Dateien in einem Container                                | OSCI-Spezifikation 1.2 bis Korrigenda 1-7  | <ul style="list-style-type: none"> <li>mit oder ohne Containersignatur</li> <li>maximal (signierte) 10 Dateien im Container mit Signaturen der hier aufgeführten Signaturformate. Container im Container werden eingerechnet.</li> <li>Summe der Dateigrößen darf 300 MB nicht übersteigen</li> </ul>   |
| ASiC-Container  | Baseline-Level S und E gemäß ETSI EN 319 162-1 V1.1.1<br>Baseline-Level S gemäß ETSI TS 103 174 V2.2.1 *   | <ul style="list-style-type: none"> <li>für ASiC-E gilt maximal 10 signierte Dateien mit CAdES- oder XML-detached Signaturen oder Zeitstempeln außerhalb des META-INF Verzeichnisses</li> <li>Summe der Dateigrößen darf 300 MB nicht übersteigen</li> </ul>   |
| PDF-Portfolio   |  | <ul style="list-style-type: none"> <li>maximal 10 (PAdES-signierte) PDF-Dateien im Portfolio</li> <li>Summe der Dateigrößen darf 300 MB nicht übersteigen</li> </ul>  |
| Exportierte XAIP mit signierter Datei und eingebettetem ERS                             | XAIP gemäß BSI TR-03125 Version 1.2.1 und 1.2.2  | <ul style="list-style-type: none"> <li>Dateien mit *AdES-B-LTA-Signaturen können nicht validiert werden</li> </ul>  |
| ZIP-Container   |  | <ul style="list-style-type: none"> <li>maximal 10 signierte Dateien; Summe der Dateigrößen darf 300 MB nicht übersteigen</li> </ul>   |
| X509-V3-Zertifikat  | Unterstützte Standards   | Bemerkungen   |
| End-Entity-Zertifikat   | RFC 5280<br>ETSI EN 319 412-1, -3, -4 Version 1.1.1<br>ETSI EN 319 412-2, -5 Version 2.1.1<br>Common-PKI-Spez. Version 2.0                             | <ul style="list-style-type: none"> <li>Gültigkeitsprüfung/Ermittlung des Niveaus und des Typs für EE-Zertifikate (z.B. für Signatur- und Siegelzertifikate oder Zertifikate für Website-Authentisierung) zu einem übergebenen Prüfzeitpunkt</li> <li>Zertifikate, die als SDI in Vertrauenslisten konfiguriert sind (z.B. CA-Zertifikate oder Zeitstempel-Zertifikate), können nicht geprüft werden, da in der Regel die Ermittlung des Sperrstatus nicht möglich ist und für sie kein Zertifikatsniveau in den Vertrauenslisten konfiguriert ist.</li> </ul> |
| * Format und Level unterstützt Beschluss 2014/148/EU und (EU) 2015/1506 der Kommission. |  |   |
| ** Format und Level unterstützt gemäß Beschluss 2011/130/EU der Kommission.             |  |   |

Die Unterstützung anderer Formatspezifikationen und älterer ETSI-Formatspezifikationen kann nicht sichergestellt werden.

## 11.2 Prüftiefe

Bei der Validierung von signierten Dateien wird als Voreinstellung eine Verschachtelung von Signaturen (Beispiel: dateiname.docx.p7s.p7s) bis zu der Prüftiefe 1 unterstützt. Die Schachtelungstiefe ist begrenzt, da ansonsten zum Beispiel so genannte ZIP-Bomben die Validierung beeinträchtigen könnten.

- Die Prüftiefe 0 bedeutet, dass alle entdeckten standardkonformen Signaturen der unterstützten Formate in einer dem Validierungsservice übergebenen Datei validiert werden. Beispiele: Alle CAdES-Signaturen in einer Datei (soweit parallele Inhaltsdatensignaturen und alle sich auf Inhaltsdatensignaturen beziehende Counter-Signaturen), alle PAdES-Signaturen (Revisionen) in einem PDF-Dokument, die XML-Containersignatur einer OSCI-Nachricht, die DKIM-Signatur in einer De-Mailnachricht oder die S/MIME-Signatur in einer E-Mail.
- Die Prüftiefe 1 beinhaltet die Prüftiefe 0. Prüftiefe 1 bedeutet, dass zusätzlich in einem dem Validierungsservice übergebenen Container (ZIP-Container, ASiC-Container oder OSCI-Nachricht mit OSCI-Container) oder in einem PDF-Portfolio sich befindende Dateien mit PAdES-Signaturen validiert werden können. Bei dieser Prüftiefe wird auch eine nochmals signierte CAdES-Signatur (z.B.: dateiname.xxx.p7s.p7s) validiert. Die Prüftiefe 1 bedeutet damit auch, dass z.B. ein ZIP in einem ZIP oder ein ZIP als Inhaltsdatei in einem ASiC-Container nicht mehr entpackt wird. Folgende Besonderheiten sind bei der Prüftiefe 1 zu beachten: In PDF-Portfolios werden ausschließlich PDF-Dokumente mit PAdES-Signaturen validiert. Signierte Anhänge in exportierten E-Mails sind trotz Prüftiefe 1 nicht automatisch validierbar.
- Als Sonderfall werden OSCI-Nachrichten behandelt. Hier gilt als Voreinstellung die Prüftiefe 2. Somit können signierte Dateien, die sich in einem ZIP befinden, welches sich wiederum in einem OSCI-Container befindet, validiert werden.

## 12 Abkürzungsverzeichnis

| Abkürzung          | Erklärung  |
|--------------------|--|
| AdES               | Advanced Electronic Signature  |
| ASiC               | Associated Signature Container   |
| ASiC-S             | ASiC simple gemäß EN 319 162-1 gemäß Baseline-Profil S oder ETSI TS 103 174 Baseline-Profil S      |
| ASiC-E             | ASiC extended ETSI EN 319 162-1 gemäß Baseline-Profil E  |
| BNetzA             | Bundesnetzagentur  |
| CA                 | Certificate Authority  |
| CAdES              | CMS Advanced Electronic Signatures   |
| CAdES-Signatur B   | CAdES-Signatur gemäß ETSI EN 319 122-1 Baseline-Profil B-B oder ETSI TS 103173 Baseline-Profil B   |
| CAdES-Signatur T   | CAdES-Signatur gemäß ETSI EN 319 122-1 Baseline-Profil B-T oder ETSI TS 103173 Baseline-Profil T   |
| CAdES-Signatur LT  | CAdES-Signatur gemäß ETSI EN 319 122-1 Baseline-Profil B-LT oder ETSI TS 103173 Baseline-Profil LT |
| CAdES-Signatur LTA | CAdES-Signatur gemäß ETSI EN 319 122-1 Baseline-Profil B-LTA                                       |
| CMS                | Cryptographic Message Syntax   |
| CRL                | Certificate Revocation List  |
| DKIM               | DomainKeys Identified Mail   |
| EC                 | Elliptic Curve Public Key Crypto System  |
| ECDSA              | Elliptic Curve Digital Signature Algorithm   |
| EE (-Zertifikat)   | End Entity (-Zertifikat)   |
| eIDAS-VO           | Electronic Identification, Authentication and Trust Services Verordnung                            |
| EN                 | Europäischer Standard (EU)   |
| ERS                | Evidence Record Syntax   |
| ETSI               | European Telecommunications Standards Institute  |
| EU                 | Europäische Union  |
| EUMS-TL            | EU Member State Trusted List   |
| JAdES-Signatur B   | JAdES-Signatur gemäß ETSI EN 119 182-1 Baseline-Profil B-B   |
| JAdES-Signatur T   | JAdES-Signatur gemäß ETSI EN 119 182-1 Baseline-Profil B-T   |
| JAdES-Signatur LT  | JAdES-Signatur gemäß ETSI EN 119 182-1 Baseline-Profil B-LT  |
| JAdES-Signatur LTA | JAdES-Signatur gemäß ETSI EN 119 182-1 Baseline-Profil B-LTA                                       |
| LDAP               | Lightweight Directory Access Protocol  |
| MD5                | Message Digest Algorithm 5   |

| <b>Abkürzung</b>   | <b>Erklärung</b>   |
|--------------------|--|
| PDF                | Portable Document Format   |
| PAdES              | PDF Advanced Electronic Signature  |
| PAdES-Signatur B   | PAdES-Signatur gemäß ETSI EN 319 142-1 Baseline-Profil B-B oder ETSI TS 103173 Baseline-Profil B   |
| PAdES-Signatur T   | PAdES-Signatur gemäß ETSI EN 319 142-1 Baseline-Profil B-T oder ETSI TS 103173 Baseline-Profil T   |
| PAdES-Signatur LT  | PAdES-Signatur gemäß ETSI EN 319 142-1 Baseline-Profil B-LT oder ETSI TS 103173 Baseline-Profil LT |
| PAdES-Signatur LTA | PAdES-Signatur gemäß ETSI EN 319 142-1 Baseline-Profil B-LTA                                       |
| PKC                | Public Key Certificate   |
| PKCS               | Public Key Cryptography Standards  |
| POE                | Proof of Existence   |
| PSS                | Probabilistic Signature Scheme   |
| OCSP               | Online Certificate Status Protocol   |
| OID                | Object Identifier  |
| OSCI               | Online Services Computer Interface   |
| QC                 | Qualified Certificate  |
| QCStatement        | Qualified Certificate Statement  |
| QES                | Qualifizierte elektronische Signatur   |
| QSCD               | Qualified Signature/Seal Creation Device   |
| qVDA               | Qualifizierter Vertrauensdiensteanbieter   |
| RFC                | Request For Comments   |
| RSA                | Rivest-Shamir-Adleman public-key cryptosystem  |
| SDI                | Service Digital Identity   |
| SHA                | Secure Hash Algorithm  |
| SigG               | Deutsches Signaturgesetz   |
| S/MIME             | Secure / Multipurpose Internet Mail Extensions   |
| SOG-IS             | Senior Officials Group Information Systems Security of the European Commission                     |
| SSCD               | Secure Signature Creation Device   |
| TR-ESOR            | Technische Richtlinie (TR) zur Beweiswerterhaltung kryptographisch signierter Dokumente (ESOR)     |
| TS                 | Technical Specification  |
| TSA                | Time Stamping Authority  |
| TSP                | Trust Service Provider   |
| TST                | Time Stamp Token   |
| URI                | Uniform Resource Identifier  |



| <b>Abkürzung</b>   | <b>Erklärung</b>  |
|--------------------|---|
| URL                | Uniform Resource Locator  |
| VDA                | Vertrauensdiensteanbieter   |
| XML                | Extensible Markup Language  |
| XAdES              | XML Advanced Electronic Signature   |
| XAdES-Signatur B   | XAdES-Signatur gemäß ETSI EN 319 132-1 Baseline-Profil B-B oder ETSI TS 103171 Baseline-Profil B    |
| XAdES-Signatur T   | XAdES-Signatur gemäß ETSI EN 319 132-1 Baseline-Profil B-T oder ETSI TS 103171 Baseline-Profil B-LT |
| XAdES-Signatur LT  | XAdES-Signatur gemäß ETSI EN 319 132-1 Baseline-Profil B-LT oder ETSI TS 103171 Baseline-Profil LT  |
| XAdES-Signatur LTA | XAdES-Signatur gemäß ETSI EN 319 132-1 Baseline-Profil B-LTA  |
| XAIP               | XML formatted Archival Information Package  |
| ZIP                | Kompressionsstandard für die verlustfreie Datenkompression  |

## 13 Abbildungsverzeichnis

|  |    |
|--|----|
| Abbildung 1: Hauptseite Governikus Prüfprotokoll.....  | 9  |
| Abbildung 2: Hauptseite Governikus Prüfprotokoll Bereich B bei der Prüfung einer Signatur ohne optionale Zeilen .....  | 10 |
| Abbildung 3: Hauptseite Governikus Prüfprotokoll Bereich B bei der Prüfung eines separaten Zertifikats.....  | 11 |
| Abbildung 4: Hauptseite Prüfprotokoll Bereich B bei der Prüfung einer Signatur mit optionalen Zeilen .....   | 12 |
| Abbildung 5: Hauptseite Prüfprotokoll Bereich C "Technischer Anhang" .....   | 13 |
| Abbildung 6: Hauptseite Bereich A des Prüfprotokolls .....   | 14 |
| Abbildung 7: Hauptseite Bereich B des Prüfprotokolls mit optionalen Zeilen .....   | 14 |
| Abbildung 8: Hauptseite Prüfprotokoll Bereich C "Technischer Anhang" .....   | 23 |
| Abbildung 9: Knoten "Niveau und Typ der Signatur" aufgeklappt (EU-qualifizierte Signatur)  | 24 |
| Abbildung 10: Knoten "Niveau und Typ der Signatur" aufgeklappt (EU-qualifizierter Zeitstempel).....  | 27 |
| Abbildung 11: Bereich B Knoten "Ergebnis der Signaturprüfung" aufgeklappt (EU-qualifizierte Signatur mit optionalen Knoten).....                                   | 33 |
| Abbildung 12: Bereich B Knoten "Prüfung des Zertifikats von <Name>" aufgeklappt, Angaben aus dem Zertifikat .....  | 40 |
| Abbildung 13: Bereich B Knoten "Prüfung des Zertifikats von <Name>", Zertifikatsprüfung ..   | 41 |
| Abbildung 14: Bereich B Knoten "Prüfung des Zertifikats von <Name>", Prüfung der Sperrstatusinformation.....   | 48 |
| Abbildung 15: Bereich B Knoten "Prüfung des Zertifikats von < Name >" aufgeklappt, wenn Zertifikat Vertrauensanker (EU-qualifizierte Signatur) .....               | 50 |
| Abbildung 16: Bereich B optionaler Knoten "Ergebnis der Prüfung des Signaturzeitstempels" aufgeklappt (EU-qualifizierter Zeitstempel) .....                        | 52 |
| Abbildung 17: Bereich B optionaler Knoten "Beweiswertbewahrung durch Archivzeitstempel" aufgeklappt.....   | 54 |
| Abbildung 18: Überschrift "Hashwertbaum" bei CAdES E ERS Signaturen .....  | 54 |
| Abbildung 19: Bereich A " Dokument-/Containerstruktur" (aufgeklappt) bei einem signierten PDF-Dokument mit zwei Signaturen .....                                   | 56 |
| Abbildung 20: Bereich A "Dokument- bzw. Containerstruktur" bei CAdES-Signaturen.....   | 57 |
| Abbildung 21: Bereich A "Dokument-/Containerstruktur" OSCI-Nachricht (aufgeklappt) .....   | 58 |
| Abbildung 22: Struktur eines PDF-Dokuments mit zwei Signaturen (aufgeklappt) .....   | 60 |
| Abbildung 23: Bereich 1 "Zusammenfassung und Struktur" bei einem signierten, manipulationsgefährdeten PDF-Dokument (Teilsignatur).....                             | 61 |
| Abbildung 24: Bereich 1 "Zusammenfassung und Struktur" bei einem signierten, manipulationsgefährdeten PDF-Dokument (unsignierte Revision zwischen Signaturen)..... | 62 |
| Abbildung 25: Bereich A Normale De-Mail-Nachricht (aufgeklappt).....   | 62 |
| Abbildung 26: Bereich A bei einer De-Mail-Bestätigungsnachricht (aufgeklappt) .....  | 68 |

Abbildung 27: Bereich A De-Mail-Bestätigungsnachricht ohne vorliegende normale De-Mailnachricht (aufgeklappt).....69

Abbildung 28: Hauptseite Governikus Prüfprotokoll mit optionaler Zusammenfassung der Prüfergebnisse mehrerer Signaturen.....72

Abbildung 29: Anzeige Inhaber und Aussteller eines Zertifikats.....74

Abbildung 30: Anhang mit Referenzen .....83