



TRUSTCENTER BUNDESNETZAGENTUR

Realisierung Übersignaturkomponente

Version 2.0

Version: 2.0
Status: Final Document
Datum: 10.03.2008
Herausgeber: T-Systems GEI GmbH
Rabinstr. 8
D-53111 Bonn
Auftraggeber: Bundesnetzagentur
Canisiusstr. 21
D-55122 Mainz

Inhaltsverzeichnis

Inhaltsverzeichnis	2
Einleitung	3
1 Gesetzliche Anforderungen	3
2 Realisierung im LDAP-Verzeichnis	3
3 Format der Übersignatur (SignaturRenewals)	3
3.1 Die Inhaltsdaten des Zeitstempels (TSTInfo)	4
3.2 Der Signaturblock (SignerInfo)	5
3.2.1 Zeitstempeldienst (SignerIdentifier)	6
3.2.2 Die signierten Attribute (SignedAttributes)	6
4 Kommentiertes Beispiel	7
5 Literaturverzeichnis	11
6 Anhang: Ergänzendes Beispiel	12

Änderungshistorie

Datum	Version	Status	Bearbeiter	Bemerkung
31.08.2007	1.0	I	Marcus Lippert	Dokument erstellt
10.03.2008	2.0	F	EG Giessmann	Finale Version

E=Dokument erstellt, I=zur internen Abstimmung, Q=QS-Geprüft, A=(externe) Abstimmung, F=Final

Einleitung

Die FlexiTrust-Installation bei der Bundesnetzagentur enthält eine Übersignaturkomponente. Diese Komponente ist in der Version 2.0 im Rahmen von FlexiTrust 3.0 Release 06550 Patch 20070911 als „Produkt für qualifizierte elektronische Signaturen“ bestätigt worden (Nachtrag Nr. 4 zur Bestätigung T-Systems.02186.TU.03.2007).

1 Gesetzliche Anforderungen

Die Übersignatur ist eine Anforderung aus der Signaturverordnung [SigV, § 17], nach der Daten mit einer qualifizierten elektronischen Signatur neu zu signieren sind, wenn diese für längere Zeit in signierter Form benötigt werden, als die für ihre Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter als geeignet beurteilt sind ([Algo]). Dieser Fall tritt 2008 für qualifizierte Zertifikate ein, die nach dem Signaturgesetz [SigG, § 7(1)] eine qualifizierte Signatur des Zertifizierungsdiensteanbieters tragen, wenn das dabei verwendete Signaturverfahren auf dem Hash-Algorithmus SHA-1 oder einem RSA-Schlüssel mit 1024 Bit beruht.

Diese Zertifikate sind vor dem Zeitpunkt des Ablaufs der Eignung der Algorithmen oder der zugehörigen Parameter mit einer neuen qualifizierten elektronischen Signatur zu versehen, diese muss nach § 17 ([SigV]), frühere Signaturen einschließen und einen qualifizierten Zeitstempel tragen.

Die hier beschriebene Komponente realisiert die gesetzlich geforderte Übersignatur in Form eines qualifizierten Zeitstempels über jedes einzelne Zertifikat. Das ist auch ausreichend, da es zum gegenwärtigen Zeitpunkt keine „früheren“ Signaturen gibt.

2 Realisierung im LDAP-Verzeichnis

In dem LDAP-Verzeichnis der Bundesnetzagentur (vgl. [VD]) sind für alle Zertifikate, die mit folgenden Signaturverfahren signiert wurden, Übersignaturen eingefügt worden.

```
x509signatureAlgorithm: 1.3.36.3.3.1.2 (RSA signature in combination  
with the cryptographic hash algorithm RIPEMD-160)
```

```
x509signatureAlgorithm: 1.2.840.113549.1.1.5 (sha-1WithRSAEncryption)
```

Alle anderen Zertifikate benötigen diese Übersignaturen noch nicht, da sie RSA-Schlüssel mit 2048 Bit in der Kombination mit den geeigneten Hash-Funktionen SHA-256 oder SHA-512 verwenden.

Die Übersignaturen (Zeitstempel) sind im LDAP-Attribut `signatureRenewals` eingetragen und über das LDAP-Protokoll abrufbar.

3 Format der Übersignatur (SignatureRenewals)

Eine einzelne Übersignatur wird als Zeitstempel nach RFC 3161 [RFC3161] realisiert. Um später weitere Übersignaturen aufnehmen zu können, werden die Übersignaturen im entsprechenden LDAP-Attribut als Folge eingetragen:

```
SignatureRenewals ::= SEQUENCE OF RenewalTimeStampToken
```

```
RenewalTimeStampToken ::= TimeStampToken
```

Dies sind die einzigen ASN.1-Definitionen in dieser Spezifikation, alle anderen Definitionen ergeben sich aus den Festlegungen des RFC 3161 und den dort angegebenen Verweisen.

Der Übersichtlichkeit halber werden in diesem Abschnitt die wichtigen Bestandteile eines Zeitstempels nach RFC 3161 noch einmal beschrieben. Für die einzelnen Datenobjekte wer-

den dazu Adressen der Form (k,n) angegeben, die man dann auch in der kompletten Beschreibung eines konkreten Datensatzes im nächsten Abschnitt wieder findet. Mit k wird dabei das Byte angegeben, nach dem der Datensatz der Länge n beginnt.

Ein RFC3161-Zeitstempel wird immer als signed-data-Objekt nach RFC 3852 gebildet:

```
SignedData ::= SEQUENCE {  
    version CMSVersion,  
    digestAlgorithms DigestAlgorithmIdentifiers,  
    encapContentInfo EncapsulatedContentInfo,  
    certificates [0] IMPLICIT CertificateSet OPTIONAL,  
    crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,  
    signerInfos SignerInfos }
```

Dieses Datenobjekt (4,768) besteht im Wesentlichen aus den Inhaltsdaten encapContentInfo und dem Signaturblock SignerInfos, die hier detailliert beschrieben werden. Die Erläuterungen zu den anderen Strukturdaten findet man in dem RFC zur „Cryptographic Message Syntax“ ([RFC3852]). Sie hier anzugeben, ist nicht erforderlich, weil die optionalen Informationen der CertificateSet und die Sperrinformationen RevocationInfoChoices in dieser Spezifikation nicht verwendet werden.

Im folgenden Abschnitt 3.1 werden zuerst die Inhaltsdaten und danach im Abschnitt 3.2 der Signaturblock beschrieben.

3.1 Die Inhaltsdaten des Zeitstempels (TSTInfo)

Im Fall eines Zeitstempels sind die Inhaltsdaten des signed-data-Objekts in Form eines TSTInfo-Datenobjekts (47,138) zu kodieren. Dazu wird ein entsprechender Typ-Bezeichner (OID) in den Inhaltsdaten angegeben. Seine einzelnen Komponenten sind im RFC 3161 festgelegt und werden hier noch einmal zitiert:

```
TSTInfo ::= SEQUENCE {  
    version                INTEGER { v1(1) },  
    policy                  TSAPolicyId,  
    messageImprint          MessageImprint,  
    -- MUST have the same value as the similar field in  
    -- TimeStampReq  
    serialNumber            INTEGER,  
    -- Time-Stamping users MUST be ready to accommodate integers  
    -- up to 160 bits.  
    genTime                 GeneralizedTime,  
    accuracy                Accuracy OPTIONAL,  
    ordering                BOOLEAN DEFAULT FALSE,  
    nonce                   INTEGER OPTIONAL,  
    -- MUST be present if the similar field was present  
    -- in TimeStampReq. In that case it MUST have the same value.  
    tsa                     [0] GeneralName OPTIONAL,  
    extensions              [1] IMPLICIT Extensions OPTIONAL }
```

Auf die Bedeutung der einzelnen Bestandteile wird im Folgenden kurz eingegangen.

Die Versionsnummer version (69,1) ist auf den Wert 1 festgelegt.

Der Verweis (72,10) auf die Zeitstempel-Richtlinien TSAPolicyId erfolgt durch einen Bezeichner (OID), der sich im CDC-Zweig der Universität Darmstadt befindet:

```
id-tudCdc OBJECT IDENTIFIER ::= {  
    iso(1) identified-organization(3) dod(6) internet(1) private(4)  
    enterprise(1) 8301 3 }
```

```
id-policies OBJECT IDENTIFIER ::= {
    id-tudCdc policies(7) }
```

```
id-sigg-signature-renewal-policy OBJECT IDENTIFIER ::= {
    id-policies sigg-signature-renewal-policy(1) }
```

Das nächste Element der Inhaltsdaten ist der `messageImprint` (84,81). Dabei handelt es sich um genau die Daten, die zum Zeitstempelservers geschickt wurden. In der Übersignatur ist dies der Hash-Wert des Zertifikats, das übersigniert werden soll. Das Zertifikat muss dazu als binäre ASN1-Struktur vorliegen. Im erläuterten Beispiel erkennt man an der Stelle (88,9) auch den Bezeichner (OID) der Hash-Funktion, die dabei verwendet wurde (SHA-512).

Bei späteren Übersignaturen wird der `messageImprint` jedoch etwas anders gebildet. Dann werden die Binärdaten des Zertifikats und aller bereits erstellten Übersignaturen zu einem Objekt zusammengefasst (Konkatenation), von dem dann der Hash-Wert berechnet wird.

Die danach folgenden Bestandteile (167,2) und (171,15) der Inhaltsdaten (`serialNumber` und `genTime`) stellen die Seriennummer des Zeitstempels, die zu seiner eindeutigen Identifizierung erforderlich ist, und die vertrauenswürdige Zeit, zu der der Zeitstempel erzeugt wurde, dar. Sie bedürfen keiner weiteren Erläuterung.

Die restlichen Komponenten sind optional und werden bei der Übersignatur nach dieser Spezifikation aus folgenden Gründen auch nicht verwendet:

- Die Genauigkeit der Zeitinformation `accuracy` wird grundsätzlich als auf die Sekunde genau angenommen. Das ist für eine Übersignatur auch ausreichend und muss deshalb nicht gesondert ausgewiesen werden.
- Wenn ein Server seine Zeitstempel strikt sequentiell erzeugt und darauf extra hingewiesen werden muss, dann soll der `ordering`-Wert gesetzt werden. Das ist aber für die Übersignatur nicht erforderlich.
- Immer wenn man bei einer Anfrage nicht über eine eigene Zeitinformation verfügt, sollte man bei der Anforderung eines Zeitstempels eine Zufallszahl (`nonce`) angeben. Damit kann man dann in der Antwort ihre Aktualität erkennen. Da ein solches Bedürfnis bei der Übersignatur nicht besteht, kann sie auch weggelassen werden.
- Schließlich kann ein Zeitstempel noch einen Hinweis auf den Aussteller (`tsa`) oder Erweiterungen (`extensions`) enthalten. Letztere sind zukünftigen Spezifikationen vorbehalten. Der Aussteller wird noch an anderen Stellen benannt, ein Bedürfnis nach einem Schutz seines Namens im Zeitstempel besteht nicht.

3.2 Der Signaturblock (SignerInfo)

Nachdem die Inhaltsdaten eines Zeitstempels (47,138) vollständig beschrieben sind, wird im Folgenden der Signaturblock (192,565) analysiert.

Er wird nach den Regeln des RFC 3852 gebildet und enthält folgende Bestandteile:

```
SignerInfo ::= SEQUENCE {
    version          CMSVersion,
    sid              SignerIdentifier,
    digestAlgorithm  DigestAlgorithmIdentifier,
    signedAttrs [0]  IMPLICIT SignedAttributes OPTIONAL,
    signatureAlgorithm SignatureAlgorithmIdentifier,
    signature        SignatureValue,
    unsignedAttrs [1] IMPLICIT UnsignedAttributes OPTIONAL }
```

Der Signaturblock enthält die Signatur (516,256) des Zeitstempels (*signature*), die nach den Regeln des RFC 3852 mit dem durch *signatureAlgorithm* eindeutig identifizierbaren Signaturalgorithmus (501,13) gebildet wird und kann außer dem Hash-Wert der Inhaltsdaten weitere Informationen enthalten. Man findet diese im Signaturblock in den so genannten signierten Attributen *signedAttrs* (285,198).

Unsignierte Attribute, wie Gegenzeichnungen oder Zertifikate, sind für die Übersignaturen nicht erforderlich und treten deshalb auch im Beispiel nicht auf.

3.2.1 Zeitstempeldienst (*SignerIdentifier*)

Zu erwähnen ist an dieser Stelle, dass zur Identifizierung des Zeitstempeldiensts (*sid*) in diesem Signaturblock zwei verschiedene Möglichkeiten zugelassen werden. Entweder kann das durch Angabe des eindeutigen ZDA-Namens und der Seriennummer des zugehörigen Zertifikats oder durch die Identifizierung des Schlüssels selbst geschehen.

```
SignerIdentifier ::= CHOICE {  
    issuerAndSerialNumber    IssuerAndSerialNumber,  
    subjectKeyIdentifier [0] SubjectKeyIdentifier }
```

Da auf die Angabe des Namens im *tsa*-Feld verzichtet wurde, wird an dieser Stelle die erste Variante mit einem so genannten *IssuerAndSerialNumber*-Objekt (199,69) benutzt.

3.2.2 Die signierten Attribute (*SignedAttributes*)

Es sind nun noch die signierten Attribute (285,198) zu beschreiben. Eigentlich ist dieses Feld optional, es muss aber verwendet werden, wenn die Inhaltsdaten (vgl. 3.1) strukturiert sind. Das ist bei dem *TSTInfo*-Datenobjekt in einem Zeitstempel der Fall und deshalb müssen die signierten Attribute vorhanden sein. Nach den Regeln des RFC 3852 gehören dazu immer das Inhaltstyp-Attribut (*ContentType*) und das Hashwert-Attribut (*MessageDigest*).

Jedes dieser beiden Attribute wird durch einen entsprechenden Bezeichner (OID) identifiziert. Auch ihre Inhalte sind festgelegt: das *ContentType*-Attribut (288,26) enthält nur den Bezeichner *id-ct-TSTInfo* und das *MessageDigest*-Attribut (316,79) nur eine reine Bytefolge, nämlich den Hash-Wert der Inhaltsdaten des Zeitstempels, also des *TSTInfo*-Datenobjekts.

Über die Anforderungen des RFC 3852 hinaus verlangt jedoch der RFC 3161 noch die Verwendung eines weiteren, die des *SigningCertificate*-Attributs (397,102).

Dieses Attribut wurde erstmals im RFC 2634 ([RFC2634]) definiert und später im RFC 5035 durch eine neue Version ergänzt ([RFC5035]). In der Übersignatur der Bundesnetzagentur wird nur das *SigningCertificateV2*-Attribut verwendet, da das ursprüngliche Format (Version 1) ausschließlich in der Kombination mit dem langfristig nicht mehr geeigneten SHA1-Algorithmus verwendet werden kann.

Auch dieses neue Attribut wird durch einen entsprechenden Bezeichner (OID) identifiziert, es enthält jedoch anstelle der einfachen Bytefolge der Version 1 strukturierte Daten.

```
ESSCertIDv2 ::= SEQUENCE {  
    hashAlgorithm    AlgorithmIdentifier DEFAULT {algorithm id-sha256},  
    certHash         Hash,  
    issuerSerial     IssuerSerial OPTIONAL }
```

Diese Informationen dienen ausschließlich zur eindeutigen Identifizierung des zur Zeitstempelsignatur gehörigen Zertifikats. Darin ist der durch den Hash-Algorithmus *hashAlgorithm* (420,13) erzeugte Hash-Wert *certHash* (435,64) enthalten. Optional könnten hier auch noch einmal der Herausgeber und die Seriennummer des Zertifikats (*issuerSerial*) für eine bessere Identifizierbarkeit angegeben werden. Dies wäre auch zweckmäßig, wenn der im

Signaturblock angegebene SignerIdentifizier nur den Schlüssel und nicht den Herausgebernamen enthält. Für die Übersignatur wird aber dort ein IssuerAndSerialNumber-Objekt benutzt, so dass hier ein zusätzliches IssuerSerial-Objekt entbehrlich ist.

4 Kommentiertes Beispiel

Im Folgenden wird der Inhalt des LDAP-Attributs „signatureRenewals“ für das Zertifikat

```
-----BEGIN CERTIFICATE-----
MIIDsDCCAxygAwIBAgICAQcwCgYGGyQDAwECBQAwPzELMAkGA1UEBhMCREUxGjAY
BgNVBAoMEUJ1bmRlc25ldHphZ2VudHVyMRQwEgYDVQDDAsxMFItQ0EgMTpQTjAe
Fw0wNjA5MDYwODM5MjJaFw0wNzEyMzEwODM2NDhaMEwxCzAJBgNVBAYTARFMRUw
EwYDVQQKDAxELVRSVVNUIEdtYkxjYkAkBgNVBAMHUQtVFJVU1RfYWtrc19DUkwT
MDJfMjAwNiAxO1BOMIGhMA0GCsGSIb3DQEBAQUAA4GPADCBiWkBgQCgy1WsY+wa
MmHTpAJ9FjqXqM26BcumBNrQUZZL16KEEZYhTdgSajgsesHhW5qGJx1gJg3JyVjg
px/uQngtKOn+nHIFDgH0FF4j7vJdQS6e4Vdau33UtdA7S/5y85f411bpEafZp23
P5V5rXoLJ/ufwhC2tx7VgN/otd6PTsmYnQIFAMAAAAGjggGwMIIBrDA0BgNVHQ8B
Af8EBAMCAQIwGAYIKwYBBQUHAQMEDDAKMAgBgQAjkyBATBkBggrBgEFBQcBAQQ+
MDwwOgYIKwYBBQUHMAGLmh0dHA6Ly9vY3NwLm5yY2EtZHMuZGU60DA4MC9vY3Nw
LW9jc3ByZXNwb25kZXIwEgYDVR0gBAswCTAHBgUrJAABATCBsQYDVR0fBIBGpMIGM
MIGjoIGgoIGdhoGabGRhcDovL2xkYXAubnJjYS1kcy5kZTozODkvQ049Q1JMLE89
QnVuZGVzbnV0emFnZW50dXIsQz1ERSxkYz1sZGFwLGRjPW5yY2EtZHMzZGM9ZGU/
Y2VydG1maWnhdGVsZXZvY2F0aW9uTG1zdDtiaw5hcnk/YmFzZT9vYmp1Y3RDbGFz
cz1jUkxEaXN0cmli dXRpb25qb21udDAAbGkrBgEEAcBtAwUEDjAMBgorBgEEAcBt
AwUBMA8GA1UdEwEB/wQFMAMBAQAwHwYDVR0jBBgwFoAUw8916sARU0UT/pd1YwBp
UwKwUwQwHQYDVR00BBYEFBpehtB7vvJfx4v/ZzmRgUoY92HdMAoGBiSkAwMBAgUA
A4GBAGq8VHU1PgWswrLOERazS7fpB+1jDqh6dWw1VjWgjbzS1S1iQUGcmg34af8
zwx0Dz3z+1K6rF0V4I1yktm4U7co0kkmVp5kgWiA7bvvdIFMGPGNoo5DFV2Uun
2yTSR+pdPGJQZDa9uj720g2IIC6i4INk0MVrc3n7AgDLgv4u
-----END CERTIFICATE-----
```

im Detail beschrieben. Der Herausgeber dieses Zertifikats ist

```
x509issuer: CN=10R-CA 1:PN, O=Bundesnetzagentur, C=DE
x509serialNumber: 263
```

Der SHA512-Hashwert dieses Zertifikats ist

```
8110cbf2 e8612d3d e706158a 8a638819 c3b6c8ca 717d8d4a 53d8112b ef3d2122
09a42f16 16818ef0 9ad90f51 18cf8573 d83d39f9 0972f1b5 b294b6db 3c9c119d
```

Das Zertifikat des Zeitstempeldienstes, das für die Übersignatur verwendet wird, ist durch den Herausgeber und seine Seriennummer

```
x509issuer: CN=12R-CA 1:PN, O=Bundesnetzagentur, C=DE
x509serialNumber: 335
```

eindeutig bestimmt:

```
-----BEGIN CERTIFICATE-----
MIIEwzCCA6ugAwIBAgICAU8wDQYJKoZIhvcNAQENBQAwPzELMAkGA1UEBhMCREUxGjAY
BgNVBAoMEUJ1bmRlc25ldHphZ2VudHVyMRQwEgYDVQDDAsxM1ItQ0EgMTpQTjAe
Fw0wNzA1MjA5MDYwODM5MjJaFw0wNzEyMzEwODM2NDhaMEwxCzAJBgNVBAYTARFMRUw
EwYDVQQKDAxELVRSVVNUIEdtYkxjYkAkBgNVBAMHUQtVFJVU1RfYWtrc19DUkwT
MDJfMjAwNiAxO1BOMIGhMA0GCsGSIb3DQEBAQUAA4GPADCBiWkBgQCgy1WsY+wa
MmHTpAJ9FjqXqM26BcumBNrQUZZL16KEEZYhTdgSajgsesHhW5qGJx1gJg3JyVjg
px/uQngtKOn+nHIFDgH0FF4j7vJdQS6e4Vdau33UtdA7S/5y85f411bpEafZp23
P5V5rXoLJ/ufwhC2tx7VgN/otd6PTsmYnQIFAMAAAAGjggGwMIIBrDA0BgNVHQ8B
Af8EBAMCAQIwGAYIKwYBBQUHAQMEDDAKMAgBgQAjkyBATBkBggrBgEFBQcBAQQ+
MDwwOgYIKwYBBQUHMAGLmh0dHA6Ly9vY3NwLm5yY2EtZHMuZGU60DA4MC9vY3Nw
LW9jc3ByZXNwb25kZXIwEgYDVR0gBAswCTAHBgUrJAABATCBsQYDVR0fBIBGpMIGM
MIGjoIGgoIGdhoGabGRhcDovL2xkYXAubnJjYS1kcy5kZTozODkvQ049Q1JMLE89
QnVuZGVzbnV0emFnZW50dXIsQz1ERSxkYz1sZGFwLGRjPW5yY2EtZHMzZGM9ZGU/
Y2VydG1maWnhdGVsZXZvY2F0aW9uTG1zdDtiaw5hcnk/YmFzZT9vYmp1Y3RDbGFz
cz1jUkxEaXN0cmli dXRpb25qb21udDAAbGkrBgEEAcBtAwUEDjAMBgorBgEEAcBt
AwUBMA8GA1UdEwEB/wQFMAMBAQAwHwYDVR0jBBgwFoAUw8916sARU0UT/pd1YwBp
UwKwUwQwHQYDVR00BBYEFBpehtB7vvJfx4v/ZzmRgUoY92HdMAoGBiSkAwMBAgUA
A4GBAGq8VHU1PgWswrLOERazS7fpB+1jDqh6dWw1VjWgjbzS1S1iQUGcmg34af8
zwx0Dz3z+1K6rF0V4I1yktm4U7co0kkmVp5kgWiA7bvvdIFMGPGNoo5DFV2Uun
2yTSR+pdPGJQZDa9uj720g2IIC6i4INk0MVrc3n7AgDLgv4u
-----END CERTIFICATE-----
```

```
dW5kZXNuZXR6YWd1bnR1cixDPURFLGRjPwXkYXAsZGM9bnJjYS1kcyxkYz1kZT9j
ZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN002JpbmFyeT9iYXN1P29iamVjdENsYXNz
PWNSTERpc3RyaWJldG1vb1BvaW50MBsGCSsGAQQBwG0DBQQMAwGCisGAQQBwG0D
BQEwDwYDVR0TAQH/BAUwAwEBADAfBgNVHSMEGDAWgBQE3p1/30NyibppSQH06Eko
3gIZbzAdBgNVHQ4EFgQUv3NAu19MindU6/Kg8HDeASqSt94wDQYJKoZIhvcNAQEN
BQADggEBAInP0q1X3JLuVtbpWzFJMq50hyiNVWPCSpWFJVL0xM0CM01e5gQVU0kT
gDT7Zs1VbeB8Sobg11civ0Gb0dS/d7CoPxx3s1fR1cbUHCECwsjJFQEn/N7+3sFs
YdETA7eDhksk2+avoJJdK23hnizmCAEtSvu3fJzQIcQhwvDYSoz3GhuLPrknVb48
UNjii3L5XPxasWrLj0hPgmBKWhLxEGZuBmoA8qHxSI5NdBpLHKDjSX8acKUr20p4
6pQ1yQENxXxhXfmYFwV/v+0GuS/LHQz8JMPCYZpuY0amMyH2SkD3Cha5uJAPEEQ
p8NJ8QEXtdvGi2JLtrWuZf+Lmc/hif0=
-----END CERTIFICATE-----
```

Damit ist auch der Name des Zeitstempeldienstes (subjectName des Zertifikats) eindeutig festgelegt, der CommonName ist in diesem Fall 12R-TSS 1:PN.

Der SHA512-Hashwert dieses Zertifikats ist

```
66f59f46 624f8bcc dba44477 d746a0d2 659d8f4e b613ce07 9c949d4d 4a6f5345
f7716145 9070ab7e ef188be3 0d5f7daf 9f3ce522 08387b22 70091c7e 41896c69
```

Die Daten des LDAP-Attributs signatureRenewals sind base64-kodiert:

```
-----BEGIN SIGNATURERENEWALS-----
MIIDBDCCAawAGCSqGSIb3DQEHAQCCAveWggLTAqEDMQ8wDQYJYIZIAWUDBAIDBQAw
gYoGCyqGSIb3DQEJEAEEoHsEeTB3AgEBBgorBgEEAcBtAwwBMFEwDQYJYIZIAWUD
BAIDBQAEQIEQy/LoYS095wYVioPjiBnDtsjKcX2NS1PYESvvPSEiCaQvFhaBjvCa
2Q9RGM+Fc9g90fkJcvG1spS22zycEZ0CAg1cGA8yMDA4MDMwNTEwMDcwN1oxggJI
MIICRAIBATBFMD8xCzAJBgNVBAYTAKRFRRowGAYDVQQKDBFCdW5kZXNuZXR6YWd1
bnR1c2EUMBIGA1UEAwMLMTJSLUNBIDE6UE4CAgFPMA0GCWCGSAF1AwQCwUAoIHV
MBoGCCsqGSIb3DQEJEAzENBgsqhkiG9w0BCRABBDBPBgkqhkiG9w0BCQQxQgRAJF5/
cp2mcBPJAVFcFvsH/yS5okSoWh0xqBHzVJDuhMyw2czv6KoTwy62J/ma2o1IGHiR
q+/J+FQI13s7PS0HQTBmBgsqhkiG9w0BCRACLzFXMFUwUzBRMA0GCWCGSAF1AwQC
AwUABEBm9Z9GYk+LzNukRHfXRqDSZZ2PTryTZgeclJ1NSm9TRfdxYUWQcKt+7xiL
4w1ffa+fPOUicDh7InAJHH5BiWxpMA0GCSqGSIb3DQEBAQUABIIBAC/JvIjRdpSK
0139T/wfScawTAoGkCVTSUpLx0j4ugiFG5UEaofkX4FhLrhwz3f7WiFAU1cX8VC
6W+E0dp4dLbkrxzmLbey7X0e8JFcvD/4UdoUZ1rQyA9MSVZ4YX//REJFWS3a0+6P
b5AddjTmcbIx0RLmEMWnVbAWBpHrtVmyN+5yUWuy9eRMjowZtPM0V++kve/kxCA
Xp0bRX1s6kxHpcP+dGQJ0KUQQPd1zSqHIU/Q0xYborKfbIiA7eFxD6ZK/kAyDaz
9sxHNnp7a86jAcynilyz9/ScrRKQyMbCGvGo78Nz6Ih0YuW5B2ZaK3PD0tKauRB9
C0deUStR15o=
-----END SIGNATURERENEWALS-----
```

Mit einem frei verfügbaren ASN1-Interpreter kann man sich diese Daten anzeigen lassen. Für die folgende Darstellung wurde dumpasn1 von Peter Gutmann in einer angepassten Version verwendet ([ASN1]). Zusätzlich wurden einige Kommentare eingefügt.

Die Struktur wird übersichtlich durch entsprechende Einrückung angezeigt. Die links stehenden Zahlenwerte *k* und *n* geben das Byte, nach dem die rechts beschriebenen Daten beginnen, und die Länge der gesamten Datenstruktur an. Diese Werte wurden als Adressen (*k,n*) auch im vorigen Abschnitt verwendet.

```
0 772: SEQUENCE { -- SignatureRenewals nach Spezifikation
4 768: . SEQUENCE { -- RenewalTimeStampToken nach Spezifikation
-- erster und einziger Zeitstempel als
-- signed-Data-Objekt
8 9: . . . OBJECT IDENTIFIER signedData (1 2 840 113549 1 7 2)
19 738: . . . [0] { -- content nach RFC 3852
23 734: . . . SEQUENCE { -- SignedData nach RFC 3852
27 1: . . . . INTEGER 3 -- CMS-Version 3
30 15: . . . . SET {
32 13: . . . . . SEQUENCE { -- Hash-Algorithmus für den Zeitstempel
34 9: . . . . . . OBJECT IDENTIFIER sha-512 (2 16 840 1 101 3 4 2 3)
45 0: . . . . . . NULL
```

```

    : . . . . . }
    : . . . . . }
47 138: . . . . . SEQUENCE {      -- EncapsulatedContentInfo nach RFC 3852
                                   -- Zeitstempelinhalts-Daten
50 11: . . . . . OBJECT IDENTIFIER tSTInfo (1 2 840 113549 1 9 16 1 4)
63 123: . . . . . [0] {
65 121: . . . . . OCTET STRING, encapsulates {
67 119: . . . . . SEQUENCE {    -- TSTInfo nach RFC 3161
69 1: . . . . . INTEGER 1      -- TSPInfo nach RFC 3161 (Version)
72 10: . . . . . OBJECT IDENTIFIER
                                   sigg-signature-renewal-policy (1 3 6 1 4 1 8301 3 7 1)
                                   -- PolicyID für signaturgesetzkonforme
                                   -- Übersignaturen
84 81: . . . . . SEQUENCE {    -- MessageImprint nach RFC 3161
86 13: . . . . . SEQUENCE {-- Hashalgorithmus für das zur Übersignatur
                                   -- vorgesehene Zertifikat 263
88 9: . . . . . OBJECT IDENTIFIER
                                   sha-512 (2 16 840 1 101 3 4 2 3)
99 0: . . . . . NULL
    : . . . . . }
101 64: . . . . . OCTET STRING -- Hash-Wert des Zertifikats 263
    : . . . . . 81 10 CB F2 E8 61 2D 3D E7 06 15 8A 8A 63 88 19
    : . . . . . C3 B6 C8 CA 71 7D 8D 4A 53 D8 11 2B EF 3D 21 22
    : . . . . . 09 A4 2F 16 16 81 8E F0 9A D9 0F 51 18 CF 85 73
    : . . . . . D8 3D 39 F9 09 72 F1 B5 B2 94 B6 DB 3C 9C 11 9D
    : . . . . . }
167 2: . . . . . INTEGER 3420 -- Seriennummer des Zeitstempels
171 15: . . . . . GeneralizedTime 05/03/2008 11:07:07GMT
                                   -- Zeitstempelzeit
    : . . . . . }
    : . . . . . }
    : . . . . . }
    : . . . . . }
188 584: . . . . . SET {      -- SignerInfos nach RFC 3852
192 580: . . . . . SEQUENCE { -- Signaturblock (SignerInfo) nach RFC 3852
196 1: . . . . . INTEGER 1   -- CMSVersion des Signaturblocks, sie muss
                                   -- nach RFC 3852 gleich 1 sein, wenn man die
                                   -- Variante mit issuerAndSerialNumber nutzt
199 69: . . . . . SEQUENCE { -- issuerAndSerialNumber-Objekt (RFC 3852)
201 63: . . . . . SEQUENCE { -- Herausgeber des TSS-Zertifikats
203 11: . . . . . SET {      -- X.500-Attribut des Herausgebers
205 9: . . . . . SEQUENCE {
207 3: . . . . . OBJECT IDENTIFIER countryName (2 5 4 6)
212 2: . . . . . PrintableString 'DE'
    : . . . . . }
    : . . . . . }
216 26: . . . . . SET {      -- X.500-Attribut des Herausgebers
218 24: . . . . . SEQUENCE {
220 3: . . . . . OBJECT IDENTIFIER organizationName (2 5 4 10)
225 17: . . . . . UTF8String 'Bundesnetzagentur'
    : . . . . . }
    : . . . . . }
244 20: . . . . . SET {      -- X.500-Attribut des Herausgebers
246 18: . . . . . SEQUENCE {
248 3: . . . . . OBJECT IDENTIFIER commonName (2 5 4 3)
253 11: . . . . . UTF8String '12R-CA 1:PN'
    : . . . . . }
    : . . . . . }
    : . . . . . }
266 2: . . . . . INTEGER 335 -- Seriennummer des TSS-Zertifikats
    : . . . . . }
270 13: . . . . . SEQUENCE { -- Hash-Algorithmus des Zeitstempels
                                   -- muss identisch zu (32,13) sein
272 9: . . . . . OBJECT IDENTIFIER sha-512 (2 16 840 1 101 3 4 2 3)

```

```

283 0: . . . . . NULL
      : . . . . . }
285 213: . . . . . [0] {      -- SignedAttributes nach RFC 3852
288 26: . . . . . SEQUENCE { -- ContentType-Attribut
290 9: . . . . . . OBJECT IDENTIFIER contentType (1 2 840 113549 1 9 3)
301 13: . . . . . . SET {      -- Inhaltsdaten des ContentType-Attributs
303 11: . . . . . . . OBJECT IDENTIFIER
      : . . . . . . . . tSTInfo (1 2 840 113549 1 9 16 1 4)
      : . . . . . . . . }
      : . . . . . . . }
      : . . . . . . }
316 79: . . . . . SEQUENCE { -- Message-Digest-Attribut
318 9: . . . . . . OBJECT IDENTIFIER
      : . . . . . . . messageDigest (1 2 840 113549 1 9 4)
329 66: . . . . . . SET {      -- Inhaltsdaten des Message-Digest-Attributs
331 64: . . . . . . . OCTET STRING
      : . . . . . . . . 24 5E 7F 72 9D A6 70 13 C9 01 51 5C 16 FB 07 FF
      : . . . . . . . . 24 B9 A2 44 A8 5A 13 B1 A8 11 F3 54 90 EE 1C CC
      : . . . . . . . . B0 D9 CC EF E8 AA 13 C3 2E B6 27 F9 80 DA 8D 48
      : . . . . . . . . 18 78 91 AB EF C9 F8 54 08 97 7B 3B 3D 2D 07 41
      : . . . . . . . . }
      : . . . . . . . }
      : . . . . . . }
397 102: . . . . . SEQUENCE { -- signingCertificateV2-Attribut
399 11: . . . . . . OBJECT IDENTIFIER
      : . . . . . . . signingCertificateV2 (1 2 840 113549 1 9 16 2 47)
412 87: . . . . . . SET {      -- Inhaltsdaten des signingCertificateV2-
      : . . . . . . . -- Attributs
414 85: . . . . . . . SEQUENCE {-- SigningCertificateV2 nach RFC 5035
416 83: . . . . . . . SEQUENCE { -- certs nach RFC 5035
418 81: . . . . . . . SEQUENCE { -- ESSCertIDv2 nach RFC 5035
420 13: . . . . . . . SEQUENCE { -- AlgorithmIdentifer für das
      : . . . . . . . . -- signingCertificateV2-Attribut
422 9: . . . . . . . . . . OBJECT IDENTIFIER
      : . . . . . . . . . . . sha-512 (2 16 840 1 101 3 4 2 3)
433 0: . . . . . . . . . . . NULL
      : . . . . . . . . . . . }
435 64: . . . . . . . . . . . OCTET STRING - Hash-Wert des Zertifikats 335
      : . . . . . . . . . . . . 66 F5 9F 46 62 4F 8B CC DB A4 44 77 D7 46 A0 D2
      : . . . . . . . . . . . . 65 9D 8F 4E B6 13 CE 07 9C 94 9D 4D 4A 6F 53 45
      : . . . . . . . . . . . . F7 71 61 45 90 70 AB 7E EF 18 8B E3 0D 5F 7D AF
      : . . . . . . . . . . . . 9F 3C E5 22 08 38 7B 22 70 09 1C 7E 41 89 6C 69
      : . . . . . . . . . . . . }
      : . . . . . . . . . . . . }
      : . . . . . . . . . . . . }
      : . . . . . . . . . . . . }
      : . . . . . . . . . . . . }
      : . . . . . . . . . . . . }
501 13: . . . . . SEQUENCE { -- SignatureAlgorithmIdentifer nach RFC 3852
503 9: . . . . . . OBJECT IDENTIFIER
      : . . . . . . . rsaEncryption (1 2 840 113549 1 1 1)
514 0: . . . . . . NULL
      : . . . . . . }
516 256: . . . . . OCTET STRING - SignatureValue nach RFC 3852
      : . . . . . . 2F C9 BC 88 EB 0E 94 8A 3B 5D FD 4F FC 1F 49 C6
      : . . . . . . B0 4C 0A 06 91 C5 53 49 4A 4B C4 E8 F8 BA 08 85
      : . . . . . . 1B 95 04 6A 87 E4 5F 81 61 2E B8 70 CE 0D DF ED
      : . . . . . . 68 9F 01 4D 5C 5F C5 42 E9 6F 84 39 DA 78 74 B6
      : . . . . . . E4 AF 1C E6 2D B7 B2 ED 73 9E F0 91 5C BC 3F F8
      : . . . . . . 51 DA 14 67 5A D0 C8 0F 4C 49 56 78 61 7F FF 44
      : . . . . . . 42 45 59 2D DA D3 EE 8F 6F 90 1D 76 34 CC 6D C6
      : . . . . . . C8 C7 44 4B 98 43 16 36 F6 C0 58 1A 47 AE D5 66
      : . . . . . . CA 7F B9 C9 65 30 CB D7 91 32 3A 16 CE D3 CC D1
      : . . . . . . 5F BE 92 F7 BF 93 10 80 5E 9D 1B 45 79 6C EA 4C
      : . . . . . . 47 A5 C3 FE 74 64 09 D0 A5 10 40 F7 75 CD 2A 87
      : . . . . . . 21 4F D0 3B 16 1B A2 B2 85 6C 88 80 ED E1 71 54

```

```
: . . . . . 3E 99 2B F9 00 C8 30 33 F6 CC 47 36 7A 7B 6B CE
: . . . . . A3 01 CC A7 8A 5C B3 F7 F4 82 AD 12 90 C8 C6 C2
: . . . . . 1A F1 A8 EF C3 73 E8 88 4E 62 E5 B9 07 66 5A 2B
: . . . . . 73 C3 D2 D2 9A B9 10 7D 0B 47 5E 51 2B 51 97 9A
: . . . . . }
: . . . . . }
: . . . . . }
: . . . . . }
: . . . . . }
```

0 warnings, 0 errors.

Das MessageDigest-Attribut (331,64) enthält die folgenden Daten

```
24 5E 7F 72 9D A6 70 13 C9 01 51 5C 16 FB 07 FF
24 B9 A2 44 A8 5A 13 B1 A8 11 F3 54 90 EE 1C CC
B0 D9 CC EF E8 AA 13 C3 2E B6 27 F9 80 DA 8D 48
18 78 91 AB EF C9 F8 54 08 97 7B 3B 3D 2D 07 41
```

Dies ist der Hash-Wert (SHA-512) der Inhaltsdaten des Zeitstempels (67,119).

Die Signatur (516,256) ist der nach PKCS#1 Version 1.5 mit dem zum TSS-Zertifikat 335 gehörigen privaten RSA-Schlüssel signierte Hash-Wert der Daten der signierten Attribute (285,198).

5 Literaturverzeichnis

- [Algo] Algorithmenkatalog: Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 22. November 2001, <http://www.bundesnetzagentur.de/>
- [ASN1] dumpasn1: ASN.1 object dumping code, Peter Gutmann, www.cs.auckland.ac.nz/~pgut001/dumpasn1.c und www.cs.auckland.ac.nz/~pgut001/dumpasn1.cfg
- [RFC2634] RFC 2634: Enhanced Security Services for S/MIME, P. Hoffman, June 1999, (Updated by RFC5035), <http://www.ietf.org/rfc/rfc2634.txt>
- [RFC3161] RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), C. Adams, P. Cain, D. Pinkas, R. Zuccherato, August 2001, <http://www.ietf.org/rfc/rfc3161.txt>
- [RFC3852] RFC 3852 Cryptographic Message Syntax (CMS), R. Housley, July 2004, (Obsoletes RFC3369) (Updated by RFC4853, RFC5083), <http://www.ietf.org/rfc/rfc3852.txt>
- [RFC5035] RFC 5035: Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility, J. Schaad, August 2007, (Updates RFC2634), <http://www.ietf.org/rfc/rfc5035.txt>
- [SigG] Gesetz über Rahmenbedingungen für elektronische Signaturen, http://bundesrecht.juris.de/bundesrecht/sigg_2001/gesamt.pdf
- [SigV] Verordnung zur elektronischen Signatur, http://bundesrecht.juris.de/sigv_2001/index.html
- [VD] Spezifikation Verzeichnisdienst Bundesnetzagentur Version 1.2, T-Systems GEI GmbH, 14.12.2007

6 Anhang: Ergänzendes Beispiel

Da in der Spezifikation der Übersignaturkomponente der Bundesnetzagentur nur die Funktion SHA-512 verwendet wird, ist bei dem kommentierten Beispiel im Abschnitt 4 die Zuordnung der Hash-Funktionen zu den entsprechenden Verfahren etwas erschwert. Um die unterschiedliche Verwendung und die Stellen zu hervorzuheben, an denen sie festgelegt wird, wird in diesem Anhang ein weiteres Beispiel eines Übersignaturen-Attributs aus dem Verzeichnis eines virtuellen Zertifizierungsdiensteanbieters angegeben und genauso wie in der obigen Spezifikation kommentiert. Dieses Beispiel einer alternativen Realisierung der Übersignatur entspricht jedoch *nicht* der Spezifikation der Bundesnetzagentur, da hier drei verschiedene Hash-Funktionen benutzt werden. Es entspricht aber den gesetzlichen Vorgaben.

Wie im obigen Beispiel werden alle Objekte durch ihre RFC-Bezeichnungen beschrieben. Der Übersichtlichkeit halber wird dies bei den „sprechenden“ Bezeichnern (OIDs) jedoch weggelassen.

```

0 1475: SEQUENCE { -- SignatureRenewals nach Spezifikation
4 702: . SEQUENCE { -- erstes RenewalTimeStampToken nach
-- Spezifikation und RFC 3161
8 9: . . . OBJECT IDENTIFIER signedData (1 2 840 113549 1 7 2)
19 687: . . . [0] { -- content nach RFC 3852
23 683: . . . . SEQUENCE { -- SignedData nach RFC 3852
27 1: . . . . . INTEGER 3 -- CMSVersion nach RFC 3852
30 15: . . . . . SET { -- DigestAlgorithmIdentifiers
32 13: . . . . . . SEQUENCE { -- Der Hash-Algorithmus für den Zeitstempel
34 9: . . . . . . . OBJECT IDENTIFIER sha-256 (2 16 840 1 101 3 4 2 1)
45 0: . . . . . . . NULL
: . . . . . . . }
: . . . . . . . }
47 164: . . . . . SEQUENCE { -- EncapsulatedContentInfo nach RFC 3852
50 11: . . . . . . OBJECT IDENTIFIER tSTInfo (1 2 840 113549 1 9 16 1 4)
63 148: . . . . . . [0] { -- eContent nach RFC 3852
66 145: . . . . . . . OCTET STRING, encapsulates {
69 142: . . . . . . . . SEQUENCE { -- TSTInfo nach RFC 3161
72 1: . . . . . . . . . INTEGER 1 -- TSP-Version
75 9: . . . . . . . . . . OBJECT IDENTIFIER
: . . . . . . . . . . . timeproof tss400 (1 3 6 1 4 1 5472 1 3)
86 81: . . . . . . . . . . SEQUENCE { -- MessageImprint nach RFC 3161 für das
-- zu schützende Zertifikat
88 13: . . . . . . . . . . . SEQUENCE {-- Der Hash-Algorithmus für das Zertifikat
90 9: . . . . . . . . . . . . OBJECT IDENTIFIER
: . . . . . . . . . . . . . sha-512 (2 16 840 1 101 3 4 2 3)
101 0: . . . . . . . . . . . . . NULL
: . . . . . . . . . . . . . }
103 64: . . . . . . . . . . . . . OCTET STRING -- SHA512-Hash-Wert des Zertifikats
: . . . . . . . . . . . . . . 8B 98 57 25 6F 24 47 BB 02 04 B3 5E 17 C4 BE 90
: . . . . . . . . . . . . . . 1A A8 78 9D E2 5E B9 27 28 90 57 D0 39 98 B5 D8
: . . . . . . . . . . . . . . 64 E0 12 CF 4F 9A 6F B6 31 31 D7 77 29 81 2B E4
: . . . . . . . . . . . . . . 9E 1C D9 2C E1 24 3D F2 F4 E0 6F 7A D8 22 08 67
: . . . . . . . . . . . . . . }
169 16: . . . . . . . . . . . . . INTEGER -- serialNumber nach RFC 3161
: . . . . . . . . . . . . . . 30 37 30 31 30 31 36 30 07 D8 02 07 0F 17 24 B8
187 15: . . . . . . . . . . . . . GeneralizedTime 07/02/2008 15:23:36 GMT
204 8: . . . . . . . . . . . . . INTEGER -- nonce nach RFC 3161
-- optionaler Zufallswert aus der Anfrage
: . . . . . . . . . . . . . . 71 92 C4 C2 F0 6B 6B 28
: . . . . . . . . . . . . . . }
: . . . . . . . . . . . . . . }
: . . . . . . . . . . . . . . }
: . . . . . . . . . . . . . . }
214 492: . . . . . SET { -- SignerInfos nach RFC 3852
218 488: . . . . . . SEQUENCE { -- einzelne SignerInfo nach RFC 3852
222 1: . . . . . . . INTEGER 1 -- CMS Version

```

```

225 69: . . . . . SEQUENCE {      -- IssuerAndSerialNumber nach RFC 3852
                                   -- SignerIdentifier nach RFC 3852
227 63: . . . . . SEQUENCE {      -- Issuer Name nach RFC 3852 (X.500)
229 11: . . . . . SET {           -- X.500-Attribut des Herausgebers
231 9: . . . . . SEQUENCE {
233 3: . . . . . OBJECT IDENTIFIER countryName (2 5 4 6)
238 2: . . . . . PrintableString 'DE'
      : . . . . . }
      : . . . . . }
242 26: . . . . . SET {           -- X.500-Attribut des Herausgebers
244 24: . . . . . SEQUENCE {
246 3: . . . . . OBJECT IDENTIFIER organizationName (2 5 4 10)
251 17: . . . . . UTF8String 'Bundesnetzagentur'
      : . . . . . }
      : . . . . . }
270 20: . . . . . SET {           -- X.500-Attribut des Herausgebers
272 18: . . . . . SEQUENCE {
274 3: . . . . . OBJECT IDENTIFIER commonName (2 5 4 3)
279 11: . . . . . UTF8String '12R-CA 1:PN'
      : . . . . . }
      : . . . . . }
292 2: . . . . . INTEGER 18193 -- CertificateSerialNumber nach X.501
                                   -- Dieses Zertifikat existiert nicht!
      : . . . . . }
296 13: . . . . . SEQUENCE {      -- Hash-Algorithmus des Zeitstempels
298 9: . . . . . OBJECT IDENTIFIER sha-256 (2 16 840 1 101 3 4 2 1)
309 0: . . . . . NULL
      : . . . . . }
311 122: . . . . . [0] {          -- SignedAttributes nach RFC 3852
313 26: . . . . . SEQUENCE {      -- ContentType-Attribut
315 9: . . . . . OBJECT IDENTIFIER contentType (1 2 840 113549 1 9 3)
326 13: . . . . . SET {          -- ContentType-Value nach RFC 3852
328 11: . . . . . OBJECT IDENTIFIER
      : . . . . . tSTInfo (1 2 840 113549 1 9 16 1 4)
      : . . . . . }
      : . . . . . }
341 43: . . . . . SEQUENCE {      -- SigningCertificate-Attribut nach RFC 5035
343 11: . . . . . OBJECT IDENTIFIER
      : . . . . . signingCertificate (1 2 840 113549 1 9 16 2 12)
356 28: . . . . . SET {          -- SigningCertificate-Value nach RFC 5035
358 26: . . . . . SEQUENCE {      -- SigningCertificate
360 24: . . . . . SEQUENCE {      -- certs nach RFC 5035
362 22: . . . . . SEQUENCE {      -- ESSCertID nach RFC 5035 (RFC 2634)
364 20: . . . . . OCTET STRING -- SHA1-Hash-Wert des
                                   -- „signierenden“ Zertifikats
      : . . . . . FE 1F 0D 6E 71 29 7E B7 BC 42 93 00 AA 18 23 51
      : . . . . . 23 DD FE DE
      : . . . . . }
      : . . . . . }
      : . . . . . }
      : . . . . . }
      : . . . . . }
386 47: . . . . . SEQUENCE {      -- MessageDigest-Attribut nach RFC 3852
388 9: . . . . . OBJECT IDENTIFIER
      : . . . . . messageDigest (1 2 840 113549 1 9 4)
399 34: . . . . . SET {          -- MessageDigest-Value nach RFC 3852
401 32: . . . . . OCTET STRING -- SHA256-Hashwert des Zeitstempels
      : . . . . . C1 FD 12 86 C4 66 47 2A 72 35 A3 B9 BD 7B 5A BC
      : . . . . . B4 C7 A7 71 BB 50 AB C5 0F 9E C4 A2 B1 C4 12 67
      : . . . . . }
      : . . . . . }
      : . . . . . }
435 13: . . . . . SEQUENCE {      -- SignatureAlgorithmIdentifier

```


NZNJnMLYAV1MWFxJQNoDvZ+SvkG2xsly4pUiF419rHfe0TI2mT2BfrWb7YReyF7g
80qf+6Q8QMEGs fv0zx1I7p8qGzNZhADBMALm3FfwhtEJoo6U3bAkyZcYfeeCLG7r
tykcjQ8NuUYVoT/Jgsd8Adux7DsRkIv+KjeQciB8FWkN41LbvAg3R107vsGXuGGJ
MfAphDoXDK/Y159rT0ZJdzUXJEVRKjkH0XAcR6b9y91CPVTKdGYg7hR8Vyt/PJhJ
qBL0Lxp1nbzajrXbxzxKMamb/S616YjtGr033UW7J3b58nNQpu8wggL9BgkqhkiG
9w0BBwKgggLuMIIC6gIBAzEPMA0GCWCGSAF1AwQCAwUAMIGKbgsqhkig9w0BCRAB
BKB7BhkwdwIBAQQYKwYBBAHAbQMhATBRMA0GCWCGSAF1AwQCAwUABEAaqHid4165
JyiqV9A5mLXyZOASz0+ab7YxMdd3KYEr5IuYVyVvJEe7AgSzXhfEvpCeHNks4SQ9
8vTgb3rYIghnAgIIFRgPMjAwODAyMTQxNTIzMzZaMYICRTCCAKECAQEwRzA/MQsw
CQYDVQQGEwJERTeAMBGA1UECgwRQnVuZGVzbnV0emFnZW50dXlxFDASBgNVBAMM
CzE0U11DQSAx01B0AgQAqrVMA0GCWCGSAF1AwQCAwUAoIGmMBoGCSqGSIsb3DQeJ
AzENBgsqhkig9w0BCRABDA3Bgsqhkig9w0BCRACLzEoMCYwJDAiBCD+Hw1ucS1+
t7xCKwCqGCNRI93+3g1ucS1+t9/t67xCKzBPBgkqhkiG9w0BCQQxQgRAo7m9e1q8
tMencbtQq8UPnsSiscQSZ/0ShsRmRypyNa05vXtavLTHp3G7UKvFD57EpyNa05vX
tavLTHp3G7UKvDA3BgkqhkiG9w0BAQowKqALBg1ghkgBZQMEAg0hFgYJKoZIhvcN
AQEIBglghkgBZQMEAg0iAwIBQASCAQDm3FfwhtEJoo6U3bAkyZcYfeeCLG7rtykc
jQ8NuUYVoT/Jgsd8Adux7DsRkIv+KjeQciB8FWkN41LbvAg3R107vsGXuGGJMfAp
hDoXDK/Y159rT0ZJdzUXJEVRKjkH0XAcR6b9y91CPVTKdGYg7hR8Vyt/PJhJqBL0
Lxp1nbzajrXbxzxKMamb/S616YjtGr033UW7J3b58nNQpu8/RB/THIS32i5qA/RJ
P6wububg+1LcUaVfxjWTSZzC2AFdTFhcSUDA72fkr5BtsbJcuKVIheJfax33jky
Npk9gX61m+2EXshe4PNKn/ukPEDDBrH79M8ZS06fKhszWYQAwtAC
-----END SIGNATURERENEWALS-----