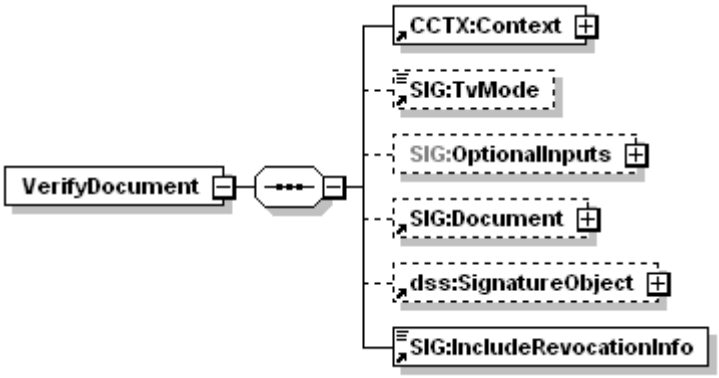
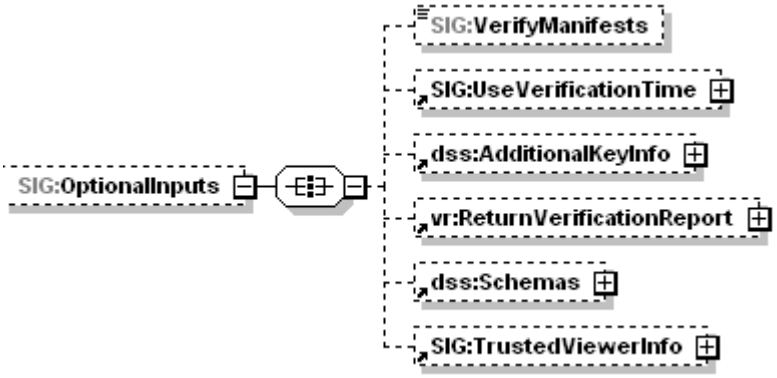
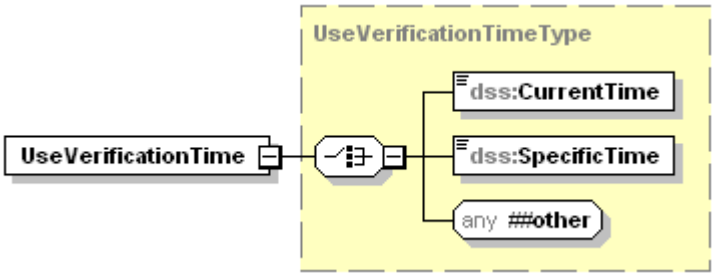
*Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.*

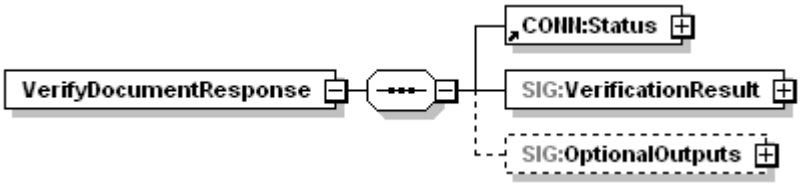
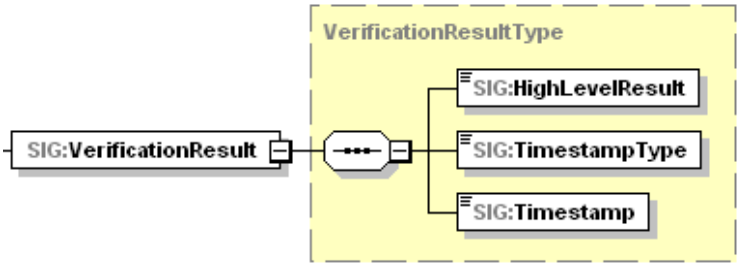
Aus den Rückmeldungen der Hersteller im Rahmen der Umsetzung des QES-Konnektors ergeben sich Anpassungen in der Profilierung des Verification Reports.

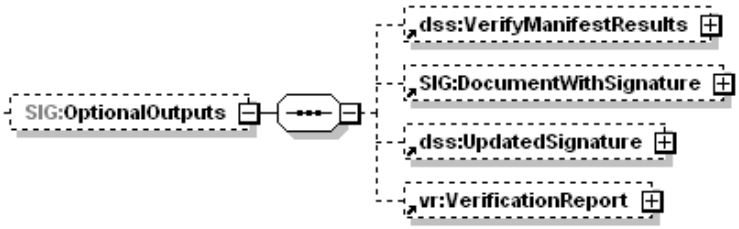
# Änderungsbedarf in gemSpec_Kon

**Tabelle 1: TAB_KON_066 Operation VerifyDocument (nonQES und QES)**

| | | |
|---|---|---|
| **Name** | `VerifyDocument` | |
| **Beschreibung** | Diese Operation verifiziert die Signatur eines Dokumentes.<br>Der Konnektor MUSS jede konform zur Außenschnittstelle SignDocument erzeugte Signatur durch VerifyDocument prüfen können. Darüber hinaus müssen im Fall QES, falls vorhanden, auch qualifizierte Zeitstempel geprüft werden. Außerdem MÜSSEN die zusätzlich geforderten Signaturverfahren zur Dokumentensignaturprüfung unterstützt werden.<br>Das Ergebnis der Prüfung wird, wenn gefordert, in Form eines standardisierten Prüfberichts in einer `VerificationReport`-Struktur gemäß [OASIS-VR] zurückgeliefert. | |
| **Aufrufparameter** |  | |
| | Name | Beschreibung |
| | `CCTX:Context` | MandantId, ClientSystemId, WorkplaceId verpflichtend; UserId nicht ausgewertet |
| | `TvMode` | Der Parameter wird im Konnektor nicht ausgewertet |
| | `SIG:OptionalInputs` | Enthält optionale Eingabeparameter (angelehnt an dss:OptionalInputs gemäß [OASIS-DSS] Section 2.7):<br>Die zulässigen optionalen Eingabeparameter sind unten erläutert. |

| | | |
|---|---|---|
| | `SIG:Document` | Enthält im Fall der Prüfung von detached oder enveloped Signaturen das zur Signatur gehörende bzw. das diese umschließende Dokument (siehe [OASIS-DSS] Section 2.4.2 und oben) |
| | `dss:SignatureObject` | Enthält die zu prüfende Signatur, wenn sie nicht im Dokument selbst eingebettet ist ([OASIS-DSS] Kapitel 4.1). Hierbei werden **XML-Signaturen** als `ds:Signature` Element und alle anderen Signaturen als `dss:Base64Signature` mit entsprechend gesetztem `Type`-Attribut (siehe `SignatureType`, Operationen SignDocument und ExternalAuthenticate) übergeben, wobei die nachfolgenden Werte unterstützt werden müssen:<br>• **CMS-Signatur** urn:ietf:rfc:5652<br>• **S/MIME-Signatur** urn:ietf:rfc:5751<br>• **PDF-Signatur** http://uri.etsi.org/02778/3<br>• **PKCS#1-Signatur** urn:ietf:rfc:3447 |
| | `SIG:IncludeRevocationInfo` | Durch diesen verpflichtenden Schalter kann der Aufrufer die Einbettung von zum Zeitpunkt der Signaturprüfung vorliegenden Sperrinformationen anfordern.<br>Ist bereits eine Sperrinformation eingebettet, so wird die neue Sperrinformation zusätzlich eingebettet.<br>Für in einer Gegensignatur enthaltene Signaturen erfolgt keine Einbettung von Sperrinformationen. |
| |  | |
| | `SIG:VerifyManifests` | Durch das in [OASIS-DSS] (Abschnitt 4.5.1) definierte Element kann die Prüfung eines ggf. vorhandenen Manifests angefordert werden. |
| |  | |
| | `SIG:UseVerificationTime` | Durch das in [OASIS-DSS] (Abschnitt 4.5.2) spezifizierte Element kann die Prüfung der Signatur bezüglich eines durch den Aufrufer bestimmten Zeitpunktes |

| | | |
|---|---|---|
| | | (`Benutzerdefinierter_Zeitpunkt`) erfolgen. |
| | `dss:AdditionalKeyInfo` | Durch das in [OASIS-DSS] (Abschnitt 4.5.4) spezifizierte Element kann zusätzliches, für die Prüfung benötigtes, Schlüsselmaterial übergeben werden. |
| | `vr:ReturnVerificationReport` | Durch dieses in [OASIS-VR] spezifizierte Element kann die Erstellung eines ausführlichen Prüfberichtes angefordert werden. Der Konnektor MUSS die Anforderungen der Konformitätsstufe 2 („Comprehensive“) erfüllen und die Profilierung aus Anhang B3 beachten. |
| | `dss:Schemas` | Durch das in [OASIS-DSS] (Abschnitt 2.8.5) definierte Element können eine Menge von XML-Schematas übergeben werden, die zur Validierung des übergebenen XML-Dokumentes verwendet werden können.<br>Zur Struktur dieses Elements siehe Beschreibung des Parameters `dss:Schemas` der Operation SignDocument. |
| | `SIG:ViewerInfo` | Der Parameter wird vom Konnektor nicht ausgewertet. |
| **Rückgabe** |  | |
| | `Status` | Enthält den Ausführungsstatus der Operation. |
| | `SIG:VerificationResult` |  <br>Das Element `Sig:VerificationResult` enthält das Ergebnis der Prüfung als Ampel, den Typ des zugehörigen angenommenen Signaturzeitpunkts und der angenommene Signaturzeitpunkt selbst. |
| | `SIG:HighLevelResult` | Das Ergebnis der Prüfung (Ampelschaltung) mit folgenden Werten:<br>• VALID: alle Signaturen sind gültig<br>• INVALID: mindestens eine der Signaturen ist ungültig<br>• INCONCLUSIVE: in allen anderen Fällen |
| | `SIG:TimestampType` | Der Typ des angenommenen Signaturzeitpunkts mit folgenden Werten:<br>• SIGNATURE_EMBEDDED_TIMESTAMP: in der Signatur eingebetter Zeitpunkt `Ermittelter_Signaturzeitpunkt` |

| | | |
|---|---|---|
| | | `_Eingebettet`<br>• QUALIFIED_TIMESTAMP: qualifizierter Zeitstempel über die Signatur `Ermittelter_Signaturzeitpunkt_Qualifiziert`<br>• SYSTEM_TIMESTAMP: Systemzeit des Konnektors bei Signaturprüfung `Ermittelter_Signaturzeitpunkt_System`<br>• USER_DEFINED_TIMESTAMP: benutzerdefinierter Zeitpunkt `Benutzerdefinierter_Zeitpunkt`<br>Als Format darf jedes zum XML-Typ "dateTime" konforme Format verwendet werden (<element name="Timestamp" type="dateTime"/>). Wenn mehrere Signaturen im Dokument vorhanden sind, wird hier der angenommene Signaturzeitpunkt der jüngsten Signatur angegeben. |
| | `SIG:Timestamp` | Im Element SIG:Timestamp wird der zu SIG:TimestampType gehörende Zeitstempel zurückgegeben. |
| | `SIG:OptionalOutputs` | Enthält (angelehnt an dss:OptionalOutputs, wie in Abschnitt 2.7 von [OASIS-DSS] beschrieben) optionale Ausgangselemente:<br>  |
| | `dss:VerifyManifestResults` | Dieses in Abschnitt 4.5.1 von [OASIS-DSS] definierte Element enthält Informationen zur Prüfung eines ggf. vorhandenen Signaturmanifests und wird zurückgeliefert, sofern beim Aufruf das `dss:VerifyManifest`-Element, aber nicht das `RequestVerificationReport` als optionales Eingabeelement übergeben wurde. |
| | `SIG:DocumentWithSignature` | Dieses in Abschnitt 4.5.8 von [OASIS-DSS] spezifizierte Element wird zurückgeliefert, falls eine in dem Dokument enthaltene Signatur (Enveloped Signature) in Verbindung mit dem `SIG:IncludeRevocationInfo`-Element geprüft wurde. |
| | `dss:UpdatedSignature` | Dieses in Abschnitt 4.5.8 von [OASIS-DSS] spezifizierte Element wird zurückgeliefert, falls eine abgesetzte (Detached Signature) oder umschließende (Enveloping Signature) in Verbindung mit dem `SIG:IncludeRevocationInfo`-Element geprüft wurde. |
| | `vr:VerificationReport` | Dieses in [OASIS-VR] spezifizierte Element wird zurückgeliefert, falls das `ReturnVerificationReport`-Element als Eingabeparameter verwendet wurde. Die Profilierung von Anhang B3 MUSS beachtet werden. |
| **Vorbedingungen** | Keine | |

| | |
|---|---|
| **Nachbedingungen** | Keine |

# Anhang B - Profilierung der Signatur- und Verschlüsselungsformate (normativ)

## B3 – Profilierung VerificationReport

### Anforderung eines ausführlichen Prüfberichts

Folgende Aufrufparameter müssen unterstützt werden:

```
<ReturnVerificationReport
xmlns="urn:oasis:names:tc:dss-x:1.0:profiles:verificationreport:schema#"
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:schemaLocation="urn:oasis:names:tc:dss-x:1.0:profiles:verificationreport:schema#
                    oasis-dssx-1.0-profiles-vr-cd1.xsd">
    <IncludeVerifier>false</IncludeVerifier>
    <IncludeCertificateValues>true</IncludeCertificateValues>
    <IncludeRevocationValues>true</IncludeRevocationValues>
    <ExpandBinaryValues>false</ExpandBinaryValues>
    <ReportDetailLevel>
        urn:oasis:names:tc:dss-x:1.0:profiles:verificationreport:reportdetail:allDetails
    </ReportDetailLevel>
</ReturnVerificationReport>
```

### Verwendung des erzeugten VerificationReport.

Für die folgenden Inhalte müssen die angegebenen Strukturen benutzen. Im Standard angegebene Pflichtfelder von erzeugten Strukturen müssen ggf. zusätzlich gefüllt werden:

a) ~~Angenommener Signaturzeitpunkt gemäß TIP1-A_5540 (QES) und TIP1-A_5545 (nonQES)~~ Prüfzeitpunkt (Systemzeit des Konnektors zum Zeitpunkt der Prüfung)

```
/VerificationReport/
    dss:VerificationTimeInfo/
        dss:VerificationTime
```

b) Signaturzeitpunkt (`Ermittelter_Signaturzeitpunkt_Eingebettet`)

```
/VerificationReport/
    IndividualReport/
        SignedObjectIdentifier/
            SignedProperties/
```

SignedSignatureProperties/
XAdES:SigningTime

~~Den zur Prüfung der Signatur verwendeten Signaturzeitpunkt als Lokalzeit ist in der SIG:VerifyDocumentResponse / SIG:VerificationResult/ SIG:Timestamp zurückgemeldet und über SIG:TimestampType qualifiziert.~~

Die Signierzeit SigningTime ist nicht nur für XAdES-Signaturen, sondern allgemein für Signaturen gemäß AdES-Baseline-Profilierung, also auch für CAdES und PAdES zu füllen.

~~c ) Der Hashalgorithmus~~

~~/VerificationReport/~~
~~IndividualReport/~~
~~SignedObjectIdentifier/~~
~~DigestAlgAndValue/~~
~~ds:DigestMethod/~~
~~@Algorithm~~

c) Angenommener Signaturzeitpunkt gemäß TIP1-A_5540 (QES) und TIP1-A_5545 (nonQES)

/VerificationReport/
IndividualReport/
Details/
dss:VerificationTimeInfo/
dss:VerificationTime

d) ~~die Daten, auf die sich die Signatur bezieht~~ der binäre Wert der Signatur

/VerificationReport/
IndividualReport/
SignedObjectIdentifier/
SignatureValue

e) Kurztext ~~und andere Signierte Attribute~~

~~Kurztext wird als Teil von SIG:DocumentWithSignature außerhalb des VerificationReport in der SIG:VerifyDocumentResponse/ zurückgemeldet.~~Der signierte Kurztext wird in folgendem XML-Element zurückgegeben:

/VerificationReport/
IndividualReport/
SignedObjectIdentifier/
SignedProperties/
Other/
SIG:ShortText
~~dss:Property~~
~~./dss:Identifier (z.B.: ShortText)~~

~~./dss:Value/AttributValue (Wert)~~

f) Das folgende Element mit den Werten true/false gibt an, ob eine Zertifikatsreferenz gemäß Anhang B2 vorhanden ist (true) oder nicht (false):

```
/VerificationReport/
    IndividualReport/
        SignedObjectIdentifier/
            SignedProperties/
                Other/
                    SIG:ReferenceToSignerCertificate
```

g) Sämtliche signierte Attribute, deren Rückgabe nicht explizit über andere Elemente geregelt ist, werden als direkt anzeigbare Key/Value-Paare zurückgeben. Dabei sind sowohl Key und Value bereits für die Anzeige formatiert. Der Key wird in einer Zeile dargestellt. Der Value wird in mehreren Zeilen dargestellt, wobei ein Zeilenumbruch durch 'CARRIAGE RETURN (CR)' 'LINE FEED (LF)' erzeugt wird und keine weiteren Steuerzeichen erlaubt sind.

```
/VerificationReport/
    IndividualReport/
        SignedObjectIdentifier/
            SignedProperties/
                Other/
                    SIG:DisplayableAttributes
```

h) das Ergebnis der Signaturprüfung

```
/VerificationReport/
    IndividualReport/
        Result
```

i) ~~im Fall einer Gegensignatur, die Kennzeichnung als Gegensignatur und den Verweis auf die gegensignierte Signatur, im Element~~

~~/DetailedSignatureReport/~~
~~Properties/~~
~~UnsignedProperties/~~
~~UnsignedSignatureProperties/~~
~~CounterSignature/~~

handelt es sich bei der Signatur um eine Gegensignatur wird diese als solche markiert

```
/DetailedSignatureReport/
    Properties/
        UnsignedProperties/
            Other/
```

SIG:CounterSignatureMarker

und mit

/DetailedSignatureReport/
Properties/
UnsignedProperties/
Other/
SIG:CounterSignatureMarker/
SignatureValueReference/
@IdRef

auf jede (eine oder mehrere) gegensignierte Signaturen verwiesen. Dabei zeigt IdRef auf den jeweiligen gegensignierten Signaturwert

/VerificationReport/
IndividualReport/
SignedObjectIdentifier/
ds:SignatureValue/
@Id

j) das Ergebnis der Zertifikatsprüfung,

/VerificationReport/
IndividualReport/
Details/
DetailedSignatureReport/
CertificatePathValidity/
PathValiditySummary/
ResultMajor

k) den Inhalt des Zertifikates, auf dem beruhend signiert wurde, ~~sowie den Inhalt in die Signatur eingefügter Attributzertifikate mit dem Prüfergebnis der im Kontext relevanten Rollen, umfasst die OIDs oid_hba_qes zur Identifikation einer QES-Signatur~~

/VerificationReport/
IndividualReport/
Details/
DetailedSignatureReport/
CertificatePathValidity/
PathValidityDetail/

CertificateValidity/
CertificateValue

l) den Signaturalgorithmus der Dokumentensignatur (URI, angelehnt an den Wertebereich des Feldes ds:SignatureMethod),

/VerificationReport/
IndividualReport/
Details/
DetailedSignatureReport/
SignatureOK/ ~~CertificatePathValidity/~~
SignatureAlgorithm ~~PathValidityDetail/~~
~~CertificateValidity/~~
~~SignatureOK/~~
~~SignatureAlgorithm/~~
~~Algorithm~~

m) einen aussagekräftigen Hinweis zum verminderten Beweiswert hinsichtlich Authentizität und Integrität der Signatur, wenn einer der bei der Signaturprüfung identifizierten und unterstützten Algorithmen zum Zeitpunkt der Signaturprüfung ~~Signaturerstellung~~ nicht mehr laut Algorithmenkatalog [ALGCAT] als geeignet eingestuft wird. Auszuwerten sind die Festlegungen des ALGCAT sowohl bezogen auf die Vergangenheit als auch auf die Zukunft

Für alle geprüften Zertifikate:
../
vr:CertificateValidity/
vr:SignatureOK/
vr:SignatureAlgorithm/
vr:Suitability/
./ResultMajor= urn:oasis:names:tc:dss:1.0:detail:invalid ~~indetermined~~
./ResultMessage="Algorithmen seit <Jahr> als unsicher eingestuft"

n) die PathValidity bis zur TrustAnchor-TSL mit

//CertificateValidity/ChainingOK/ResultMajor (ab dem zweiten Zertifikat in der Kette)
//CertificateValidity/CertificateStatus/CertStatusOK/ResultMajor
//CertificateValidity/CertificateValue
Für das Feld TrustAnchor ist
"urn:oasis:names:tc:dss-x:1.0:profiles:verificationreport:trustanchor:certDataBase"
zu verwenden.

o) Prüfergebnis des Gültigkeitszeitraums

/VerificationReport/
IndividualReport/
Details/
DetailedSignatureReport/

CertificatePathValidity/
PathValidityDetail/
CertificateValidity/
ValidityPeriodOK/
ResultMajor

p) Prüfung der Extensions

/VerificationReport/
IndividualReport/
Details/
DetailedSignatureReport/
CertificatePathValidity/
PathValidityDetail/
CertificateValidity/
ExtensionsOK/
ResultMajor

q) Zeitstempel und Herkunft der OCSP-Antwort für das Signaturzertifikat

/VerificationReport/
IndividualReport/
Details/
DetailedSignatureReport/
CertificatePathValidity/
PathValidityDetail/
CertificateValidity/
CertificateStatus/
RevocationEvidence/
OCSPValidity/
OCSPIdentifier/
./XAdES:ResponderID/XAdES:ByName
./XAdES:ProducedAt

r) OCSP Antwort für das Signaturzertifikats

/VerificationReport/
IndividualReport/
Details/
/vr:DetailedSignatureReport/
vr:CertificatePathValidity/
vr:PathValidityDetail/
vr:CertificateValidity/
vr:CertificateStatus/
vr:RevocationEvidence/

vr:OCSPValidity/
vr:OCSPValue

## Sonderfälle:

### Signatur mit Attributzertifikaten

Es wird für jedes Attributzertifikat, das von der Signatur umfasst wird, ein Element

/VerificationReport/
IndividualReport/
SignedObjectIdentifier/
SignedProperties/
SignedSignatureProperties/
SignerRole/
CertifiedRoles/
AttributeCertificateValidity

angelegt. ~~Attributzertifikate außerhalb der Signatur werden in einem eigenen IndividualReport behandelt, bei allDetails mit IndividualAttributeCertificateReport.~~

### Dokument mit parallelen Signaturen

Für jede Signatur wird ein IndividualReport erzeugt.

### Dokument mit Signatur und Gegensignatur

Für jede Signatur wird ein IndividualReport erzeugt.

### Dokument mit Signatur und qualifiziertem Zeitstempel

Für den Zeitstempel wird ein eigener IndividualReport mit IndividualTimeStampReport erzeugt.

# Anhang D - Übersicht über die verwendeten Versionen

**Tabelle 2: TAB_KON_688 Version der Schemas aus dem Namensraum des Konnektors**

| Schemas aus dem Namensraum des Konnektors „http://ws.gematik.de/conn“ | | |
|---|---|---|
| | | |
| | XSD Name | CardEvents.xsd |
| | XSD Schemaversion | 6.0.0 |
| | TargetNamespace | http://ws.gematik.de/conn/CardEvents/v6.0 |
| | | |
| | XSD Name | CardService.xsd |
| | XSD Schemaversion | 8.1.1 |
| | TargetNamespace | http://ws.gematik.de/conn/CardService/v8.1 |
| | | |
| | XSD Name | CardServiceCommon.xsd |
| | XSD Schemaversion | 2.0.0 |
| | TargetNamespace | http://ws.gematik.de/conn/CardServiceCommon/v2.0 |
| | | |
| | XSD Name | CardTerminalInfo.xsd |
| | XSD Schemaversion | 8.1.0 |
| | TargetNamespace | http://ws.gematik.de/conn/CardTerminalInfo/v8.1 |
| | | |
| | XSD Name | CardTerminalService.xsd |
| | XSD Schemaversion | 1.1.1 |
| | TargetNamespace | http://ws.gematik.de/conn/CardTerminalService/v1.1 |
| | | |
| | XSD Name | CertificateService.xsd |
| | XSD Schemaversion | 6.0.1 |
| | TargetNamespace | http://ws.gematik.de/conn/CertificateService/v6.0 |
| | | |
| | XSD Name | CertificateServiceCommon.xsd |
| | XSD Schemaversion | 2.0.0 |
| | TargetNamespace | http://ws.gematik.de/conn/CertificateServiceCommon/2.0 |
| | | |
| | XSD Name | ConnectorCommon.xsd |
| | XSD Schemaversion | 5.0.0 |
| | TargetNamespace | http://ws.gematik.de/conn/ConnectorCommon/v5.0 |
| | | |
| | XSD Name | ConnectorContext.xsd |
| | XSD Schemaversion | 2.0.0 |
| | TargetNamespace | http://ws.gematik.de/conn/ConnectorContext/v2.0 |
| | | |
| | XSD Name | EncryptionService.xsd |
| | XSD Schemaversion | 6.1.1 |
| | TargetNamespace | http://ws.gematik.de/conn/EncryptionService/v6.1 |
| | | |
| | XSD Name | EventService.xsd |
| | XSD Schemaversion | 7.2.1 |
| | TargetNamespace | http://ws.gematik.de/conn/EventService/ v7.2 |
| | | |
| | XSD Name | ServiceDirectory.xsd |
| | XSD Schemaversion | 3.1.0 |

| | | |
|---|---|---|
| | TargetNamespace | http://ws.gematik.de/conn/ServiceDirectory/v3.1 |
| | | |
| | XSD Name | SignatureService.xsd |
| | XSD Schemaversion | ~~7.4.0~~ 7.4.1 |
| | TargetNamespace | http://ws.gematik.de/conn/SignatureService/v7.4 |

# Änderung in SignatureService.xsd

```
<!-- Version History
        version: V7.4.1
                        ===========
                        *** C_6087: Elemente ShortText, CounterSignatureMarker,
DiplayableAttributes, ReferenceToSignerCertificate für die Verwendung im VerificationReport
        version: V7.4.0
                        ===========
                        *** Anpassungen für Signaturproxy statt xTV
        version: V7.3.0
                        ===========
                        *** ShortText wird optional (KOM-LE)
        version: V7.2.0
                        ===========
                        *** KeyReference wird gelöscht (P12: C_4528)
        version: V7.1.0
                        ===========
                        *** ServicePolicy durch GenerateUnderSignature ersetzt
         End of Version History--> <schema …
xmlns:SIG="http://ws.gematik.de/conn/SignatureService/v7.4" … version="7.4.1">
        …
        <element name="ShortText">
                <simpleType>
                        <restriction base="string">
                                <maxLength value="1000"/>
                        </restriction>
                </simpleType>
        </element>
        <element name="CounterSignatureMarker">
                <complexType>
                        <sequence>
                                <element name="SignatureValueReference"
maxOccurs="unbounded">
                                        <complexType>
                                                <attribute name="IdRef" type="IDREF"/>
                                        </complexType>
                                </element>
                        </sequence>
                </complexType>
        </element>
        <element name="DiplayableAttributes">
                <complexType>
```

```
                    <sequence>
                        <element name="DisplayableAttribute" maxOccurs="unbounded">
                            <complexType>
                                <sequence>
                                    <element name="Key">
                                        <simpleType>
                                            <restriction base="string">
                                                <maxLength
value="80"/>
                                            </restriction>
                                        </simpleType>
                                    </element>
                                    <element name="Value">
                                        <simpleType>
                                            <restriction base="string">
                                                <maxLength
value="8000"/>
                                            </restriction>
                                        </simpleType>
                                    </element>
                                </sequence>
                            </complexType>
                        </element>
                    </sequence>
                </complexType>
            </element>
            <element name="ReferenceToSignerCertificate" type="boolean"/>
            </schema>
```