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.

Änderungsbedarf in gemSpec_Kon

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 benutzt werden. 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

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) 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~~

Der signierte Kurztext wird in folgendem XML-Element zurückgegeben:

/VerificationReport/
IndividualReport/
SignedObjectIdentifier/
SignedProperties/
Other/
SIG:ShortText

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~~
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/
SignatureAlgorithm

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 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
./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.~~

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.