BSI

Bundesamt für Sicherheit in der Informationstechnik

SPEZIFIKATION ZUR ENTWICKLUNG INTEROPERABLER VERFAHREN UND KOMPONENTEN NACH SIGG/SIGV

SIGNATUR-INTEROPERABILITÄTSSPEZIFIKATION SIGI

ABSCHNITT A1
ZERTIFIKATE
ANHÄNGE

STAND: 30.04.99
VERSION 4.0

Godesberger Allee 183, 53175 Bonn - Postfach 20 03 63, 53133 Bonn
Telefon: (0228) 9582 - 0, Telefax: (0228) 9582 - 400
Internet: www.bsi.bund.de

ABSCHNITT A1
ZERTIFIKATE
ANHÄNGE

Andreas Berger, Alfred Giessler, Petra Glöckner, Wolfgang Schneider
GMD – Forschungszentrum Informationstechnik GmbH
Institut für Telekooperationstechnik
Dolivostr. 15, 64293 Darmstadt

INHALTSVERZEICHNIS

ANHANG ? NAMENSKONVENTIONEN

Namen werden in Zertifikaten an sehr vielen Stellen zu unterschiedlichen Zwecken benutzt und können dabei unterschiedlichen Formaten unterworfen sein. Im Rahmen der SigI-Spezifikation spielt daher die Festlegung der Namenskonventionen eine wichtige Rolle. Die folgende Tabelle gibt eine Übersicht über das Vorkommen und die Benutzung von Namen in Zertifikaten. In der ersten Spalte werden die technischen Namen der relevanten Zertifikatskomponenten aufgeführt. Die zweite Spalte enthält Verweise auf Abschnitte dieses Dokumentes, in denen die die einzelnen Komponenten beschrieben sind. Die Bedeutung der Komponenten wird in der dritten Spalte aufgeführt.

Tabelle 50: Benutzung von Namen in Zertifikaten

KOMPONENTE	REFERENZ	BEDEUTUNG
issuer	2.3.4	Identifizierung einer Zertifizierungsstelle
subject	2.3.6	Identifizierung eines Zertifikatsinhabers
subjectAltName	2.3.9.5	Zusätzliche alternative Namen von Zertifikatsinhabern
issuerAltName	2.3.9.6	Zusätzliche alternative Namen von Zertifizierungsstellen

Anhang ?.1 Eindeutige Identifizierung von Signaturschlüsselinhabern

Konform zum Signaturgesetz soll der Name in einem Zertifikat eine Person identifizieren, d.h. der Name muß die Person praktisch eindeutig benennen. Es reicht nicht, daß eine Person über weitere Angaben im Zertifikat identifiziert werden kann, da die Bindung der digitalen Signatur an einen Namen und einer damit verbundenen Identität entscheidend ist.

Das Signaturgesetz verlangt nun eine eindeutige Identifizierung des Signaturschlüssel-Inhabers. Es wird dabei genügen, eine “praktische” Eindeutigkeit zu fordern, wie sie auch jetzt schon im Rechtsverkehr üblich ist. Adressat eines solchen Namens ist die verifizierende Person, die in die Lage versetzt werden soll, über diesen Namen Vertrauen in die geleistete Unterschrift zu haben. Daraus folgt, daß dieser Name sprechend im Sinne einer Verwendung durch Personen sein sollte und daß dieser Name diejenigen Daten enthalten sollte, die im jeweiligen Anwendungskontext als üblich erachtet werden.

Eine Regelung dieser Art schließt nicht aus, daß ein Signaturschlüssel-Inhaber verschiedene Namen führen kann. Diese sind dann in der Regel abhängig von den verschiedenen Rollen des Signaturschlüssel-Inhabers. Eine Privatperson könnte ein Zertifikat für die Verwendung zu Kommunikation mit Behörden besitzen. Dieses würde die Person als Staatsbürger identifizieren. Dieselbe Person könnte ein weiteres Zertifikat besitzen, welches sie für private Geschäftszwecke verwendet. Dieses Zertifikat könnte beispielsweise die postalische Adresse beinhalten. Daneben sind ebenfalls Zertifikate denkbar, die eine Verbindung zu einem bestimmten Arbeitgeber bestätigen und für Erklärungen im Namen des Unternehmens verwendet

wird. Ähnliches gilt für Zertifikate, die von Standesvereinigungen als Bestätigung der Mitgliedschaft ausgestellt werden.

Anhang ?.2 Pseudonymisierung von Signaturschlüsselinhabern

Da Zertifikate gemäß Signaturgesetz nur für natürliche Personen ausgestellt werden können, sind auch Zertifikate von Zertifizierungsstellen, Verzeichnisdiensten und Zeitstempeldiensten an natürliche Personen gebunden. Anstelle eines Namens kann jedes Signaturschlüssel-Zertifikat aber auch ein unverwechselbares Pseudonym enthalten, das dem Signaturschlüssel-Inhaber eindeutig zugeordnet ist. Diese Regelung gilt für Endbenutzer, den Zeitstempeldienst, den Verzeichnisdienst und für Zertifizierungsstellen gleichermaßen.

Um Pseudonyme als solche kenntlich machen zu können, wurde im Rahmen der SigI-Spezifikation der alternative Typname *nameOrPseudoym* innerhalb der Datenstruktur *PersonalData* definiert (siehe Kapitel 2.3.9.5), der entweder ein Pseudonym oder den gesetzlichen Namen aufnehmen kann. Um Pseudonyme mehrfach vergeben zu können, muß als weiteres Attribut das Teilfeld *nameDistingusher* innerhalb der Datenstruktur *PersonalData* dem Namen hinzugefügt werden. Hierdurch wird die Eindeutigkeit der Pseudonyme gewährleistet.

Anhang ?.3 Benutzung von Distinguished Names

Formal besteht der technische Name eines Signaturschlüssel-Inhabers aus einer Sequenz von Attributen. Jedes Attribut besteht aus einer lesbaren Zeichenkette zusammen mit einer expliziten Typbezeichnung. Dies ermöglicht in vielen Fällen eine leichtere automatische Verarbeitung von Bezeichnungen, beispielsweise auch bei der Darstellung der Namen von Signaturschlüssel-Inhabern durch konforme Software.

Besonders geeignet für eine Namenvergabe ist der X.500 *Distinguished Name*, da dieser bereits eine große Auswahl an Typenbezeichnungen bietet. Die verwendeten Attribute sollten nur auf die Person und ihre Rolle bezogen sein und keine weitere Angaben über die Zertifizierungsstelle oder Zertifikatsmerkmale, wie beispielsweise die Seriennummer, enthalten.

Sofern eine Zertifizierungsstelle X.500 *Distinguished Names* zur technischen Identifikation von Signaturschlüssel-Inhabern verwenden will, sollten diese aus den oben angegebenen Attributen zusammengesetzt sein. Die so konstruierten *Distinguished Names* können (müssen aber nicht) in einem X.500-Verzeichnisdienst existieren. Die primäre Verwendung *der Distinguished Names* ist die Angabe von Attributen, die eine Person für eine bestimmte Anwendung technisch eindeutig identifiziert.

Eine Zertifizierungsstelle kann auch extern vorgebene *Distinguished Names* verwenden. Dies kann beispielsweise der Fall sein, wenn eine externe Stelle (Kammer, Behörde, Unternehmen, usw.) die Rolle einer Registrierungsstelle ausführt und Zertifikate für Mitarbeiter bei einer Zertifizierungsstelle bezieht. In einem solchen Fall muß sich die Zertifizierungsstelle

davon überzeugen, daß die im angegebenen *Distinguished Name* vorgegebenen Attribute den Signaturschlüssel-Inhaber korrekt identifizieren.

Die vorgeschlagenen Typen, ihre Kurzbezeichnungen und Objektbezeichner finden sich in folgenden Tabelle.

Tabelle 51: Attribute in *Distinguished Name*-Typen

OBJEKT-BEZEICHNER	KURZ-FORM	BEDEUTUNG DES ATTRIBUTES, BEISPIELE
COUNTRY	(C)	Bezeichnung des Landes nach ISO-3166, im Rahmen des Signaturgesetzes sollten Namen immer einen Hinweis auf das Land enthalten, beispielsweise `C=DE.`
ORGANIZATION	(O)	Bezeichnung eines Unternehmens, sollte der üblichen Bezeichnung des Unternehmens im externen Sprachgebrauch entsprechen.
ORGANI-ZATIONAL UNIT	(OU)	Bezeichnung einer untergeordneten Organisationseinheit oder Abteilung innerhalb eines Unternehmens. Sollte nicht zur Unterscheidung von örtlich getrennten Niederlassungen verwendet werden.
COMMON NAME	(CN)	Die übliche Bezeichnung einer Person. Hier sollte der Name der Person so eingetragen sein, wie er im Personalausweis steht.
SURNAME	(S)	Nachname einer Person. Dieses Attribut kann zu besseren Unterscheidung bei unterschiedlichen Konventionen verwendet werden. Beispiel: `CN=Ludwig van Beethoven, S=Beethoven`
LOCALITY	(L)	Angabe eines geographischen Ortes. Hier werden beispielsweise Städte, Gemeinden oder Bundesländer beschrieben. `L=Darmstadt | L=64283 Darmstadt | L=Darmstadt 64283`
STREET ADDRESS	(ST)	Angabe einer Straße als Teil einer postalischen Adresse `ST=Dolivostr. 15 | ST=Dolivostraße 15`
TITLE	(T)	Angabe eines Titels: `T=` Prof. `| T=Dr. . | T=Graf`
SERIAL NUMBER	(SN)	Angabe einer Seriennummer, sofern zwischen verschiedenen Personen unterschieden werden muß. Kann auch zur Beschreibung eines Geburtsdatums gebraucht werden.
OBJEKT-BEZEICHNER	KURZ-FORM	BEDEUTUNG DES ATTRIBUTES, BEISPIELE
		`CN=Vorname Name, SN=7, O=Organisation, C=DE`
STATE OR PROVINCE	(SP)	Präziser zur Angabe von Bundesländern, wenn nicht *Locality* verwendet wird `SP=HESSEN`
EMAIL ADDRESS	(EMAIL)	Sofern dieses Attribut im Distinguished Name kodiert werden soll. Angabe einer electronic Mail Adresse im Format des RFC 822 (user@domain). Die Mailadresse sollte mit gleichem Inhalt auch in den alternativeName angegeben werden.
DOMAIN COMPONENT	(DC)	Definition eines *DomainName*-Teilnamens `CN=Vorname Name,` EMAIL=user@orgunit.org.de`, DC=org,`

		`DC=de` Ermöglicht die Kodierung von DNS-Namen als Teil von *Distinguished Names* [RFC 2247 98]

Anhang ?.4 Benutzung von E-Mail-Adressen

Namen im Format für E-Mail-Adressen im Internet sind global eindeutig. Sie werden vom Betreiber eines bestimmten Mailsystems vergeben. Da E-Mail-Adressen auch nicht-sprechend (beispielsweise `u1123@ccso.uiuc.edu`) sein können, sollte ein normal lesbarer Name beigefügt werden, der wiederum ein Name oder ein Pseudonym sein kann. Bei der Anzeige sollte neben der Mailadresse auch der Name angezeigt werden.

Analog zu den extern vergebenen *Distinguished Names* muß der Signaturschlüsselinhaber hier bei der Registrierung den Nachweis erbringen, daß er der legitime Benutzer dieser E-Mail Adresse ist.

E-Mail-Adressen können entweder mit einer Zuweisung `EMAIL=Attribut` im *Distinguished Name* oder als *rfc822name* in den alternativen Namen festgelegt werden. Sind beide vorhanden (etwa aus Kompatibilitätsgründen für Software, die alternative Namen in Zertifikaten nicht auswerten kann und diese Informationen immer aus dem *subject*-Feld liest), so müssen die beiden Mailadressen übereinstimmen. Der Spezifikation der Mailadresse im alternativen Namen ist – in Anlehnung an PKIX – der Vorzug zu geben.

Anhang ?.5 X.500 Directory Distinguished Names

Der X.509 Standard für Zertifikate stammt ursprünglich aus der Normierungsarbeit für den weltweiten Directorystandard X.500. Die in X.509v3 spezifizierten *Distinguished Names* sind ihrem Ursprung nach Namen innerhalb dieses Verzeichnisdienstes. Durch die Verwendung dieses Zertifikatformats auch außerhalb des X.500 Kontextes wurde diese Vorgabe obsolet. In vielen Anwendungen wird der *Distinguished Name* als eine geordnete Folge von Attributen verarbeitet und nicht für Zugriffe auf ein X.500 Verzeichnis verwendet.

Im Rahmen des SigI-Profils sollte der im Zertifikat angegebene *Distinguished Name* nicht für Zugriffe auf einen Verzeichnisdienst verwendet werden. Wenn eine Zertifizierungsstelle explizit einen X.500-Verzeichnisdienstnamen in einem Zertifikat angeben möchte, so sollte dieser in den *subjectAltName* als *directoryName* gehalten werden. Anwendungen, die diesen Namen vorfinden, können diesen als Namen innerhalb des X.500-Directory verwenden.

ANHANG ?I ERMITTLUNG VON DIENSTADRESSEN VON ZERTIFIZIERUNGSSTELLEN

Zertifizierungsstellen bieten neben dem Zertifizierungssdienst einen Verzeichnisdienst und einen Zeitstempeldienst an. Daneben können auch noch weitere Dienste angeboten werden, etwa ein Dienst für den Abruf von Sperrlisten oder weitere Prüf- und Beglaubigungsdienste.

Zur Verwendung dieser Dienste sollte die Anwendungsinfrastruktur in der Lage sein, aus dem Namen einer Zertifizierungsstelle oder aus zusätzlichen Angaben in den Zertifikaten, die technischne Adressen dieser Dienste automatisch zu ermitteln. Beispielsweise ist es bei der Prüfung einer Signatur mit Hilfe des Verzeichnisdienstes notwendig, die technische Adresse des Verzeichnisdienstes aus den Angaben im Signaturschlüsselzertifikat oder dem Zertifikat der Zertifizerungsstelle zu ermitteln, wenn diese Information nicht direkt im Zertifikat enthalten ist.

Zur Angabe von Dienstadressen existieren in PKIX private Erweiterungen für X.509 Zertifikate (*authorityInfoAccess*, siehe 2.3.9.15.1). Hier werden Dienstadressen der Zertifizierungsstelle explizit im Signatuschlüsselzertifikat des Signaturschlüssel-Inhabers abgelegt. Vorteil dieser Lösung ist die explizite Angabe der Adressen, so daß die Ermittlung der technischen Adressen auf Seite der Anwendung sehr einfach zur realisieren ist. Nachteil ist dabei, daß die Adressierung explizit erfolgt. Eine Veränderung der Adressen, beispielsweise bei der Übernahme einer Zertifizierungsstelle durch eine andere, kann nachträglich nicht ohne Sperrung und Neuerstellung aller betroffenen Zertifikate erfolgen. Ebenso ist die Einführung neuer Dienste nur schwer möglich.

Alternativ zur expliziten Angabe der Dienste und Dienstadresse im Zertifikat können die Dienstadressen aus den Namensangaben der Zertifizierungsstelle gebildet werden. Zum einen kann die Adresse eines Dienstes durch eine Kombination des üblichen Dienstnamens mit dem Namen der Zertifizierungsstelle gebildet werden. Damit ist es für Zertifizierungsstellen leicht möglich, neue Dienste anzubieten. Als zweite Möglichkeit bietet sich an, die angebotenen Dienste und deren Adressen in einem öffentlich zugänglichen Verzeichnis zu hinterlegen. Der Eintrag in diesem Verzeichnis wird durch den Namen der Zertifizierungsstelle identifiziert.

Im folgenden wird exemplarisch beschrieben, wie eine Anwendung die in den Zertifikaten angegebenen Felder zur Ermittlung von Dienstadressen verwenden kann.

In der privaten PKIX Erweiterung *authorityInfoAccess* werden Dienst und Dienstadresse explizit angegeben. Der Anwendung ist der Objektbezeichner des gewünschten Dienstes bekannt. Über diesen identifiziert sie den entsprechenden Eintrag und verwendet die dort angegebene Dienstadresse. Wenn eine Zertifizierungsstelle diese Methode verwendet, sollte sie der Entwicklung der PKIX Protokolle folgen und diese auch vollständig implementieren.

Aus dem Feld *issuerAltName* in der Ausprägung *dNSName* kann eine Anwendung die Adressen des Dienstes ermitteln, indem sie das unter [RFC 2052 96] beschriebene Verfahren anwendet. Dies ist die empfohlene Vorgehensweise, sofern eine Zertifizierungsstelle ihre Dienste über das Internet anbieten möchte.

Aus dem Feld *issuerAltName* in der Ausprägung *rfc822Name* kann eine Anwendung aus dem Teilnamen nach dem @-Zeichen auf den Domainnamen der Zertifizierungsstelle schliessen und dann ebenfalls das unter [RFC2052 96] beschriebene Verfahren anwenden. Gegebenenfalls muß der Vorgang mit einer verkürzten Version des Namens wiederholt werden, sofern keine Dienstadresse zu ermitteln war. Eine alleinige Angabe des *rfc822Name* in einem Zertifikat wird nicht empfohlen, so daß das hier kurz beschriebene Verfahren nur als letzte Möglichkeit in Betracht kommen sollte.

Über das Feld *ipAddress* könnte eine Anwendung den direkten Kontakt zu einem Dienst an dieser Adresse versuchen. Diese Vorgehensweise wird nicht empfohlen.

Über die Angaben im Feld *directoryName* kann ein Eintrag im globalen X.500 Verzeichnisdienst ermittelt werden. In diesem Eintrag kann die Anwendung aus dem Attribut für den gewünschten Dienst die Dienstadresse ermitteln. Dies ist der empfohlene Weg für Anwendungen, sofern die Zertifizierungsstelle ihre Dienste und Dienstadressen im X.500 Verzeichnisdienst vorhalten möchte.

Über die Angaben im Feld *issuer* kann ebenfalls ein Eintrag im globalen X.500 Verzeichnisdienst ermittelt werden. Analog zum oben angegeben Beispiel legt die Zertifizierungsstelle hier ihre Dienste und Dienstadressen ab. Der Verwendung des Feldes *directoryName* ist der Vorzug gegenüber dem Feld *issuer* zu geben. Aus Kompatibilitätsgründen kann es sinnvoll sein, beide Felder in den Zertifikaten anzugeben. Dann sollten über beide dort angegebenen Namen dieselben Informationen über Dienste abrufbar sein.

Bei allen diesen Methoden ist darauf zu achten, daß die Angaben der Dienste und Dienstadressen manipuliert werden können. X.509v3-konforme Anwendungen sollten vor der Verwendung der angebenen Dienste sicherstellen, daß sie mit dem gewünschten Dienst mit der gewünschten Zertifizierungsstelle verbunden sind. Ebenfalls sind Vorkehrungen zu treffen, um bei fehlerhaften oder fehlenden Angaben den Benutzer der Anwendung zu informieren.

ANHANG ?II OBJEKTBEZEICHNER

Die folgende Tabelle enthält eine Übersicht über alle Objektbezeichner der X.509v3-Zertifikate, die in diesem Dokument benutzt wurden.

Tabelle 52: Objektbezeichner

OBJEKTBEZEICHNERNUMMERN	OBJEKTBEZEICHNERNAMEN	REFERENZ
0	**itu-t**	
0 2	administration	
0 2 262	bmpt	
0 2 262 1	telekom	
0 2 262 1 10	security	
0 2 262 1 10 12	?	
0 2 262 1 10 12 0	liabiltyLimitationFlag	2.3.9.15.2
1	**iso**	
1 2	member-body	
1 2 840	data country code, USA	
1 2 840 10045	ansi-x9-62	
1 2 840 10045 1	ecdsa-with-SHA1	2.3.7
1 2 840 10045 2	id-PublicKeyType	
1 2 840 10045 2 1	id-ecPublicKey	2.7.3
1 2 840 113549	rsadsi	
1 2 840 113549 1	pkcs	
1 2 840 113549 1 1	pkcs-1	
1 2 840 113549 1 1 1	rsaEncryption	2.3.7
1 2 840 113549 1 1 5	sha1WithRSAEncryption	2.3.7
1 3	identified-organization	
1 3 6	dod	
1 3 6 1	internet	
1 3 6 1 5	security	
1 3 6 1 5 5	mechanisms	
1 3 6 1 5 5 7	pkix	
1 3 6 1 5 5 7 1	id-pe, private extensions	
1 3 6 1 5 5 7 1 1	authorityInfoAccess	2.3.9.15.1
1 3 6 1 5 5 7 2	id-qt, qualifier types	
1 3 6 1 5 5 7 2 1	cps	2.3.9.4
1 3 6 1 5 5 7 2 2	unotice	2.3.9.4
1 3 6 1 5 5 7 3	id-kp, key purposes	
1 3 6 1 5 5 7 3 8	timeStamping	2.3.9.3
1 3 6 1 5 5 7 48	id-ad, access description	
1 3 6 1 5 5 7 48 1	ocsp	2.3.9.15.1
1 3 6 1 5 5 7 48 2	caIssuers	2.3.9.15.1
1 3 14	OIW	
1 3 14 3	secsig	
1 3 14 3 2	algorithm	
1 3 14 3 2 11	rsaSignature	2.3.7
1 3 14 3 2 12	dsa	2.3.7
1 3 14 3 2 20	dsaCommon	2.3.7
1 3 14 3 2 27	dsaWithSHA1	2.1

Fortsetzung von Tabelle 52: Objektbezeichner

OBJEKTBEZEICHNERNUMMERN	OBJEKTBEZEICHNERNAMEN	REFERENZ
1 3 36	teletrust	
3	algorithm	
3	signatureAlgorithm	
1	rsaSignature	
1	rsaSignatureWithsha1	2.1
2	rsaSignatureWithripemd160	2.1
2	ecsieSign	
1	ecsieSignWithshs1	2.1
2	ecsieSignWithripemd160	2.1
4	signatureScheme	
2	sigS_ISO9796-2	
2	sigS_ISO9796-2Withrsa	2.1
3	sigS_ISO9796-2rnd	2.1
8	id-sigi	
1	id-sig-cp	
1	id-sig-cp-sigconform	2.3.9.4
2	id-sig-kp	
1	id-sig-kp-directoryService	2.3.9.3
3	id-sig-at	
1	id-sig-at-dateOfCertGen	2.3.9.15.3
2	id-sig-at-procuration	2.3.9.15.4
3	id-sig-at-admission	2.3.9.15.5
4	id-sig-at-monetaryLimit	2.3.9.15.6
5	id-sig-at-declationOfMajority	2.3.9.15.7
6	id-sig-at-iCCSN	2.3.9.15.8
7	id-sig-at-pKReference	2.3.9.15.9
8	id-sig-at-restriction	2.3.9.15.10
9	id-sigi-at-retrieveIfAllowed	A5
10	id-sigi-at-requestedCertificate	A5
11	id-sigi-at-namingAuthorities	2.3.9.15.5
12	id-sigi-at-certInDirSince	A5
13	id-sigi-at-certHash	A5
4	id-sigi-at-on	
1	id-sigi-at-on-personalData	2.3.9.5
2	**joint-iso-ccitt**	
5	ds	
4	attributeType	
3	commonName	4.3
4	surName	4.3
5	serialNumber	4.3
6	countryName	4.3
7	localityName	4.3
8	stateOrProvinceName	4.3
10	organizationName	4.3
11	organizationalUnit	4.3
12	title	4.3
15	businessCategory	4.3
17	postalCode	4.3
47	givenName	4.3

Fortsetzung von Tabelle 52: Objektbezeichner

OBJEKTBEZEICHNERNUMMERN	OBJEKTBEZEICHNERNAMEN	REFERENZ
2 5 8	algorithm	
1	encryptionAlgorithm	
1	rsa	2.3.7
29	id-ce, certificate extensions	
9	subjectDirectoryAttributes	2.3.9.11
14	subjectKeyIdentifier	2.3.9.8
15	keyUsage	2.3.9.2
16	privateKeyUsagePeriod	2.3.9.14
17	subjectAltName	2.3.9.5
18	issuerAltName	2.3.9.6
19	basicConstraints	2.3.9.1
30	nameConstraints	2.3.9.13
31	cRLDistributionPoints	2.3.9.9
32	certificatePolicies	2.3.9.4
33	policyMapping	2.3.9.10
35	authorityKeyIdentifier	2.3.9.7
36	policyConstraints	2.3.9.12
37	extKeyUsage	2.3.9.3

ANHANG ?V BEISPIELE FÜR ZERTIFIKATE

In diesem Abschnitt werden Beispiele für Zertifikate der RegTP, von Zertifizierungsstellen, der Verzeichnisdienste, der Zeitstempeldienste und von Teilnehmern gegeben. Allen diesen Beispielen liegen die ASN.1-Typdefinitionen von X.509v3-Zertifikatsformaten zugrunde. Hierauf aufbauend werden für jeden der genannten Zertifikatstypen eine ASN.1-Wertedefinition, deren zugehörige und interpretierte DER-Kodierung, sowie der komplette Hexadezimalcode angegeben. Die einzelnen Wertedefinitionen wurden willkürlich vorgegeben und für diese manuelle Eingabe wurden mit Hilfe des GMD-Tools SECUDE [SEC 98] die zugehörige DER-Kodierung und der Hexcode der Beispielzertifikate erzeugt.

Hinweise

In den folgenden Zertifikatsbeispielen wurden die Gültigkeitszeitpunkte von Secude mit dem UTCTime-Format erstellt. Sie müssen für SigI-konforme Zertifikate durch GeneralizedTime-Formate ersetzt werden. Außerdem muß noch die obligatorische *PersonalData*-Komponente im *subject alternative name*, die den gesetzlichen Namen des Zertifikatsinhabers enthält, in die Zertifikatstruktur integriert werden (siehe Abschnitt 2.3.9.5). Bei der Ausgabe des Hexadezimalcodes wurden die Tagfelder durch Fettschrift, die Längenfelder durch Normalschrift und die Wertefelder durch Kursivschrift hervorgehoben.

Anhang IV.1 Wurzelzertifikat der RegTP

Die folgende ASN.1-Wertedefinition *regtpExampleCertificate* vom Typ *Certificate* enthält ein Beispiel für ein Wurzelzertifikat der RegTP. Für dieses Zertifikat wurden die folgenden Annahmen gemacht:

Wurzelzertifikat

- Version des Zertifikates: 2, X.509v3
- Seriennummer des Zertifikates: 0
- Innerer Signaturalgorithmus: sha1WithRSASignature
- Herausgeber des Zertifikates: CN=Wurzelzertifizierungsstelle, SN=1, OU=rca, O=regtp, C=DE
- Beginn der Gültigkeit: 1.1.1998, 0 Uhr, GMT
- Ende der Gültigkeit: 1.1.2004, 0 Uhr, GMT
- Inhaber des Zertifikates: CN=Wurzelzertifizierungsstelle, SN=1, OU=rca, O=regtp, C=DE
- Öffentlicher Schlüssel: rsaEncryption mit Schlüssellänge 2048 Bit

Erweiterungen

- Identifizierung des öffentlichen Schlüssels des Zertifikaterstellers: AuthorityCertIssuer und AuthorityCertSerialNumber
- Identifizierung des öffentlichen Schlüssels des Zertifikateinhabers: KeyIdentifier als SHA1-Hashwert des Schlüssels
- Nutzungsart des Schlüssels: keyCertSign
- Zertifizierungsrichtlinien: SigI-Konformität, OID: sigconform
- Alternativer Name des Zertifikaterstellers: RFC822: rca@regtp.de; URI: http://www.regtp.de/rootcert.cer
- Zertifikaterstellung: cA=TRUE

Private Erweiterungen

- Zulassungskennung: TRUE
- Erstellungsdatum des Zertifikates: 1.1.1998, 0 Uhr, GMT
- Zulassung: Zulassung als Wurzelzertifizierungsstelle
- Äußerer Signaturalgorithmus: sha1WithRSASignature, Länge 2048 Bit

ASN.1-Wertedefinition

```
regtpExampleCertificate Certificate ::= {
   tbsCertificate {
      version           2,
      serialNumber      0
      signature {
         algorithm      { 1 3 14 3 2 29 }
         parameters     NULL },
      issuer            { "CN=Wurzelzertifizierungsstelle, SN=1, OU=rca,
                        O=regtp, C=DE" },
      validity          {
         notBefore      "980101000000Z",
         notAfter       "040101000000Z" },
      subject           { "CN=Wurzelzertifizierungsstelle, SN=1, OU=rca,
                        O=regtp, C=DE" },
      subjectPublicKeyInfo {
         algorithm {
            algorithm   { 1 2 840 113549 1 1 1 },
            parameters  NULL },
         subjectPublicKey    `...`B },
      extensions {
         authorityKeyIdentifier {
            extnId      { 2 5 29 35 },
```

```
            extnValue   `...`O },
         subjectKeyIdentifier {
            extnId      { 2 5 29 14 },
            extnValue   `...`O },
         keyUsage {
            extnId      { 2 5 29 15 },
            critical    TRUE,
            extnValue   `000001000`B } },
         certificatePolicies {
            extnId      { 2 5 29 32 },
            extnValue   { 1 3 36 8 1 1 } },
         issuerAltName {
            extnId      { 2 5 29 18 },
            extnValue   { "rca@regtp.de",
                          "http://www.regtp.de/rootcert.cer" } },
         basicConstraints {
            extnId      { 2 5 29 19 },
            critical    TRUE,
            extnValue   { cA TRUE } },
         liabilityLimitationFlag {
            extnId      { 0 2 262 1 10 12 0 },
            extnValue   TRUE },
         dateOfCertGen {
            extnId      { 1 3 36 8 3 1 },
            extnValue   "19980101000000Z" },
         atAdmission {
            extnId      { 1 3 36 8 3 3 },
            extnValue   "Zulassung als Wurzelzertifizierungsstelle" } } }
   signatureAlgorithm {
      algorithm         { 1 3 14 3 2 29 },
      parameters        NULL },
   signature            `...`B }
```

Zugehörige DER-Kodierung

```
SEQUENCE length = 1171 {
        SEQUENCE length = 895 {
            [0] (constructed) length = 3 { INTEGER 2 }
            INTEGER 0
            SEQUENCE length = 9 {
                OBJECT IDENTIFIER 1.3.14.3.2.RSASignatureWithSHA1(29)
                NULL }
            SEQUENCE length = 93 {
                SET length = 11 {
                    SEQUENCE length = 9 {
                        OBJECT IDENTIFIER 2.5.4.countryName(6)
                        PrintableString "DE" } }
                SET length = 14 {
                    SEQUENCE length = 12 {
                        OBJECT IDENTIFIER 2.5.4.organizationName(10)
                        PrintableString "regtp" } }
                SET length = 12 {
                    SEQUENCE length = 10 {
```

```
                OBJECT IDENTIFIER 2.5.4.organizationalUnitName(11)
                PrintableString "rca" } }
        SET length = 10 {
            SEQUENCE length = 8 {
                OBJECT IDENTIFIER 2.5.4.serialNumber(5)
                PrintableString "1" } }
        SET length = 36 {
            SEQUENCE length = 34 {
                OBJECT IDENTIFIER 2.5.4.commonName(3)
                PrintableString "Wurzelzertifizierungsstelle" } } }
    SEQUENCE length = 30 {
        UTCTime "980101000000Z"
        UTCTime "040101000000Z" }
    SEQUENCE length = 93 {
        SET length = 11 {
            SEQUENCE length = 9 {
                OBJECT IDENTIFIER 2.5.4.countryName(6)
                PrintableString "DE" } }
        SET length = 14 {
            SEQUENCE length = 12 {
                OBJECT IDENTIFIER 2.5.4.organizationName(10)
                PrintableString "regtp" } }
        SET length = 12 {
            SEQUENCE length = 10 {
                OBJECT IDENTIFIER 2.5.4.organizationalUnitName(11)
                PrintableString "rca" } }
        SET length = 10 {
            SEQUENCE length = 8 {
                OBJECT IDENTIFIER 2.5.4.serialNumber(5)
                PrintableString "1" } }
        SET length = 36 {
            SEQUENCE length = 34 {
                OBJECT IDENTIFIER 2.5.4.commonName(3)
                PrintableString "Wurzelzertifizierungsstelle" } } }
    SEQUENCE length = 290 {
        SEQUENCE length = 13 {
            OBJECT IDENTIFIER 1.2.840.113549.1.1.rsaEncryption(1)
            NULL }
        BIT STRING number of bits = 2160  encapsulated ASN.1 {
            SEQUENCE length = 266 {
                INTEGER 0x00f742321b8e43cab352fab0401121f142d2 ...
                INTEGER 65537 } } }
    [3] (constructed) length = 356 {
        SEQUENCE length = 352 {
            SEQUENCE length = 109 {
                OBJECT IDENTIFIER 2.5.29.authorityKeyIdentifier(35)
                OCTET STRING length = 102  encapsulated ASN.1 {
                    SEQUENCE length = 100 {
                        [1] (constructed) length = 95 {
                            [4] (constructed) length = 93 {
                                SET length = 11 {
                                    SEQUENCE length = 9 {
                                  OBJECT IDENTIFIER 2.5.4.countryName(6)
                                        PrintableString "DE" } }
                                SET length = 14 {
                                    SEQUENCE length = 12 {
                               OBJECT IDENTIFIER 2.5.4.organizationName(10)
                                        PrintableString "regtp" } }
                                SET length = 12 {
                                    SEQUENCE length = 10 {
                             OBJECT IDENTIFIER 2.5.4.organizationalUnitName(11)
                                        PrintableString "rca" } }
                                SET length = 10 {
```

```
                                        SEQUENCE length = 8 {
                                    OBJECT IDENTIFIER 2.5.4.serialNumber(5)
                                            PrintableString "1" } }
                                       SET length = 36 {
                                        SEQUENCE length = 34 {
                                     OBJECT IDENTIFIER 2.5.4.commonName(3)
                        PrintableString "Wurzelzertifizierungsstelle" } } } }
                                  [2] length = 1 content: 00" } } }
                    SEQUENCE length = 29 {
                        OBJECT IDENTIFIER 2.5.29.subjectKeyIdentifier(14)
                        OCTET STRING length = 22  encapsulated ASN.1 {
                            OCTET STRING length = 20 content:
                               720ce33b9e2311b3bce327597f3fa64142e31f62" } }
                    SEQUENCE length = 14 {
                        OBJECT IDENTIFIER 2.5.29.keyUsage(15)
                        BOOLEAN TRUE
                        OCTET STRING length = 4  encapsulated ASN.1 {
                            BIT STRING number of bits = 6 content: 04" } }
                    SEQUENCE length = 18 {
                        OBJECT IDENTIFIER 2.5.29.certificatePolicies(32)
                        OCTET STRING length = 11  encapsulated ASN.1 {
                            SEQUENCE length = 9 {
                             SEQUENCE length = 7 {
                              OBJECT IDENTIFIER 1.3.16.8.1.sigconform(1)}}}}
                    SEQUENCE length = 57 {
                        OBJECT IDENTIFIER 2.5.29.issuerAltName(18)
                        OCTET STRING length = 50  encapsulated ASN.1 {
                            SEQUENCE length = 48 {
                                [1] length = 12 content:
                                    726361407265674702e6465"
                                [6] length = 32 content:
                                    687474703a2f2f7777772e72656 ... " } } }
                    SEQUENCE length = 15 {
                        OBJECT IDENTIFIER 2.5.29.basicConstraints(19)
                        BOOLEAN TRUE
                        OCTET STRING length = 5  encapsulated ASN.1 {
                            SEQUENCE length = 3 { BOOLEAN TRUE } } }
                    SEQUENCE length = 14 {
                        OBJECT IDENTIFIER 0.2.262.1.10.12.LiabLimFlag(0)
                        OCTET STRING length = 3  encapsulated ASN.1
                            { BOOLEAN TRUE } }
                    SEQUENCE length = 26 {
                        OBJECT IDENTIFIER 1.3.36.8.3.dateOfCerGen(1)
                        OCTET STRING length = 17  encapsulated ASN.1 {
                            GeneralizedTime "19980101000000Z" }  }
                    SEQUENCE length = 52 {
                        OBJECT IDENTIFIER 1.3.36.8.3.admission(3)
                        OCTET STRING length = 43  encapsulated ASN.1 {
                            PrintableString
                            "Zulassung als Wurzelzertifizierungsstelle"}}}}}
            SEQUENCE length = 9 {
                OBJECT IDENTIFIER 1.3.14.3.2.RSASignatureWithSHA1(29)
                NULL }
            BIT STRING number of bits = 2048 content:
                678c9f72c2714173efa5a54eb8ff81e5db95 ..." }
```

Interpretierte DER-Kodierung

```
Version:                2 (X.509v3-1996)
SubjectName:            CN=Wurzelzertifizierungsstelle, SN=1, OU=rca,
                        O=regtp, C=DE
```

```
IssuerName:                CN=Wurzelzertifizierungsstelle, SN=1, OU=rca,
                           O=regtp, C=DE
SerialNumber:              0 (decimal)
Validity  -  NotBefore:    Thu Jan 01 01:00:00 1998 (980101000000Z)
NotAfter:                  Wed Jan 01 01:00:00 2004 (040101000000Z)
Public Key Fingerprint:    15C6 6449 D3D8 45E3 2119 C2FB C019 36FD
SubjectKey:                Algorithm RSA (OID 1.2.840.113549.1.1.1), NULL

Certificate extensions:
Authority Key Identifier:
    Authority Cert Issuer: DName: CN=Wurzelzertifizierungsstelle, SN=1,
                                  OU=rca, O=regtp, C=DE
    Authority Cert Serial Number: 0
Subject Key Identifier:    720C E33B 9E23 11B3 BCE3 2759 7F3F A641 42E3 1F62
Key Usage:                 (CRITICAL) keyCertSign
Certificate Policies:      sigconform (OID 1.3.36.8.1.1)
Issuer alternative names:  RFC822: rca@regtp.de
Issuer alternative names:  URI: http://www.regtp.de/rootcert.cer
Basic Constraints:         allowed to act as a CA !

Private extensions:
LiabilityLimitationFlag:   (OID 0.2.262.1.10.12.0): Boolean: TRUE
DateOfCertGen:             (OID 1.3.36.8.3.1):      GeneralTime:
                           |19980101000000Z                 |
Admission:                 (OID 1.3.36.8.3.3):      PrintableString:
                           |Zulassung als Wurzelzertifizieru|
                           |ngsstelle                       |

Signature:                 Algorithm sha1WithRSASignature
                           (OID 1.3.14.3.2.29), NULL
Certificate Fingerprint:   12:19:BB:1E:8E:C2:08:89:D2:E5:3E:AA:12:BF:D3:3D
```

Kompletter Hexadezimalcode

```
      0  30820493 30820F3F  A0030201 02020100      |0...0...........|
     10  30090605 2B0E0302  1D05003O 5D310B30      |0...+......0]1.0|
     20  09060355 04061302  44453110 300C0603      |...U....DE1.0...|
     30  55040A13 05726567  74703110 300A0603      |U....regtp1.0...|
     40  55040B13 03726361  310A3008 06035504      |U....rca1.0...U.|
     50  05130131 31243022  06035504 03131B57      |...11$0"..U....W|
     60  75727A65 6C7A6572  74696669 7A696572      |urzelzertifizier|
     70  756E6773 7374656C  6C653001E 170D3938      |ungsstelle0...98|
     80  30313031 30303030  30305A17 0D303430      |0101000000Z..040|
     90  31303130 30303030  305A305D 310B3009      |101000000Z0]1.0.|
     A0  06035504 06130244  45310E30 0C060355      |..U....DE1.0...U|
     B0  040A1305 72656774  70310C30 0A060355      |....regtp1.0...U|
     C0  040B1303 72636131  0A300806 03550405      |....rca1.0...U..|
     D0  13013131 24302206  03550403 131B5775      |..11$0"..U....Wu|
     E0  727A656C 7A657274  6966697A 69657275      |rzelzertifizieru|
     F0  6E677373 74656C6C  65308201 22300D06      |ngsstelle0.."0..|
    100  092A8648 86F70D01  01010500 03820100      |.*.H............|
    110  00308201 0A028201  0100F742 321B8E43      |.0.........B2..C|
    120  CAB352FA B0401121  F142D2C3 C11990F2      |..R..@.!.B......|
    130  853F4CA4 90CECBD2  85E84548 7F6051A4      |.?L.......EH.`Q.|
    140  F28D69CF 18082565  18CDDFD5 12A25322      |..i...%e......S"|
    150  8A1D3643 0DB10DC3  51D46C8C DFC9CDB2      |..6C....Q.l.....|
    160  0B26142F EEB936F5  9C878785 9B759991      |.&./..6......u..|
    170  A918ADB0 0F648DC4  303A987D 2DDD9B71      |.....d..0:.}-..q|
    180  DCC877CB A2E1F10A  9FFCCF16 657EC498      |..w.........e~..|
    190  21DDB131 2CEADDF1  5B986F0B 838B125E      |!..1,...[.o....^|
    1A0  ABBA2100 F198BE76  A6FAC670 C75106B5      |..!....v...p.Q..|
    1B0  CA650706 CAF9D507  895EF83F 8122A05F      |.e.......^.?."._|
```

```
1C0  609F9583 66685832  C87D28E9 F7C002A8      |`...fhX2.}(.....|
1D0  C8F017F8 83B20F14  0E0A1077 83613FC9      |...........w.a?.|
1E0  B30C1A5B A168B0E2  E7528F15 FC6A9CA9      |...[.h...R...j..|
1F0  B6B6A9DE C2F56709  0BC8AD4F EF98C02F      |......g....O.../|
200  F20B5D8C 535933C4  FB81D118 ADF147ED      |..].SY3.......G.|
210  1FD29AF8 A3609C6E  F8290203 01000103      |.....`.n.)......|
220  82016430 82016030  6D060355 1D230466      |..d0..`0m..U.#.f|
230  3064A15F A45D310B  30090603 55040613      |0d._.]1.0...U...|
240  02444531 0E300C06  03550408 13055265      |.DE1.0...U....re|
250  67747031 0C300A06  03550403 13037263      |gtp1.0...U....rc|
260  61310A30 08060355  04051301 31312430      |a1.0...U....11$0|
270  22060355 0403131B  5775727A 656C7A65      |"..U....Wurzelze|
280  72746966 697A6965  72756E67 73737465      |rtifizierungsste|
290  6C6C6582 01003001D 06035510 0E04160400    |lle...0...U.....|
2A0  14720CE3 3B9E2311  B3BCE327 597F3FA6      |.r..;.#....'Y.?.|
2B0  4142E31F 62300E06  03551D0F 01010FF04     |AB..b0...U......|
2C0  04030202 04301206  03551D20 04300B3009    |.....0...U. ..0.|
2D0  30070605 2B240801  01303906 035551D12     |0...+$...09..U..|
2E0  04323030 810C7263  61407265 6774702E      |.200..rca@regtp.|
2F0  64658620 68747470  3A2F2F77 77772E72      |de. http://www.r|
300  65677470 2E64652F  726F6F74 63657274      |egtp.de/rootcert|
310  2E636572 300F0603  551D1301 01FF0405      |.cer0...U.......|
320  30030101 FF300E06  07028206 010A0C00      |0....0..........|
330  04030101 FF301A06  052B2408 03010411      |.....0...+$.....|
340  180F3139 39383031  30313030 30303030      |..199801010000000|
350  5A30340 6052B2408  03030420 13295A75      |Z04..+$....+.)Zu|
360  6C617373 756E6720  616C7320 5775727A      |lassung als Wurz|
370  656C7A65 72746966  697A6965 72756E67      |elzertifizierung|
380  73737465 6C6C6530  09060520 0E03021D      |sstelle0...+....|
390  05000382 01010067  8C9F72C2 714173EF      |.......g..r.qAs.|
3A0  A5A54EB8 FF81E5DB  95B6B41C 41A92160      |..N.........A.!`|
3B0  C516F40D 69FE8E1E  4B16B3EB 00F7EBAA      |....i...K.......|
3C0  21BEB1D2 2D1F56E7  1F7B3F80 9D3A6CE9      |!...-.V..{?..:l.|
3D0  8A773CBB 3C593B8B  EE9C3FC3 E6E81CAC      |.w<.<Y;...?.....|
3E0  BD4A4677 4FE6D771  93E4D77F 5984AA96      |.JFwO..q....Y...|
3F0  99E1A47A 97B95300  07614BC3 0384EE8B      |...z..S..aK.....|
400  3435C303 E1195C6C  3BC7E344 6DAEE8CC      |45....\l;..Dm...|
410  C5248B96 C77494EF  34E27F3C 3E7375A2      |.$...t..4..<>su.|
420  1402525D 3F38A422  78A9EA40 1570F7D8      |..R]?8."x..@.p..|
430  2159C41C 7B58373E  D1A901D6 51C9C3CA      |!Y..{X7>....Q...|
440  1628CDBF 6DADF548  D8C065CE 6B5709C8      |.(..m..H..e.kW..|
450  5BDE435B 5276260D  F3FBB7C7 47BF16FF      |[.C[Rv&.....G...|
460  BFF06CCD D267D348  76036A97 20903D7D      |..l..g.Hv.j. .=}|
470  C420B180 D0BBA1AF  395E0456 496E8761      |. ......9^.VIn.a|
480  5169219F DD6A84DC  C14C7F5C 7A5E129D      |Qi!..j...L.\z^..|
490  494B3DD9 3924CC                           |IK=.9$.         |
```

Aus dem Offset des Hexdumps läßt sich die Speichergröße des Wurzelzertifikates als ('496'H=4*256+9*16+6=) 1174 Bytes ablesen.

Anhang IV.2 Verzeichnisdienstzertifikat

Die folgende ASN.1-Wertedefinition *directoryServiceExampleCertificate* vom Typ *Certificate* enthält ein Beispiel für ein Verzeichnisdienstzertifikat. Die Zuordnung eines Verzeichnisdienstzertifikats zu der entsprechenden Zertifizierungsstelle soll über den Namen des Zertifikatsinhabers stattfinden. Für das Verzeichnisdienstzertifikat wurden die folgenden Annahmen gemacht:

Verzeichnisdienstzertifikat

- Version des Zertifikates: 2, X.509v3
- Seriennummer des Zertifikates: 2
- Innerer Signaturalgorithmus: sha1WithRSASignature
- Herausgeber des Zertifikates: CN=Wurzelzertifizierungsstelle, SN=1, OU=rca, O=regtp, C=DE
- Beginn der Gültigkeit: 1.1.1998, 0 Uhr, GMT
- Ende der Gültigkeit: 1.1.2004, 0 Uhr, GMT
- Inhaber des Zertifikates: CN=Verzeichnisdienst, SN=1, OU=VD, O=dirser, C=DE
- Öffentlicher Schlüssel: rsaEncryption mit Schlüssellänge 1024 Bit

Erweiterungen

- Identifizierung des öffentlichen Schlüssels des Zertifikaterstellers: AuthorityCertIssuer und AuthorityCertSerialNumber
- Identifizierung des öffentlichen Schlüssels des Zertifikatinhabers: KeyIdentifier als SHA1-Hashwert des Schlüssels
- Nutzungsart des Schlüssels: non repudiation, cRLSign
- Erweiterte Schlüsselverwendung: Verzeichnisdienst, OID: directoryService
- Zertifizierungsrichtlinien: SigI-Konformität, OID: sigconform
- Alternativer Name des Zertifikatinhabers: RFC822: ds@dirserv.de
- Alternativer Name des Zertifikaterstellers: RFC822: rca@regtp.de, URI: http://www.regtp.de/rootcert.cer
- Zertifikaterstellung: cA=FALSE
- Sperrlisteninformation: URI: http://www.regtp.de/crls

Private Erweiterungen

- Zulassungskennung: TRUE

- Erstellungsdatum des Zertifikates: 1.1.1998, 0Uhr, GMT
- Zulassung: Zulassung als Verzeichnisdienststelle
- Äußerer Signaturalgorithmus: sha1WithRSASignature, Länge 2048 Bit

ASN.1-Wertedefinition

```
directoryServiceExampleCertificate       Certificate ::= {
   tbsCertificate {
    version                  2,
    serialNumber             2
    signature {
      algorithm              { 1 3 14 3 2 29 }
      parameters             NULL },
    issuer                   {"CN=Wurzelzertifizierungsstelle, SN=1, OU=rca,
                             O=regtp, C=DE" },
    validity                 {
      notBefore              "980101000000Z",
      notAfter               "040101000000Z" },
    subject                  { "CN=Verzeichnisdienst, SN=1, OU=vd, O=dirser,
                             C=DE" },
    subjectPublicKeyInfo {
      algorithm {
         algorithm           { 1 2 840 113549 1 1 1 },
         parameters          NULL },
      subjectPublicKey       `...`B },
    extensions {
      authorityKeyIdentifier {
         extnId              { 2 5 29 35 },
         extnValue           `...`O },
      subjectKeyIdentifier {
         extnId              { 2 5 29 14 },
         extnValue           `...`O },
      keyUsage {
         extnId              { 2 5 29 15 },
         critical            TRUE,
         extnValue           `010000100`B } },
      extendedKeyUsage {
         extnId              { 2 5 29 37 },
         critical            TRUE,
         extnValue           { { 1 3 36 8 2 1 } } },
      certificatePolicies {
         extnId              { 2 5 29 32 },
         extnValue           { 1 3 36 8 1 1 } },
      subjectAltName {
         extnId              { 2 5 29 18 },
         extnValue           " ds@dirserv.de" },
      issuerAltName {
         extnId              { 2 5 29 18 },
         extnValue           { "rca@regtp.de",
                             "http://www.regtp.de/rootcert.cer" } },
      basicConstraints {
         extnId              { 2 5 29 19 },
         critical            TRUE,
         extnValue           { cA FALSE } },
      cRLDistributionPoints {
         extnId              { 2 5 29 31 },
         extnValue           { "http://www.regtp.de/crls" } },
```

```
      liabilityLimitationFlag {
         extnId             { 0 2 262 1 10 12 0 },
         extnValue          TRUE },
      dateOfCertGen {
         extnId             { 1 3 36 8 3 1 },
         extnValue          "19980101000000Z" },
      admission {
         extnId             { 1 3 36 8 3 3 },
         extnValue          "Zulassung als Verzeichnisdienststelle" } } }
   signatureAlgorithm {
      algorithm             { 1 3 14 3 2 29 },
      parameters            NULL },
   signature                `...`B }
```

Zugehörige DER-Kodierung

```
SEQUENCE length = 1112 {
        SEQUENCE length = 836 {
            [0] (constructed) length = 3 { INTEGER 2 }
            INTEGER 2
            SEQUENCE length = 9 {
                OBJECT IDENTIFIER 1.3.14.3.2.RSASignatureWithSHA1(29)
                NULL }
            SEQUENCE length = 93 {
                SET length = 11 {
                    SEQUENCE length = 9 {
                        OBJECT IDENTIFIER 2.5.4.countryName(6)
                        PrintableString "DE" } }
                SET length = 14 {
                    SEQUENCE length = 12 {
                        OBJECT IDENTIFIER 2.5.4.organizationName(10)
                        PrintableString "regtp" } }
                SET length = 12 {
                    SEQUENCE length = 10 {
                        OBJECT IDENTIFIER 2.5.4.organizationalUnitName(11)
                        PrintableString "rca" } }
                SET length = 10 {
                    SEQUENCE length = 8 {
                        OBJECT IDENTIFIER 2.5.4.serialNumber(5)
                        PrintableString "1" } }
                SET length = 36 {
                    SEQUENCE length = 34 {
                        OBJECT IDENTIFIER 2.5.4.commonName(3)
                        PrintableString "Wurzelzertifizierungsstelle" } } }
            SEQUENCE length = 30 {
                UTCTime "980101000000Z"
                UTCTime "040101000000Z" }
            SEQUENCE length = 83 {
                SET length = 11 {
                    SEQUENCE length = 9 {
                        OBJECT IDENTIFIER 2.5.4.countryName(6)
                        PrintableString "DE" } }
                SET length = 15 {
                    SEQUENCE length = 13 {
                        OBJECT 2.5.4.organizationName(10)
                        PrintableString "dirser" } }
                SET length = 11 {
                    SEQUENCE length = 9 {
                        OBJECT IDENTIFIER 2.5.4.organizationalUnitName(11)
                        PrintableString "vd" } }
                SET length = 10 {
```

```
            SEQUENCE length = 8 {
                OBJECT IDENTIFIER 2.5.4.serialNumber(5)
                PrintableString "1" } }
        SET length = 26 {
            SEQUENCE length = 24 {
                OBJECT IDENTIFIER 2.5.4.commonName(3)
                PrintableString "Verzeichnisdienst" } } }
    SEQUENCE length = 159 {
        SEQUENCE length = 13 {
            OBJECT IDENTIFIER 1.2.840.113549.1.1.rsaEncryption(1)
            NULL }
        BIT STRING number of bits = 1120  encapsulated ASN.1 {
            SEQUENCE length = 137 {
                INTEGER 0x00fd142256ec56a2f2910a88c96ca284360 ...
                INTEGER 65537 } } }
    [3] (constructed) length = 439 {
        SEQUENCE length = 435 {
            SEQUENCE length = 109 {
                OBJECT IDENTIFIER 2.5.29.authorityKeyIdentifier(35)
                OCTET STRING length = 102  encapsulated ASN.1 {
                    SEQUENCE length = 100 {
                        [1] (constructed) length = 95 {
                            [4] (constructed) length = 93 {
                                SET length = 11 {
                                    SEQUENCE length = 9 {
                                  OBJECT IDENTIFIER 2.5.4.countryName(6)
                                        PrintableString "DE" } }
                                SET length = 14 {
                                    SEQUENCE length = 12 {
                               OBJECT IDENTIFIER 2.5.4.organizationName(10)
                                        PrintableString "regtp" } }
                                SET length = 12 {
                                    SEQUENCE length = 10 {
                              OBJECT IDENTIFIER 2.5.4.organizationalUnitNam
                                        PrintableString "rca" } }
                                SET length = 10 {
                                    SEQUENCE length = 8 {
                                 OBJECT IDENTIFIER 2.5.4.serialNumber(5)
                                        PrintableString "1" } }
                                SET length = 36 {
                                    SEQUENCE length = 34 {
                                  OBJECT IDENTIFIER 2.5.4.commonName(3)
                       PrintableString "Wurzelzertifizierungsstelle" } } } }
                                [2] length = 1 content: 00" } } }
                SEQUENCE length = 29 {
                    OBJECT IDENTIFIER 2.5.29.subjectKeyIdentifier(14)
                    OCTET STRING length = 22  encapsulated ASN.1 {
                        OCTET STRING length = 20 content:
                            fa8c669e895ae1927619bd649f06c23f7559ad4d" }}
                SEQUENCE length = 14 {
                    OBJECT IDENTIFIER 2.5.29.keyUsage(15)
                    BOOLEAN TRUE
                    OCTET STRING length = 4  encapsulated ASN.1 {
                        BIT STRING number of bits = 7 content: 42" } }
                SEQUENCE length = 19 {
                    OBJECT IDENTIFIER 2.5.29.extKeyUsage(37)
                    BOOLEAN TRUE
                    OCTET STRING length = 9  encapsulated ASN.1 {
                        SEQUENCE length = 7 {
                           OBJECT IDENTIFIER 1.3.36.8.2.dirService(1)}}}
                SEQUENCE length = 18 {
                    OBJECT IDENTIFIER 2.5.29.certificatePolicies(32)
                    OCTET STRING length = 11  encapsulated ASN.1 {
```

```
                        SEQUENCE length = 9 {
                           SEQUENCE length = 7 {
                             OBJECT IDENTIFIER 1.3.36.8.1.sigconf(1)}}}}
                SEQUENCE length = 24 {
                    OBJECT IDENTIFIER 2.5.29.subjectAltName(17)
                    OCTET STRING length = 17  encapsulated ASN.1 {
                        SEQUENCE length = 15 {
                            [1] length = 13 content:
                                647340646972736572762e6465" } } }
                SEQUENCE length = 57 {
                    OBJECT IDENTIFIER 2.5.29.issuerAltName(18)
                    OCTET STRING length = 50  encapsulated ASN.1 {
                        SEQUENCE length = 48 {
                            [1] length = 12 content:
                                726361407265677 4702e6465"
                            [6] length = 32 content:
                                687474703a2f2f7777772e726567747..."} } }
                SEQUENCE length = 12 {
                    OBJECT IDENTIFIER 2.5.29.basicConstraints(19)
                    BOOLEAN TRUE
                    OCTET STRING length = 2  encapsulated ASN.1 {
                        SEQUENCE length = 0 { } } }
                SEQUENCE length = 41 {
                    OBJECT IDENTIFIER 2.5.29.cRLDistributionPoints(31)
                    OCTET STRING length = 34  encapsulated ASN.1 {
                        SEQUENCE length = 32 {
                            SEQUENCE length = 30 {
                                [0] (constructed) length = 28 {
                                    [0] (constructed) length = 26 {
                                        [6] length = 24 content:
             687474703a2f2f7777772e72656774702e64652f63726c73"}}}}}}
                SEQUENCE length = 14 {
                    OBJECT IDENTIFIER 0.2.262.1.10.12.liabLimFlag(0)
                    OCTET STRING length = 3  encapsulated ASN.1 {
                        BOOLEAN TRUE } }
                SEQUENCE length = 26 {
                    OBJECT IDENTIFIER 1.3.36.8.3.dateOfCertGen(1)
                    OCTET STRING length = 17  encapsulated ASN.1 {
                        GeneralizedTime "19980101000000Z" } }
                SEQUENCE length = 48 {
                    OBJECT IDENTIFIER 1.3.36.8.3.admission(3)
                    OCTET STRING length = 39  encapsulated ASN.1 {
                        PrintableString
                           "Zulassung als Verzeichnisdienststelle" }}}}}
        SEQUENCE length = 9 {
            OBJECT IDENTIFIER 1.3.14.3.2.RSASignatureWithSHA1(29)
            NULL }
        BIT STRING number of bits = 2048 content:
            92e90712a23797b9ce961d5062bb5d2106ed2d89eed256a78bf51e ..." }
```

Interpretierte DER-Kodierung

```
Version:                    2 (X.509v3-1996)
SubjectName:                CN=Verzeichnisdienst, SN=1, OU=vd, O=dirser, C=DE
IssuerName:                 CN=Wurzelzertifizierungsstelle, SN=1, OU=rca,
O=regtp, C=DE
SerialNumber:               2 (decimal)
Validity  -  NotBefore:     Thu Jan 01 01:00:00 1998 (980101000000Z)
             NotAfter:      Thu Jan 01 01:00:00 2004 (040101000000Z)
Public Key Fingerprint:     3D89 5C3D 57A1 B505 DDB6 3421 7157 BCC2
SubjectKey:                 Algorithm RSA (OID 1.2.840.113549.1.1.1), NULL
```

```
Certificate extensions:
Authority Key Identifier:
    Authority Cert Issuer: DName: CN=Wurzelzertifizierungsstelle, SN=1,
                                  OU=rca, O=regtp, C=DE
    Authority Cert Serial  Number: 0
Subject Key Identifier:    FA8C 669E 895A E192 7619 BD64 9F06 C23F 7559 AD4D
Key Usage:                 (CRITICAL) nonRepudiation, cRLSign
Extended Key Usage:        kp-directoryService (OID 1.3.36.8.2.1)
Certificate Policies:      sigconform (OID 1.3.36.8.1.1)
Subject alternative names: RFC822: ds@dirserv.de
Issuer alternative names:  RFC822: rca@regtp.de
Issuer alternative names:  URI: http://www.regtp.de/rootcert.cer
Basic Constraints:         NOT allowed to act as a CA !
CRL Distribution Points:
CRL Distribution Point Names: URI: http://www.regtp.de/crls

Private extensions:
LiabilityLimitationFlag:   (OID 0.2.262.1.10.12.0): Boolean: TRUE
DateOfCertGen:             (OID 1.3.36.8.3.1):      GeneralTime:
                                 |19980101000000Z                |
Admission:                 (OID 1.3.36.8.3.3):      PrintableString:
                           |Zulassung als Verzeichnisdiensts|
                           |telle                           |

Signature:          Algorithm sha1WithRSASignature (OID 1.3.14.3.2.29), NULL
Certificate Fingerprint:   9F:11:EF:CF:FD:E3:43:EE:73:CE:96:D8:20:D7:9E:DA
```

Kompletter Hexadezimalcode

```
   0  30820458 30820344  A0030201 02020102      |0..X0..D........|
  10  30090605 2B0E0302  1D05003O 5D310B30      |0...+......0]1.0|
  20  09060355 04061302  44453110 300C0603      |...U....DE1.0...|
  30  55040A13 05726567  74703100 300A0603      |U....regtp1.0...|
  40  55040B13 03726361  31300800 06035504      |U....rca1.0...U.|
  50  05130131 31243022  06035504 03131B57      |...11$0"..U....W|
  60  75727A65 6C7A6572  74696669 7A696572      |urzelzertifizier|
  70  756E6773 7374656C  6C653001E 170D3938      |ungsstelle0...98|
  80  30313031 30303030  30305A17 0D303430      |0101000000Z..040|
  90  31303130 30303030  305A3053 310B3009      |101000000Z0S1.0.|
  A0  06035504 06130244  45310F30 0D060355      |..U....DE1.0...U|
  B0  040A1306 64697273  65723100 30090603      |....dirser1.0...|
  C0  55040B13 02766431  0A300806 03550405      |U....vd1.0...U..|
  D0  13013131 1A301806  03550403 13115665      |..11.0...U....Ve|
  E0  727A6569 63686E69  73646965 6E737430      |rzeichnisdienst0|
  F0  819F300D 06092A86  4886F70D 01010105      |..0...*.H.......|
 100  00038180 00308189  02818100 FD142256      |.....0........"V|
 110  EC56A2F2 910A88C9  6CA28436 07B05A09      |.V......l..6..Z.|
 120  E7A4C374 135727C3  80C8370F 4961D035      |...t.W'...7.Ia.5|
 130  E54AE317 2C991FAC  9604C6D4 95710A40      |.J..,........q.@|
 140  E1F55662 E60E96D9  328E12BA F29263AB      |..Vb....2.....c.|
 150  506BB899 DEE8AC1C  C0016F16 F16CDBC8      |Pk........o..l..|
 160  886909A0 8859D1AC  BB6543ED A9782F0C      |.i...Y...eC..x/.|
 170  FBE84BE9 E4D7D0AD  7396AF5B 3EF690EA      |..K.....s..[>...|
 180  25AEB9C1 A44DC1D3  C6B8D049 02030100      |%....M.....I....|
 190  01A38201 B7308201  B3306D06 03551D23      |.....0...0m..U.#|
 1A0  04663064 A15FA45D  310B3009 06035504      |.f0d._.]1.0...U.|
 1B0  06130244 45310E30  0C060355 040A1305      |...DE1.0...U....|
 1C0  72656774 70310C30  0A060355 040B1303      |regtp1.0...U....|
```

```
1D0  72636131 0A300806  03550405 13013131  |rca1.0...U....11|
1E0  24302206 03550403  131B5775 727A656C  |$0"..U....Wurzel|
1F0  7A657274 6966697A  69657275 6E677373  |zertifizierungss|
200  74656C6C 65820100  301D0603 551D0E04  |telle...0...U...|
210  1604 14FA 8C669E89  5AE19276 19BD649F  |.....f..Z..v..d.|
220  06C23F75 59AD4D30  0E060355 1D0F0101  |..?uY.M0...U....|
230  FF040403 02014230  13060355 1D250101  |.......0...U.%..|
240  FF040930 07060528  24080201 30120603  |...0...+$...0...|
250  551D2004 0B300930  07060528 24080101  |U. ..0.0...+$...|
260  30180603 551D1104  11300F81 0D647340  |0...U....0...ds@|
270  64697273 6572762E  64653039 06035510  |dirserv.de09..U.|
280  12043230 30810C72  63614072 65677470  |..200..rca@regtp|
290  2E646586 20687474  703A2F2F 7777772E  |.de. http://www.|
2A0  72656774 702E6465  2F726F6F 74636572  |regtp.de/rootcer|
2B0  742E6365 72300C06  03551D13 01010FF04  |t.cer0...U......|
2C0  02300030 29060355  1D1F0422 30203018  |.0.0)..U..."0 0.|
2D0  A01CA01A 86186874  74703A2F 2F777777  |......http://www|
2E0  2E726567 74702E64  652F6372 6C73300E  |.regtp.de/crls0.|
2F0  06070282 06010A0C  00040301 01FF301A  |..............0.|
300  06052B24 08030104  11180F31 39393830  |..+$.......19980|
310  31303130 30303030  305A3030 06052B24  |101000000Z00..+$|
320  08030304 27132550  756C6173 73756E67  |....'.%Zulassung|
330  20616C73 20566572  7A656963 686E6973  | als Verzeichnis|
340  6469656E 73747374  656C6C65 30090605  |dienststelle0...|
350  2B0E0302 1D050003  82010100 92E90712  |+...............|
360  A23797B9 CE961D50  62BB5D21 06ED2D89  |.7.....Pb.]!..-.|
370  EED256A7 8BF51EC9  3D9ED612 82258814  |..V.....=....%..|
380  650667FE 309FA40F  41CFEE86 61A14CC5  |e.g.0...A...a.L.|
390  E1E3AD61 2A29BFE9  FCD656F7 7577766A  |...a*)....V.uwvj|
3A0  BED9680E B3395C77  D1D63BE3 225E7C87  |..h..9\w..;."^|.|
3B0  EDD79344 00A99BA2  D05D5397 254F1CE8  |...D.....]S.%O..|
3C0  F5EC7F6E 6C0ABB35  95CDF48D 550273DC  |...nl..5....U.s.|
3D0  CFACA2E8 C6A73F40  C5CD9589 9AFFDA3F  |......?@.......?|
3E0  43546D95 2172D1A5  04FF5AFD 1BAB0DF0  |CTm.!r....Z.....|
3F0  1910E6A5 083C3526  BAC26DF9 EB2675FA  |.....<5&..m..&u.|
400  98F6F585 F8EC1AF5  E8FECA5F 92A18F1B  |..........._....|
410  CE5BF409 A7533678  7DE34F2F 84FD5FB3  |.[...S6x}.O/.._.|
420  4E8ABDAB 8BA92604  D02A26E5 03006EF3  |N.....&..*&...n.|
430  31249EB3 916B600B  2CEE30C3 3A1540AD  |1$...k`.,.0.:.@.|
440  1A6F271E 60B4F8BF  518E3663 ABC5E9B8  |.o'.`...Q.6c....|
450  2C669AED 39D06E45  B4F36688           |,f..9.nE..f.    |
```

Aus dem Offset des Hexdumps läßt sich die Speichergröße des Verzeichnisdienstzertifikates als ('45B'H= 4*256+5*16+11=) 1115 Bytes ablesen.

Anhang IV.3 Zeitstempeldienstzertifikat

Die folgende ASN.1-Wertedefinition *timeStampingServiceExampleCertificate* vom Typ *Certificate* enthält ein Beispiel für ein Zeitstempeldienstzertifikat. Die Zuordnung eines Zeitstempeldienstzertifikats zu der entsprechenden Zertifizierungsstelle soll über den Namen des Zertifikatsinhabers stattfinden. Für das Zeitstempeldienstzertifikat wurden die folgenden Annahmen gemacht:

Zeitstempeldienstzertifikat

- Version des Zertifikates: 2, X.509v3
- Seriennummer des Zertifikates: 1
- Innerer Signaturalgorithmus: sha1WithRSASignature
- Herausgeber des Zertifikates: CN=Wurzelzertifizierungsstelle, SN=1, OU=rca, O=regtp, C=DE
- Beginn der Gültigkeit: 1.1.1998, 0 Uhr, GMT
- Ende der Gültigkeit: 1.1.2004, 0 Uhr, GMT
- Inhaber des Zertifikates: CN=Zeitstempeldienst, SN=1, OU=zsd O=time, C=DE
- Öffentlicher Schlüssel: rsaEncryption mit Schlüssellänge 1024 Bit

Erweiterungen

- Identifizierung des öffentlichen Schlüssels des Zertifikaterstellers: AuthorityCertIssuer und AuthorityCertSerialNumber
- Identifizierung des öffentlichen Schlüssels des Zertifikatinhabers: KeyIdentifier als SHA1-Hashwert des Schlüssels
- Nutzungsart des Schlüssels: non repudiation
- Erweiterte Schlüsselverwendung: Zeitstempeldienst, OID: timeStamping
- Zertifizierungsrichtlinien: SigI-Konformität, OID: sigconform
- Alternativer Name des Zertifikatinhabers: RFC822: ts@timeserv.de
- Alternativer Name des Zertifikaterstellers: RFC822: rca@regtp.de; URI: http://www.regtp.de/rootcert.cer
- Zertifikaterstellung: cA=FALSE
- Sperrlisteninformation: URI: http://www.regtp.de/crls

Private Erweiterungen

- Zulassungskennung: TRUE

- Erstellungsdatum des Zertifikates: 1.1.1998, 0 Uhr, GMT
- Zulassung: Zulassung als Zeitstempeldienststelle
- Äußerer Signaturalgorithmus: sha1WithRSASignature, Länge 2048 Bit

ASN.1-Wertedefinition

```
timeStampingServiceExampleCertificate   Certificate ::= {
   tbsCertificate {
    version                  2,
    serialNumber             1
    signature {
      algorithm              { 1 3 14 3 2 29 }
      parameters             NULL },
    issuer                   { "CN=Wurzelzertifizierungsstelle, SN=1,
                             OU=rca, O=regtp, C=DE" },
    validity                 {
      notBefore              "980101000000Z",
      notAfter               "040101000000Z" },
    subject                  { "CN=Zeitstempeldienst, SN=1, OU=zsd, O=time,
                             C=DE" },
    subjectPublicKeyInfo {
      algorithm {
         algorithm           { 1 2 840 113549 },
         parameters          1024 },
      subjectPublicKey       `...`B },
    extensions {
      authorityKeyIdentifier {
            extnId           { 2 5 29 35 },
            extnValue        `...`O },
      subjectKeyIdentifier {
            extnId           { 2 5 29 14 },
            extnValue        `...`O },
      keyUsage {
            extnId           { 2 5 29 15 },
            critical         TRUE,
            extnValue        `010000000`B } },
      extendedKeyUsage {
            extnId           { 2 5 29 37 },
            critical         TRUE,
            extnValue        { { 1 3 6 1 5 5 8 3 8 } } },
      certificatePolicies {
            extnId           { 2 5 29 32 },
            extnValue        { 1 3 36 8 1 1 } },
      subjectAltName {
            extnId           { 2 5 29 18 },
            extnValue        "ts@timeserv.de" },
      issuerAltName {
            extnId           { 2 5 29 18 },
            extnValue        {"rca@regtp.de",
                             "http://www.regtp.de/rootcert.cer" } },
      basicConstraints {
            extnId           { 2 5 29 19 },
            critical         TRUE,
            extnValue        { cA FALSE } },
      cRLDistributionPoints {
            extnId           { 2 5 29 31 },
            extnValue        { "http://www.regtp.de/crls" } },
```

```
      liabilityLimitationFlag {
            extnId          { 0 2 262 1 10 12 0 },
            extnValue       TRUE },
      dateOfCertGen {
            extnId          { 1 3 36 8 3 1 },
            extnValue       "19980101000000Z" },
      atAdmission {
            extnId          { 1 3 36 8 3 3 },
            extnValue       "Zulassung als Zeitstempeldienststelle" } } }
   signatureAlgorithm {
     algorithm              { 1 3 14 3 2 29 },
     parameters             NULL },
   signature                `...`B }
```

Zugehörige DER-Kodierung

```
SEQUENCE length = 1115 {
        SEQUENCE length = 839 {
            [0] (constructed) length = 3 { INTEGER 2 }
            INTEGER 1
            SEQUENCE length = 9 {
                OBJECT IDENTIFIER 1.3.14.3.2.RSASignatureWithSHA1(29)
                NULL }
            SEQUENCE length = 93 {
                SET length = 11 {
                    SEQUENCE length = 9 {
                        OBJECT IDENTIFIER 2.5.4.countryName(6)
                        PrintableString "DE" } }
                SET length = 14 {
                    SEQUENCE length = 12 {
                        OBJECT IDENTIFIER 2.5.4.organizationName(10)
                        PrintableString "regtp" } }
                SET length = 12 {
                    SEQUENCE length = 10 {
                        OBJECT IDENTIFIER 2.5.4.organizationalUnitName(11)
                        PrintableString "rca" } }
                SET length = 10 {
                    SEQUENCE length = 8 {
                        OBJECT IDENTIFIER 2.5.4.serialNumber(5)
                        PrintableString "1" } }
                SET length = 36 {
                    SEQUENCE length = 34 {
                        OBJECT IDENTIFIER 2.5.4.commonName(3)
                        PrintableString "Wurzelzertifizierungsstelle" } } }
            SEQUENCE length = 30 {
                UTCTime "980101000000Z"
                UTCTime "040101000000Z" }
            SEQUENCE length = 82 {
                SET length = 11 {
                    SEQUENCE length = 9 {
                        OBJECT IDENTIFIER 2.5.4.countryName(6)
                        PrintableString "DE" } }
                SET length = 13 {
                    SEQUENCE length = 11 {
                        OBJECT IDENTIFIER 2.5.4.organizationName(10)
                        PrintableString "time" } }
                SET length = 12 {
                    SEQUENCE length = 10 {
                        OBJECT IDENTIFIER 2.5.4.organizationalUnitName(11)
                        PrintableString "zsd" }
                }
```

```
        SET length = 10 {
            SEQUENCE length = 8 {
                OBJECT IDENTIFIER 2.5.4.serialNumber(5)
                PrintableString "1" } }
        SET length = 26 {
            SEQUENCE length = 24 {
                OBJECT IDENTIFIER 2.5.4.commonName(3)
                PrintableString "Zeitstempeldienst" } } }
    SEQUENCE length = 159 {
        SEQUENCE length = 13 {
            OBJECT IDENTIFIER 1.2.840.113549.1.1.rsaEncryption(1)
            NULL }
        BIT STRING number of bits = 1120  encapsulated ASN.1 {
            SEQUENCE length = 137 {
                INTEGER 0x00fd2b4ccd036031981c67dedd99bedfde ...
                INTEGER 65537 } } }
    [3] (constructed) length = 443 {
        SEQUENCE length = 439 {
            SEQUENCE length = 109 {
                OBJECT IDENTIFIER 2.5.29.authorityKeyIdentifier(35)
                OCTET STRING length = 102  encapsulated ASN.1 {
                    SEQUENCE length = 100 {
                        [1] (constructed) length = 95 {
                            [4] (constructed) length = 93 {
                                SET length = 11 {
                                    SEQUENCE length = 9 {
                                  OBJECT IDENTIFIER 2.5.4.countryName(6)
                                            PrintableString "DE" } }
                                SET length = 14 {
                                    SEQUENCE length = 12 {
                             OBJECT IDENTIFIER 2.5.4.organizationName(10)
                                            PrintableString "regtp" } }
                                SET length = 12 {
                                    SEQUENCE length = 10 {
                           OBJECT IDENTIFIER 2.5.4.organizationalUnitName(11)
                                            PrintableString "rca" } }
                                SET length = 10 {
                                    SEQUENCE length = 8 {
                                 OBJECT IDENTIFIER 2.5.4.serialNumber(5)
                                            PrintableString "1" } }
                                SET length = 36 {
                                    SEQUENCE length = 34 {
                                  OBJECT IDENTIFIER 2.5.4.commonName(3)
                       PrintableString "Wurzelzertifizierungsstelle"}}}}
                                [2] length = 1 content: 00" } } }
                SEQUENCE length = 29 {
                    OBJECT IDENTIFIER 2.5.29.subjectKeyIdentifier(14)
                    OCTET STRING length = 22  encapsulated ASN.1 {
                        OCTET STRING length = 20 content:
                           0bca31b8e2e8d35e1d7612f5a57178ce0bc39c4d" } }
                SEQUENCE length = 14 {
                    OBJECT IDENTIFIER 2.5.29.keyUsage(15)
                    BOOLEAN TRUE
                    OCTET STRING length = 4  encapsulated ASN.1 {
                        BIT STRING number of bits = 2 content: 40" } }
                SEQUENCE length = 22 {
                    OBJECT IDENTIFIER 2.5.29.37
                    BOOLEAN TRUE
                    OCTET STRING length = 12  encapsulated ASN.1 {
                      SEQUENCE length = 10 {
                    OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.timeStamping(8)}}}
                SEQUENCE length = 18 {
                    OBJECT IDENTIFIER 2.5.29.certificatePolicies(32)
```

```
                        OCTET STRING length = 11  encapsulated ASN.1 {
                            SEQUENCE length = 9 {
                              SEQUENCE length = 7 {
                                OBJECT IDENTIFIER 1.3.36.8.1.sigconf(1) }}}}
                    SEQUENCE length = 25 {
                        OBJECT IDENTIFIER 2.5.29.subjectAltName(17)
                        OCTET STRING length = 18  encapsulated ASN.1 {
                            SEQUENCE length = 16 {
                                [1] length = 14 content:
                                    74734074696d65736572762e6465" } } }
                    SEQUENCE length = 57 {
                        OBJECT IDENTIFIER 2.5.29.issuerAltName(18)
                        OCTET STRING length = 50  encapsulated ASN.1 {
                            SEQUENCE length = 48 {
                                [1] length = 12 content:
                                    726361407265674702e6465"
                                [6] length = 32 content:
                                    687474703a2f2f7777772e ..." } } }
                    SEQUENCE length = 12 {
                        OBJECT IDENTIFIER 2.5.29.basicConstraints(19)
                        BOOLEAN TRUE
                        OCTET STRING length = 2  encapsulated ASN.1 {
                            SEQUENCE length = 0 { } } }
                    SEQUENCE length = 41 {
                        OBJECT IDENTIFIER 2.5.29.cRLDistributionPoints(31)
                        OCTET STRING length = 34  encapsulated ASN.1 {
                            SEQUENCE length = 32 {
                                SEQUENCE length = 30 {
                                    [0] (constructed) length = 28 {
                                        [0] (constructed) length = 26 {
                                            [6] length = 24 content:
                                            687474703a2f2f777777 ..." }}}}}}
                    SEQUENCE length = 14 {
                        OBJECT IDENTIFIER 0.2.262.1.10.12.liabLimFlag(0)
                        OCTET STRING length = 3  encapsulated ASN.1 {
                            BOOLEAN TRUE } }
                    SEQUENCE length = 26 {
                        OBJECT IDENTIFIER 1.3.36.8.3.dateOfCertGen(1)
                        OCTET STRING length = 17  encapsulated ASN.1 {
                            GeneralizedTime "19980101000000Z" } }
                    SEQUENCE length = 48 {
                        OBJECT IDENTIFIER 1.3.36.8.3.admission(3)
                        OCTET STRING length = 39  encapsulated ASN.1 {
                            PrintableString
                            "Zulassung als Zeitstempeldienststelle" }}}}}
            SEQUENCE length = 9 {
                OBJECT IDENTIFIER 1.3.14.3.2.RSASignatureWithSHA1(29)
                NULL }
            BIT STRING number of bits = 2048 content:
                7ca2e45bb670c128abaafc346972cb5f188eafe5fa028df28d643c43a ..." }
```

Interpretierte DER-Kodierung

```
Version:                    2 (X.509v3-1996)
SubjectName:                CN=Zeitstempeldienst, SN=1, OU=zsd, O=time, C=DE
IssuerName:                 CN=Wurzelzertifizierungsstelle, SN=1, OU=rca,
O=regtp, C=DE
SerialNumber:               1 (decimal)
Validity  -  NotBefore:     Thu Jan 01 01:00:00 1998 (980101000000Z)
             NotAfter:      Thu Jan 01 01:00:00 2004 (040101000000Z)
Public Key Fingerprint:     BCCA 6C71 BA66 EB7E D801 0C6C 5568 9727
SubjectKey:                 Algorithm RSA (OID 1.2.840.113549.1.1.1), NULL
```

```
Certificate extensions:
Authority Key Identifier:
    Authority Cert Issuer: DName: CN=Wurzelzertifizierungsstelle, SN=1,
                                  OU=rca, O=regtp, C=DE
    Authority Cert Serial  Number: 0
Subject Key Identifier:    0BCA 31B8 E2E8 D35E 1D76 12F5 A571 78CE 0BC3 9C4D
Key Usage:                 (CRITICAL) nonRepudiation
Extended Key Usage:        kp-timeStamping (OID 1.3.6.1.5.5.7.3.8)
Certificate Policies:      sigconform (OID 1.3.36.8.1.1)
Subject alternative names: RFC822: ts@timeserv.de
Issuer alternative names:  RFC822: rca@regtp.de
Issuer alternative names:  URI: http://www.regtp.de/rootcert.cer
Basic Constraints:         NOT allowed to act as a CA !
CRL Distribution Points:
CRL Distribution Point Names: URI: http://www.regtp.de/crls

Private extensions:
LiabilityLimitationFlag:  (OID 0.2.262.1.10.12.0): Boolean: TRUE
DateOfCertGen:            (OID 1.3.36.8.3.1):      GeneralTime:
                                 |19980101000000Z                |
Admission:                (OID 1.3.36.8.3.3):      PrintableString:
                          |Zulassung als Zeitstempeldiensts|
                          |telle                           |

Signature:          Algorithm sha1WithRSASignature (OID 1.3.14.3.2.29), NULL
Certificate Fingerprint:  62:20:61:70:95:A3:72:4D:5A:E1:40:29:9C:2B:21:E0
```

Kompletter Hexadezimalcode

```
     0  30820458 30820347  A0030201 02020101      |0..[0..G........|
    10  30090605 2B0E0302  1D050030 5D310B30      |0...+......0]1.0|
    20  09060355 04061302  44453110 300C0603      |...U....DE1.0...|
    30  55040A13 05726567  74703110 300A0603      |U....regtp1.0...|
    40  55040B13 03726361  31304A30 08060355      |U....rca1.0...U.|
    50  05130131 31243022  06035504 03131B57      |...11$0"..U....W|
    60  75727A65 6C7A6572  74696669 7A696572      |urzelzertifizier|
    70  756E6773 7374656C  6C653001E 170D3938     |ungsstelle0...98|
    80  30313031 30303030  30305A17 0D303430      |0101000000Z..040|
    90  31303130 30303030  305A3052 310B3009      |101000000Z0R1.0.|
    A0  06035504 06130244  45310D30 0B060355      |..U....DE1.0...U|
    B0  040A1304 74696D65  310C300A 06035504      |....time1.0...U.|
    C0  0B13037A 7364310A  30080603 55040513      |...zsd1.0...U...|
    D0  01313111A 30180603  55040313 115A6569     |.11.0...U....Zei|
    E0  74737465 6D70656C  6469656E 73743081      |tstempeldienst0.|
    F0  9F300D06 092A8648  86F70D01 01010500      |.0...*.H........|
   100  03818D00 30818902  818100FD 2B4CCD03      |....0.......+L..|
   110  6031981C 67DEDD99  BEDFDE58 0932F375      |`1..g......X.2.u|
   120  D08794C6 278AED52  212A2212 4975E396      |....'..R!*".Iu..|
   130  BF5FFD72 2B8A59A7  9D9EC1BD 77F19FB2      |._.r+.Y.....w...|
   140  8D642568 7E9976F8  0028EBE0 B282FB6A      |.d%h~.v..(.....j|
   150  ED19AA55 C5ACB3CC  55A7221D 4145673B      |...U....U.".AEg;|
   160  E54F7503 B4C130F2  7AE556FF C83A0C4B      |.Ou...0.z.V..:.K|
   170  E9F334B8 98CF614B  7AD640E3 C7D353D6      |..4...aKz.@...S.|
   180  525E8556 A27A6A5D  18931102 03010001      |R^.V.zj].........|
   190  A38201BB 308201B7  306D0603 551D2304      |....0...0m..U.#.|
   1A0  663064A1 5FA45D31  0B300906 03550406      |f0d._.]1.0...U..|
   1B0  13024445 310E300C  06035504 0A130572      |..DE1.0...U....r|
   1C0  65677470 310C300A  06035504 0B130372      |egtp1.0...U....r|
   1D0  6361310A 30080603  55040513 01313124      |ca1.0...U....11$|
```

```
1E0  3022 0603 5504 0313  1B57 5725 7A65 6C7A      |0"..U....Wurzelz|
1F0  6572 7469 6669 7A69  6572 756E 6773 7374      |ertifizierungsst|
200  656C 6C65 8201 0030  1D06 0355 1D0E 0416      |elle...0...U....|
210  0414 0BCA 31B8 E2E8  D35E 1D76 12F5 A571      |....1....^.v...q|
220  78CE 0BC3 9C4D 300E  0603 551D 0F01 01FF      |x....M0...U.....|
230  0404 0302 0640 3016  0603 551D 2501 01FF      |......0...U.%...|
240  040C 300A 0608 2B06  0105 0507 0308 3012      |..0...+.......0.|
250  0603 551D 2004 0B30  0930 0706 052B 2408      |..U. ..0.0...+$.|
260  0101 3019 0603 551D  1104 1230 1081 0E74      |..0...U....0...t|
270  7340 7469 6D65 7365  7276 2E64 6530 3906      |s@timeserv.de09.|
280  0355 1D12 0432 3030  810C 7263 6140 7265      |.U...200..rca@re|
290  6774 702E 6465 8620  6874 7470 3A2F 2F77      |gtp.de. http://w|
2A0  7772 E72 6567 7470  2E64 652F 726F 6F74      |ww.regtp.de/root|
2B0  6365 7274 2E63 6572  300C 0603 551D 1301      |cert.cer0...U...|
2C0  01FF 0402 3000 3029  0603 551D 1F04 2230      |....0.0)..U..."0|
2D0  2030 1EA0 1CA0 1A86  1868 7474 703A 2F2F      | 0.......http://|
2E0  7777 772E 7265 6774  702E 6465 2F63 726C      |www.regtp.de/crl|
2F0  7330 0E06 0702 8206  010A 0C00 0403 0101      |s0..............|
300  FF30 1A06 052B 2408  0301 0411 180F 3139      |.0...+$.......19|
310  3938 3031 3031 3030  3030 3030 5A30 3006      |980101000000Z00.|
320  052B 2408 0303 0427  1325 5A75 6C61 7373      |.+$....'.%Zulass|
330  756E 6720 616C 7320  5A65 6974 7374 656D      |ung als Zeitstem|
340  7065 6C64 6965 6E73  7473 7465 6C65 3006      |peldienststelle0|
350  0906 052B 0E03 021D  0500 0382 0101 007C      |...+...........||
360  A2E4 5BB6 70C1 28AB  AAFC 3469 72CB 5F18      |..[.p.(...4ir._.|
370  8EAF E5FA 028D F28D  643C 43A0 1FAB BDA7      |........d<C.....|
380  D3FE 2CA9 B537 751B  B1F5 48A8 E3DC 7DB7      |..,..7u...H...}.|
390  9752 6BFA 2B12 D8E4  AF22 1C80 60B4 1251      |.Rk.+....".."`..Q|
3A0  3C86 7CB9 A82E 9E2F  1CFA 07ED CBA4 D803      |<.|..../........|
3B0  518E 7536 B38D 5E92  F3EC C368 BF90 DFC0      |Q.u6..^....h....|
3C0  D35B E8B5 0697 C6CB  B74E 5DB0 D86D B4F7      |.[.......N]..m..|
3D0  BEED B2A4 601D CBC7  E29F 5F32 372E E7DA      |....`....._27...|
3E0  F79D EB1B FE0C BCF8  6E05 4A80 6083 46D8      |........n.J.`.F.|
3F0  C70F B5FB A6B7 60D7  A5E0 EC9D 4761 BB13      |......`.....Ga..|
400  2FDA 7DEB ADDF 44B6  91C4 8A82 6A4D 3749      |/.}...D.....jM7I|
410  4320 EB38 E68A 29AE  46DA A85A C6E1 F662      |C .8..).F..Z...b|
420  30CB 7B1A 99BA 57DC  A6E7 EC43 0333 ECBA      |0.{...W....C.3..|
430  56E4 C3C8 924E AA20  BE52 9FC2 C1FB 165F      |V....N. .R....._|
440  CA0F 655C C17A A338  A85F A833 A7C6 73F0      |..e\.z.8._.3..s.|
450  D79A 0362 D20F E7E0  A14E 5BE1 CE82 40        |...b.....N[...@ |
```

Aus dem Offset des Hexdumps läßt sich die Speichergröße des Zeitstempeldienstzertifikates als ('45E'H= 4*256+5*16+14=) 1118 Bytes ablesen.

Anhang IV.4 Zertifizierungsstellenzertifikat

Die folgende ASN.1-Wertedefinition *caExampleCertificate* vom Typ *Certificate* enthält ein Beispiel für ein Zertifizierungsstellenzertifikat. Für dieses Zertifikat wurden die folgenden Annahmen gemacht:

Zertifizierungsstellenzertifikat

- Version des Zertifikates: 2, X.509v3
- Seriennummer des Zertifikates 3
- Innerer Signaturalgorithmus: sha1WithRSASignature
- Herausgeber des Zertifikates: CN=Wurzelzertifizierungsstelle, SN=1, OU=rca, O=regtp, C=DE
- Beginn der Gültigkeit: 1.1.1998, 0 Uhr, GMT
- Ende der Gültigkeit: 1.1.2004, 0 Uhr, GMT
- Inhaber des Zertifikates: CN=Zertifizierungsstelle, SN=1, OU=ca, O=cert, C=DE
- Öffentlicher Schlüssel: rsaEncryption mit Schlüssellänge 2048 Bit

Erweiterungen

- Identifizierung des öffentlichen Schlüssels des Zertifikaterstellers: AuthorityCertIssuer und AuthorityCertSerialNumber
- Identifizierung des öffentlichen Schlüssels des Zertifikinhabers: KeyIdentifier als SHA1-Hashwert des Schlüssels
- Nutzungsart des Schlüssels: keyCertSign
- Zertifizierungsrichtlinien: SigI-Konformität , OID: sigconform
- Alternativer Name des Zertifikatinhabers: RFC822: ca@cert.de
- Alternativer Name des Zertifikaterstellers: RFC822: rca@regtp.de; URI: http://www.regtp.de/rootcert.cer
- Zertifikaterstellung: cA=TRUE
- Sperrlisteninformation: URI: http://www.regtp.de/crls

Private Erweiterungen

- Zulassungskennung: TRUE
- Erstellungsdatum des Zertifikates: 1.1.1998, 0 Uhr, GMT
- Zulassung: Zulassung als Zertifizierungsstelle

- Äußerer Signaturalgorithmus: sha1WithRSASignature, Länge 2048 Bit

ASN.1-Wertedefinition

```
caExampleCertificate    Certificate  ::= {
   tbsCertificate {
    version                 2,
    serialNumber            3
    signature {
      algorithm             { 1 3 14 3 2 29 }
      parameters            2048 },
    issuer                  { "CN=Wurzelzertifizierungsstelle, SN=1,
                            OU=cert, O=regtp, C=DE" },
    validity                {
      notBefore             "980101000000Z",
      notAfter              "040101000000Z" },
    subject                 { "CN=Zertifizierungsstelle, SN=1, OU=ca,
                            O=cert, C=DE" },
    subjectPublicKeyInfo {
      algorithm {
         algorithm          { 1 2 840 113549 1 1 1 },
         parameters         NULL },
      subjectPublicKey      `...`B },
    extensions {
      authorityKeyIdentifier {
         extnId             { 2 5 29 35 },
         extnValue          `...`O },
      subjectKeyIdentifier {
         extnId             { 2 5 29 14 },
         extnValue          `...`O },
      keyUsage {
         extnId             { 2 5 29 15 },
         critical           TRUE,
         extnValue          `000001000`B } },
      certificatePolicies {
         extnId             { 2 5 29 32 },
         extnValue          { 1 3 36 8 1 1 } },
      subjectAltName {
         extnId             { 2 5 29 17 },
         extnValue          "ca@cert.de" },
      issuerAltName {
         extnId             { 2 5 29 18 },
         extnValue          {"rca@regtp.de",
                            "http://www.regtp.de/rootcert.cer" } },
      basicConstraints {
         extnId             { 2 5 29 19 },
         critical           TRUE,
         extnValue          { cA TRUE } },
      cRLDistributionPoints {
         extnId             { 0 2 262 1 10 12 0 },
         extnValue          "http://www.regtp.de/crls" },
      liabilityLimitationFlag {
         extnId             { 2 5 29 31 },
         extnValue          TRUE },
      dateOfCertGen {
         extnId             { 1 3 36 8 3 1 },
         extnValue          "19980101000000Z" },
```

```
      atAdmission {
         extnId             { 1 3 36 8 3 3 },
         extnValue          "Zulassung als Zertifizierungsstelle" } } }
    signatureAlgorithm {
      algorithm             { 1 3 14 3 2 29 },
      parameters            NULL },
    signature               `...`B }
```

Zugehörige DER-Kodierung

```
SEQUENCE length = 1223 {
        SEQUENCE length = 947 {
            [0] (constructed) length = 3 {
                INTEGER 2 }
            INTEGER 3
            SEQUENCE length = 9 {
                OBJECT IDENTIFIER 1.3.14.3.2.RSASignatureWithSHA1(29)
                NULL }
            SEQUENCE length = 93 {
                SET length = 11 {
                    SEQUENCE length = 9 {
                        OBJECT IDENTIFIER 2.5.4.countryName(6)
                        PrintableString "DE" } }
                SET length = 14 {
                    SEQUENCE length = 12 {
                        OBJECT IDENTIFIER 2.5.4.organizationName(10)
                        PrintableString "regtp" } }
                SET length = 12 {
                    SEQUENCE length = 10 {
                        OBJECT IDENTIFIER 2.5.4.organizationalUnitName(11)
                        PrintableString "rca" } }
                SET length = 10 {
                    SEQUENCE length = 8 {
                        OBJECT IDENTIFIER 2.5.4.serialNumber(5)
                        PrintableString "1" } }
                SET length = 36 {
                    SEQUENCE length = 34 {
                        OBJECT IDENTIFIER 2.5.4.commonName(3)
                        PrintableString "Wurzelzertifizierungsstelle" } } }
            SEQUENCE length = 30 {
                UTCTime "980101000000Z"
                UTCTime "040101000000Z" }
            SEQUENCE length = 85 {
                SET length = 11 {
                    SEQUENCE length = 9 {
                        OBJECT IDENTIFIER 2.5.4.countryName(6)
                        PrintableString "DE" } }
                SET length = 13 {
                    SEQUENCE length = 11 {
                        OBJECT IDENTIFIER 2.5.4.organizationName(10)
                        PrintableString "cert" } }
                SET length = 11 {
                    SEQUENCE length = 9 {
                        OBJECT IDENTIFIER 2.5.4.organizationalUnitName(11)
                        PrintableString "ca" } }
                SET length = 10 {
                    SEQUENCE length = 8 {
                        OBJECT IDENTIFIER 2.5.4.serialNumber(5)
                        PrintableString "1" } }
                SET length = 30 {
                    SEQUENCE length = 28 {
```

```
                OBJECT IDENTIFIER 2.5.4.commonName(3)
                PrintableString "Zertifizierungsstelle" } } }
        SEQUENCE length = 290 {
            SEQUENCE length = 13 {
                OBJECT IDENTIFIER 1.2.840.113549.1.1.rsaEncryption(1)
                NULL }
            BIT STRING number of bits = 2160  encapsulated ASN.1 {
                SEQUENCE length = 266 {
                    INTEGER 0x00f50b86392f705adfa139ed27a22de5bec9f5 ...
                    INTEGER 65537 } } }
        [3] (constructed) length = 416 {
            SEQUENCE length = 412 {
                SEQUENCE length = 109 {
                    OBJECT IDENTIFIER 2.5.29.authorityKeyIdentifier(35)
                    OCTET STRING length = 102  encapsulated ASN.1 {
                        SEQUENCE length = 100 {
                            [1] (constructed) length = 95 {
                                [4] (constructed) length = 93 {
                                    SET length = 11 {
                                        SEQUENCE length = 9 {
                                      OBJECT IDENTIFIER 2.5.4.countryName(6)
                                            PrintableString "DE" } }
                                    SET length = 14 {
                                        SEQUENCE length = 12 {
                                OBJECT IDENTIFIER 2.5.4.organizationName(10)
                                            PrintableString "regtp" } }
                                    SET length = 12 {
                                        SEQUENCE length = 10 {
                              OBJECT IDENTIFIER 2.5.4.organizationalUnitName(11)
                                            PrintableString "rca" } }
                                    SET length = 10 {
                                        SEQUENCE length = 8 {
                                   OBJECT IDENTIFIER 2.5.4.serialNumber(5)
                                            PrintableString "1" } }
                                    SET length = 36 {
                                        SEQUENCE length = 34 {
                                     OBJECT IDENTIFIER 2.5.4.commonName(3)
                             PrintableString "Wurzelzertifizierungsstelle" }}}}
                                  [2] length = 1 content: 00" } } }
                    SEQUENCE length = 29 {
                        OBJECT IDENTIFIER 2.5.29.subjectKeyIdentifier(14)
                        OCTET STRING length = 22  encapsulated ASN.1 {
                            OCTET STRING length = 20 content:
                               9234a3102b08e46f4f1cac09df0c31d5ea62add7" } }
                    SEQUENCE length = 14 {
                        OBJECT IDENTIFIER 2.5.29.keyUsage(15)
                        BOOLEAN TRUE
                        OCTET STRING length = 4  encapsulated ASN.1 {
                            BIT STRING number of bits = 6 content: 04" } }
                    SEQUENCE length = 18 {
                        OBJECT IDENTIFIER 2.5.29.certificatePolicies(32)
                        OCTET STRING length = 11  encapsulated ASN.1 {
                            SEQUENCE length = 9 {
                              SEQUENCE length = 7 {
                                OBJECT IDENTIFIER 1.3.36.8.1.sigconf(1) }}}}
                    SEQUENCE length = 21 {
                        OBJECT IDENTIFIER 2.5.29.subjectAltName(17)
                        OCTET STRING length = 14  encapsulated ASN.1 {
                            SEQUENCE length = 12 {
                                [1] length = 10 content:
                                    636140636572742e6465" } } }
                    SEQUENCE length = 57 {
                        OBJECT IDENTIFIER 2.5.29.issuerAltName(18)
```

```
                    OCTET STRING length = 50  encapsulated ASN.1 {
                        SEQUENCE length = 48 {
                            [1] length = 12 content:
                                726361407265674702e6465"
                            [6] length = 32 content:
                                687474703a2f2f7777772e726567747 ..." }}}
                SEQUENCE length = 15 {
                    OBJECT IDENTIFIER 2.5.29.basicConstraints(19)
                    BOOLEAN TRUE
                    OCTET STRING length = 5  encapsulated ASN.1 {
                        SEQUENCE length = 3 { BOOLEAN TRUE } } }
                SEQUENCE length = 41 {
                    OBJECT IDENTIFIER 2.5.29.cRLDistributionPoints(31)
                    OCTET STRING length = 34  encapsulated ASN.1 {
                        SEQUENCE length = 32 {
                            SEQUENCE length = 30 {
                                [0] (constructed) length = 28 {
                                    [0] (constructed) length = 26 {
                                        [6] length = 24 content:
                                            687474703a2f2f77 ..." }}}}}}
                SEQUENCE length = 14 {
                    OBJECT IDENTIFIER 0.2.262.1.10.12.liabLimFlag(0)
                    OCTET STRING length = 3  encapsulated ASN.1 {
                        BOOLEAN } }
                SEQUENCE length = 26 {
                    OBJECT IDENTIFIER 1.3.36.8.3.dateOfCertGen(1)
                    OCTET STRING length = 17  encapsulated ASN.1 {
                        GeneralizedTime "19980101000000Z" } }
                SEQUENCE length = 46 {
                    OBJECT IDENTIFIER 1.3.36.8.3.admission(3)
                    OCTET STRING length = 37  encapsulated ASN.1 {
                        PrintableString
                            "Zulassung als Zertifizierungsstelle" }}}}}
        SEQUENCE length = 9 {
            OBJECT IDENTIFIER 1.3.14.3.2.RSASignatureWithSHA1(29)
            NULL }
        BIT STRING number of bits = 2048 content:
            2587705292678aa66e7db4462759da5155e41df72abcfa581651... "}
```

Interpretierte DER-Kodierung

```
Version:                    2 (X.509v3-1996)
SubjectName:                CN=Zertifizierungsstelle, SN=1, OU=ca, O=cert,
                            C=DE
IssuerName:                 CN=Wurzelzertifizierungsstelle, SN=1, OU=rca,
                            O=regtp, C=DE
SerialNumber:               3 (decimal)
Validity  -  NotBefore:     Thu Jan 01 01:00:00 1998 (980101000000Z)
             NotAfter:      Thu Jan 01 01:00:00 2004 (040101000000Z)
Public Key Fingerprint:     97E7 BF22 29F2 5D56 F962 6D7A 63B2 F2F3
SubjectKey:                 Algorithm RSA (OID 1.2.840.113549.1.1.1), NULL

Certificate extensions:
Authority Key Identifier:
    Authority Cert Issuer: DName: CN=Wurzelzertifizierungsstelle, SN=1,
                                  OU=rca, O=regtp, C=DE
    Authority Cert Serial  Number: 0
Subject Key Identifier:     9234 A310 2B08 E46F 4F1C AC09 DF0C 31D5 EA62 ADD7
Key Usage:                  (CRITICAL) keyCertSign
Certificate Policies:       sigconform (OID 1.3.36.8.1.1)
Subject alternative names: RFC822: ca@cert.de
Issuer alternative names:   RFC822: rca@regtp.de
Issuer alternative names:   URI: http://www.regtp.de/rootcert.cer
```

```
Basic Constraints:         allowed to act as a CA !
CRL Distribution Points:
CRL Distribution Point Names: URI: http://www.regtp.de/crls

Private extensions:
LiabilityLimitationFlag:   (OID 0.2.262.1.10.12.0): Boolean: TRUE
DateOfCertGen:             (OID 1.3.36.8.3.1):      GeneralTime:
                           |19980101000000Z                |
Admission:                 (OID 1.3.36.8.3.3):      PrintableString:
                           |Zulassung als Zertifizierungsste|
                           |lle                             |

Signature:          Algorithm sha1WithRSASignature (OID 1.3.14.3.2.29), NULL
Certificate Fingerprint:  BA:CB:F8:E3:6B:B0:36:64:5A:A9:31:59:10:9B:37:2F
```

Kompletter Hexadezimalcode

```
      0  308204C7 308203B3  A0030201 02020103      |0...0...........|
     10  30090605 2B0E0302  1D05003D 5D310B30      |0...+......0]1.0|
     20  09060355 04061302  4445310E 300C0603      |...U....DE1.0...|
     30  55040A13 05726567  74703100 300A0603      |U....regtp1.0...|
     40  55040B13 03726361  3100A008 06035504      |U....rca1.0...U.|
     50  05130131 31243022  06035504 03131B57      |...11$0"..U....W|
     60  75727A65 6C7A6572  74696669 7A696572      |urzelzertifizier|
     70  756E6773 7374656C  6C653001E 170D3938      |ungsstelle0...98|
     80  30313031 30303030  30305A17 0D303430      |0101000000Z..040|
     90  31303130 30303030  305A3055 310B3009      |101000000Z0U1.0.|
     A0  06035504 06130244  45310D30 0B060355      |..U....DE1.0...U|
     B0  040A1304 63657274  310B3009 06035504      |....cert1.0...U.|
     C0  0B130263 61310A30  08060355 04051301      |...ca1.0...U....|
     D0  31311E30 1C060355  04031315 5A657274      |11.0...U....Zert|
     E0  6966697A 69657275  6E677373 74656C6C      |ifizierungsstell|
     F0  65308201 22300D06  092A8648 86F70D01      |e0.."0...*.H....|
    100  01010500 03820100F 00308201 0A028201      |.........0......|
    110  0100F50B 86392F70  5ADFA139 ED27A22D      |.....9/pZ..9.'.-|
    120  E5BEC9F5 F79B8A08  2DA64A1B 93FAC162      |........-.J....b|
    130  1E666DA4 8139E17E  5D01602D E5BCBCB8      |.fm..9.~].`-....|
    140  0E5E0928 E25D78A5  02155AB4 16942D75      |.^.(.]x...Z...-u|
    150  F528E1B7 F7047D94  9702A638 AFC28756      |.(....}....8...V|
    160  597100A9 8E922CFC  83F1AD1F 14EDC179      |Yq....,........y|
    170  79534735 69A99503  C2B04E35 9B1B22E4      |ySG5i.....N5..".|
    180  FF4658F6 6F632C72  D3A72A09 D5EE34DE      |.FX.oc,r..*...4.|
    190  F00FD17E EDBA3928  122695D2 F2C3967B      |...~..9(.&.....{|
    1A0  CD5BF4A7 8520ABD2  1386CA5D A0EBC0A3      |.[... .....]....|
    1B0  815BE55A 09D948E7  F05F1E45 89B125D8      |.[.Z..H._.E..%.|
    1C0  4C8BD4CB 873FFB85  67E15048 AB2DDDCE      |L....?..g.PH.-..|
    1D0  5370558A 2D0BE72A  5C569306 FC607AD4      |SpU.-..*\V...`z.|
    1E0  D4444080 A3A8FBB9  412AA535 91ADAD10      |.D@.....A*.5....|
    1F0  440F5BF1 6796C17C  C4C09E8F EDA4D396      |D.[.g..|........|
    200  AA0A68DF 757293DB  779584E4 2104E963      |..h.ur..w...!..c|
    210  90030203 010001A3  8201A030 82019C30      |...........0...0|
    220  6D060355 1D230466  3064A15F A45D310B      |m..U.#.f0d._.]1.|
    230  30090603 55040613  02444531 0E300C06      |0...U....DE1.0..|
    240  0355040A 13057265  67747031 0C300A06      |.U....regtp1.0..|
    250  0355040B 13037263  6131 0A30 08060355      |.U....rca1.0...U|
    260  04051301 31312430  22060355 04031315      |....11$0"..U....|
    270  5775727A 656C7A65  72746966 697A6965      |Wurzelzertifizie|
    280  72756E67 73737465  6C6C6582 01003001D     |rungsstelle...0.|
```

```
290  0603551D 0E04160414 9234A3 102B08E4      |..U.......4..+..|
2A0  6F4F1CAC 09DF0C31  D5EA62AD D7300E06      |oO.....1..b..0..|
2B0  03551D0F 0101FF04  04030202 04301206      |.U...........0..|
2C0  03551D20 040B3009  30070605 2B240801      |.U. ..0.0...+$..|
2D0  01301506 03551D11  040E300C 810A6361      |.0...U....0...ca|
2E0  40636572 742E6465  30390603 551D1204      |@cert.de09..U...|
2F0  32303081 0C726361  40726567 74702E64      |200..rca@regtp.d|
300  65862068 7474703A  2F2F7777 772E7265      |e. http://www.re|
310  6774702E 64652F72  6F6F7463 6572742E      |gtp.de/rootcert.|
320  63657230 0F060355  1D130101 FF040530      |cer0...U.......0|
330  03010101FF 30290603 551D1F04 22302030      |....0)..U..."0 0|
340  1EA01CA0 1A861868  7474703A 2F2F7777      |.......http://ww|
350  772E7265 6774702E  64652F63 726C7330      |w.regtp.de/crls0|
360  0E060702 8206010A  0C000403 0101FF30      |...............0|
370  1A06052B 24080301  04111180F 31393938      |...+$.......1998|
380  30313031 30303030  30305A30 2E06052B      |010100000Z0...+|
390  24080303 04251323  5A756C61 7373756E      |$....%.#Zulassun|
3A0  6720616C 73205A65  72746966 697A6965      |g als Zertifizie|
3B0  72756E67 73737465  6C6C6530 09060528      |rungsstelle0...+|
3C0  0E03021D 05000382  01010025 87705292      |...........%.pR.|
3D0  678AA66E 7DB44627  59DA5155 E41DF72A      |g..n}.F'Y.QU...*|
3E0  BCFA5816 5158A0D8  6CA62F20 8FD4F287      |..X.QX..l./ ....|
3F0  17E9C8D1 3A37C1D6  F9B4A94A 02E20913      |....:7.....J....|
400  DE1753FA 74F96325  EA5F3D68 C252DEA1      |..S.t.c%._=h.R..|
410  388C2049 21977C72  E2CD276B 5D1CD8CE      |8. I!.|r..'k]...|
420  1C55ECF4 CA05317C  FF027E41 D5DF8436      |.U....1|..~A...6|
430  AC12D681 6B4912F6  6CC3627B 4213C482      |....kI..l.b{B...|
440  8D601576 842D8DB0  622375C0 35C4E59A      |.`.v.-..b#u.5...|
450  9B4DD740 8B302CE6  7FBA0FFD 3A5B0C9C      |.M.@.0,.....:[..|
460  FF58C2B7 9742A176  3D99D7B1 2766A2F4      |.X...B.v=...'f..|
470  434A363D 6EFC350F  7123B7FB 99DCF63C      |CJ6=n.5.q#.....<|
480  09BAE04E 00E469B0  5075AD58 DF4D8724      |...N..i.Pu.X.M.$|
490  D9C7FA21 ADDC532A  EA2A2821 71DFA591      |...!..S*.*(!q...|
4A0  55A06F71 408B5629  B7529255 AFF13B4E      |U.oq@.V).R.U..;N|
4B0  D7F4D824 9F9B53F9  DC649211 3D163BBD      |...$..S..d..=.;.|
4C0  49BA5846 F38B82D2  72E29B                 |I.XF....r..     |
```

Aus dem Offset des Hexdumps läßt sich die Speichergröße des Zertifizierungsstellenzertifikates als ('4CA'H= 4*256+12*16+10=) 1226 Bytes ablesen.

Anhang IV.5 Teilnehmerzertifikat

Die folgende ASN.1-Wertedefinition *userExampleCertificate* vom Typ *Certificate* enthält ein Beispiel für ein Teilnehmerzertifikat. Für dieses Zertifikat wurden die folgenden Annahmen gemacht:

Teilnehmerzertifikat

- Version des Zertifikates: 2, X.509v3
- Seriennummer des Zertifikates: 1
- Innerer Signaturalgorithmus: sha1WithRSASignature
- Herausgeber des Zertifikates: CN=Zertifizierungsstelle, SN=1, OU=ca, O=cert, C=DE
- Beginn der Gültigkeit: 1.1.1999, 0 Uhr, GMT
- Ende der Gültigkeit: 1.1.2000, 0 Uhr, GMT
- Inhaber des Zertifikates: CN=Name-des-Arztes, T=Dr., SN=1, O=KV Hessen, C=DE
- Schlüsselalgorithmus: rsaEncryption mit Schlüssellänge 1024 Bit

Erweiterungen

- Identifizierung des öffentlichen Schlüssels des Zertifikaterstellers: AuthorityCertIssuer und AuthorityCertSerialNumber
- Identifizierung des öffentlichen Schlüssels des Zertifikinhabers: KeyIdentifier als SHA1-Hashwert des Schlüssels
- Nutzungsart des Schlüssels: non repudiation
- Zertifizierungsrichtlinien: SigI-Konformität , OID: sigconform
- Alternativer Name des Zertifikatinhabers: RFC822: arzt@kvh.de
- Alternativer Name des Zertifikaterstellers: RFC822: ca@cert.de
- Zertifikaterstellung: cA=FALSE
- Sperrlisteninformation: URI: http://www.cert.de/crls

Private Erweiterungen

- Zulassungskennung: TRUE
- Erstellungsdatum des Zertifikates: 18.6.1998, 12Uhr, GMT
- Zulassung: KV Hessen: Zulassung als Arzt:

Zulassungsnummer 1000010

- Äußerer Signaturalgorithmus: sha1WithRSASignature, Länge 2048 Bit

ASN.1-Wertedefinition

```
caExampleCertificate    Certificate  ::= {
   tbsCertificate {
     version               2,
     serialNumber          1
     signature {
        algorithm          { 1 3 14 3 2 29 }
        parameters         NULL },
     issuer                { "CN=Zertifizierungsstelle, SN=1, OU=ca,
                           O=cert, C=DE" },
     validity              {
        notBefore          "990101000000Z",
        notAfter           "000101000000Z" },
     subject               { "CN=Name-des-Arztes, T=Dr., SN=1,
                           O=KV Hessen, C=DE" },
     subjectPublicKeyInfo {
        algorithm {
           algorithm       { rsaEncryption },
           parameters      1024 },
        subjectPublicKey   `...`B },
     extensions {
        authorityKeyIdentifier {
           extnId          { 2 5 29 35 },
           extnValue       `...`O },
        subjectKeyIdentifier {
           extnId          { 2 5 29 14 },
           extnValue       `...`O },
        keyUsage {
           extnId          { 2 5 29 15 },
           critical        TRUE,
           extnValue       `010000000`B } },
        certificatePolicies {
           extnId              { 2 5 29 32 },
           extnValue       { 1 3 36 8 1 1 } },
        subjectAltName {
           extnId          { 2 5 29 17 },
           extnValue       "arzt@kvh.de" },
        issuerAltName {
           extnId          { 2 5 29 18 },
           extnValue       "ca@cert.de" },
        basicConstraints {
           extnId          { 2 5 29 19 },
           critical        TRUE,
           extnValue       { cA FALSE } },
        cRLDistributionPoints {
           extnId          { 2 5 29 31 },
           extnValue       "http://www.cert.de/crls" },
        liabilityLimitationFlag {
           extnId          { 0 2 262 1 10 12 0 },
           extnValue       TRUE },
        dateOfCertGen {
           extnId          { 1 3 36 8 3 1 },
           extnValue       "19980618120000Z" },
```

```
         atAdmission {
            extnId          { 1 3 36 8 3 3 },
            extnValue       "KV Hessen: Zulassung als Arzt:
                             Zulassungsnummer: 1000010"
                            } }
      signatureAlgorithm {
         algorithm          { 1 3 14 3 2 29 },
         parameters         NULL },
      signature             `...`B }
```

Zugehörige DER-Kodierung

```
SEQUENCE length = 1057 {
        SEQUENCE length = 781 {
            [0] (constructed) length = 3 { INTEGER 2 }
            INTEGER 1
            SEQUENCE length = 9 {
                OBJECT IDENTIFIER 1.3.14.3.2.RSASignatureWithSHA1(29)
                NULL }
            SEQUENCE length = 85 {
                SET length = 11 {
                    SEQUENCE length = 9 {
                        OBJECT IDENTIFIER 2.5.4.countryName(6)
                        PrintableString "DE" } }
                SET length = 13 {
                    SEQUENCE length = 11 {
                        OBJECT IDENTIFIER 2.5.4.organizationName(10)
                        PrintableString "cert" } }
                SET length = 11 {
                    SEQUENCE length = 9 {
                        OBJECT IDENTIFIER 2.5.4.organizationalUnitName(11)
                        PrintableString "ca" } }
                SET length = 10 {
                    SEQUENCE length = 8 {
                        OBJECT IDENTIFIER 2.5.4.serialNumber(5)
                        PrintableString "1" } }
                SET length = 30 {
                    SEQUENCE length = 28 {
                        OBJECT IDENTIFIER 2.5.4.commonName(3)
                        PrintableString "Zertifizierungsstelle" } } }
            SEQUENCE length = 30 {
                UTCTime "990101000000Z"
                UTCTime "000101000000Z" }
            SEQUENCE length = 85 {
                SET length = 11 {
                    SEQUENCE length = 9 {
                        OBJECT IDENTIFIER 2.5.4.countryName(6)
                        PrintableString "DE" } }
                SET length = 18 {
                    SEQUENCE length = 16 {
                        OBJECT IDENTIFIER 2.5.4.organizationName(10)
                        PrintableString "KV Hessen" } }
                SET length = 10 {
                    SEQUENCE length = 8 {
                        OBJECT IDENTIFIER 2.5.4.serialNumber(5)
                        PrintableString "1" } }
                SET length = 12 {
                    SEQUENCE length = 10 {
                        OBJECT IDENTIFIER 2.5.4.title(12)
                        PrintableString "Dr." } }
                SET length = 24 {
```

```
            SEQUENCE length = 22 {
                OBJECT IDENTIFIER 2.5.4.commonName(3)
                PrintableString "Name-des-Arztes" } } }
        SEQUENCE length = 159 {
            SEQUENCE length = 13 {
                OBJECT IDENTIFIER 1.2.840.113549.1.1.rsaEncryption(1)
                NULL }
            BIT STRING number of bits = 1120  encapsulated ASN.1 {
                SEQUENCE length = 137 {
                    INTEGER 0x00ffcdb8e47f23262b308203165abc87832f8b ...
                    INTEGER 65537 } } }
        [3] (constructed) length = 390 {
            SEQUENCE length = 386 {
                SEQUENCE length = 101 {
                    OBJECT IDENTIFIER 2.5.29.authorityKeyIdentifier(35)
                    OCTET STRING length = 94  encapsulated ASN.1 {
                        SEQUENCE length = 92 {
                            [1] (constructed) length = 87 {
                                [4] (constructed) length = 85 {
                                    SET length = 11 {
                                        SEQUENCE length = 9 {
                                      OBJECT IDENTIFIER 2.5.4.countryName(6)
                                            PrintableString "DE" } }
                                    SET length = 13 {
                                        SEQUENCE length = 11 {
                                OBJECT IDENTIFIER 2.5.4.organizationName(10)
                                            PrintableString "cert" } }
                                    SET length = 11 {
                                        SEQUENCE length = 9 {
                              OBJECT IDENTIFIER 2.5.4.organizationalUnitName(11)
                                            PrintableString "ca" } }
                                    SET length = 10 {
                                        SEQUENCE length = 8 {
                                 OBJECT IDENTIFIER 2.5.4.serialNumber(5)
                                            PrintableString "1" }
                                    SET length = 30 {
                                        SEQUENCE length = 28 {
                                  OBJECT IDENTIFIER 2.5.4.commonName(3)
                                PrintableString "Zertifizierungsstelle" }}}}
                                [2] length = 1 content: 03" } } }
                    SEQUENCE length = 29 {
                        OBJECT IDENTIFIER 2.5.29.subjectKeyIdentifier(14)
                        OCTET STRING length = 22  encapsulated ASN.1 {
                            OCTET STRING length = 20 content:
                               a7e555c82b3f92a5f4809373f84175636a74f4d8" } }
                    SEQUENCE length = 14 {
                        OBJECT IDENTIFIER 2.5.29.keyUsage(15)
                        BOOLEAN TRUE
                        OCTET STRING length = 4  encapsulated ASN.1 {
                            BIT STRING number of bits = 2 content: 40" } }
                    SEQUENCE length = 18 {
                        OBJECT IDENTIFIER 2.5.29.certificatePolicies(32)
                        OCTET STRING length = 11  encapsulated ASN.1 {
                            SEQUENCE length = 9 {
                              SEQUENCE length = 7 {
                                OBJECT IDENTIFIER 1.3.36.8.1.sigconf(1) }}}}
                    SEQUENCE length = 22 {
                        OBJECT IDENTIFIER 2.5.29.subjectAltName(17)
                        OCTET STRING length = 15  encapsulated ASN.1 {
                            SEQUENCE length = 13 {
                                [1] length = 11 content:
```

```
                                61727a74406b76682e6465" } } }
                        SEQUENCE length = 21 {
                            OBJECT IDENTIFIER 2.5.29.issuerAltName(18)
                            OCTET STRING length = 14  encapsulated ASN.1 {
                                SEQUENCE length = 12 {
                                    [1] length = 10 content:
                                        636140636572742e6465" } } }
                        SEQUENCE length = 12 {
                            OBJECT IDENTIFIER 2.5.29.basicConstraints(19)
                            BOOLEAN TRUE
                            OCTET STRING length = 2  encapsulated ASN.1 {
                                SEQUENCE length = 0 { } } }
                        SEQUENCE length = 40 {
                            OBJECT IDENTIFIER 2.5.29.cRLDistributionPoints(31)
                            OCTET STRING length = 33  encapsulated ASN.1 {
                                SEQUENCE length = 31 {
                                    SEQUENCE length = 29 {
                                        [0] (constructed) length = 27 {
                                            [0] (constructed) length = 25 {
                                                [6] length = 23 content:
                                                    687474703a2f2f77 ..." }}}}}}
                        SEQUENCE length = 14 {
                            OBJECT IDENTIFIER 0.2.262.1.10.12.liabLimFlag(0)
                            OCTET STRING length = 3  encapsulated ASN.1 {
                                BOOLEAN TRUE } }
                        SEQUENCE length = 26 {
                            OBJECT IDENTIFIER 1.3.36.8.3.dateOfCertGen(1)
                            OCTET STRING length = 17  encapsulated ASN.1 {
                                GeneralizedTime "19980618120000Z" } }
                        SEQUENCE length = 67 {
                            OBJECT IDENTIFIER 1.3.36.8.3.admission(3)
                            OCTET STRING length = 58  encapsulated ASN.1 {
                                PrintableString "KV Hessen: Zulassung als Arzt:
                                   Zulassungsnummer: 1000010" }}}}}
                SEQUENCE length = 9 {
                    OBJECT IDENTIFIER 1.3.14.3.2.RSASignatureWithSHA1(29)
                    NULL }
                BIT STRING number of bits = 2048 content:
                    1bd4098ef80d4e7e7305ca98525da172515639 ... " }
```

Interpretierte DER-Kodierung

```
Version:                    2 (X.509v3-1996)
SubjectName:                CN=Name-des-Arztes, T=Dr., SN=1, O=KV Hessen,
                            C=DE
IssuerName:                 CN=Zertifizierungsstelle, SN=1, OU=ca, O=cert,
                            C=DE
SerialNumber:               1 (decimal)
Validity  -  NotBefore:     Fri Jan 01 01:00:00 1999 (990101000000Z)
               NotAfter:    Sat Jan 01 01:00:00 2000 (000101000000Z)
Public Key Fingerprint:     AE5B E66A D981 27D7 17B9 74F1 359A 3F55
SubjectKey:                 Algorithm RSA (OID 1.2.840.113549.1.1.1), NULL

Certificate extensions:
Authority Key Identifier:
    Authority Cert Issuer: DName: CN= Zertifizierungsstelle, SN=1,
                                  OU=ca, O=cert, C=DE
    Authority Cert Serial  Number: 3
Subject Key Identifier:     A7E5 55C8 2B3F 92A5 F480 9373 F841 7563 6A74 F4D8
Key Usage:                  (CRITICAL) nonRepudiation
Certificate Policies:       sigconform (OID 1.3.36.8.1.1)
Subject alternative names: RFC822: arzt@kvh.de
Issuer alternative names:  RFC822: ca@cert.de
```

```
Basic Constraints:         NOT allowed to act as a CA !
CRL Distribution Points:
CRL Distribution Point Names: URI: http://www.cert.de/crls

Private extensions:
LiabilityLimitationFlag:  (OID 0.2.262.1.10.12.0): Boolean: TRUE
DateOfCertGen:            (OID 1.3.36.8.3.1):      GeneralTime:
                          |19980618120000Z                |
Admission:                (OID 1.3.36.8.3.3):      PrintableString:
                          |KV Hessen: Zulassung als Arzt: Z|
                          |ulassungsnummer: 1000010        |

Signature:          Algorithm sha1WithRSASignature (OID 1.3.14.3.2.29), NULL
Certificate Fingerprint:  97:12:D1:82:10:70:87:01:DD:C5:3A:F9:D5:B0:60:D1
```

Kompletter Hexadezimalcode

```
   0  30820421 30820308  A0030201 02020101      |0..!0...........|
  10  30090605 2B0E0302  1D050030 55310B30      |0...+......0U1.0|
  20  09060355 04061302  44453110 300B0603      |...U....DE1.0...|
  30  55040A13 04636572  74310B30 09060355      |U....cert1.0...U|
  40  040B1302 6361310A  30080603 55040513      |....ca1.0...U...|
  50  01311E30 1C060355  04031315 5A657274      |.11.0...U....Zer|
  60  74696669 7A696572  756E6773 7374656C      |tifizierungsstel|
  70  6C653031 170D3939  30313031 30303030      |le0...9901010000|
  80  30305A17 0D303030  31303130 30303030      |00Z..00010100000|
  90  305A3055 310B3009  06035504 06130244      |0Z0U1.0...U....D|
  A0  45311230 10060355  040A1309 4B562048      |E1.0...U....KV H|
  B0  65737365 6E310A30  08060355 04051301      |essen1.0...U....|
  C0  31310C30 0A060355  040C1303 44722E31      |11.0...U....Dr.1|
  D0  18301606 03550403  130F4E61 6D652D64      |.0...U....Name-d|
  E0  65732D41 727A7465  73301F30 0D060900      |es-Arztes0..0...|
  F0  2A864886 F70D0101  01050003 818D0030      |*.H...........0|
 100  81890281 8100FFCD  B8E47F23 262B3082      |..........#&+0.|
 110  03165ABC 87832F8B  2ED3BBA4 A4A49F51      |..Z.../........Q|
 120  5E0673B9 CA55AB65  AE7A602B F26FF22E      |^.s..U.e.z`+.o..|
 130  C18FF9CC 08E98395  E7E10E1F 3E7FC853      |............>..S|
 140  F97B8869 03E0D334  10CE0173 40345A73      |.{.i...4...s@4Zs|
 150  870D394C 01EE7B75  30AE162D 9F954D81      |..9L..{u0..-..M.|
 160  9639FD63 BF20DAE0  D0274802 1851ADD2      |.9.c. ...'H..Q..|
 170  66F7DA6F C2275B93  24506E8C 32D522DC      |f..o.'[.$Pn.2.".|
 180  BBCFF374 BB1D0203  010001A3 82018630      |...t..........0|
 190  82018230 65060355  1D23045E 305CA157      |...0e..U.#.^0\.W|
 1A0  A4553110 30090603  55040613 02444531      |.U1.0...U....DE1|
 1B0  0D300B06 03550403  13046365 72743110      |.0...U....cert1.|
 1C0  30090603 55040B13  02636131 0A300806      |0...U....ca1.0..|
 1D0  03550405 13013131  1E301C06 03550403      |.U....11.0...U..|
 1E0  13155A65 72746966  697A6965 72756E67      |..Zertifizierung|
 1F0  73737465 6C6C6582  01030301 D0603551D      |sstelle...0...U.|
 200  0E04160 414A7E555  C82B3F92 A5F48093      |.......U.+?.....|
 210  73F84175 636A74F4  D8300E06 03551D0F      |s.Aucjt..0...U..|
 220  01010FF04 04030206  40301206 03551D20      |.........0...U. |
 230  040B3009 30070605  2B240801 01301606      |..0.0...+$...0..|
 240  03551D11 040F300D  810B6172 7A74406B      |.U....0...arzt@k|
 250  76682E64 65301506  03551D12 040E300C      |vh.de0...U....0.|
 260  810A6361 40636572  742E6465 300C0603      |..ca@cert.de0...|
 270  551D1301 01FF0402  30003028 06035510      |U.......0.0(..U.|
 280  1F042130 1F301DA0  1BA01986 17687474      |..!0.0......htt|
```

```
290  703A2F2F 7777772E  63657274 2E64652F      |p://www.cert.de/|
2A0  63726C73 300E0607  02820601 0A0C0004      |crls0...........|
2B0  030101FF 301A0605  2B240803 01041118      |....0...+$......|
2C0  0F313939 38303631  38313230 3030305A      |.19980618120000Z|
2D0  30430605 2B240803  03043A13 384B5620      |0C..+$....:.8KV |
2E0  48657373 656E3A20  5A756C61 7373756E      |Hessen: Zulassun|
2F0  6720616C 73204172  7A743A20 5A756C61      |g als Arzt: Zula|
300  7373756E 67736E75  6D6D6572 3A203130      |ssungsnummer: 10|
310  30303031 30300906  052B0E03 021D0500      |000100...+......|
320  03820101 001BD409  8EF80D4E 7E7305CA      |...........N~s..|
330  98525DA1 72515639  AB4DDA2E 864EE93E      |.R].rQV9.M...N.>|
340  FD95F376 CB57DC78  8B9C8025 34534440      |...v.W.x...%4SD@|
350  78DF4DC9 706854EC  12BD1236 C103E83A      |x.M.phT....6...:|
360  E49835FC B5BE1902  B9C9EEC5 DA5EB1BE      |..5.........^..|
370  3D1B3643 EF1545E9  0A12D1EF A7A2A8C1      |=.6C..E.........|
380  BB4B1E2F A454D65F  2EF303F5 F982EA5D      |.K./.T._.......]|
390  B0730208 F1A39E0A  419DD359 42239408      |.s......A..YB#..|
3A0  22AE6FF0 3EDB879F  9C9D0542 EE43CF6A      |".o.>......B.C.j|
3B0  22D7DC4F 5AF52407  B9219B0F B4458362      |"..OZ.$..!...E.b|
3C0  A4B02B60 633CBC30  C46F7CF1 ADF1258A      |..+`c<.0.o|...%.|
3D0  D768177E 5050AA3D  7C14C06F 4823C6C4      |.h.~PP.=|..oH#..|
3E0  E9F5D48C 719E07C6  C80EC034 AD6DE3CB      |....q......4.m..|
3F0  71924C1F CF97F817  589F1855 A1B44ADF      |q.L.....X..U..J.|
400  1C2905DD 9E8D1202  85A5B317 82B2A25B      |.).............[|
410  41095A79 2C184D39  8D23DBBA 1DF76377      |A.Zy,.M9.#....cw|
420  59B27918 B9                               |Y.y..           |
```

Aus dem Offset des Hexdumps läßt sich die Speichergröße des Teilnehmerzertifikates als ('424'H= 4*256+2*16+4=) 1060 Bytes ablesen.

ANHANG V ASN.1 DEFINITIONEN

Dieser Abschnitt enthält eine Zusammenfassung aller ASN.1-Definitionen in alphabetischer Reihenfolge, die in diesem Dokument benutzt werden.

```
AccessDescription   ::= SEQUENCE {
    accessMethod            OBJECT IDENTIFIER,
    accessLocation          GeneralName }

admission           EXTENSION ::= {
    SYNTAX                  AdmissionSyntax
    IDENTIFIED BY           id-sigi-at-admission }

Admissions          ::= SEQUENCE {
    admissionAuthority      [0]  GeneralName OPTIONAL,
    namingAuthority         [1]  NamingAuthority OPTIONAL,
    professionInfos         SEQUENCE OF ProfessionInfo }

AdmissionSyntax     ::= SEQUENCE {
    admissionAuthority      GeneralName OPTIONAL,
    contentsOfAdmissions    SEQUENCE OF Admissions }

Algorithmidentifier ::= SEQUENCE {
    algorithm               OBJECT IDENTIFIER,
    parameters              ANY DEFINED BY algorithm OPTIONAL }

atAdmission         ATTRIBUTE ::=  {
    WITH SYNTAX             AdmissionSyntax
    SINGLE VALUE
    ID                      id-sigi-at-admission }

atDeclarationOfMajority ATTRIBUTE  ::=  {
    WITH SYNTAX             DeclarationOfMajoritySyntax
    SINGLE VALUE
    ID                      id-sigi-at-declarationOfMajority }

atMonetaryLimit     ATTRIBUTE      ::=  {
    WITH SYNTAX             MonetaryLimitSyntax
    SINGLE VALUE
    ID                      id-sigi-at-monetaryLimit }

atProcuration       ATTRIBUTE ::=  {
    WITH SYNTAX             ProcurationSyntax
    SINGLE VALUE
    ID                      id-sigi-at-procuration }

atRestriction       ATTRIBUTE ::=  {
    WITH SYNTAX                    RestrictionSyntax
    SINGLE VALUE
    ID                             id-sigi-at-restriction }

AttCertValidityPeriod   ::=   SEQUENCE {
    notBeforeTime           GeneralizedTime,
    notAfterTime            GeneralizedTime }

ATTRIBUTE           ::= CLASS {
    &id                     OBJECT IDENTIFIER UNIQUE,
    &Type }
WITH SYNTAX {
    SYNTAX                  &Type
    IDENTIFIED BY           &id }

Attribute           ::= SEQUENCE {
    type                    AttributeType,
```

```
    values                      SET OF AttributeValue
AttributeCertificate    ::=   SEQUENCE {
    tbsAttributeCertificate  TBSAttributeCertificate,
    signatureAlgorithm       AlgorithmIdentifier,
    signature                BIT STRING }
AttributesSyntax    ::= SEQUENCE SIZE (1..MAX) OF Attribute
AttributeType       ::= ATTRIBUTE.&id
AttributeType       ::= OBJECT IDENTIFIER
AttributeTypeAndValue   ::=   SEQUENCE {
    type                     AttributeType,
    value                    AttributeValue }
AttributeValue      ::= ANY DEFINED BY AttributeType
AttributeValue      ::= ATTRIBUTE.&Type
authorityInfoAccess EXTENSION ::= {
WITH SYNTAX {
    SYNTAX                   AuthorityInfoAccessSyntax
    IDENTIFIED BY            id-ce-authorityInfoAccess }
AuthorityInfoAccessSyntax     ::=
    SEQUENCE SIZE (1..MAX) OF AccessDescription
authorityKeyIdentifier EXTENSION   ::= {
WITH SYNTAX {
    SYNTAX                   AuthorityKeyIdentifier
    IDENTIFIED BY            id-ce-authorityKeyIdentifier }
AuthorityKeyIdentifier  ::=   SEQUENCE {
    keyIdentifier                [0] KeyIdentifier   OPTIONAL,
    authorityCertIssuer          [1] GeneralNames    OPTIONAL,
    authorityCertSerialNumber    [2] CertificateSerialNumber OPTIONAL }
BaseDistance        ::= INTEGER (0..MAX)
basicConstraints EXTENSION    ::= {
WITH SYNTAX {
    SYNTAX                   BasicConstraintsSyntax
    IDENTIFIED BY            id-ce-basicConstraints }
BasicConstraintsSyntax  ::=   SEQUENCE {
    cA                       BOOLEAN DEFAULT FALSE,
    pathLenConstraint        INTEGER (0..MAX) OPTIONAL }
Certificate         ::= SEQUENCE {
    tbsCertificate           TBSCertificate,
    signatureAlgorithm       AlgorithmIdentifier,
    signature                BIT STRING }
certificatePolicies EXTENSION ::= {
WITH SYNTAX {
    SYNTAX                   CertificatePoliciesSyntax
    IDENTIFIED BY            id-ce-extKeyUsage }
CertificatePoliciesSyntax     ::=
    SEQUENCE SIZE (1..MAX) OF PolicyInformation
CertificateSerialNumber ::=   INTEGER
CertPolicyId        ::= OBJECT IDENTIFIER
CRLDistPointsSyntax     ::=   SEQUENCE SIZE (1..MAX) OF
                              DistributionPoint
```

```
cRLDistributionPoints EXTENSION    ::= {
WITH SYNTAX {
    SYNTAX                  CRLDistPointsSyntax
    IDENTIFIED BY           id-ce- cRLDistributionPoints }

dateOfCertGen       EXTENSION ::= {
    SYNTAX                  DateOfCertGenSyntax
    IDENTIFIED BY           id-sigi-at-dateOfCertGen }

DateOfCertGenSyntax     ::=   GeneralizedTime

declarationOfMajority   EXTENSION  ::= {
    SYNTAX                  DeclarationOfMajoritySyntax
    IDENTIFIED BY           id-sigi-at-declarationOfMajority }

DeclarationOfMajoritySyntax   ::= CHOICE {
    notYoungerThan          [0] IMPLICIT INTEGER,
    fullAgeAtCountry        [1] IMPLICIT SEQUENCE {
      fullAge               BOOLEAN DEFAULT TRUE,
      country               PrintableString (SIZE(2)) DEFAULT "DE" }
    dateOfBirth             [2] GeneralizedTime }

DirectoryString     ::= CHOICE {
    printableString         PrintableString (SIZE (1..maxSize))
    teletexString           TeletexString (SIZE (1..maxSize))
    bmpString               BMPString (SIZE (1..maxSize))
    universalString         UniversalString (SIZE (1..maxSize)) }

DistributionPoint   ::= SEQUENCE {
    distributionPoint       [0]  DistributionPointName OPTIONAL,
    reasons                 [1]  ReasonFlags OPTIONAL,
    cRLIssuer               [2]  GeneralNames OPTIONAL }

DistributionPointName   ::=   CHOICE {
    fullName                [0]  GeneralNames,
    nameRelativeToCRLIssuer [1]  RelativeDistinguishedName }

dsa ALGORITHM PARAMETER DSAParameters   ::=  {algorithm 12}

dsaCommon ALGORITHM PARAMETER NULL ::=  {algorithm 20}

DSAParameters       ::= SEQUENCE {
    prime1                  INTEGER,
    prime2                  INTEGER,
    base                    INTEGER }

DSAPublicKey        ::= INTEGER

ECDSAPublicKey      ::= OCTET STRING

Ecdsa-SigValue      ::= SEQUENCE {
    r                       INTEGER,
    s                       INTEGER }

EDIPartyName        ::= SEQUENCE {
    nameAssigner            [0]  DirectoryString OPTIONAL,
    partyName               [1]  DirectoryString }

EXTENSION           ::= CLASS {
    &id                     OBJECT IDENTIFIER UNIQUE,
    &ExtType }
WITH SYNTAX {
    SYNTAX                  &ExtnType
    IDENTIFIED BY           &id }

Extension           ::= SEQUENCE {
    extnId                  OBJECT IDENTIFIER,
    critical                BOOLEAN DEFAULT FALSE,
```

```
    extnValue                   OCTET STRING }
Extensions                ::= SEQUENCE (1..MAX) OF Extension

extKeyUsage EXTENSION     ::= {
WITH SYNTAX {
    SYNTAX                      ExtKeyUsageSyntax
    IDENTIFIED BY               id-ce-extKeyUsage }

ExtKeyUsageSyntax         ::= SEQUENCE SIZE (1..MAX) OF KeyPurposeId

GeneralName               ::= CHOICE {
    otherName                   [0]  OTHER-NAME,
    rfc822Name                  [1]  IA5String,
    dNSName                     [2]  IA5String,
    x400Address                 [3]  ORAddress,
    directoryName               [4]  Name,
    ediPartyName                [5]  EDIPartyName,
    uniformResourceIdentifier   [6]  IA5String,
    iPAddress                   [7]  OCTET STRING,
    registeredID                [8]  OBJECT IDENTIFIER }

GeneralNames              ::= SEQUENCE SIZE (1..MAX) OF GeneralName

GeneralSubtree            ::= SEQUENCE {
    base                        GeneralName,
    minimum                     [0]  BaseDistance DEFAULT 0,
    maximum                     [1]  BaseDistance OPTIONAL }

GeneralSubtrees           ::= SEQUENCE SIZE (1..MAX) OF
    GeneralSubtree

iCCSN                     EXTENSION ::= {
    SYNTAX                      ICCSNSyntax
    IDENTIFIED BY               id-sigi-at-iCCSN }

ICCSNSyntax               ::= IMPLICIT OCTETSTRING (SIZE(15..23))

issuerAltName EXTENSION   ::= {
WITH SYNTAX {
    SYNTAX                      IssuerAltName
    IDENTIFIED BY               id-ce-issuerAltName }

IssuerAndSerial           ::= SEQUENCE{
    issuer                      GeneralName
    serial                      CertificateSerialNumber }

IssuerAltName             ::= GeneralNames

IssuerSerial              ::= SEQUENCE {
    issuer                      GeneralNames,
    serial                      CertificateSerialNumber,
    issuerUID                   UniqueIdentifier OPTIONAL }

KeyIdentifier                 ::=   OCTET STRING

KeyPurposeId              ::= OBJECT IDENTIFIER

KeySize                   ::= INTEGER

keyUsage EXTENSION        ::= {
WITH SYNTAX {
    SYNTAX                      KeyUsage
    IDENTIFIED BY               id-ce-keyUsage }

KeyUsage                  ::= BIT STRING {
    digitalSignature            (0),
    nonRepudiation              (1),
    keyEncipherment             (2),
```

```
    dataEncipherment          (3),
    keyAgreement              (4),
    keyCertSign               (5),
    cRLSign                   (6),
    encipherOnly              (7),
    decipherOnly              (8) }

liabilityLimitationFlag EXTENSION  ::= {
WITH SYNTAX {
    SYNTAX                    BOOLEAN DEFAULT FALSE
    IDENTIFIED BY             certExtensionLiabilityLimitationFlag }

monetaryLimit        EXTENSION ::= {
    SYNTAX                    MonetaryLimitSyntax
    IDENTIFIED BY             id-sigi-at-monetaryLimit

MonetaryLimitSyntax ::= SEQUENCE {
    currency                  PrintableString (SIZE(3)),
    amount                    INTEGER,
    exponent                  INTEGER }

Name                 ::= CHOICE { RDNSequence }

nameConstraints EXTENSION     ::= {
WITH SYNTAX {
    SYNTAX                    NameConstraintsSyntax
    IDENTIFIED BY             id-ce-nameConstraints }

NameConstraintsSyntax   ::=   SEQUENCE {
    permittedSubtrees         [0]  GeneralSubtrees OPTIONAL,
    excludedSubtrees          [1]  GeneralSubtrees OPTIONAL }

NameOrPseudonym      ::= CHOICE {
    surAndGivenName           SEQUENCE {
      surName                 DirectoryString,
      givenName               SEQUENCE OF DirectoryString },
    pseudoNym                 DirectoryString }

NamingAuthority      ::= SEQUENCE {
    namingAuthorityId         OBJECT IDENTIFIER OPTIONAL,
    namingAuthorityUrl        IA5String OPTIONAL,
    namingAuthorityText       DirectoryString OPTIONAL }

OTHER-NAME           ::= SEQUENCE {
    type-id                   OBJECT IDENTIFIER,
    value                     [0]  EXPLICIT ANY DEFINED BY type-id }

PersonalData         ::= SEQUENCE {
    nameOrPseudonym           NameOrPseudonym,
    nameDistinguisher         [0]  INTEGER             OPTIONAL,
    dateOfBirth               [1]  DirectoryString     OPTIONAL,
    placeOfBirth              [2]  DirectoryString     OPTIONAL,
    gender                    [3]  PrintableString     OPTIONAL,
    postalAddress             [4]  DirectoryString     OPTIONAL }

pKReference          EXTENSION ::= {
    SYNTAX                    PKReferenceSyntax
    IDENTIFIED BY             id-sigi-at-pKReference }

PKReferenceSyntax    ::= OCTETSTRING (SIZE(20))

policyConstraints EXTENSION   ::= {
WITH SYNTAX {
    SYNTAX                    PolicyConstraintsSyntax
    IDENTIFIED BY             id-ce-policyConstraints }

PolicyConstraints         ::=   SEQUENCE {
```

```
    requireExplicitPolicy           [0]   SkipCerts OPTIONAL,
    inhibitPolicyMapping            [1]   SkipCerts OPTIONAL }

PolicyConstraintsSyntax ::=
    SEQUENCE SIZE (1..MAX) OF PolicyConstraints

PolicyInformation   ::= SEQUENCE {
    policyIdentifier        CertPolicyId,
    policyQualifiers        SEQUENCE SIZE (1..MAX) OF
                            PolicyQualifierInfo OPTIONAL}

policyMappings EXTENSION ::= {
WITH SYNTAX {
    SYNTAX                  PolicyMappingsSyntax
    IDENTIFIED BY           id-ce-policyMappings

PolicyMappingsSyntax    ::=   SEQUENCE SIZE (1..MAX) OF
SEQUENCE {
    issuerDomainPolicy      CertPolicyId,
    subjectDomainPolicy     CertPolicyId }

PolicyQualifierId   ::= OBJECT IDENTIFIER

PolicyQualifierInfo ::= SEQUENCE {
    policyQualifierId       PolicyQualifierId,
    qualifier               ANY DEFINED BY policyQualifierId }

privateKeyUsagePeriod EXTENSION    ::= {
WITH SYNTAX {
    SYNTAX                  PrivateKeyUsagePeriod
    IDENTIFIED BY           id-ce-privateKeyUsagePeriod }

PrivateKeyUsagePeriod   ::=   SEQUENCE {
    notBefore               [0]  GeneralizedTime OPTIONAL,
    notAfter                [1]  GeneralizedTime OPTIONAL }

procuration          EXTENSION ::= {
    SYNTAX                  ProcurationSyntax
    IDENTIFIED BY           id-sigi-at-procuration }

ProcurationSyntax   ::= SEQUENCE OF {
    country                 PrintableString (SIZE(2)) OPTIONAL,
    typeOfSubstitution      DirectoryString OPTIONAL,
    signingFor              SigningFor }

ProfessionInfo      ::= SEQUENCE OF {
    namingAuthority         [0]  NamingAuthority OPTIONAL,
    professionItems         SEQUENCE OF DirectoryString,
    registrationNumber      PrintableString OPTIONAL,
    addProfessionInfo       OCTET STRING OPTIONAL }

RDNSequence         ::= SEQUENCE OF RelativeDistinguishedName

ReasonFlags         ::= BIT STRING {
    unused(0),
    keyCompromise(1),
    cACompromise(2),
    affiliationChanged(3),
    superseded(4),
    cessationOfOperation (5),
    certificateHold(6) }

RelativeDistinguishedName     ::=  SET OF AttributeTypeAndValue

restriction          EXTENSION ::= {
    SYNTAX                  RsestrictionSyntax
    IDENTIFIED BY           id-sigi-at-restriction }
```

```
RestrictionSyntax   ::= DirectoryString

rsa ALGORITHM PARAMETER KeySize    ::=  {encryptionAlgorithm 1}

rsaEncryption ALGORITHM PARAMETER NULL  ::=  { pkcs-1 1 }

RSAPublicKey        ::= SEQUENCE {
   modulus                  INTEGER,
   publicExponent           INTEGER }

rsaSignature ALGORITHM PARAMETER NULL   ::=  { algorithm 11 }

SigningFor          ::= CHOICE {
   thirdPerson              GeneralName,
   cerRef                   IssuerAndSerial }

SkipCerts                ::=   INTEGER (0..MAX)

subjectAltName EXTENSION ::= {
WITH SYNTAX {
   SYNTAX                   SubjectAltName
   IDENTIFIED BY            id-ce-subjectAltName }

SubjectAltName      ::= GeneralNames

subjectDirectoryAttributes EXTENSION    ::= {
WITH SYNTAX {
   SYNTAX                   AttributesSyntax
   IDENTIFIED BY            id-ce-subjectDirectoryAttributes } }

subjectKeyIdentifier EXTENSION     ::= {
WITH SYNTAX {
   SYNTAX                   SubjectKeyIdentifier
   IDENTIFIED BY            id-ce-subjectKeyIdentifier }

SubjectKeyIdentifier    ::=   KeyIdentifier

SubjectPublicKeyInfo    ::=   SEQUENCE {
   algorithm                AlgorithmIdentifier,
   subjectPublicKey         BIT STRING }

TBSAttributeCertificate ::=   SEQUENCE {
   version                  Version DEFAULT v1,
   subject                  CHOICE {
     baseCertificateID      [0]  IssuerSerial,
     subjectName            [1]  GeneralNames },
   issuer                   GeneralNames,
   signature                AlgorithmIdentifier,
   serialNumber             CertificateSerialNumber,
   attrCertValidityPeriod   AttCertValidityPeriod,
   attributes               SEQUENCE OF Attribute,
   issuerUniqueID           UniqueIdentifier OPTIONAL,
   extensions               Extensions OPTIONAL }

TBSCertificate      ::= SEQUENCE {
   version                  [0]  EXPLICIT Version DEFAULT v1,
   serialNumber             CertificateSerialNumber,
   signature                AlgorithmIdentifier,
   issuer                   Name,
   validity                 Validity,
   subject                  Name,
   subjectPublicKeyInfo     SubjectPublicKeyInfo,
   issuerUniqueID           [1]  IMPLICIT UniqueIdentifier OPTIONAL,
   subjectUniqueID          [2]  IMPLICIT UniqueIdentifier OPTIONAL,
   extensions               [3]  EXPLICIT Extensions Optional }

Time                ::= CHOICE {
```

```
    utcTime                 UTCTime,
    generalizedTime         GeneralizedTime }
UniqueIdentifier    ::= BIT STRING
Validity            ::= SEQUENCE {
    notBefore               Time,
    notAfter                Time }
Version             ::= INTEGER { v1(0), v2(1), v3(2) }
```

Objektbezeichner

```
algorithm OBJECT IDENTIFIER ::= { 1 3 14 3 2 }
ansi-x9-62 OBJECT IDENTIFIER ::= { 1 2 840 10045 }
certExtensionLiabilityLimitationFlag OBJECT IDENTIFIER ::=
    { 0 2 262 1 10 12 0 }
certificateExtension OBJECT IDENTIFIER ::= { 2 5 29 }
ecamvSign OBJECT IDENTIFIER ::= { 1 3 36 3 3 2 }
ecdsa-with-sha1 OBJECT IDENTIFIER ::= { 1 2 840 10045 1 }
encryptionAlgorithm OBJECT IDENTIFIER ::= { 2 5 8 1 }
id-ad OBJECT IDENTIFIER ::= { 1 3 6 1 5 5 7 48 }
id-ad-caIssuers OBJECT IDENTIFIER ::= { 1 3 6 1 5 5 7 48 2 }
id-ad-ocsp OBJECT IDENTIFIER ::= { 1 3 6 1 5 5 7 48 1 }
id-ce OBJECT IDENTIFIER ::= { 2 5 29 }
id-ce-authorityKeyIdentifier OBJECT IDENTIFIER ::= {2 5 29 35}
id-ce-basicConstraints OBJECT IDENTIFIER ::= { 2 5 29 19 }
id-ce-certificatePolicies OBJECT IDENTIFIER ::= { 2 5 29 32 }
id-ce-cRLDistributionPoints OBJECT IDENTIFIER ::= {2 5 29 31 }
id-ce-extKeyUsage OBJECT IDENTIFIER ::= { 2 5 29 37 }
id-ce-issuerAltName OBJECT IDENTIFIER ::= { 2 5 29 18 }
id-ce-keyUsage OBJECT IDENTIFIER ::= { 2 5 29 15 }
id-ce-nameConstraints OBJECT IDENTIFIER ::= { 2 5 29 30 }
id-ce-policyConstraints OBJECT IDENTIFIER ::= { 2 5 29 36 }
id-ce-policyMappings OBJECT IDENTIFIER ::= { 2 5 29 33 }
id-ce-privateKeyUsagePeriod OBJECT IDENTIFIER ::= { 2 5 29 16}
id-ce-subjectAltName OBJECT IDENTIFIER ::= { 2 5 29 17 }
id-ce-subjectDirectoryAttributes OBJECT IDENTIFIER::= {2 5 29 9}
id-ce-subjectKeyIdentifier OBJECT IDENTIFIER ::= { 2 5 29 14}
id-ecPublicKey OBJECT IDENTIFIER ::= { 1 2 840 10045 2 1 }
id-kp OBJECT IDENTIFIER ::= { 1 3 6 1 5 5 7 3 }
id-kp-time-Stamping OBJECT IDENTIFIER ::= { 1 3 6 1 5 5 7 3 7 }
id-pe OBJECT IDENTIFIER ::= { 1 3 6 1 5 5 7 1 }
id-pe-authorityInfoAccess OBJECT IDENTIFIER ::= {1 3 6 1 5 5 7 1 1}
```

id-pkix OBJECT IDENTIFIER ::= { 1 3 6 1 5 5 7 }
id-publicKeyType OBJECT IDENTIFIER ::= { 1 2 840 10045 2 }
id-sigi OBJECT IDENTIFIER ::= { 1 3 36 8 }
id-sigi-at OBJECT IDENTIFIER ::= { 1 3 36 8 3 }
id-sigi-at-admission OBJECT IDENTIFIER ::= { 1 3 36 8 3 3 }
id-sigi-at-dateOfCertGen OBJECT IDENTIFIER ::= { 1 3 36 8 3 1}
id-sigi-at-declarationOfMajority OBJECT IDENTIFIER ::= { 1 3 36 8 3 5 }
id-sigi-at-iCCSN OBJECT IDENTIFIER ::= { 1 3 36 8 3 6 }
id-sigi-at-monetaryLimit OBJECT IDENTIFIER ::= { 1 3 36 8 3 4}
id-sigi-at-pKReference OBJECT IDENTIFIER ::= { 1 3 36 8 3 7 }
id-sigi-at-procuration OBJECT IDENTIFIER ::= { 1 3 36 8 3 2 }
id-sigi-at-restriction OBJECT IDENTIFIER ::= { 1 3 36 8 3 8 }
id-sigi-kp OBJECT IDENTIFIER ::= { 1 3 36 8 2 }
id-sigi-kp-directoryService OBJECT IDENTIFIER ::= {1 3 36 8 2 1 }
id-sigi-on OBJECT IDENTIFIER ::= { 1 3 36 8 4 }
id-sigi-on-personalData OBJECT IDENTIFIER ::= { 1 3 36 8 4 1 }
pkcs-1 OBJECT IDENTIFIER ::= { 1 2 840 113549 1 1 1 }

ANHANG VI ABKÜRZUNGEN UND BEGRIFFE

Bemerkung

Begriffe und Definitionen aus dem Bereich der Sichterheitstechnik werden international in englischer Sprache formuliert. Die folgendene Tabelle enthält deutsche Übersetzungen zu den wichtigsten englischen Fachausdrücken und eine Erläuterung von häufig benutzten Abkürzungen. Formale Namen von technischen Objekten, die für die Verarbeitung von Systemen benötigt werden und für die es eine eigene formale Syntax gibt, werden in der Tabelle durch Kursivschrift hervorgehoben.

Tabelle 53: Abkürzungen und Begriffe

ABKÜRZUNG	ENGLISCH	DEUTSCH
*	wild card	Platzhaltersymbol für Teilstrings
||		Konkatenierung von Daten
	admission	BSI-spezifische Erweiterung für Zulassungsinformation
	algorithm identifier *AlgorithmIdentifier*	Eindeutiger Bezeichner des kryptographischen Algorithmus, der von einer Zertifizierungsstelle zum Signieren eines Zertifikates benutzt wird
	alternative subject name *subjectAltName*	Zertifikatserweiterung, die einen oder mehrere alternative Namen für Zertifikatsinhaber enthält, durch die zusätzliche Identitäten an den Zertifikatsinhaber gebunden werden
ANS	american national standard	US-Normen
ANSI	american national standards institute	US-Normungsgremium
ASN.1	abstract syntax notation one	abstrakte Notation zur Beschreibung von Datentypen und Datenwerten
	atAdmission	BSI-spezifisches Attribut für Zulassungsinformationen
	atMonetaryLimit	BSI-spezifisches Attribut für monetäre Beschränkungen
	*atProcuration**t*	BSI-spezifisches Attribut für Vertretungsmacht
	attributes	Feld eines Attributzertifkates, das die eigentlichen Nutzdaten eines Attributzertifikates enthält, die syntaktisch in der Form von X.500-Verzeichnisdienstattributen aufgebaut sind
	authority key identifier *authorityKeyIdentifier*	Feld einer Zertifikatserweiterung, das zur Identifizierung eines bestimmten öffentlichen Schlüssels einer Zertifizierungsstelle dient
	base certificate identifier *baseCertificateID*	Feld eines Attribut-Zertifikates, durch das – alternativ zum subject-Feld – indirekt der Name des Zertifikatsinhabers über den Namen der Zertifizierungsstelle, die das Zertifikat ausgestellt hat, und die zugehörige Seriennummer des Zertifikates angeben werden kann

ABKÜRZUNG	ENGLISCH	DEUTSCH
	basic constraints *basicConstraints*	Zertifikatserweiterung, die anzeigt, ob ein Zertifikatsinhaber in der Rolle als Zertifizierungsstelle auftreten kann und ob eine Bechränkung der Zertifizierungspfadlänge vorliegt
BER	basic encoding rules	Variante von ASN.1-Kodierungsvorschriften, mehrdeutig
BSI		Bundesamt für Sicherheit in der Informationstechnik
C	country	Länderbezeichnung nach ISO 3166, Attribut in *distinguished name*-Typen
CA	certification authority	Zertifizierungsstelle
CCITT	comité consultatif internatio-nal pour télégraphique et téléphonique (international consultative committee for telephone and telegraph	
	certificate public key certificate	Zertifikat, gemäß X.509 digital signierte Datenstruktur, welche die Bindung der Identiät eines Zertifikatsinhabers zu einem öffentlichen Schlüssel herstellt
	certificate and CRL repository	Ablage für Zertifikate und Zertifikats-Sperrlisten
	certificate and CRL retrieval	Suche von Zertifikaten und Zertifikats-Sperrlisten
	certificate policies *certificatePolicies*	Zertifikatserweiterung, die zur Anzeige der Verfahrensweisen bei der Erstellung eines Zertifikates durch eine Zertifizierungsstelle und der Zwecke, die mit dem Zertifikat verbunden sind, dient
	certificate renewal	Erneuerung von Zertifikaten
	certificate revocation	Sperren von Zertifikaten
	certificate user	Zertifikatsbenutzer: eine Person oder ein System, das Zertifikate benutzt
	certification path	Zertifizierungsweg: Eine geordnete Folge von Zertifikaten, beginnend mit dem Zertifikat, dessen öffentlichen Schlüssel ein Benutzer kennt, bis hin zu einem Zertifikat, dessen öffentlicher Schlüssel von einem Benutzer zu validieren ist
	certification request	Zertifikatsanforderung
CHA	certificate holder authorization	Rechte von Zertifikatsinhabern
CHR	card holder reference	Referenzierung des öffentlichen Schlüssels einer Zertifizierungsstelle
	client	Kunde, Kommunikationspartner, Teilnehmer, Anwendungs-programm
CN	common name	Personenname, Attribut in *distinguished name*-Typen
	confidentiality key management certificate	Zertifikat für vertrauliche Schlüsselverwaltung
CPI	certificate profile identifier	Kennzeichnung des Aufbaus von Authentisierungszertifikaten

ABKÜRZUNG	ENGLISCH	DEUTSCH
CPS	certification practise statement	spezielles *PolicyQualifiers*-Merkmal, das veröffentlichte Aussagen einer Zertifizierungsstelle über die Erfahrungen enthält, die sie bei der Erstellung von Zertifikaten gemacht hat
	critical	Zertifikatsfeld, das die Wichtigkeit einer Zertifikatserweiterung anzeigt
CRL	certificate revocation list	Liste zurückgezogener Zertifikate, Sperrliste
	CRL diestribution points *cRLDistribututionPoints*	Zertifikatserweiterung, die Informationen enthält, die zur Beschaffung von Sperrlisten dienen
	cross-certification	gegenseitige Zertifizierung basierend auf einem Netzwerk-Vertrauensmodell
CV	card verifiable certificates	Zertifikate zur Authentisierung von Terminal und Chipkarte
DAP	directory access protocol	Protokoll für den Zugriff auf ein X.500-Verzeichnis
	data encipherment *dataEncipherment*	Bit im Feld der Zertifikatserweiterung *keyUsage*, das die Schlüsselnutzungsart " Verschlüsselung von Nutzdaten" anzeigt
	dateOfCertGen	BSI-spezifische Erweiterung für das Erstellungsdatum eines Zertifikates
DC	domain component	Teilname eines Domänennamens, Attribut in *distinguished name*-Typen
DE	data element	Datenelement, Chipkarten
	decipher only *decipherOnly*	Bit im Feld der Zertifikatserweiterung *keyUsage*, das die Schlüsselnutzungsart: "Schlüsselaustauschverfahren zur alleinigen Entschlüsselung von Daten" anzeigt
DER	distinguished encoding rules	Variante von ASN.1-Kodierungsvorschriften
	digital signature *digitalSignature*	Bit im Feld der Zertifikatserweiterung *keyUsage*, das die Schlüsselnutzungsart "allgemeine Prüfung digitaler Signaturen zur Authentifizierung" anzeigt
	digital signature public key certificate	Signaturzertifikat basierend auf öffentlichen Schlüsseln
DIN		Deutsches Institut für Normung e.V.
DIR	directory service	Verzeichnisdienst
	directory attributes of a subject *subjectDirectoryAttributes*	Zertifikatserweiterung, die zur Bereitstellung von Verzeichnis-Attributwerten für einen Zertifikatsinhaber dient
	distinguished name *distinguishedName*	eindeutiger Name, der nach X.500 definiert wird
DNS	domain name system	Methode zur Konvertierung zwischen Namen und Adressen im Internet
DO	data object	Datenobjekt, Chipkarten
DSA	digital signature algorithm	asymmetricher Verschlüsselungsalgorithmus zum Generieren digitaler Signaturen

ABKÜRZUNG	ENGLISCH	DEUTSCH
DSI	digital signature input	Signatur-Verschlüsselungsformate
DSS	digital signature standard	von Nist entwickelter Standard für digitale Signaturen bestehend aus DSA und SHA-1
ECDSA	elliptic curve digital signature algorithm	Signaturalgorithmus basierend auf elliptischen Kurven
	end entity	Endanwender: Person als Anwender von Zertifikaten oder Endanwendersystem, das der Inhaber eines Zertifikates ist.
	encipher only *encipherOnly*	Bit im Feld der Zertifikatserweiterung *keyUsage*, das die Schlüsselnutzungsart "Schlüsselaustauschverfahren zur alleinigen Verschlüsselung von Daten" anzeigt
	explicit text *explictText*	Teilfeld des *unotice*-Merkmalanzeigefeldes, das den Namen einer Organisation sowie einen Text enthält, der eine spezielle Aussage dieser Organisation darstellt
	extended key usage *extKeyUsage*	Zertifikatserweiterung, die zur Definition von anwendungsabhängigen Nutzungsarten von zertifizierten Schlüsseln, zusätzlich oder alternativ zum *keyUsage*-Erweiterungsfeld, benutzt werden kann
	extension value *extnValue*	Zertifikatsfeld, das den Wert einer Zertifikatserweiterung enthält.
	extensions	optionales Zertifikatsfeld, das weitere Zertifikatserweiterungen enthält
	extensions identifier *extId*	Zertifikatsfeld, das den Objektbezeichner einer Zertifikatserweiterung enthält
FTP	file transfer protocol	Filetransferprotokoll
	generalized time format *GeneralizedTime*	ASN.1-Typ für allgemeine Datums- und Zeitformate
GMT	Greenwich Mean Time	Greenwich-Zeit
HTML	hyper text markup language	auf SGML basierende Sprache zur Beschreibung von Hypertext-Dokumenten
HTTP	hypertext transfer protocol	Protokoll zum Laden von Dokumenten und/oder beschreibenden Kopfinformationen des WWW
ICC	integrated circuit card	Chipkarte
ICCSN	integrated circuit serial number	Seriennummer von Chipkarten
IEC	international electrotechnical commission	internationales Normungsgremium auf dem Gebiet der Elektrik und Elektronik
IETF	internet engineering task force	verantwortliches Gremium zur Entwicklung von Internet-Standards
IFD	interface device	Schnittstelle, Chipkarte
	inhibition of policy mapping *inhibitPolicyMapping*	optionalesFeld der *policyConstraints*-Zertifikatserweiterung, das die Anzahl von weiteren Zertifikaten enthält, die

ABKÜRZUNG	ENGLISCH	DEUTSCH
		Zertifizierungspfad folgen können, ehe eine Anerkennung fremder Zertifizierungsrichtlinien verboten ist
IP	internet protocol	Übertragungsprotokoll der Netzwerkebene
IPSEC	internet protocol security	internet protocol, das Authentizität, Vertraulichkeit und Integrität gewährleistet
ISO	international organization for standardization	internationales Standardisierungsgremium
	isssuer alternative name *issuertAltName*	Zertifikatserweiterung, die einen oder mehrere alternative Namen für den Ersteller eines Zertifikates oder einer Zertifikats-Sperrliste enthält, durch die zusätzliche Identitäten aus dem Internetbereich an die Zertifizierungsstelle gebunden werden
	issuer	Zertifikatsfeld, das einen eindeutigen Namen der ausstellenden Zertifizierungsstelle enthält
	issuer domain policy *issuerDomainPolicy*	Teilfeld der *PolicyMappings*-Zertifikatserweiterung, die einer Inhaberzertifizierungsstelle Informationen über die Sicherheitsrichtlinien der Erstellerzertifizierungstelle liefert,
	issuer unique identifier *issuerUniqueIdentifier*	optionales Zertifikatsfeld, das einen eindeutigen Bezeichner für die ausstellende Zertifikatserstelle enthält
ITU	international telecommunication union	Standardisierungsbehörde der UN
ITU-T	telecommunication standardization sector of ITU	Teilbereich der ITU (früher als CCITT bezeichnet), der für die Standardisierung im Telekommunikationsbereich zuständig ist.
	key agreement *keyAgreement*	Bit im Feld der Zertifikatserweiterung keyUsage, das die Schlüsselnutzungsart “Schlüsselaustauschverfahren” anzeigt
	key encipherment *keyEncipherment*	Bit im Feld der Zertifikatserweiterung keyUsage, das die Schlüsselnutzungsart “Schlüsseltransport, Schlüsselverwaltung” anzeigt
	key identifier of a subject *subjectKeyIdentifier*	Feld einer Zertifikatserweiterung, das zur Identifizierung eines bestimmten öffentlichen Schlüssels eines Zertifizikatsinhabers dient
	key management certificate	Zertifikat für Schlüsselverwaltung
	key usage *keyUsage*	Feld einer Zertifikatserweiterung, das zur Anzeige der Verwendungszwecke, des in einem Zertifikat enthaltenen Schlüssels, dient
L	locality	Angabe eine geographishen Ortes, Attribut in *distinguished name*-Typen
LDAP	lightweight directory acces protocol	Zugriffsprotokoll für Klienten auf Verzeichnisse, Alternative zu X.500
LSB	least significant bit	niederwertigstes Bit
MIME	multipurpose internet mail extensions	Internet-Standardformat für erweiterte elektronische Post

ABKÜRZUNG	ENGLISCH	DEUTSCH
MISPC	minimum interoperability specification for PKI components	Spezifikation zur Entwicklung zusammenarbeitsfähiger Verfahren und Komponenten in einer öffentlichen Sicherheitsinfrastruktur
	monetaryLimit	BSI-spezifische Erweiterung für monetäre Beschränkungen
MSB	most significant bit	höchstwertiges Bit
	name constraints *nameConstraints*	Zertifikatserweiterung, die den Namensraum anzeigt in dem Namen von Zertifikatsinhabern in aufeinanderfolgenden Zertifikaten eines Zertifizierungspfades liegen müssen
NIST	national institue of standards and technology	nationales US-Institut (früher als NBS, national bureau of standards bezeichnet), das für Normen und deren technische Anwendungen zuständig ist
	non-reputiation *nonRepudiation*	Bit im Feld der Zertifikatserweiterung keyUsage, das die Schlüsselnutzungsart “Prüfung digitaler Signaturen zur Sicherung der Verbindlichkeit von Dokumenten und/oder Aktionen” anzeigt
	not valid after *notAfter*	Zertifikatsfeld, das das Ende der Gültigkeit eines Zertifikates festlegt
	not valid before *notBefore*	Zertifikatsfeld, das den Beginn der Gültigkeit eines Zertifikates festlegt
O	organization	Bezeichnung einer Organisation, Attribut in *distinguished name*-Typen
OCSP	online certificate status protocol	Anwendungsprotokoll zur Bestimmung des aktuellen Zustandes eines digitalen Zertifikates ohne die Benutzng von Sperrlisten
OID	object identifier	Objektbezeichner
OIW	Open systems environment implementors workshop	Objektbezeichnerzweig unter dem Objektbezeichnerzweig iso(1)-identified-organization(3)-OIW(14)
ORA	organizational registration authority	Organisationsregistierungsstelle
OU	organizational unit	Bezeichnung einer untergeordneten Organisation, Atrtribut in *distinguished name*-Typen
	out-of band transaction or communication	Transaktionen oder Kommunikation, die außerhalb der zugrundeliegenden Infrastruktur abläuft
PCA	policy certification authority	Wurzelzertifizierungsstelle
PCT	private communication technology	Protokoll entwickelt von Microsoft und Visa International für sichere Kommunikation im Internet
PEM	privacy enhaunced mail	Internetstandard für sichere elektronische Post
	period of private key usage *privateKeyUsagePeriod*	Zertifikatserweiterung, die zur Festlegung von unterschiedlichen Gültigkeitsdauern von Zertifikaten und privaten Schlüsseln, die für digitale Signaturzwecke benutzt werden, dient
PK	public key	öffentlicher Schlüssel

ABKÜRZUNG	ENGLISCH	DEUTSCH
PKCS	public key crypto systems	Kryptosysteme basierend auf öffentlichen Schlüsseln
	public key cryptographic standard	RSA-Standards im Sicherheitsbereich
PKI	public key infrastructure	Sicherheitsinfrastruktur basierend auf öffentlichen Schlüsseln
PKIX	internet public key infrastructure	Internetprotokolle für die Sicherheitsinfrastruktur im Internet basierend auf öffentlichen Schlüsseln
PN	*pseudoNym*	BSI-spezifisches Attribut für Pseudonyme in *distinguished* name-Typen
	policy constraints *policyConstraints*	Zertifikatserweiterung, die zur Spezifikation von Beschränkungen dient, die zusätzlich bei der Überprüfung von Zertifizierungspfaden zu beachten sind
	policy domain of a subject *subjectDomainPolicy*	Teilfeld der *PolicyMappings*-Zertifikatserweiterung, die einer Erstellerzertifizierungstelle Informationen über die Sicherheitsrichtlinien der Inhaberzertifizierungsstelle liefert, die mit den eigenen Sicherheitsrichlinien vergleichbar und somit von ihr akzeptierbar sind.
	policy identifier *policyIdentifier*	Feld des Typs *PolicyInformation*, das einen Objektbezeichner einer bestimmten angewandten Verfahrensweise enthält
	policy information *PolicyInformation*	Feld der Zertifikatserweiterung *certificatePolicies*, das Informationen über eine bestimmte angewandte Verfahrensweise enthält
	policy mappings *PolicyMappings*	Zertifikatserweiterung, die in Zertifikaten für Zertifizierungsstellen zur Anzeige der Äquivalenz von Sicherheitsrichtlinien von unterschiedlichen Zertifizierungsstellen dient
	policy qualifiers *policyQualifiers*	optionales Feld des Typs *PolicyInformation*, das weitere Merkmale einer bestimmten angewandten Verfahrensweise enthält
	Procuration	BSI-spezifische Erweiterung für Vertretungsmacht
	public key information of a subject *subjectPublicKeyInfo*	Zertifikatsfeld, das den öffentlichen Schlüssel des Zertifkatsinhabers enthält
RA	registration authority	Registrierungsstelle, an die eine Zertifizierungsstelle bestimmte Verwaltungsaufgaben delegieren kann
RCA	root CA	Wurzelzertifizierungsinstanz, zuständige Behörde
	reference to notice *noticeRef*	Teilfeld des *unotice*-Merkmalanzeigefeldes, das den Namen einer Organisation sowie einen numerischen Textverweis enthält, der auf eine spezielle Aussage dieser Organisation hinweist, die als Text vorbereitet worden ist
RegTP		Regulierungsbehörde für Telekommunikation und Post

ABKÜRZUNG	ENGLISCH	DEUTSCH
	required explicit policies *requireExplicitPolicy*	optionalesFeld der *policyConstraints*-Zertifikatserweiterung, das die Anzahl von weiteren Zertifikaten enthält, die im Zertifizierungspfad folgen können, ehe bestimmte, explizite Sicherheitsrichtlinien benötigt werden
	respository	Ablage, Verwahrungsort, Verzeichnis
		System oder ein Verbund verteilter Systeme, die Zertifikate und Zertifikats-Sperrlisten speichern und deren Verteilung an Endanwender unterstützen
RFC	request for comment	Internet-Report
RIPEMD-160		Von H.Dobbertin, A. Bosselaers und B. Preneel entwickelte Hashfunktion, die einen 160 Bit langen Hashwert ergibt. Der RIPEMD-160 ist eine Verbesserung des RIPEMD.
RSA	Rivest Shamir Adleman Algorithm	asymmetrischer Verschlüsselungsalgorithmus zum Verschlüsseln und Signieren von Daten
		US-Firma, die Kryptoprotokolle und -software entwickelt und die das Patent an dem Algorithmus besitzt
S	surname	Nachnahme einer Person, Attribut in *distinguished name*-Typen
S/MIME	secure/multipurpose internet mail extensions	Protokoll, das zusätzlich zu MIME digitale Signaturen und Verschlüsselung enthält
SECSIG	security special interest group of OIW	spezielle Arbeitsgruppe innerhalb von OIW, sie sich mit Sicherheitsfragen beschäftigt
SET	secure electronic transaction	Protokoll entwickelt von Visa und MasterCard für sichere elektronische Transaktionen
SGML	standard generalized markup language	Standard zur allgemeinen Beschreibung von Dokumenten, dient als Grundlage für HTML
SHA-1	secure hash algorithm 1	Hashfunktion, Weiterentwicklung von SHA
SigG		Gesetz zur digitalen Signatur
SigV		Verordnung zur digitalen Signatur
SN	serial number *serialNumber*	Zertifikatsfeld, das die Seriennummer des Zertifikates enthält, die innerhalb der Zertifizierungsstelle eindeutig sein muß
SP	state or province	Bezeichnung eines Bundeslandes, Attribut in *distinguished name*-Typen
ST	street address	Straße als Teil einer postalischen Adresse, Attribut in *distinguished name*-Typen
	subject	Zertifikatsfeld, das einen eindeutigen Namen des Zertifikatsinhabers enthält
T	title	Angabe eines Titels, Attribut in *distinguished name*-Typen
	to be signed certificat information *tbsCertificate*	Bestandteile eines Zertifikats, die von einer Zertifizierungsstelle zu signieren sind
TSS	time stamp service	Zeitstempeldienst

ABKÜRZUNG	ENGLISCH	DEUTSCH
	unique identifier of a subject *subjectUniqueIdentifier*	optionales Zertifikatsfeld, das einen eindeutigen Bezeichner für einen Zertifikatsinhaber enthält
URI	universal resource identifier	weltweit eindeutiger Bezeichner für Betriebsmittel
URL	universal resource location	weltweit eindeutiger Name für den Ort eines Betriebsmittels
	user notice *unotice*	spezielles *PolicyQualifiers*-Merkmal, das zur Anzeige für Endanwender dient, daß ein Zertifikat benutzt wurde
UTCTime	coordinated universal time	ASN.1-Typ für Datums- und Zeitformate, Weltzeit
	validation of certificate signature *keyCertSign*	Bit im Feld der Zertifikatserweiterung keyUsage, das die Schlüsselnutzungsart “Prüfung der Zertifikatssignatur einer Zertifizierungsstelle anzeigt
	validation of CRL signature *cRLSign*	Bit im Feld der Zertifikatserweiterung *keyUsage*, das die Schlüsselnutzungsart “Prüfung der Sperrlistensignatur einer Zertifizierungsstelle” anzeigt
	validity	Zertifikatsfeld, das den Gültigkeitszeitraum des Zertifikates enthält
	version	Zertifikatsfeld, das die Versionsnummer des Zertifikats-formates enthält
WWW	world wide web	Dienst zum Laden von graphischen Informationen über das Internet
ZS		Zertifizierungsstelle

LITERATUR

[ANS X9.30] ANSI X9.30-199x:.*Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry, Part 1: The Digital Signature Algorithm (DSA)*, 1992

[ANS X9.31] ANSI X9.31-199x: *Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry, Part 1: The RSA Signature Algorithm*, 199?

[ANS X9.62] ANSI X9.62-199x: *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, 1997

[CCITT X.208 88] CCITT X.208:*Specification of Abstract Syntax Notation One (ASN.1)*, 1988

[DIN SigG/V 98] DIN NI-17.4: *Spezifikation der Schnittstelle zu Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV, Version 1.0*, Dezember 1998

[ISO CD 15782] ISO CD 15782: *Security Management and General Banking Operations* , 1998

[ISO/IEC 9796-2] ISO/IEC 9796-2: *IT-Security Techniques - Digital Signaturs Schemes Giving Message Recovery- Part 2: Mechanisms using a hash-function* , 1996

[ISO/IEC 14888] ISO/IEC 14888: *IT-Security Techniques - Digital Signatures With Appendix- Part 3: Certificate-Based Mechanisms* , 1997

[ITU-T X.411] ITU-T X.411: *Information Technology - Message Handling Systems - Message Transfer SystemAbstract service definition and procedures*, 19??

[ITU-T X.500 97] ITU-T X.500: *Information Technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services*, 1997

[ITU-T X.501 97] ITU-T X.501: *Information Technology - Open Systems Interconnection - The Directory:Models*, 1997

[ITU-T X.520 95] ITU-T X.520: *Information Technology - Open Systems Interconnection - The Directory: Selected Attribute Types*, 1995

[ITU-T X.660 92] ITU-T X.660: *Information Technology - Open Systems Interconnection - Procedures for the operation of OSI Registration Authorities: General procedures*, 1992

[ITU-T X.681 94] ITU-T X.681: *Information Technology - Abstract Syntax Notation One (ASN.1): Information object specification*, 1994

[ITU-T X.690 94] ITU-T X.690: *Information Technology - ASN.1 Encoding Rules - Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*, 1994

[MISPC 97] William Burr, Donna Dodson, Noel Nazario, W. Timothy Polk*: Minimum Interoperability Specification for PKI Components*, Version 1, June 1997

[MKAT 97] *Regulierungsbehörde für Telekommunikation und Post: Maßnahmenkatalog für digitale Signaturen, Version 1.0*, November 1997

[MTRUST 96] Fritz Bauspieß, *TelTrusT: MailTrusT Spezifikation, Version 1.1*, Dezember 1996

[OIW 95] OIW, *Stable Implementation Agreements for Open Systems Interconnection Protocols: Part 12 - OS Security*, June 1995

[PKCS1 93] RSA Laboratories, Technical Note, *PKCS #1: RSA Encryption Standard*, Version 1.5, November 1993

[PKCS7 93] RSA Laboratories, Redwood City, California*: The Public-Key Cryptography Standards (PKCS)*, November 1993

[PKIX CP 98] S. Santesson*: Internet Public Key Infrastructure -Qualified Certificates (QC)*, Dezember 1998

[PKIX ECDSA 97] L. Bassham, D. Johnson*: Internet Public Key Infrastructure -Representation of Elliptic Curve Digital Signature Algorithml (ECDSA) Keys and Signatures in Internet X.509 Public Key Infrastructure Certificates*, November 1997

[PKIX OCSP 97] Michael Myers*: Internet Public Key Infrastructure -Online Certificate Status Protocol (OCSP)*, November 1997

[PKIX PRO 97] R. Housley, W. Ford, W. Polk, and D. Solo*: Internet Public Key Infrastructure - X.509 Certificate and CRL Profile*, July 1998

[RFC 791 81] J. B. Postel: *Internet Protocol*, 1981

[RFC 822 82] David H. Crocker: *Standard for the Format of ARPA Internet Text Messages: Message Encryption and Authentication*, August 1982

[RFC 1035 87] P. Mockapetris: *Domain Names - Implementation and Specification*, 1987

[RFC 1422 93] S. Kent: *Privacy Enhancement for Internet Electronic Mail - Part II: Certificate-Based Key Management*, February 1993

[RFC 1630 94] T. Berners-Lee: *Universal Resource Identifiers in WWW*, 1994

[RFC 1959 96] T. Howes, and M. Smith: *An LDAP URL Format*, June 1996

[RFC 2052 96] A. Gulbrandsen, and M. Smith: *A DNS RR for specifying the location of services (DNS SRV)*, October 1996

[RFC 2247 98] S. Kille, M. Wahl, A. Grimstad, R. Huber and S. Sataluri: *Using Domains in LDAP/X.500 Distinguished Name*, January 1998

[RIPEMD-160 96] H. Dobbertin, A. Bosselaers, and B. Preneel: *A strengthened version of RIPEMD*, April 1996

[SigG 97] BRD: *Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG), Artikel 3, Gesetz zur digitalen Signatur (Signaturgesetz - SigG)*, Juli 1997

[SigV 97] BRD: *Verordnung zur digitalen Signatur (Signaturverordnung - SigV*), Juli 1997

[TS ZF 98] TeleSec, Deutsche Telekom AG: *Zertifikatsformate im Zertifizierungsbereich Signaturgesetz*, Mai 1998

[SEC 98] GMD, SECUDE-Tool: *http://www.darmstadt.gmd.de/secude/*, 1998