Dieses Dokument ist lediglich eine Dokumentationshilfe, für deren Richtigkeit die Organe der Union keine Gewähr übernehmen

►B ►C1 **ENTSCHEIDUNG DER KOMMISSION**

vom 16. Oktober 2009

über Maßnahmen zur Erleichterung der Nutzung elektronischer Verfahren über „einheitliche Ansprechpartner“ gemäß der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates über Dienstleistungen im Binnenmarkt

(Bekannt gegeben unter Aktenzeichen K(2009) 7806)

(Text von Bedeutung für den EWR)

(2009/767/EG) ◄

(ABl. L 274 vom 20.10.2009, S. 36)

Geändert durch:

		Amtsblatt		
		Nr.	Seite	Datum
►M1	Beschluss 2010/425/EU der Kommission vom 28. Juli 2010	L 199	30	31.7.2010
►M2	Verordnung (EU) Nr. 519/2013 der Kommission vom 21. Februar 2013	L 158	74	10.6.2013

Berichtigt durch:

►C1	Berichtigung, ABl. L 299 vom 14.11.2009, S. 18 (2009/767/EG)
►C2	Berichtigung, ABl. L 4 vom 7.1.2011, S. 6 (2009/767/EG)

▼B
▼C1

ENTSCHEIDUNG DER KOMMISSION

vom 16. Oktober 2009

über Maßnahmen zur Erleichterung der Nutzung elektronischer Verfahren über „einheitliche Ansprechpartner“ gemäß der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates über Dienstleistungen im Binnenmarkt

(Bekannt gegeben unter Aktenzeichen K(2009) 7806)

(Text von Bedeutung für den EWR)

(2009/767/EG)

DIE KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN —

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft,

gestützt auf die Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über Dienstleistungen im Binnenmarkt ([1]), insbesondere auf Artikel 8 Absatz 3,

in Erwägung nachstehender Gründe:

(1) Zu den Verwaltungsvereinfachungspflichten, die den Mitgliedstaaten durch Kapitel II der Richtlinie 2006/123/EG, insbesondere Artikel 5 und 8, auferlegt werden, gehören die Verpflichtung zur Vereinfachung der für die Aufnahme und die Ausübung einer Dienstleistungstätigkeit geltenden Verfahren und Formalitäten und die Verpflichtung, dafür zu sorgen, dass alle diese Verfahren und Formalitäten von Dienstleistungserbringern problemlos aus der Ferne und elektronisch über die einheitlichen Ansprechpartner abgewickelt werden können.

(2) Die Abwicklung der Verfahren und Formalitäten über die einheitlichen Ansprechpartner muss nach Artikel 8 der Richtlinie 2006/123/EG grenzüberschreitend zwischen den Mitgliedstaaten möglich sein.

(3) Damit die Verpflichtungen zur Vereinfachung der Verfahren und Formalitäten und zur Erleichterung der grenzüberschreitenden Nutzung der einheitlichen Ansprechpartner erfüllt werden können, müssen die elektronischen Verfahren auf einfachen Lösungen beruhen, auch in Bezug auf die Verwendung elektronischer Signaturen. Wenn bei konkreten Verfahren und Formalitäten nach angemessener Risikoabschätzung ein hohes Sicherheitsniveau oder die Gleichwertigkeit mit einer handschriftlichen Unterschrift für notwendig erachtet wird, könnten von Dienstleistungserbringern für bestimmte Verfahren oder Formalitäten fortgeschrittene elektronische Signaturen verlangt werden, die auf einem qualifizierten Zertifikat beruhen und mit oder ohne sichere Signaturerstellungseinheit erstellt wurden.

([1]) ABl. L 376 vom 27.12.2006, S. 36.

▼C1

(4) Der Gemeinschaftsrahmen für elektronische Signaturen wurde durch die Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen ([1]) geschaffen. Um die wirksame grenzüberschreitende Verwendung fortgeschrittener elektronischer Signaturen, die auf einem qualifizierten Zertifikat beruhen, zu erleichtern, sollte das Vertrauen in diese elektronischen Signaturen gestärkt werden, und zwar unabhängig davon, in welchem Mitgliedstaat der Unterzeichner oder der Zertifizierungsdiensteanbieter, der das qualifizierte Zertifikat ausstellt, niedergelassen ist. Dies könnte dadurch erreicht werden, dass die Informationen, die zur Prüfung der elektronischen Signaturen notwendig sind, in vertrauenswürdiger Form leicht zugänglich gemacht werden, darunter insbesondere Informationen über die in einem Mitgliedstaat beaufsichtigten bzw. akkreditierten Zertifizierungsdiensteanbieter und die von ihnen angebotenen Dienstleistungen.

(5) Es ist dafür zu sorgen, dass die Mitgliedstaaten diese Informationen auf Grundlage einer gemeinsamen Vorlage öffentlich zugänglich machen, um ihre Nutzung zu erleichtern und um zu gewährleisten, dass die Angaben hinreichend ausführlich sind, damit der Empfänger die elektronische Signatur prüfen kann —

HAT FOLGENDE ENTSCHEIDUNG ERLASSEN:

Artikel 1

Verwendung und Anerkennung elektronischer Signaturen

1. Sofern dies aufgrund einer angemessenen Abschätzung der bestehenden Risiken gerechtfertigt und mit Artikel 5 Absätze 1 und 3 der Richtlinie 2006/123/EG vereinbar ist, können die Mitgliedstaaten für die Abwicklung bestimmter Verfahren und Formalitäten über die einheitlichen Ansprechpartner gemäß Artikel 8 der Richtlinie 2006/123/EG verlangen, dass der Dienstleistungserbringer fortgeschrittene elektronische Signaturen verwendet, die auf einem qualifizierten Zertifikat beruhen und mit oder ohne sichere Signaturerstellungseinheit gemäß der Richtlinie 1999/93/EG erstellt wurden.

2. Die Mitgliedstaaten akzeptieren für die Abwicklung der in Absatz 1 genannten Verfahren und Formalitäten alle fortgeschrittenen elektronischen Signaturen, die auf einem qualifizierten Zertifikat beruhen und mit oder ohne sichere Signaturerstellungseinheit erstellt wurden, dürfen diese Anerkennung aber auf jene fortgeschrittenen elektronischen Signaturen beschränken, die auf einem qualifizierten Zertifikat beruhen und von einer sicheren Signaturerstellungseinheit erstellt werden, sofern das mit der in Absatz 1 genannten Risikoabschätzung vereinbar ist.

3. Die Mitgliedstaaten dürfen die Anerkennung fortgeschrittener elektronischer Signaturen, die auf einem qualifizierten Zertifikat beruhen und mit oder ohne sichere Signaturerstellungseinheit erstellt wurden, nicht von Erfordernissen abhängig machen, durch die Dienstleistungserbringer bei der Nutzung der elektronischen Verfahren über die einheitlichen Ansprechpartner behindert würden.

([1]) ABl. L 13 vom 19.1.2000, S. 12.

▼C1

4. Absatz 2 hindert die Mitgliedstaaten nicht an der Anerkennung anderer elektronischer Signaturen als fortgeschrittener elektronischer Signaturen, die auf einem qualifizierten Zertifikat beruhen und mit oder ohne sichere Signaturerstellungseinheit erstellt wurden.

Artikel 2

Erstellung, Führung und Veröffentlichung von vertrauenswürdigen Listen

1. Jeder Mitgliedstaat sorgt entsprechend den im Anhang festgelegten technischen Spezifikationen für die Erstellung, Führung und Veröffentlichung einer „vertrauenswürdigen Liste“ mit Mindestangaben über die von ihm beaufsichtigten bzw. akkreditierten Zertifizierungsdiensteanbieter, die öffentlich qualifizierte Zertifikate ausstellen.

▼M1

2. Die Mitgliedstaaten erstellen und veröffentlichen die vertrauenswürdige Liste entsprechend den im Anhang festgelegten Spezifikationen sowohl in einer vom Menschen unmittelbar lesbaren Form als auch in maschinenlesbarer Form.

2a. Die Mitgliedstaaten versehen die maschinenlesbare Form ihrer vertrauenswürdigen Liste mit einer elektronischen Signatur und veröffentlichen mindestens die vom Menschen unmittelbare lesbare Form der vertrauenswürdigen Liste über einen sicheren Kanal, um ihre Authentizität und Integrität zu gewährleisten.

3. Die Mitgliedstaaten teilen der Kommission Folgendes mit:

a) die Stelle(n), die für die Erstellung, Führung und Veröffentlichung der vertrauenswürdigen Liste in der vom Menschen unmittelbar lesbaren und der maschinenlesbaren Form zuständig ist/sind;

b) die Veröffentlichungsorte der vom Menschen unmittelbar lesbaren sowie der maschinenlesbaren Form der vertrauenswürdigen Liste;

c) das Public-Key-Zertifikat, das für den sicheren Kanal verwendet wurde, über den die vom Menschen unmittelbare lesbare Form der vertrauenswürdigen Liste veröffentlicht wird, bzw., falls die vom Menschen unmittelbar lesbare Form der vertrauenswürdigen Liste mit einer elektronischen Signatur versehen ist, das Public-Key-Zertifikat, mit dem diese Liste signiert wurde;

d) das Public-Key-Zertifikat, das für die elektronische Signatur der vertrauenswürdigen Liste in der maschinenlesbaren Form verwendet wurde;

e) jegliche Änderungen in Bezug auf die Buchstaben a bis d.

4. Die Kommission stellt allen Mitgliedstaaten über einen sicheren Kanal zu einem authentifizierten Web-Server die ihr gemäß Absatz 3 von den Mitgliedstaaten übermittelten Informationen sowohl in einer vom Menschen unmittelbar lesbaren Form als auch in maschinenlesbarer Form bereit.

▼C1

Artikel 3

Geltung

Diese Entscheidung gilt ab dem 28. Dezember 2009.

Artikel 4

Adressaten

Diese Entscheidung ist an die Mitgliedstaaten gerichtet.

▼C1

ANHANG

TECHNISCHE SPEZIFIKATIONEN FÜR EINE GEMEINSAME VORLAGE FÜR EINE „VERTRAUENSWÜRDIGE LISTE DER BEAUFSICHTIGTEN BZW. AKKREDITIERTEN ZERTIFIZIERUNGSDIENSTEANBIETER“

VORWORT

1. **Allgemeines**

Zweck der gemeinsamen Vorlage für die „vertrauenswürdige Liste der beaufsichtigten bzw. akkreditierten Zertifizierungsdiensteanbieter“ der Mitgliedstaaten ist die Festlegung einer gemeinsamen Methode zur Bereitstellung von Informationen über den Aufsichts- bzw. Akkreditierungsstatus der Zertifizierungsdienste von Zertifizierungsdiensteanbietern ([1]) (Certification Service Providers — CSPs), die von den Mitgliedstaaten beaufsichtigt werden bzw. akkreditiert sind, hinsichtlich der Einhaltung der entsprechenden Bestimmungen der Richtlinie 1999/93/EG. Dies beinhaltet auch die Bereitstellung historischer Informationen über den Aufsichts- bzw. Akkreditierungsstatus der beaufsichtigten bzw. akkreditierten Zertifizierungsdienste.

Zu den für die vertrauenswürdige Liste (Trusted List — TL) zwingend erforderlichen Angaben zählen Mindestinformationen über beaufsichtigte bzw. akkreditierte CSPs, die qualifizierte Zertifikate (QCs) ([2]) gemäß den Bestimmungen der Richtlinie 1999/93/EG (Artikel 3 Absatz 3, Artikel 3 Absatz 2 und Artikel 7 Absatz 1 Buchstabe a ausstellen, einschließlich Informationen über QCs zur Unterstützung einer elektronischen Signatur und Informationen darüber, ob die Signatur von einer sicheren Signaturerstellungseinheit (Secure Signature Creation Device — SSCD) ([3]) erzeugt wurde.

Zusatzinformationen über andere beaufsichtigte bzw. akkreditierte CSPs, die keine QCs ausstellen, sondern Dienste im Zusammenhang mit elektronischen Signaturen bieten (z. B. CSPs, die Zeitstempel, Zeitstempel-Tokens oder nicht qualifizierte Zertifikate ausstellen usw.), können auf einzelstaatlicher Basis freiwillig in die vertrauenswürdige Liste aufgenommen werden.

Diese Informationen dienen vor allem zur Validierung qualifizierter elektronischer Signaturen (Qualified Electronic Signatures — QES) und fortgeschrittener elektronischer Signaturen (Advanced Electronic Signatures — AdES) ([4]), die auf einem qualifizierten Zertifikat beruhen ([5]) ([6]).

Die vorgeschlagene gemeinsame Vorlage ist kompatibel mit einer Implementierung auf Grundlage der Spezifikationen laut ETSI TS 102 231 ([7]), die im Zusammenhang mit der Erstellung, Veröffentlichung, dem Speicherort, dem Zugriff, der Authentifizierung und der Aufsicht derartiger Listen verwendet werden.

([1]) Definition nach Artikel 2 Absatz 11 der Richtlinie 1999/93/EG.
([2]) Definition nach Artikel 2 Absatz 10 der Richtlinie 1999/93/EG.
([3]) Definition nach Artikel 2 Absatz 6 der Richtlinie 1999/93/EG.
([4]) Definition nach Artikel 2 Absatz 2 der Richtlinie 1999/93/EG.
([5]) Für eine von einem QC unterstützte AdES wird im vorliegenden Dokument die Kurzbezeichnung „$AdES_{QC}$“ verwendet.
([6]) Hinweis: Die grenzüberschreitende Nutzung einiger elektronischer Dienste, die auf einfachen AdES basieren, wird ebenfalls vereinfacht, wenn die unterstützenden Zertifizierungsdienste (z. B. die Ausstellung nicht qualifizierter Zertifikate) Bestandteil der beaufsichtigten bzw. akkreditierten Dienste sind, die ein Mitgliedstaat in den freiwilligen Angaben seiner vertrauenswürdigen Liste anführt.
([7]) ETSI TS 102 231 — Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information.

▼C1

2. **Leitlinien zur Bearbeitung von Einträgen in der TL**

2.1 *TL der beaufsichtigten bzw. akkreditierten Zertifizierungsdienste*

Einschlägige Zertifizierungsdienste und Zertifizierungsdiensteanbieter in einer einzigen Liste

Die vertrauenswürdige Liste eines Mitgliedstaats ist definiert als die Aufsichts- bzw. Akkreditierungsstatusliste der Zertifizierungsdienste von Zertifizierungsdiensteanbietern, die vom entsprechenden Mitgliedstaat im Hinblick auf die Einhaltung der entsprechenden Bestimmungen der Richtlinie 1999/93/EG beaufsichtigt werden bzw. akkreditiert sind.

Eine solche vertrauenswürdige Liste muss beinhalten:

— alle Zertifizierungsdiensteanbieter laut Definition in Artikel 2 Absatz 11 der Richtlinie 1999/93/EG (d. h. „eine Stelle oder eine juristische oder natürliche Person, die Zertifikate ausstellt oder anderweitige Dienste im Zusammenhang mit elektronischen Signaturen bereitstellt“);

— die im Hinblick auf die Einhaltung der entsprechenden Bestimmungen der Richtlinie 1999/93/EG beaufsichtigt werden bzw. akkreditiert sind.

Anhand der Definitionen und Bestimmungen der Richtlinie 1999/93/EG lassen sich, insbesondere in Bezug auf die entsprechenden CSPs und deren Aufsichts- bzw. freiwillige Akkreditierungssysteme, zwei Arten von CSPs unterscheiden: Dies sind einerseits die CSPs, die QCs für die Öffentlichkeit ausstellen (CSP_{QC}), andererseits die CSPs, die keine QCs für die Öffentlichkeit ausstellen, aber „anderweitige (sonstige) Dienste im Zusammenhang mit elektronischen Signaturen“ erbringen:

— **CSPs, die QCs ausstellen**

  — Diese müssen von dem Mitgliedstaat, in dem sie ansässig sind, beaufsichtigt werden (wenn sie in einem Mitgliedstaat ansässig sind) und können im Hinblick auf die Einhaltung der Bestimmungen der Richtlinie 1999/93/EG, einschließlich der Anforderungen laut Anhang I (Anforderungen an qualifizierte Zertifikate) und Anhang II (Anforderungen an Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen), auch akkreditiert werden. QCs ausstellende CSPs, die in einem Mitgliedstaat akkreditiert sind, müssen trotzdem dem entsprechenden Aufsichtssystem dieses Mitgliedstaats unterliegen, es sei denn, dass sie nicht in diesem Mitgliedstaat ansässig sind.

  — Das jeweilige „Aufsichtssystem“ (bzw. „freiwillige Akkreditierungssystem“) ist definiert und muss den Anforderungen der Richtlinie 1999/93/EG, insbesondere Artikel 3 Absatz 3, Artikel 8 Absatz 1, Artikel 11, Erwägungsgrund 13 (bzw. Artikel 2 Absatz 13, Artikel 3 Absatz 2, Artikel 7 Absatz 1 Buchstabe a, Artikel 8 Absatz 1, Artikel 11, Erwägungsgrund 4 sowie 11 bis 13), entsprechen.

— **CSPs, die keine QCs ausstellen**

  — Diese können einem „freiwilligen Akkreditierungssystem“ (gemäß Definition und in Übereinstimmung mit der Richtlinie 1999/93/EG) und/oder einem einzelstaatlich festgelegten „anerkannten Genehmigungssystem“ („recognised approval scheme“) unterliegen, das auf nationaler Ebene zur Aufsicht der Einhaltung der Bestimmungen der Richtlinie und gegebenenfalls einzelstaatlicher Bestimmungen im Zusammenhang mit der Erbringung von Zertifizierungsdiensten (im Sinne von Artikel 2 Absatz 11 der Richtlinie) eingerichtet wird.

  — Einige der infolge der Erbringung eines Zertifizierungsdienstes generierten oder ausgestellten physischen oder binären (logischen) Objekte könnten, sofern sie den einzelstaatlichen Bestimmungen und Erfordernissen entsprechen, eine spezielle „Qualifizierung“ beanspruchen, doch wird die Bedeutung einer derartigen „Qualifizierung“ voraussichtlich auf die einzelstaatliche Ebene beschränkt sein.

▼C1

Die vertrauenswürdige Liste eines Mitgliedstaats muss Mindestinformationen über beaufsichtigte bzw. akkreditierte CSPs, die qualifizierte Zertifikate für die Öffentlichkeit gemäß den Bestimmungen der Richtlinie 1999/93/EG (Artikel 3 Absatz 3, Artikel 3 Absatz 2 und Artikel 7 Absatz 1 Buchstabe a ausstellen, Informationen über das QC zur Unterstützung der elektronischen Signatur und Informationen darüber, ob die Signatur von einer sicheren Signaturerstellungseinheit erzeugt wurde, beinhalten.

Zusatzinformationen über andere beaufsichtigte bzw. akkreditierte Dienste von CSPs, die keine QCs für die Öffentlichkeit ausstellen (z. B. CSPs, die Zeitstempel, Zeitstempel-Tokens oder nicht qualifizierte Zertifikate ausstellen usw.), können auf einzelstaatlicher Basis freiwillig in die vertrauenswürdige Liste aufgenommen werden.

Die vertrauenswürdige Liste dient dazu,

— zuverlässige Informationen zusammenzutragen und bereitzustellen über den Aufsichts- bzw. Akkreditierungsstatus der Zertifizierungsdienste von Zertifizierungsdiensteanbietern, die von dem Mitgliedstaat, der für die Erstellung und Führung der Liste, die zur Einhaltung der entsprechenden Bestimmungen der Richtlinie 1999/93/EG beitragen soll, beaufsichtigt werden bzw. akkreditiert sind;

— die Validierung elektronischer Signaturen, die von den angeführten beaufsichtigte bzw. akkreditierten Zertifizierungsdiensten der gelisteten CSPs unterstützt werden, zu vereinfachen.

Einheitliche Aufsichts- bzw. Akkreditierungsstatuswerte

Jeder Mitgliedstaat erstellt und führt nur eine einzige TL, aus der der Aufsichts- und/oder Akkreditierungsstatus der Zertifizierungsdienste, die von den von diesem Mitgliedstaat beaufsichtigten bzw. akkreditierten CSPs erbracht werden, hervorgeht.

Die Tatsache, dass ein Dienst gegenwärtig entweder beaufsichtigt wird oder akkreditiert ist, ist Bestandteil seines aktuellen Status. Darüber hinaus kann ein Aufsichts- oder Akkreditierungsstatus „laufend“ (ongoing), „in Einstellung begriffen“ (in cessation), „beendet“ (ceased) oder sogar „widerrufen“ (revoked) sein. Während seiner gesamten Lebensdauer kann ein Zertifizierungsdienst zwischen Aufsichts- und Akkreditierungsstatus wechseln ([1]).

Die nachstehende Abbildung 1 beschreibt den zu erwartenden Wechsel zwischen Aufsichts- bzw. Akkreditierungsstatus eines einzelnen Zertifizierungsdienstes:

([1]) D. h. ein in einem Mitgliedstaat angesiedelter Zertifizierungsdiensteanbieter, der einen Zertifizierungsdienst anbietet, der anfänglich von dem Mitgliedstaat (Aufsichtsbehörde) beaufsichtigt wird, kann, nach Ablauf einer bestimmten Frist, eine freiwillige Akkreditierung des gegenwärtig beaufsichtigten Zertifizierungsdienstes beschließen. Umgekehrt kann ein Zertifizierungsdiensteanbieter in einem anderen Mitgliedstaat entscheiden, einen akkreditierten Zertifizierungsdienst nicht zu beenden, sondern seinen Status von Akkreditierung auf Aufsicht zu setzen, z. B. aus geschäftlichen und/oder wirtschaftlichen Gründen.

▼C1

Zu erwartender Wechsel zwischen Überwachungs-Akkreditierungsstatus eines einzelnen CSP

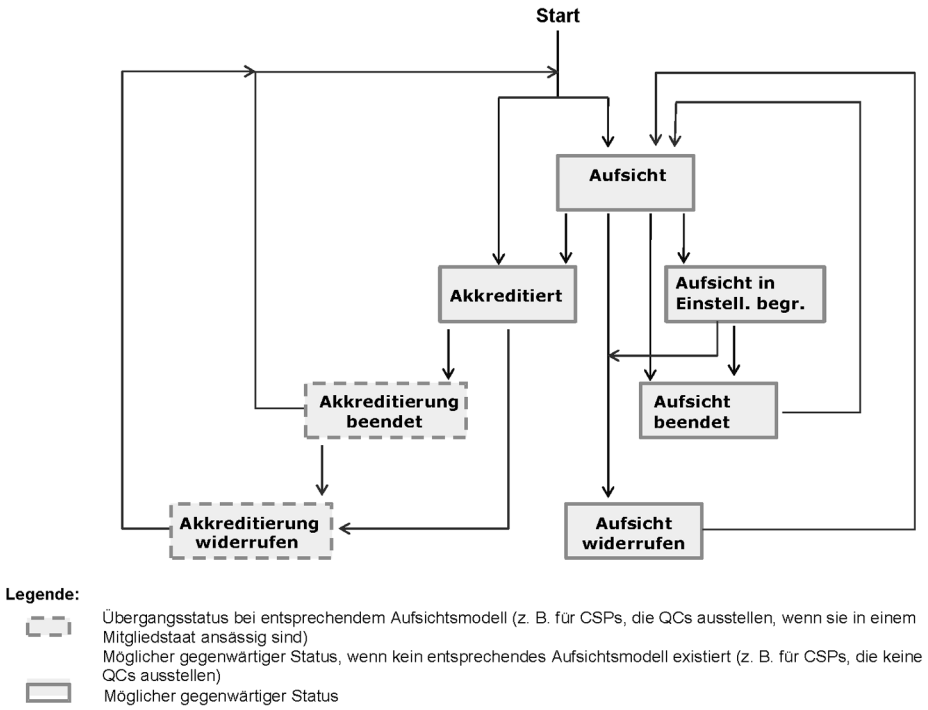


Abbildung 1

Ein Zertifizierungsdienst, der QCs ausstellt, muss beaufsichtigt werden (wenn er in einem Mitgliedstaat angesiedelt ist) und kann freiwillig akkreditiert werden. Der „gegenwärtige Statuswert“ eines solchen Dienstes, wenn er in einer vertrauenswürdigen Liste aufscheint, kann jeder der oben angeführten Statuswerte sein. Allerdings ist zu beachten, dass „Akkreditierung beendet“ und „Akkreditierung widerrufen“ nur in Fällen, in denen CSP_{QC}-Dienste in einem Mitgliedstaat ansässig sind, „Aufsichtsstatus“-Werte sein müssen, da derartige Dienste standardmäßig beaufsichtigt werden müssen (selbst wenn sie nicht oder nicht mehr akkreditiert sind).

Mitgliedstaaten, die ein einzelstaatlich definiertes „anerkanntes Genehmigungssystem“ einrichten oder eingerichtet haben, das auf nationaler Ebene zur Aufsicht der Einhaltung der Bestimmungen der Richtlinie 1999/93/EG und möglicher einzelstaatlicher Bestimmungen im Zusammenhang mit der Erbringung von Zertifizierungsdiensten (im Sinne von Artikel 2 Absatz 11 der Richtlinie) durch CSPs, die keine QCs ausstellen, dient, müssen dieses Genehmigungssystem (bzw. diese Genehmigungssysteme) in eine der beiden nachstehenden Kategorien einordnen:

— „freiwillige Akkreditierung“ wie in der Richtlinie 1999/93/EG (Artikel 2 Absatz 13, Artikel 3 Absatz 2, Artikel 7 Absatz 1 Buchstabe a, Artikel 8 Absatz 1, Artikel 11, Erwägungsgrund 4 sowie 11 bis 13) definiert und geregelt;

— „Aufsicht“ wie in der Richtlinie 1999/93/EG vorgesehen und durch nationale Bestimmungen und Anforderungen unter Berücksichtigung der einzelstaatlichen gesetzlichen Vorschriften umgesetzt.

▼C1

Dementsprechend kann ein Zertifizierungsdienst, der keine QCs ausstellt, beaufsichtigt oder freiwillig akkreditiert werden. Der „gegenwärtige Statuswert“ eines solchen Dienstes, wenn er in einer vertrauenswürdigen Liste aufscheint, kann jeder der oben angeführten Statuswerte sein (siehe Abbildung 1).

Die vertrauenswürdige Liste muss Angaben zu den Aufsichts- bzw. Akkreditierungssystemen enthalten, die ihr zugrunde liegen, insbesondere:

— Informationen über das Aufsichtssystem, das für alle CSP_{QC} gilt;

— Ggf. Informationen über das einzelstaatliche „freiwillige Akkreditierungssystem“, das für alle CSP_{QC} gilt;

— Ggf. Informationen über das Aufsichtssystem, das für alle CSPs gilt, die keine QCs ausstellen;

— Ggf. Informationen über das einzelstaatliche „freiwillige Akkreditierungssystem“, das für alle CSPs gilt, die keine QCs ausstellen;

Die beiden letzteren Informationsgruppen sind für dem Zertifikat vertrauende Parteien von entscheidender Bedeutung zur Beurteilung des Qualitäts- und Sicherheitsgrads derartiger, auf einzelstaatlicher Ebene für CSPs, die keine QCs ausstellen, eingerichteter Aufsichts- bzw. Akkreditierungssysteme. Wenn in der TL im Hinblick auf Dienste von CSPs, die keine QCs ausstellen, Informationen über den Aufsichts- bzw. Akkreditierungsstatus enthalten sind, sind die oben genannten Informationen auf TL-Ebene durch die Verwendung von „Scheme information URI“ (Abschnitt 5.3.7 — von den Mitgliedstaaten bereitgestellte Informationen), „Scheme type/community/rules“ (Abschnitt 5.3.9 — Verwendung eines allen Mitgliedstaaten gemeinsamen Texts und optionaler, vom Mitgliedstaat bereitgestellter, spezifischer Informationen) und „TSL policy/legal notice“ (Abschnitt 5.3.11 — ein allen Mitgliedstaaten gemeinsamer Text, der auf die Richtlinie 1999/93/EG Bezug nimmt sowie die Möglichkeit bietet, einen länderspezifischen Text bzw. Verweise hinzuzufügen) bereitzustellen. Zusätzliche „Qualification“-Informationen auf der Ebene der einzelstaatlichen Aufsichts- bzw. Akkreditierungssysteme für CSPs, die keine QCs ausstellen, können ggf. und wenn erforderlich (z. B. zur Unterscheidung zwischen verschiedenen Qualitäts- bzw. Sicherheitsstufen) auf der Dienstebene durch die Verwendung der Erweiterung „additionalServiceInformation“ (Abschnitt 5.8.2) als Teil der „Service information extension“ (Abschnitt 5.5.9) bereitgestellt werden. Weitere Informationen zu den entsprechenden technischen Spezifikationen enthält Kapitel I.

Obwohl möglicherweise unterschiedliche Stellen in einem Mitgliedstaat für die Aufsicht bzw. Akkreditierung von Zertifizierungsdiensten in diesem Mitgliedstaat zuständig sind, darf für einen Zertifizierungsdienst (laut ETSI TS 102 231 [1] identifiziert durch seine „Service digital identity“) nur ein einziger Eintrag vorhanden sein und der Aufsichts- bzw. Akkreditierungsstatus muss entsprechend aktualisiert werden. Die Bedeutung der oben angegebenen Statuswerte ist in Abschnitt 5.5.4 der ausführlichen technischen Spezifikationen in Kapitel I erläutert.

2.2 *TL-Einträge zur Validierung von QES und $AdES_{QC}$*

Der wichtigste Schritt bei der Erstellung der TL ist die Festlegung des zwingend erforderlichen Teils der TL, nämlich der „List of services“ für jeden CSP, der QCs ausstellt, damit die Ausstellungssituation jedes QC-ausstellenden Zertifizierungsdienstes korrekt erfasst und gewährleistet ist, so dass die in jedem Eintrag enthaltenen Informationen die Validierung von QES und $AdES_{QC}$ (in Kombination mit dem Inhalt des vom CSP im Rahmen des in diesem Eintrag enthaltenen Zertifizierungsdienstes ausgestellten Anwender-QC) ermöglichen.

[1] ETSI TS 102 231 — Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information.

▼C1

Da kein wirklich interoperables und grenzüberschreitendes Profil für das QC existiert, können die erforderlichen Informationen auch noch andere Angaben als die „Service digital identity“ einer einzelnen (Root) CA enthalten. Dies gilt insbesondere für Informationen zur Angabe des QC-Status des ausgestellten Zertifikats und darüber, ob die unterstützten Signaturen von einer SSCD erzeugt wurden. Die für die Erstellung, Bearbeitung und Führung der TL zuständige Stelle in einem Mitgliedstaat (d. h. der „Scheme operator“ gemäß ETSI TS 102 231) muss daher für jeden von der TL abgedeckten CSP_{QC} das gegenwärtige Profil und den Zertifikatsinhalt jedes ausgestellten QC berücksichtigen.

Im Idealfall sollte jedes ausgestellte QC die vom ETSI definierte Erklärung zur QcCompliance ([1]) enthalten, wenn angegeben wird, dass es sich um ein QC handelt. Wenn angegeben wird, dass ein QC von einer SSCD zur Erzeugung elektronischer Signaturen unterstützt wird, sollte es die vom ETSI definierte QcSSCD-Erklärung enthalten bzw. sollte jedes ausgestellte QC einen der Object Identifiers (OIDs) der QCP/QCP + Zertifikatrichtlinien gemäß ETSI TS 101 456 ([2]) beinhalten. Die Verwendung unterschiedlicher Normen durch CSPs, die QCs ausstellen, der große Auslegungsspielraum dieser Normen und das fehlende Bewusstsein hinsichtlich des Vorhandenseins und der Rangordnung normativer technischer Spezifikationen und Standards hat zu inhaltlichen Unterschieden bei den gegenwärtig ausgestellten QCs geführt (z. B. werden die vom ETSI definierten Qc-Erklärungen nur teilweise benutzt). Dementsprechend können sich die Empfänger nicht einfach auf das Zertifikat des Unterzeichners (und die dazugehörige Kette bzw. den dazugehörigen Pfad) verlassen, um zumindest auf maschinenlesbare Art und Weise festzustellen, ob es sich bei dem Zertifikat, das eine elektronische Signatur unterstützt, tatsächlich um ein QC handelt, und ob die elektronische Signatur durch eine SSCD erzeugt wurde.

Durch Ergänzung der Felder „Service type identifier“ („Sti“), „Service name“ („Sn“) und „Service digital identity“ („Sdi“) ([3]) mit den im Feld „Service information extensions“ („Sie“) enthaltenen Informationen kann mit Hilfe der vorgeschlagenen gemeinsamen Vorlage für eine TL ein spezieller Typ eines qualifizierten Zertifikats, das von einem gelisteten CSP, der QCs ausstellt, ausgestellt wird, vollständig bestimmt werden. Dabei werden auch Informationen darüber übermittelt, ob das QC von einer SSCD unterstützt wird (wenn diese Angabe im ausgestellten QC fehlt). Natürlich gehört zu diesem Eintrag auch eine spezielle Angabe über den „Service current status“ („Scs“). Dies geht aus Abbildung 2 unten hervor.

Die Aufnahme eines Dienstes in die Liste mit Angabe der „Sdi“ einer (Root) CA würde sicherstellen (durch den QCs ausstellenden CSP, aber auch durch die für diesen CSP zuständige Aufsichts- bzw. Akkreditierungsstelle), dass jedes von dieser (Root) CA(-Hierarchie) ausgestellte Anwenderzertifikate ausreichende vom ETSI definierte und maschinenlesbare Informationen enthält, um festzustellen, ob es sich um ein QC handelt und ob dieses von einer SSCD unterstützt wird. Erweist sich beispielsweise Letzteres als nicht zutreffend (wenn das QC z. B. keinen maschinenlesbaren Hinweis laut ETSI-Norm darauf enthält, ob es von einer SSCD unterstützt wird), dann kann durch die reine Angabe der „Sdi“ dieser (Root) CA nur angenommen werden, dass über diese (Root) CA-Hierarchie ausgestellte QCs nicht von einer SSCD unterstützt werden. Damit diese QCs als von einer SSCD unterstützt betrachtet werden können, sollte diese Information in die „Sie“ aufgenommen werden (dadurch wird auch angegeben, dass dies vom QCs ausstellenden CSP gewährleistet wird und eine Aufsicht bzw. Akkreditierung durch die zuständige Stelle erfolgt).

([1]) Vgl. ETSI TS 101 862 — Electronic Signatures and Infrastructures (ESI): Qualified Certificate Profile.

([2]) ETSI TS 101 456 — Electronic Signature and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.

([3]) D. h. zumindest ein X.509v3-Zertifikat der ausstellenden QCA oder einer übergeordneten CA im Zertifizierungspfad.

▼C1

Allgemeine Grundsätze — Bearbeitungsvorschriften — CSP_{QC}-Einträge (gelistete Dienste)

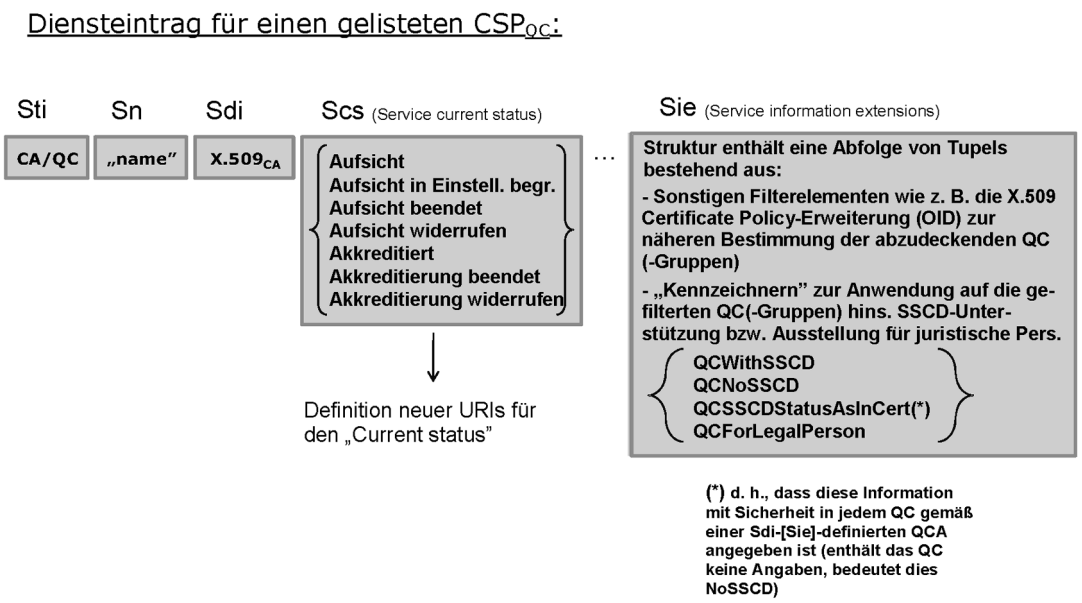


Abbildung 2

Diensteintrag für einen gelisteten CSP, der QCs ausstellt, in der im TSL-Format implementierten TL

Die vorliegenden technischen Spezifikationen für eine gemeinsame Vorlage für eine TL erlauben die Verwendung einer Kombination bestehend aus fünf Hauptinformationsteilen im Diensteeintrag:

— „Service type identifier" („Sti"), z. B. zur Identifikation einer CA, die QCs ausstellt („CA/QC");

— „Service name" („Sn");

— „Service digital identity" („Sdi") zur Identifikation eines gelisteten Dienstes, z. B. (zumindest) das X.509v3-Zertifikat für eine CA, die QCs ausstellt;

— Für CA/QC-Dienste optionale „Service information extensions" („Sie"), die die Aufnahme eines Tupels oder einer Reihe von Tupeln erlauben, von denen jedes folgende Angaben enthält:

  — Kriterien zur näheren Identifikation (Filterung) des Dienstes (d. h. die Gruppe qualifizierter Zertifikate), für welchen im Hinblick auf die Angabe der SSCD-Unterstützung (bzw. der Ausstellung für juristische Personen) Zusatzinformationen erforderlich sind bzw. angegeben werden, aus dem durch die „Sdi" identifizierten Zertifizierungsdienst;

  — Entsprechende Informationen („Qualifier" — „Kennzeichner") darüber, ob diese näher identifizierte Dienstegruppe qualifizierter Zertifikate von einer SSCD unterstützt wird und ob diese entsprechenden Informationen in einer genormten, maschinenlesbaren Form Bestandteil des QC sind; und bzw. oder Informationen darüber, dass solche QCs für juristische Personen ausgestellt werden (standardmäßig ist davon auszugehen, dass sie nur natürlichen Personen ausgestellt werden).

▼C1

— Der „Current status“ für diesen Diensteintrag liefert Informationen darüber,

— ob es sich um einen beaufsichtigten oder einen akkreditierten Dienst handelt und

— über den Aufsichts- bzw. Akkreditierungsstatus selbst.

2.3 *Leitlinien zur Bearbeitung und Nutzung von CSP_{QC}-Diensteeinträgen*

Allgemeine Leitlinien zur Bearbeitung:

1. Wenn sichergestellt ist (garantiert durch den CSP_{QC} und beaufsichtigt bzw. akkreditiert durch die Aufsichts- (Supervisory Body — SB) bzw. Akkreditierungsstelle (Accreditation Body — AB)), dass für einen durch eine „Sdi“ identifizierten, gelisteten Dienst jedes von einer SSCD unterstützte QC die vom ETSI definierte Erklärung zur QcCompliance, die QcSSCD-Erklärung und/oder einen QCP + Object Identifier (OID) enthält, reicht die Verwendung einer entsprechenden „Sdi“ aus. Das „Sie“-Feld kann in diesem Fall optional verwendet werden und muss keine Angaben über die SSCD-Unterstützung enthalten.

2. Wenn sichergestellt ist (garantiert durch den CSP_{QC} und beaufsichtigt bzw. akkreditiert durch die SB bzw. AB), dass für einen durch eine „Sdi“ identifizierten, gelisteten Dienst jedes nicht von einer SSCD unterstützte QC die Erklärung zur QcCompliance und bzw. oder einen QCP + OID enthält und keine QcSSCD-Erklärung oder einen QCP + OID enthalten soll, reicht die Verwendung einer entsprechenden „Sdi“ aus. Das „Sie“-Feld kann in diesem Fall optional verwendet werden und muss keine Angaben über die SSCD-Unterstützung enthalten (d. h. das Zertifikat wird nicht von einer SSCD unterstützt).

3. Wenn sichergestellt ist (garantiert durch den CSP_{QC} und beaufsichtigt bzw. akkreditiert durch die SB bzw. AB), dass für einen durch eine „Sdi“ identifizierten, gelisteten Dienst jedes QC die Erklärung zur QcCompliance enthält und einige, aber nicht alle, dieser QCs von einer SSCD unterstützt werden sollen (die Unterscheidung kann z. B. durch verschiedene CSP-spezifische Certificate-Policy-OIDs oder sonstige CSP-spezifische Informationen im QC, direkt oder indirekt, maschinenlesbar oder nicht, getroffen werden), der Dienst aber WEDER die QcSSCD-Erklärung NOCH den QCP(+) OID des ETSI enthält, reicht die Verwendung einer entsprechenden „Sdi“ möglicherweise nicht aus UND das „Sie“-Feld muss für eindeutige Angaben zur SSCD-Unterstützung sowie eine potenzielle Informationserweiterung zur Identifikation der abgedeckten Gruppe von Zertifikaten verwendet werden. Infolgedessen wird wahrscheinlich die Aufnahme verschiedener „SSCD support information values“ für eine „Sdi“ erforderlich, sofern das „Sie“-Feld verwendet wird.

4. Wenn sichergestellt ist (garantiert durch den CSP_{QC} und beaufsichtigt bzw. akkreditiert durch die SB bzw. AB), dass für einen durch eine „Sdi“ identifizierten, gelisteten Dienst kein QC die Erklärung zur QcCompliance, den QCP OID, die QcSSCD-Erklärung oder den QCP + OID enthält, aber gewährleistet ist, dass einige, aber nicht alle, der über diese „Sdi“ ausgestellten Anwenderzertifikate als QCs gedacht sind und bzw. oder von SSCDs unterstützt werden (die Unterscheidung kann z. B. durch verschiedene CSP_{QC}-spezifische Certificate-Policy-OIDs oder sonstige CSP_{QC}-spezifische Informationen im QC, direkt oder indirekt, maschinenlesbar oder nicht, getroffen werden), reicht die Verwendung einer entsprechenden „Sdi“ nicht aus UND das „Sie“-Feld muss für eindeutige Angaben zur SSCD-Unterstützung verwendet werden. Infolgedessen wird wahrscheinlich die Aufnahme verschiedener „SSCD support information values“ für eine „Sdi“ erforderlich, wenn das „Sie“-Feld verwendet wird.

▼C1

Generell kann für einen in der Vertrauensliste enthaltenen CSP von einem Diensteeintrag pro X.509v3-Zertifikat für einen CA/QC-Zertifizierungsdienst, d. h. eine Zertifizierungsstelle, die (direkt) QCs ausstellt, ausgegangen werden. Unter bestimmten Umständen und bei sorgfältiger Verwaltung kann sich die Aufsichts- bzw. Akkreditierungsstelle eines Mitgliedstaats dazu entschließen, das X.509v3-Zertifikat einer Root oder Upper Level CA (d. h. einer Zertifizierungsstelle, die nicht direkt Anwender-QC ausstellt, sondern eine CA-Hierarchie bis hinunter zu CAs, die QCs für Anwender ausstellen, zertifiziert) als „Sdi“ eines einzigen Eintrags in der Diensteliste eines gelisteten CSP zu verwenden. Die Konsequenzen (Vorteile und Nachteile) der Verwendung des X.509v3-Zertifikats einer Root oder Upper Level CA als „Sdi“-Wert von TL-Diensteeinträgen müssen von den Mitgliedstaaten gründlich erwogen und getragen werden. Im Falle dieser zulässigen Abweichung von der üblichen Vorgangsweise muss der Mitgliedstaat die erforderliche Dokumentation bereitstellen, um den Aufbau und die Verifizierung des Zertifizierungspfads zu ermöglichen.

Das nachstehende Beispiel dient zur Veranschaulichung der allgemeinen Leitlinien zur Bearbeitung: Im Falle eines CSP_{QC}, der eine Root CA verwendet, unter der mehrere CAs QCs und Nicht-QCs ausstellen, dessen QCs jedoch nur die Erklärung zur QcCompliance, aber keine Informationen über eine SSCD-Unterstützung enthalten, würde die Angabe nur der „Sdi“ der Root CA auf der Grundlage der oben ausgeführten Regeln bedeuten, dass KEINES der aufgrund dieser Root CA-Hierarchie ausgestellten QCs von einer SSCD unterstützt wird. Liegt tatsächlich eine SSCD-Unterstützung der QCs vor, wird dringend empfohlen, bei zukünftig auszustellenden QCs die QcSSCD-Erklärung zu verwenden. Zwischenzeitlich (bis das letzte QC, das diese Information nicht enthält, abläuft), sollte die TSL das Feld „Sie“ und die entsprechende Erweiterung „Qualifications“ nutzen, z. B. zum Filtern von Zertifikaten durch spezielle CSP_{QC}-definierte OIDs, die von den CSP_{QC} potenziell zur Unterscheidung zwischen unterschiedlichen QC-Typen (einige mit, einige ohne SSCD-Unterstützung) verwendet werden und im Hinblick auf diese gefilterten Zertifikate durch die Nutzung von „Kennzeichnern“ eindeutige „SSCD support information“ enthalten.

Die allgemeinen Leitlinien zur Nutzung von Anwendungen und Diensten im Zusammenhang mit elektronischen Signaturen oder Produkten, die auf einer TSL-Implementierung einer vertrauenswürdigen Liste gemäß den vorliegenden technischen Spezifikationen basieren, lauten folgendermaßen:

Ein „CA/QC“-„Sti“-Eintrag (ebenso wie ein CA/QC-Eintrag, der durch die Verwendung der „Sie“-„additionalServiceInformation“-Erweiterung näher als „RootCA/QC“ bestimmt wurde)

— bedeutet, dass alle durch die mit „Sdi“ identifizierte CA (ebenso bei der CA-Hierarchie, die von der mit „Sdi“ identifizierten RootCA ausgeht) ausgestellten Anwenderzertifikate QCs sind, vorausgesetzt, dass dies im Zertifikat durch die Verwendung der entsprechenden Erklärungen (d. h. QcC, QcSSCD) und/oder der vom ETSI definierten QCP(+) OIDs angegeben wird (und von der Aufsichts- bzw. Akkreditierungsstelle gewährleistet wird, vgl. „Allgemeine Leitlinien zur Bearbeitung“ oben).

Hinweis: Wenn keine „Sie“-„Qualification“-Informationen vorhanden sind oder ein als QC bezeichnetes Anwenderzertifikat nicht durch einen entsprechenden „Sie“-Eintrag näher bezeichnet ist, wird die Korrektheit der maschinenlesbaren Informationen im QC beaufsichtigt bzw. akkreditiert. Damit wird gewährleistet, dass die Verwendung (oder Nicht-Verwendung) der entsprechenden Erklärungen (d. h. QcC, QcSSCD) und bzw. oder der vom ETSI definierten QCP(+) OIDs den Angaben des CSP_{QC} entspricht.

▼C1

— und WENN „Sie“-„Qualification“-Informationen vorhanden sind, müssen — zusätzlich zur obigen Standard-Auslegungungsregel — Zertifikate, die durch die Verwendung dieses „Sie“-„Qualification“-Eintrags identifiziert werden, der auf dem Grundsatz einer Abfolge von „Filtern“ zur näheren Identifikation einer Gruppe von Zertifikaten beruht und Zusatzinformationen zu „SSCD-Support“ und bzw. oder „Legal person as subject“ enthält (z. B. jene Zertifikate, die einen speziellen OID in der Certificate Policy-Erweiterung enthalten und/oder ein spezielles „Key usage“-Muster aufweisen und/oder durch die Verwendung eines speziellen Werts, der in einem eigenen Feld oder einer Erweiterung des Zertifikats aufscheint, gefiltert werden usw.), anhand der nachstehenden Gruppe von „Kennzeichnern“, die die fehlenden Angaben im entsprechenden QC ausgleichen, interpretiert werden. D. h.:

— Angabe von SSCD-Unterstützung:

  — Bedeutung des Kennzeichnerwerts „QCWithSSCD“: „QC unterstützt durch eine SSCD“ oder

  — Bedeutung des Kennzeichnerwerts „QCNoSSCD“: „QC nicht durch eine SSCD unterstützt“ oder

  — Bedeutung des Kennzeichnerwerts „QCSSCDStatusAsInCert“: Angaben über SSCD-Unterstützung in jedem QC im Rahmen der unter „Sdi“-„Sie“ angegebenen Informationen in diesem CA/QC-Eintrag sichergestellt;

  UND/ODER

— Angabe der Ausstellung für juristische Person:

  — Bedeutung des Kennzeichnerwerts „QCForLegalPerson“: „Zertifikat wurde für juristische Person ausgestellt“

2.4 *Dienste, die „CA/QC“-Dienste unterstützen, aber nicht Bestandteil der „CA/QC“-„Sdi“ sind*

Auch Fälle, in denen CRLs (Certificate Revocation List — Zertifikatsperrliste) und OCSP-Responses durch Schlüssel signiert sind, die nicht von einer CA stammen, die QCs ausstellt („CA/QC“), sollten abgedeckt werden. Dies kann durch die Auflistung dieser Dienste als solche in der TSL-Implementierung der TL erfolgen (d. h. mit einem „Service type identifier“, der durch eine „additional-ServiceInformation“-Erweiterung näher bestimmt wird, die ein OCSP oder einen CRL-Dienst als Bestandteil der Bereitstellung von QCs ausweist; z. B. mit dem Dienstetyp „OCSP/QC“ bzw. „CRL/QC“), da diese Dienste als Teil der beaufsichtigten bzw. akkreditierten „qualifizierten“ Dienste im Zusammenhang mit der Erbringung von QC-Zertifizierungsdiensten betrachtet werden können. Selbstverständlich sind OCSP-Responder oder CRL-Aussteller, deren Zertifikate von CAs anhand der Hierarchie eines gelisteten CA/QC-Dienstes signiert werden, als „valid“ (gültig) und dem Statuswert des gelisteten CA/QC-Dienstes entsprechend zu betrachten.

Eine ähnliche Bestimmung kann für Zertifizierungsdienste gelten, die nicht qualifizierte Zertifikate (vom Diensttyp „CA/PKC“) unter Verwendung der Standard-OCSP- und CRL-Dienstetypen nach ETSI TS 102 231 ausstellen.

Dabei ist zu berücksichtigen, dass die TSL-Implementierung der TL Sperrdienste beinhalten MUSS, wenn das AIA-Feld der Endzertifikate keine entsprechenden Informationen enthält oder nicht von einer gelisteten CA signiert ist.

2.5 *Ansätze für ein interoperables QC-Profil*

Generell muss versucht werden, die Anzahl der Diensteeinträge (unterschiedliche „Sdi“) so weit wie möglich zu reduzieren. Dabei muss jedoch auf eine korrekte Identifikation jener Dienste geachtet werden, die mit der Ausstellung von QCs und der Bereitstellung zuverlässiger Informationen darüber, ob diese QCs von einer SSCD unterstützt werden, sofern diese Information im ausgestellten QC fehlt, in Zusammenhang stehen.

▼C1

Im Idealfall sollte die Verwendung des „Sie“-Felds und der „Qualification“-Erweiterung (streng) auf die so zu lösenden speziellen Fälle beschränkt werden, da QCs hinsichtlich des angegebenen qualifizierten Status und der SSCD-Unterstützung ausreichende Informationen enthalten sollten.

Soweit möglich sollten sich die Mitgliedstaaten um die Annahme und Verwendung interoperabler QC-Profile bemühen.

3. **Struktur der gemeinsamen Vorlage für die vertrauenswürdige Liste**

Die vorgeschlagene gemeinsame Vorlage für eine vertrauenswürdige Liste der Mitgliedstaaten wird anhand der nachstehenden Kategorien von Informationen strukturiert:

1. Informationen über die vertrauenswürdige Liste und ihre Ausstellungsmodalitäten;

2. Eine Abfolge von Feldern, die eindeutige Informationen zur Identifizierung jedes beaufsichtigten bzw. akkreditierten CSP enthalten (die Abfolge ist optional; d. h. wenn sie nicht verwendet wird, wird die Liste als leer betrachtet; das bedeutet, dass in Bezug auf die vertrauenswürdige Liste in dem entsprechenden Mitgliedstaat kein CSP beaufsichtigt wird oder akkreditiert ist);

3. Für jeden gelisteten CSP eine Abfolge von Feldern zur eindeutigen Identifizierung eines beaufsichtigten bzw. akkreditierten Zertifizierungsdienstes, der von dem CSP erbracht wird (diese Abfolge muss mindestens einen Eintrag haben);

4. Für jeden gelisteten beaufsichtigten bzw. akkreditierten Zertifizierungsdienst eine Angabe des gegenwärtigen Status des Dienstes sowie der Statusentwicklung (History).

In Bezug auf einen QCs ausstellenden CSP, muss die eindeutige Identifikation eines in die Liste aufzunehmenden beaufsichtigten bzw. akkreditierten Zertifizierungsdienstes Situationen berücksichtigen, in denen im qualifizierten Zertifikat keine ausreichenden Angaben über dessen „qualifizierten“ Status und eine mögliche SSCD-Unterstützung verfügbar sind. Auch der Tatsache, dass der Großteil der (kommerziellen) CSPs nur eine einzige qualifizierte CA zur Ausstellung verschiedener Typen qualifizierter und nicht qualifizierter Anwenderzertifikate verwendet, muss Rechnung getragen werden.

Die Anzahl der Einträge pro anerkanntem CSP in der Liste könnte verringert werden, sofern eine oder mehrere Upper CA existieren; d. h. im Zusammenhang mit einer kommerziellen CA-Hierarchie von einer Root CA bis hinunter zu ausstellenden CAs. Doch selbst in diesen Fällen darf nicht von dem Grundsatz abgewichen werden, dass ein eindeutiger Bezug zwischen einem CSP_{QC}-Zertifizierungsdienst und der Gruppe von Zertifikaten, die als QCs identifiziert werden sollen, gewährleistet sein muss.

1. *Informationen über die vertrauenswürdige Liste und ihre Ausstellungsmodalitäten*

Die nachstehenden Informationen sind Teil dieser Kategorie:

— Ein Tag zur Identifikation der vertrauenswürdigen Liste bei elektronischen Suchvorgängen und zur Bestätigung ihres Zwecks, wenn die Liste in menschenlesbarer Form konsultiert wird;

— Ein Identifikator für Format und Formatversion der vertrauenswürdigen Liste;

— Eine Abfolge- (oder Release-)Nummer;

— Angaben zum Typ der vertrauenswürdigen Liste (z. B. Angabe der Tatsache, dass diese vertrauenswürdigen Liste Informationen über den Aufsichts- bzw. Akkreditierungsstatus der Zertifizierungsdienste von CSPs enthält, die von dem entsprechenden Mitgliedstaat unter Einhaltung der Bestimmungen gemäß Richtlinie 1999/93/EG beaufsichtigt werden bzw. akkreditiert sind);

▼C1

— Angaben über den Eigentümer der vertrauenswürdigen Liste (z. B. Name, Adresse, Kontaktdaten usw. der für die Erstellung, sichere Veröffentlichung und Führung der Vertrauensliste zuständigen Stelle des Mitgliedstaats);

— Angaben zu dem oder zu den Aufsichts- bzw. Akkreditierungssystem(en), denen die vertrauenswürdigen Liste unterliegt; dazu zählen u. a.:

  — das Land, für das die Liste gilt,

  — Angaben zu oder Verweise auf Orte, an denen Informationen über das oder die System(e) verfügbar sind (Vorlage, Vorschriften, Kriterien, Anwendergemeinschaft, Typen usw.)

  — Aufbewahrungszeitraum (historischer) Informationen.

— Richtlinien und/oder rechtlicher Hinweis, Haftung, Verantwortungsbereiche;

— Veröffentlichungsdatum und Zeitpunkt der nächsten planmäßigen Aktualisierung.

2. *Eindeutige Informationen zur Identifizierung jedes vom System anerkannten CSP*

Diese Informationen müssen mindestens Folgendes umfassen:

— Offizielle Bezeichnung der CSP-Einrichtung gemäß amtlicher Registrierung (je nach Praxis im jeweiligen Mitgliedstaat kann hier auch die UID der CSP-Einrichtung angegeben werden);

— Adresse und Kontaktdaten des CSP;

— Zusatzinformationen über den CSP, die entweder direkt oder mittels Verweis auf eine Download-Adresse angegeben werden können.

3. *Für jeden gelisteten CSP eine Abfolge von Feldern zur eindeutigen Identifizierung eines von dem CSP erbrachten Zertifizierungsdienstes, der im Rahmen der Richtlinie 1999/93/EG beaufsichtigt wird bzw. akkreditiert ist*

Diese Informationen müssen für jeden Zertifizierungsdienst eines gelisteten CSP mindestens Folgendes umfassen:

— Einen Identifikator für den Typ des Zertifizierungsdienstes (aus dem z. B. hervorgeht, dass es sich bei dem beaufsichtigten bzw. akkreditierten Zertifizierungsdienst des CSP um eine Zertifizierungsstelle handelt, die QCs ausstellt);

— Den (Handels-)Namen dieses Zertifizierungsdienstes;

— Einen eindeutigen, unverwechselbaren Identifikator des Zertifizierungsdienstes;

— Zusatzinformationen über den Zertifizierungsdienst (z. B. direkt angegeben oder mittels Verweis auf eine Download-Adresse, Zugangsinformationen in Bezug auf den Dienst);

— Für CA- bzw. QC-Dienste eine optionale Abfolge von Informationstupeln, von denen jedes folgende Angaben enthält:

  i. Kriterien zur näheren Identifikation (Filterung) des Dienstes (d. h. die Gruppe qualifizierter Zertifikate), für welchen im Hinblick auf die Angabe der SSCD-Unterstützung (bzw. der Ausstellung für juristische Personen) Zusatzinformationen erforderlich sind bzw. angegeben werden, aus dem durch die „Sdi“ identifizierten Zertifizierungsdienst;

  ii. Verknüpfte „Kennzeichner“, die darüber informieren, ob die Gruppe qualifizierter Zertifikate dieses näher identifizierten Dienstes von einer SSCD unterstützt wird und/oder ob solche QCs juristischen Personen ausgestellt werden (standardmäßig ist davon auszugehen, dass sie nur natürlichen Personen ausgestellt werden).

▼C1

4. *Für jeden gelisteten Zertifizierungsdienst eine Angabe des gegenwärtigen Status des Dienstes sowie der Statusentwicklung*

Diese Informationen müssen mindestens Folgendes umfassen:

— Einen Identifikator des „Current status“;

— Datum und Uhrzeit des Beginns des „Current status“;

— Historische Informationen zu diesem Status.

4. **Begriffsbestimmungen und Abkürzungen**

Für dieses Dokument gelten folgende Begriffsbestimmungen und Kurzbezeichnungen:

Begriff	Kurzbezeichnung	Begriffsbestimmung
Zertifizierungsdiensteanbieter (Certification Service Provider)	CSP	Definition nach Artikel 2 Absatz 11 der Richtlinie 1999/93/EG.
Zertifizierungsstelle (Certification Authority)	CA	Eine CA ist ein CSP. Sie kann zur Ausstellung von Anwenderzertifikaten die privaten Signaturschlüssel mehrerer technischer CAs verwenden, von denen jeder über ein Zertifikat verfügt. Eine CA ist eine Stelle, die von einem oder mehreren Anwendern mit der Erstellung und Zuweisung von Zertifikaten betraut wird. Optional kann die Zertifizierungsstelle die Benutzerschlüssel erstellen [ETSI TS 102 042]. Die CA kann durch die Identifikationsangaben im „Issuer“-Feld des CA-Zertifikats zur Zertifizierung des zum privaten Signaturschlüssel der CA gehörigen öffentlichen Schlüssels, die von der CA zur Ausstellung von Anwenderzertifikaten verwendet werden, identifiziert werden. Eine CA kann über mehrere Signaturschlüssel verfügen. Jeder Signaturschlüssel einer CA wird durch einen eindeutigen Identifikator identifiziert, der Teil des Felds „Authority Key Identifier“ im Zertifikat der CA ist.
Zertifizierungsstelle, die qualifizierte Zertifikate ausstellt	CA/QC	Eine CA, welche die Anforderungen laut Anhang II der Richtlinie 1999/93/EG erfüllt und qualifizierte Zertifikate ausstellt, die Anhang I der Richtlinie 1999/93/EG entsprechen.
Zertifikat	Zertifikat	Definition nach Artikel 2 Absatz 9 der Richtlinie 1999/93/EG.
Qualifiziertes Zertifikat (Qualified Certificate)	QC	Definition nach Artikel 2 Absatz 10 der Richtlinie 1999/93/EG.
Unterzeichner (Signatory)	Unterzeichner	Definition nach Artikel 2 Absatz 3 der Richtlinie 1999/93/EG.
Aufsicht (Supervision)	Aufsicht	Der Begriff „Aufsicht“ wird in der Bedeutung der Richtlinie 1999/93/EG („Überwachung“ in Artikel 3 Absatz 3) verwendet. Die Richtlinie sieht vor, dass die Mitgliedstaaten ein angemessenes System zur Überwachung der auf ihrem Staatsgebiet ansässigen CSPs einrichten, die qualifizierte Zertifikate für die Öffentlichkeit ausstellen, damit die Einhaltung der Bestimmungen der Richtlinie gewährleistet ist.
Freiwillige Akkreditierung (Voluntary Accreditation)	Akkreditierung	Definition nach Artikel 2 Absatz 13 der Richtlinie 1999/93/EG.
vertrauenswürdige Liste (Trusted List)	TL	Bezeichnet die Liste, aus welcher der Aufsichts- bzw. Akkreditierungsstatus der Zertifizierungsdienste von Zertifizierungsdiensteanbietern, die vom jeweiligen Mitgliedstaat beaufsichtigt werden bzw. akkreditiert sind, hervorgeht, um den Bestimmungen der Richtlinie 1999/93/EG Genüge zu tun.

▼C1

Begriff	Kurzbezeichnung	Begriffsbestimmung
Statusliste vertrauenswürdiger Dienste (Trust Service Status List)	TSL	Form einer signierten Liste, die als Grundlage zur Darstellung von Statusinformationen über vertrauenswürdige Dienste gemäß den Spezifikationen laut ETSI TS 102 231 dient.
Vertrauenswürdiger Dienst (Trust Service)		Ein Dienst, der das Vertrauen in elektronische Transaktionen erhöht (üblicherweise aber nicht unbedingt im Zusammenhang mit kryptografischen Methoden oder vertraulichen Daten) (ETSI TS 102 231).
Vertrauenswürdiger Diensteanbieter (Trust Service Provider)	TSP	Stelle, die einen oder mehrere (elektronische) Vertrauensdienste erbringt. (Dieser Begriff wird breiter angewendet als CSP.)
Token für vertrauenswürdigen Dienst (Trust Service Token)	TrST	Ein physisches oder binäres (logisches) Objekt, das infolge der Verwendung eines Vertrauensdienstes erzeugt oder ausgestellt wird. Beispiele für binäre TrSTs sind Zertifikate, CRLs, Zeitstempel-Tokens und OCSP-Responses.
Qualifizierte elektronische Signatur (Qualified Electronic Signature)	QES	Eine von einem QC unterstützte AdES, die von einer SSCD gemäß Definition laut Artikel 2 der Richtlinie 1999/93/EG erstellt wird.
Fortgeschrittene elektronische Signatur (Advanced Electronic Signature)	AdES	Definition nach Artikel 2 Absatz 2 der Richtlinie 1999/93/EG.
Von einem qualifizierten Zertifikat unterstützte fortgeschrittene elektronische Signatur	$AdES_{QC}$	Bezeichnet eine elektronische Signatur, die die Erfordernisse einer AdES erfüllt und von einem der Definition in Artikel 2 der Richtlinie 1999/93/EG entsprechenden QC unterstützt wird.
Sichere Signaturerstellungseinheit (Secure Signature Creation Device)	SSCD	Definition nach Artikel 2 Absatz 6 der Richtlinie 1999/93/EG.

KAPITEL I

AUSFÜHRLICHE SPEZIFIKATIONEN FÜR DIE GEMEINSAME VORLAGE FÜR DIE „VERTRAUENSWÜRDIGE LISTE DER BEAUFSICHTIGTEN BZW. AKKREDITIERTEN ZERTIFIZIERUNGSDIENSTEANBIETER“

Die im nachstehenden Teil dieses Dokuments verwendeten Schlüsselbegriffe „MUSS“ bzw. „MÜSSEN“, „DARF NICHT“ bzw. „DÜRFEN NICHT“, „ERFORDERLICH“, „SOLLTE(N)“, „SOLLTE(N) NICHT“, „EMPFOHLEN“, „KANN“ bzw. „KÖNNEN“ und „OPTIONAL“ sind in Anlehnung an die in englischer Sprache in RFC 2119 ([1]) vorliegenden Begriffe auszulegen.

►**M1** Diese Spezifikationen beruhen auf den im Dokument ETSI TS 102231 v3.1.2 enthaltenen Spezifikationen und Anforderungen. Soweit die vorliegenden Spezifikationen keine speziellen Anforderungen vorgeben, MÜSSEN die Anforderungen aus ETSI TS 102231 v.3.1.2 in ihrer Gesamtheit erfüllt werden. ◄ Sehen die vorliegenden Spezifikationen spezielle Anforderungen vor, MÜSSEN diese den entsprechenden Anforderungen laut ETSI TS 102 231 gegenüber vorrangig behandelt werden. Sie werden jedoch durch die Formatspezifikationen in ETSI TS 102 231 ergänzt. Bei Widersprüchen zwischen den vorliegenden und den Spezifikationen laut ETSI TS 102 231 MUSS den vorliegenden Spezifikationen normative Wirkung eingeräumt werden.

([1]) IETF RFC 2119: „Key words for use in RFCs to indicate Requirements Levels“.

▼C1

Zumindest Unterstützung für die englische Sprache (EN) MUSS implementiert werden und zur Verfügung stehen. Potenziell können eine oder mehrere zusätzliche Landessprachen unterstützt werden.

Datums- und Zeitangaben MÜSSEN Abschnitt 5.1.4 von ETSI TS 102 231 entsprechen.

Die Verwendung von URIs MUSS Abschnitt 5.1.5 von ETSI TS 102 231 entsprechen.

Informationen über das Herausgabesystem der vertrauenswürdigen Liste

Tag

TSL tag (Abschnitt 5.2.1)

Dieses Feld ist ERFORDERLICH und MUSS Abschnitt 5.2.1 von ETSI TS 102 231 entsprechen.

▼M1

———————

▼C1

Scheme Information

TSL version identifier (Abschnitt 5.3.1)

Dieses Feld ist ERFORDERLICH und MUSS auf „3“ gesetzt werden (ganze Zahl).

TSL sequence number (Abschnitt 5.3.2)

▼M1

Dieses Feld ist ERFORDERLICH. Es MUSS die laufende Nummer der TSL enthalten. Beginnend bei „1“ bei der ersten Veröffentlichung der TSL, MUSS dieser ganzzahlige Wert bei jeder neuen Ausgabe der TSL erhöht werden. Der Wert DARF bei der Erhöhung des obigen „TSL version identifier“ NICHT zurück auf „1“ gesetzt werden.

▼C1

TSL type (Abschnitt 5.3.3)

▼M1

Dieses Feld zur Angabe des Typs der TSL ist ERFORDERLICH. Es MUSS auf http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic (Generic) gesetzt werden.

▼C1

Anmerkung: Zur Einhaltung von ETSI TS 102 231, Abschnitt 5.3.3, zur Angabe des speziellen TSL-Typs mit einem Verweis auf das Vorhandensein der vorliegenden Spezifikationen zur TSL-Implementierung der vertrauenswürdigen Liste ([1]) der Mitgliedstaaten und um es einem Parser zu erlauben, zu bestimmen, welche Formen der folgenden Felder ([2]) zu erwarten sind, wenn diese Felder spezielle (oder alternative) Bedeutungen je nach Typ der entsprechenden TSL (in diesem Fall handelt es sich um eine vertrauenswürdige Liste eines Mitgliedstaats) haben, MUSS der obige spezielle URI registriert und folgendermaßen beschrieben werden:

([1]) D. h. die Aufsichts- bzw. Akkreditierungsstatusliste der Zertifizierungsdienste von Zertifizierungsdiensteanbietern, die vom entsprechenden Mitgliedstaat im Hinblick auf die Einhaltung der entsprechenden Bestimmungen der Richtlinie 1999/93/EG beaufsichtigt werden bzw. akkreditiert sind (die „vertrauenswürdige Liste“).

([2]) D. h. die Felder, die in ETSI TS 102 231 — Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information angegeben und durch die vorliegenden Spezifikationen zur Erstellung der vertrauenswürdigen Listen der Mitgliedstaaten definiert sind.

▼M1

URI: http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic

▼C1

Beschreibung: Eine TSL-Implementierung einer Aufsichts- bzw. Akkreditierungsstatusliste der Zertifizierungsdienste von Zertifizierungsdiensteanbietern, die von dem Mitgliedstaat beaufsichtigt werden bzw. akkreditiert sind, der durch unmittelbare Aufsicht (sei es freiwillig oder durch gesetzliche Vorschriften) für die Einhaltung der anwendbaren Bestimmungen der Richtlinie 1999/93/EG bei der TSL-Implementierung verantwortlich ist.

Scheme operator name (Abschnitt 5.3.4)

Dieses Feld ist ERFORDERLICH. Es MUSS den Namen der für die Erstellung, Veröffentlichung und Führung der einzelstaatlichen vertrauenswürdigen Liste in dem Mitgliedstaat zuständigen Stelle enthalten. Das Feld MUSS die offizielle Bezeichnung enthalten, unter der der entsprechende Rechtsträger oder die beauftragte Stelle (z. B. bei staatlichen Verwaltungsbehörden) tätig ist. Angegeben werden MUSS die für die offizielle Registrierung oder Autorisierung verwendete Bezeichnung, an die alle formellen Mitteilungen zu richten sind. Es MUSS sich um eine Abfolge mehrsprachiger Zeichenketten handeln, die mit Englisch (EN) als obligatorischer und potenziell einer oder mehreren zusätzlichen Landessprache(n) implementiert werden MÜSSEN.

Hinweis: Ein Land KANN über separate Aufsichts- und Akkreditierungsstellen und sogar über zusätzliche Einrichtungen für beliebige operative Aktivitäten verfügen. ►M1 Es obliegt jedem einzelnen Mitgliedstaat, den „Scheme operator“ der TSL-Implementierung der TL des Mitgliedstaats zu benennen. ◄ Es wird davon ausgegangen, dass die Aufsichtsstelle, die Akkreditierungsstelle und der „Scheme operator“ (wenn es sich um separate Stellen handelt) unterschiedliche Zuständigkeits- und Haftungsbereiche haben.

Jede Situation, in der mehrere Stellen für Aufsicht, Akkreditierung oder operative Aspekte zuständig sind, MUSS konsequent reflektiert und in der „Scheme information“ als Bestandteil der TL sowie in den systemspezifischen Informationen im „Scheme information URI“ (Abschnitt 5.3.7) als solche identifiziert werden.

▼M1

Der benannte „Scheme operator“ (Abschnitt 5.3.4) signiert die TSL.

▼C1

Scheme operator address (Abschnitt 5.3.5)

Dieses Feld ist ERFORDERLICH. Es MUSS die Adresse des im Feld „Scheme operator name“ (Abschnitt 5.3.4) benannten Rechtsträgers oder der beauftragten Stelle für den Versand von postalischen und elektronischen Mitteilungen enthalten. Es MUSS die „PostalAddress“ (d. h. Straße, Hausnummer, Ort, [Staat oder Bundesland], [Postleitzahl] und den ISO 3166-1 Alpha-2-Ländercode) gemäß Abschnitt 5.3.5.1 sowie die „ElectronicAddress“ (d. h. E-Mail und/oder Website-URI) gemäß Abschnitt 5.3.5.2 beinhalten.

Scheme name (Abschnitt 5.3.6)

Dieses Feld zur Angabe des Systemnamens ist ERFORDERLICH. Es MUSS sich um eine Abfolge mehrsprachiger Zeichenketten handeln (wobei EN die obligatorische Sprache ist und potenziell eine oder mehrere zusätzliche Landessprachen verwendet werden können), die folgendermaßen definiert sind:

▼C1

— Die EN-Fassung MUSS eine folgendermaßen aufgebaute Zeichenkette sein:

CC:EN_name_value

dabei ist

— „CC“ = der im Feld „Scheme territory“ (Abschnitt 5.3.10) verwendete ISO 3166-1 Alpha-2-Ländercode;

— „:“ = das Trennzeichen;

▼M1

— „EN_name_value“ = „Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC and its implementation in the referenced Member State’s laws;“

▼C1

— Die landesspezifischen Sprachfassungen der Mitgliedstaaten MÜSSEN folgendermaßen aufgebaute Zeichenketten sein:

CC:name_value

dabei ist

— „CC“ = der im Feld „Scheme territory“ (Abschnitt 5.3.10) verwendete ISO 3166-1 Alpha-2-Ländercode;

— „:“ = das Trennzeichen;

— „name_value“ = Die amtliche Übersetzung des obigen Werts „EN_name_value“ in die Landessprache (für das Deutsche: „Aufsichts- bzw. Akkreditierungsstatusliste der Zertifizierungsdienste von Zertifizierungsdiensteanbietern, die von der zuständigen Stelle des entsprechenden Mitgliedstaats im Hinblick auf die Einhaltung der entsprechenden Bestimmungen der Richtlinie 1999/93/EG beaufsichtigt werden bzw. akkreditiert sind“.).

Der Systemname dient zur eindeutigen, namentlichen Identifikation des im Feld „Scheme information URI“ bezeichneten Systems und gewährleistet, dass — wenn ein „Scheme operator“ mehrere Systeme betreibt — jedes davon eindeutig benannt ist.

Die Mitgliedstaaten und „Scheme operators“ MÜSSEN sicherstellen, dass jedes System einen eindeutigen Namen trägt, wenn ein Mitgliedstaat oder ein „Scheme operator“ mehrere Systeme betreibt.

Scheme information URI (Abschnitt 5.3.7)

Dieses Feld ist ERFORDERLICH und MUSS den bzw. die URI(s) enthalten, unter denen Anwender (auf das Zertifikat vertrauende Parteien) systemspezifische Informationen erhalten (dabei ist EN obligatorisch und eine oder mehrere Landessprachen sind potenziell zusätzlich möglich). Es MUSS sich um eine Abfolge mehrsprachiger Zeiger handeln (wobei EN die obligatorische Sprache ist und potenziell eine oder mehrere Landessprachen verwendet werden können). Der bzw. die entsprechende(n) URI(s) MUSS bzw. MÜSSEN einen Pfad zu angemessenen Informationen über das System („appropriate information about the scheme“) bieten.

Diese angemessenen Informationen MÜSSEN zumindest Folgendes enthalten:

— Allgemeine, einleitende Informationen, die hinsichtlich Umfang und Hintergrund der vertrauenswürdigen Liste und der zugrunde liegenden Aufsichts- bzw. Akkreditierungssysteme für alle Mitgliedstaaten identisch sind. Der gemeinsame Wortlaut lautet folgendermaßen:

▼C1

„The present list is the TSL implementation of [name des entsprechenden Mitgliedstaats] ‚Trusted List of supervised/accredited Certification Service Providers' providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by [name of the relevant Member State] for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

The Trusted List aims at:

— listing and providing reliable information on the supervision/accreditation status of certification services from Certification Service Providers, who are supervised/accredited by [name of the relevant Member State] for compliance with the relevant provisions laid down in Directive 1999/93/EC;

— facilitating the validation of electronic signatures supported by those listed supervised/accredited certification services from the listed CSPs.

The Trusted List of a Member State provides a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3.3, 3.2 and Art. 7.1(a)), including information on the QC supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

The CSPs issuing Qualified Certificates (QCs) listed here are supervised by [name of the relevant Member State] and may also be accredited for compliance with the provisions laid down in Directive 1999/93/EC, including with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). The applicable ‚supervision' system (respectively ‚voluntary accreditation' system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Art. 3.3, Art. 8.1, Art. 11 (respectively, Art. 2.13, Art. 3.2, Art. 7.1(a), Art. 8.1, Art. 11).

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates usw.) are included in the Trusted List and the present TSL implementation at a national level on a voluntary basis."

— Spezifische Informationen über das bzw. die zugrunde liegende(n) Aufsichts- bzw. Akkreditierungssystem(e), insbesondere ([1]):

— Informationen über das Aufsichtssystem, das für alle CSP_{QC} gilt;

([1]) Die letzten beiden Informationsgruppen sind von entscheidender Bedeutung zur Beurteilung des Qualitäts- und Sicherheitsgrads solcher Aufsichts- bzw. Akkreditierungssysteme durch die auf das Zertifikat vertrauenden Parteien. Diese Informationsgruppen werden auf TL-Ebene bereitgestellt; und zwar durch die Verwendung von „Scheme information URI" (Abschnitt 5.3.7 — von den Mitgliedstaaten bereitgestellte Informationen), „Scheme type/community/rules" (Abschnitt 5.3.9 — Verwendung eines allen Mitgliedstaaten gemeinsamen Texts) und „TSL policy/legal notice" (Abschnitt 5.3.11 — ein allen Mitgliedstaaten gemeinsamer Text, der auf die Richtlinie 1999/93/EG Bezug nimmt sowie die Möglichkeit bietet, einen länderspezifischen Text bzw. Verweise hinzuzufügen). Zusätzliche Informationen über einzelstaatliche Aufsichts- bzw. Akkreditierungssysteme für CSPs, die keine QCs ausstellen, können auf der Dienstebene ggf. und wenn erforderlich (z. B. zur Unterscheidung zwischen verschiedenen Qualitäts-/Sicherheitsgraden) durch die Verwendung der „Scheme service definition URI" (Abschnitt 5.5.6) bereitgestellt werden.

▼C1

— Ggf. Informationen über das einzelstaatliche freiwillige Akkreditierungssystem, das für alle CSP_{QC} gilt;

— Ggf. Informationen über das Aufsichtssystem, das für alle CSPs gilt, die keine QCs ausstellen;

— Ggf. Informationen über das einzelstaatliche freiwillige Akkreditierungssystem, das für alle CSPs gilt, die keine QCs ausstellen.

— Diese spezifischen Informationen MÜSSEN für jedes oben genannte zugrunde liegende System zumindest Folgendes enthalten:

— Allgemeine Beschreibung;

— Informationen über das von der Aufsichts- bzw. Akkreditierungsstelle durchgeführte Verfahren zur Aufsicht bzw. Akkreditierung von CSPs sowie über das von den CSPs zur Aufsicht bzw. Akkreditierung durchgeführte Verfahren;

— Informationen über die Kriterien, anhand welcher CSPs beaufsichtigt bzw. akkreditiert werden.

— Ggf. spezielle Informationen über die besondere „Qualification“, auf welche die infolge der Bereitstellung eines Zertifizierungsdienstes generierten oder ausgestellten physischen oder binären (logischen) Objekte Anspruch haben können, wenn sie den einzelstaatlichen Bestimmungen und Anforderungen entsprechen, einschließlich der Bedeutung einer derartigen „Qualification“ und der entsprechenden einzelstaatlichen Bestimmungen und Anforderungen.

Weitere länderspezifische Informationen über das System KÖNNEN zusätzlich auf freiwilliger Basis bereitgestellt werden. Diese MÜSSEN umfassen:

— Informationen über die Kriterien und Vorschriften zur Auswahl von Aufsichtspersonen bzw. Prüfern und zur Festlegung, wie CSPs von diesen beaufsichtigt (kontrolliert) bzw. akkreditiert (geprüft) werden;

— Weitere Kontaktdaten und allgemeine Informationen über den Betrieb des Systems.

Status determination approach (Abschnitt 5.3.8)

Dieses Feld ist ERFORDERLICH und MUSS den Identifikator des Ansatzes zur Statusermittlung enthalten. Der nachstehende spezielle URI MUSS verwendet werden, wie unten beschrieben und registriert:

URI: http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/StatusDetn/appropriate

Beschreibung: Der Status gelisteter Dienste wird von oder im Namen des „Scheme operator“ in einem entsprechenden Mitgliedstaat anhand eines angemessenen Systems bestimmt, das die „Aufsicht“ (und ggf. „freiwillige Akkreditierung“) von Zertifizierungsdiensteanbietern erlaubt, die auf dem Staatsgebiet dieses Mitgliedstaats (oder, im Fall der „freiwilligen Akkreditierung“ in einem Drittland) ansässig sind, und die gemäß Artikel 3 Absatz 3 (bzw. Artikel 3 Absatz 2 oder Artikel 7 Absatz 1 Buchstabe a) der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen qualifizierte Zertifikate für die Öffentlichkeit ausstellen. Dieses angemessene System kann gegebenenfalls auch die „Aufsicht“ bzw. „freiwillige Akkreditierung“ von Zertifizierungsdiensteanbietern, die keine qualifizierten Zertifikate ausstellen, auf der Grundlage einzelstaatlich definierter und festgelegter „anerkannter Genehmigungssysteme“ („recognised approval scheme(s)“) ermöglichen. Diese „anerkannten Genehmigungssysteme“ dienen auf einzelstaatlicher Ebene zur Aufsicht der Einhaltung der Bestimmungen der Richtlinie 1999/93/EG durch CSPs, die keine QCs ausstellen, und können im Hinblick auf die Bereitstellung solcher Zertifizierungsdienste potenziell durch einzelstaatliche Bestimmungen erweitert werden.

▼C1

Scheme type/community/rules (Abschnitt 5.3.9)

Dieses Feld ist ERFORDERLICH und MUSS mindestens die nachstehenden registrierten URIs enthalten:

— Ein allen vertrauenswürdigen Listen der Mitgliedstaaten gemeinsamer URI, der auf einen deskriptiven Text verweist, der für alle TLs gelten MUSS:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/common

Der deskriptive Text enthält:

— Angaben über die Teilnahme des Systems des Mitgliedstaats (identifiziert über „TSL type“ (Abschnitt 5.3.3) und „Scheme name“ (Abschnitt 5.3.6)) am Gesamtsystem (d. h. eine TSL, die Zeiger auf alle Mitgliedstaaten enthält, die eine TL in Form einer TSL veröffentlichen und pflegen);

— Angaben, wo Benutzer die Richtlinien bzw. Vorschriften erhalten, anhand welcher die in die Liste aufgenommenen Dienste bewertet werden MÜSSEN und anhand welcher sich der Typ der TSL (Abschnitt 5.3.3) bestimmen lässt;

— Angaben, wo Benutzer eine Anleitung zur Verwendung und Auslegung des Inhalts der TSL-Implementierung der vertrauenswürdigen Liste erhalten. Diese Verwendungsvorschriften MÜSSEN, unabhängig vom Typ des gelisteten Dienstes und dem/den Aufsichts- bzw. Akkreditierungssystem(en) den vertrauenswürdigen Listen aller Mitgliedstaaten gemeinsam sein.

Deskriptiver Text:

„Participation in a scheme

Each Member State must create a ‚Trusted List of supervised/accredited Certification Service Providers‘ providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by the relevant Member State for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

The present TSL implementation of such Trusted Lists is also to be referred to in the list of links (pointers) towards each Member State's TSL implementation of their Trusted List, compiled by the European Commission.

Policy/rules for the assessment of the listed services

The Trusted List of a Member State must provide a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3.3, 3.2 and Art. 7.1(a)), including information on the Qualified Certificate (QC) supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

▼C1

The CSPs issuing Qualified Certificates (QCs) must be supervised by the Member State in which they are established (if they are established in a Member State), and may also be accredited, for compliance with the provisions laid down in Directive 1999/93/EC, including with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). CSPs issuing QCs that are accredited in a Member State must still fall under the appropriate supervision system of that Member State unless they are not established in that Member State. The applicable ‚supervision' system (respectively ‚voluntary accreditation' system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Art. 3.3, Art. 8.1, Art. 11 (respectively, Art. 2.13, Art. 3.2, Art. 7.1(a), Art. 8.1, Art. 11)

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates usw.) may be included in the Trusted List and the present TSL implementation at a national level on a voluntary basis.

CSPs not issuing QCs but providing ancillary services, may fall under a ‚voluntary accreditation' system (as defined in and in compliance with Directive 1999/93/EC) and/or under a nationally defined ‚recognised approval scheme' implemented on a national basis for the supervision of compliance with the provisions laid down in Directive 1999/93/EC and possibly with national provisions with regard to the provision of certification services (in the sense of Art. 2.11 of the Directive). Some of the physical or binary (logical) objects generated or issued as a result of the provision of a certification service may be entitled to receive a specific ‚qualification' on the basis of their compliance with the provisions and requirements laid down at national level but the meaning of such a ‚qualification' is likely to be limited solely to the national level.

Interpretation of the TSL implementation of the Trusted List

The general user guidelines for electronic signature applications, services or products relying on a TSL implementation of a Trusted List according to the Annex of Commission Decision 2009/767/EG are as follows:

A ‚CA/QC',Service type identifier' (‚Sti') entry (similarly a CA/QC entry further qualified as being a ‚RootCA/QC' through the use of ‚Service information extension' (‚Sie') additionalServiceInformation extension)

— indicates that from the ‚Service digital identifier' (‚Sdi') identified CA (similarly within the CA hierarchy starting from the ‚Sdi' identified RootCA) from the corresponding CSP (see associated TSP information fields), all issued end-entity certificates are Qualified Certificates (QCs) provided that it is claimed as such in the certificate through the use of appropriate ETSI TS 101 862 defined QcStatements (i.e. QcC, QcSSCD) and/or ETSI TS 101 456 defined QCP(+) OIDs (and this is guaranteed by the issuing CSP and ensured by the Member State Supervisory/Accreditation Body)

▼C1

Note: if no ‚Sie',Qualification' information is present or if an end-entity certificate that is claimed to be a QC is not ‚further identified' through a related ‚Sie' entry, then the ‚machine-processable' information to be found in the QC is supervised/accredited to be accurate. That means that the usage (or not) of the appropriate ETSI defined QcStatements (i.e. QcC, QcSSCD) and/or ETSI defined QCP(+) OIDs is ensured to be in accordance with what it is claimed by the CSP issuing QCs.

— and IF ‚Sie',Qualification' information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this ‚Sie',Qualification' entry, which is constructed on the principle of a sequence of ‚filters' further identifying a set of certificates, must be considered according to the associated ‚qualifiers' providing some additional information regarding ‚SSCD support' and/or ‚Legal person as subject' (e.g. those certificates containing a specific OID in the Certificate Policy extension, and/or having a specific ‚Key usage' pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension usw.). Those qualifiers are part of the following set of ‚qualifiers' used to compensate for the lack of information in the corresponding QC content, and that are used respectively:

— to indicate the nature of the SSCD support:

— ‚QCWithSSCD' qualifier value meaning ‚QC supported by an SSCD', or

— ‚QCNoSSCD' qualifier value meaning ‚QC not supported by an SSCD', or

— ‚QCSSCDStatusAsInCert' qualifier value meaning that the SSCD support information is ensured to be contained in any QC under the ‚Sdi'-‚Sie' provided information in this CA/QC entry;

AND/OR

— to indicate issuance to Legal Person:

— ‚QCForLegalPerson' qualifier value meaning ‚Certificate issued to a Legal Person'

The general interpretation rule for any other ‚Sti' type entry is that the listed service named according to the ‚Sn' field value and uniquely identified by the ‚Sdi' field value has a current supervision/accreditation status according to the ‚Scs' field value as from the date indicated in the ‚Current status starting date and time'. Specific interpretation rules for any additional information with regard to a listed service (e.g. ‚Service information extensions' field) may be found, when applicable, in the Member State specific URI as part of the present ‚Scheme type/community/rules' field.

Please refer to the Technical specifications for a Common Template for the ‚Trusted List of supervised/accredited Certification Service Providers' in the Annex of Commission Decision 2009/767/EG for further details on the fields, description and meaning for the TSL implementation of the Member States' Trusted Lists."

▼C1

— Ein für alle vertrauenswürdigen Listen der Mitgliedstaaten unterschiedlicher spezieller URI, der auf einen deskriptiven Text verweist, der für die TL dieses Mitgliedstaats gelten MUSS:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/CC

dabei ist CC = der im Feld „Scheme territory“ (Abschnitt 5.3.10) verwendete ISO 3166-1 Alpha-2-Ländercode

Der deskriptive Text enthält:

— Angaben, wo Benutzer die Richtlinien/Vorschriften des angegebenen Mitgliedstaats erhalten, anhand welcher die in die Liste aufgenommenen Dienste aufgrund des entsprechenden Aufsichtssystems und der freiwilligen Akkreditierungssysteme des Mitgliedstaats bewertet werden MÜSSEN.

— Angaben, wo Benutzer eine länderspezifische Anleitung des entsprechenden Mitgliedstaats zur Verwendung und Auslegung des Inhalts der TSL-Implementierung der vertrauenswürdigen Liste im Hinblick auf Zertifizierungsdienste, bei denen es sich nicht um die Ausstellung von QCs handelt, erhalten. Dadurch kann in Bezug auf CSPs, die keine QCs ausstellen, eine potenzielle Granularität in den einzelstaatlichen Aufsichts- bzw. Akkreditierungssystemen demonstriert und gezeigt werden, wie die Felder „Scheme service definition URI“ (Abschnitt 5.5.6) und „Service information extension“ zu diesem Zweck verwendet werden.

Die Mitgliedstaaten KÖNNEN aufgrund des obigen länderspezifischen URI zusätzliche URIs definieren (d. h. URIs, die auf diesem hierarchischen spezifischen URI basieren).

Scheme territory (Abschnitt 5.3.10)

Im Zusammenhang mit den vorliegenden Spezifikationen ist dieses Feld ERFORDERLICH und MUSS das Land angeben, in dem das System angesiedelt ist (ISO 3166-1 Alpha-2-Ländercode).

TSL policy/legal notice (Abschnitt 5.3.11)

Im Zusammenhang mit den vorliegenden Spezifikationen ist dieses Feld ERFORDERLICH und MUSS die Richtlinien des Systems oder einen rechtlichen Hinweis zum Rechtsstatus des Systems bzw. die vom System in der Rechtsordnung, der es angehört, erfüllten rechtlichen Anforderung bzw. alle Beschränkungen und Bedingungen enthalten, unter denen die TL veröffentlicht und gepflegt wird.

Es MUSS sich um eine Abfolge mehrsprachiger Zeichenketten (Klartext) handeln, die aus zwei Teilen besteht:

— Ein erster obligatorischer Teil, der den TLs aller Mitgliedstaaten gemeinsam ist, (dabei ist EN obligatorisch und eine oder mehrere Landessprachen sind potenziell möglich), aus dem hervorgeht, dass der anwendbare Rechtsrahmen Richtlinie 1999/93/EG und ihre entsprechende Umsetzung in die einzelstaatlichen Gesetze des im Feld „Scheme Territory“ angegebenen Mitgliedstaats ist.

Englische Fassung des gemeinsamen Texts:

„The applicable legal framework for the present TSL implementation of the Trusted List of supervised/accredited Certification Service Providers for [name of the relevant Member State] is the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and its implementation in [name of the relevant Member State] laws.“

▼C1

Fassung des gemeinsamen Texts in deutscher Sprache:

— Der anwendbare Rechtsrahmen für die vorliegende TSL-Implementierung der vertrauenswürdigen Liste beaufsichtigter bzw. akkreditierter Zertifizierungsdiensteanbieter für [Name des entsprechenden Mitgliedstaats] ist die Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen und ihre Umsetzung in das einzelstaatliche Recht von [Name des entsprechenden Mitgliedstaats].

— Ein zweiter optionaler Teil, der speziell auf jede TL zugeschnitten wird (dabei ist EN obligatorisch und eine oder mehrere Landessprachen sind potenziell möglich) und der Verweise auf spezielle anwendbare einzelstaatliche Rechtsrahmen enthält (z. B. insbesondere im Zusammenhang mit einzelstaatlichen Aufsichts- bzw. Akkreditierungssystemen für CSPs, die keine QCs ausstellen).

Historical information period (Abschnitt 5.3.12)

Dieses Feld ist ERFORDERLICH und MUSS die (ganzzahlige) Frist enthalten, während welcher historische Informationen in der TSL bereitgestellt werden. Dieser ganzzahlige Wert ist als Anzahl der Tage anzugeben und MUSS im Zusammenhang mit den vorliegenden Spezifikationen größer oder gleich 3 653 sein (d. h., dass die TSL-Implementierungen der TLs der Mitgliedstaaten historische Informationen enthalten MÜSSEN, die mindestens zehn Jahre zurückgehen). Höhere Werte sollten die Rechtsvorschriften in Bezug auf die Aufbewahrung von Daten in dem jeweiligen unter „Scheme Territory“ (Abschnitt 5.3.10) angegebenen Mitgliedstaat berücksichtigen.

Pointers to other TSLs (Abschnitt 5.3.13)

Im Zusammenhang mit den vorliegenden Spezifikationen ist dieses Feld ERFORDERLICH und MUSS, wenn vorhanden, den Zeiger zur einem ETSI TS 102 231-konformen Formular der von den EG zusammengestellten Linkliste (mit Zeigern) zu allen TSL-Implementierungen der vertrauenswürdigen Listen der Mitgliedstaaten enthalten. Die Spezifikationen laut ETSI TS 102 231, Abschnitt 5.3.13 sind anwendbar. Außerdem ist die Verwendung der optionalen digitalen Identität erforderlich, die für den Herausgeber der TSL steht, auf die verwiesen wird, und die formatiert ist, wie in Abschnitt 5.5.3 angegeben.

Hinweis: Während der Wartezeit auf die von den EG zusammengestellte, ETSI TS 102 231-konforme Linkliste zu den TSL-Implementierungen der TLs der Mitgliedstaaten DARF dieses Feld NICHT verwendet werden.

List issue date and time (Abschnitt 5.3.14)

Dieses Feld ist ERFORDERLICH und MUSS Datum und Zeit enthalten (UTC als Zulu ausgedrückt), zu denen die TSL veröffentlich wurde, wobei der Datum-Zeit-Wert anzugeben ist, wie in ETSI TS 102 231, Abschnitt 5.1.4, definiert.

Next update (Abschnitt 5.3.15)

Dieses Feld ist ERFORDERLICH und MUSS das späteste Datum und den spätesten Zeitpunkt angeben (UTC als Zulu ausgedrückt), zu denen die nächste TSL veröffentlich wird, bzw. für abgeschlossene TSL den Wert null enthalten. Der Datum-Zeit-Wert ist anzugeben, wie in ETSI TS 102 231, Abschnitt 5.1.4, definiert.

Erfolgen keine Zwischenstatusänderungen in Bezug auf von dem System abgedeckte TSPs oder Dienste, MUSS die TSL bis zum Ablauf der letzten herausgegebenen TSL neu veröffentlicht werden.

Im Zusammenhang mit den vorliegenden Spezifikationen DARF die Differenz zwischen Datum und Zeit für die nächste Aktualisierung („Next update“) und dem Veröffentlichungszeitpunkt („List issue date and time“) sechs (6) Monate NICHT übersteigen.

▼C1

Distribution points (Abschnitt 5.3.16)

Dieses Feld ist OPTIONAL. Wird es verwendet, MUSS es die Orte angeben, an denen die aktuelle TSL-Implementierung der TL sowie Aktualisierungen der gegenwärtigen TL veröffentlicht werden. Bei Angabe mehrerer Verteilungspunkte („Distribution points“) MÜSSEN diese alle identische Exemplare der gegenwärtigen TSL oder ihrer aktualisierten Fassung bereitstellen. Wird dieses Feld verwendet, ist es als nicht leere Abfolge von Zeichenketten formatiert, von denen jede RFC 3986 ([1]) entspricht.

Scheme extensions (Abschnitt 5.3.17)

Dieses Feld ist OPTIONAL und wird im Zusammenhang mit den vorliegenden Spezifikationen nicht verwendet.

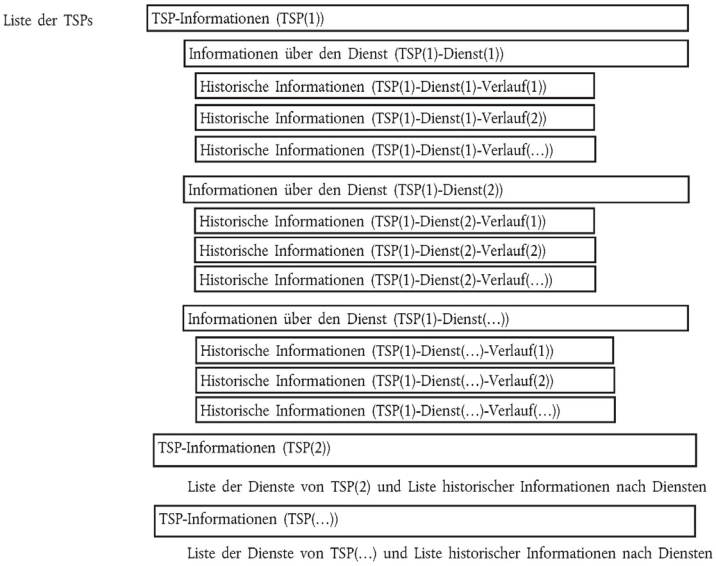
List of Trust Service Providers

Dieses Feld ist OPTIONAL.

Wenn im Rahmen des Systems in einem Mitgliedstaat keine CSPs beaufsichtigt bzw. akkreditiert werden bzw. wurden, MUSS dieses Feld weggelassen werden. Es wurde jedoch vereinbart, dass ein Mitgliedstaat, selbst wenn aufgrund des Systems kein CSP beaufsichtigt oder akkreditiert wurde, trotzdem eine TSL implementieren MUSS, in der dieses Feld fehlt. Das Fehlen eines CSP in der Liste MUSS bedeuten, dass es in dem unter „Scheme Territory“ genannten Land keine beaufsichtigten bzw. akkreditierten CSPs gibt.

Wenn im Rahmen des Systems ein oder mehrere CSP-Dienste beaufsichtigt bzw. akkreditiert werden bzw. wurden, MUSS das Feld eine Abfolge enthalten, die jeden CSP identifiziert, der einen oder mehrere solche beaufsichtigten bzw. akkreditierten Dienste erbringt. Dazu gehören auch Einzelheiten über den Aufsichts- bzw. Akkreditierungsstatus und historische Informationen über den Status jedes Dienstes des CSP (in der Abbildung unten gilt: TSP = CSP).

▼C2



([1]) IETF RFC 3986: „Uniform Resource Identifiers (URI): Generic syntax“.

▼C1

Die Liste der TSPs ist strukturiert, wie in der Abbildung oben dargestellt. Für jeden TSP existiert eine Abfolge von Feldern, die Informationen über den TSP enthalten („TSP Information“), gefolgt von einer Liste der Dienste. Für jeden so aufgelisteten Dienst existiert wiederum eine Abfolge von Feldern, die Informationen über den Dienst enthalten („Service Information“), und eine Abfolge von Feldern mit Informationen über die historische Statusentwicklung des Dienstes („Service approval history“).

TSP Information

TSP(1)

T S P n a m e (Abschnitt 5.4.1)

Dieses Feld ist ERFORDERLICH und MUSS den Namen des für die im Rahmen des Systems beaufsichtigten oder akkreditierten Dienste zuständigen Rechtsträgers enthalten. Es handelt sich um eine Abfolge mehrsprachiger Zeichenketten (wobei EN die obligatorische Sprache ist und potenziell eine oder mehrere Landessprachen verwendet werden können). Dieser Name MUSS die Bezeichnung sein, die für die offizielle Registrierung verwendet wurde, und an die formelle Mitteilungen zu richten wären.

T S P t r a d e n a m e (Abschnitt 5.4.2)

Dieses Feld ist OPTIONAL und MUSS, wenn vorhanden, einen alternativen Namen enthalten, mit dem sich der CSP im Zusammenhang mit der Erbringung der Dienste bezeichnet, die in der vorliegenden TSL im Eintrag „TSP name“ (Abschnitt 5.4.1) aufscheinen.

Hinweis: Wenn ein einziger CSP-Rechtsträger Dienste unter verschiedenen „TSP trade names“ oder in unterschiedlichen Rahmen erbringt, können so viele CSP-Einträge erstellt werden wie nötig (z. B. „TSP Name/Trade Name“-Einträge). Alternativ kann jeder einzelne CSP (Rechtsträger) nur einmal, aber mit entsprechenden Kontextinformationen gelistet werden. Es obliegt dem „Scheme operator“ des Mitgliedstaats, die günstigste Methode mit dem CSP zu erörtern und zu vereinbaren.

T S P a d d r e s s (Abschnitt 5.4.3)

Dieses Feld ist ERFORDERLICH und MUSS die Adresse des im Feld „TSP name“ (Abschnitt 5.4.1) benannten Rechtsträgers oder der beauftragten Stelle für den Versand von postalischen und elektronischen Mitteilungen enthalten. Es MUSS die „PostalAddress“ (d. h. Straße, Hausnummer, Ort, [Staat oder Bundesland], [Postleitzahl] und den ISO 3166-1 Alpha-2-Ländercode) gemäß Abschnitt 5.3.5.1 sowie die „ElectronicAddress“ (d. h. E-Mail und/oder Website-URI) gemäß Abschnitt 5.3.5.2 enthalten.

T S P i n f o r m a t i o n U R I (Abschnitt 5.4.4)

Dieses Feld ist ERFORDERLICH und MUSS den/die URI(s) enthalten, unter denen Anwender (z. B. auf das Zertifikat vertrauende Parteien) CSP-spezifische Informationen erhalten. Es MUSS sich um eine Abfolge mehrsprachiger Zeiger handeln (wobei EN die obligatorische Sprache ist und potenziell eine oder mehrere Landessprachen verwendet werden können). Der/die entsprechende(n) URI(s) MUSS/MÜSSEN einen Pfad zu Angaben über die allgemeinen Geschäftsbedingungen des CSP, seine Verfahren, rechtliche Aspekte, Kundendienstrichtlinien und andere generischen Information enthalten, die für alle Dienste gelten, die unter diesem CSP-Eintrag in der TSL aufscheinen.

Hinweis: Wenn ein einziger CSP-Rechtsträger Dienste unter verschiedenen „TSP trade names“ oder in unterschiedlichen Rahmen erbringt, und für jeden davon genau ein TSP-Eintrag existiert, MUSS dieses Feld Informationen über die spezielle Dienstegruppe enthalten, die unter einem bestimmten „TSP Trade Name“-Eintrag angeführt ist.

▼C1

TSP information extensions (Abschnitt 5.4.5)

Dieses Feld ist OPTIONAL und KANN, wenn vorhanden, vom „Scheme operator“ gemäß den Spezifikationen in ETSI TS 102 231 (Abschnitt 5.4.5) zur Angabe spezieller Informationen verwendet werden, die anhand der Regeln des entsprechenden Systems auszulegen sind.

List of Services

Dieses Feld ist ERFORDERLICH und MUSS eine Abfolge enthalten, die jeden der anerkannten Dienste des CSP, dessen Genehmigungsstatus (und die historische Entwicklung dieses Status) identifiziert. Mindestens ein Dienst muss angeführt sein (selbst wenn die enthaltenen Informationen rein historischer Natur sind).

Da die Aufbewahrung historischer Informationen über gelistete Dienste im Rahmen der vorliegenden Spezifikationen ERFORDERLICH ist, MÜSSEN diese historischen Informationen vorgehalten werden, selbst wenn der gegenwärtige Status des Dienstes kein Aufscheinen in der Liste erfordern würde (z. B. weil der Dienst eingestellt wurde). Deshalb MUSS ein CSP zur Bereitstellung historischer Informationen auch dann in der Liste aufscheinen, wenn sein einziger gelisteter Dienst nicht mehr aktuell ist.

Service Information

TSP(1) Service(1)

Service type identifier (Abschnitt 5.5.1)

▼M1

Dieses Feld ist ERFORDERLICH und MUSS den Identifikator der Dienstleistungstyps („TSL type“) laut den vorliegenden TSL-Spezifikationen enthalten (d. h. /eSigDir-1999-93-EC-TrustedList/TSLType/generic).

▼C1

Wenn der gelistete Dienst im Zusammenhang mit der Ausstellung qualifizierter Zertifikate steht, MUSS der angegebene URI folgendermaßen lauten: http://uri.etsi.org/TrstSvc/Svctype/CA/QC (eine Zertifizierungsstelle, die qualifizierte Zertifikate ausstellt).

Wenn der gelistete Dienst im Zusammenhang mit der Ausstellung von Tokens für vertrauenswürdige Dienste steht, bei denen es sich nicht um QCs handelt, und die Ausstellung von QCs nicht unterstützt, MUSS es sich bei dem angegebenen URI um einen der in ETSI 102 231 definierten und in Abschnitt D.2, der sich auf dieses Feld bezieht, enthaltenen handeln. Dies MUSS auch für Tokens für vertrauenswürdige Dienste gelten, die nach der einzelstaatlichen Gesetzgebung der Mitgliedstaaten in Bezug auf die Einhaltung spezieller Qualifikationen beaufsichtigt werden bzw. akkreditiert sind (z. B. so genannte qualifizierte Zeitstempel-Tokens in DE oder HU). Bei dem angegebenen URI MUSS es sich um einen der in ETSI 102 231 definierten und in Abschnitt D.2, der sich auf dieses Feld bezieht, enthaltenen handeln (z. B. TSA für einzelstaatlich definierte qualifizierte Zeitstempel-Tokens). Ggf. KANN eine solche spezielle einzelstaatliche Qualifizierung der Tokens für vertrauenswürdige Dienste im Diensteintrag enthalten sein. Zu diesem Zweck MUSS die „additionalServiceInformation“-Erweiterung (Abschnitt 5.8.2) in Abschnitt 5.5.9 („Service information extension“) verwendet werden.

▼C1

Generell MUSS für einen in der vertrauenswürdigen Liste enthaltenen CSP (d. h. eine Zertifizierungsstelle, die (direkt) QCs ausstellt) unter den gelisteten Zertifizierungsdiensten ein Eintrag pro X.509v3-Zertifikat (z. B. für einen CA/QC-Zertifizierungsdienst) existieren. Unter bestimmten Umständen und bei sorgfältiger Verwaltung und Unterstützung KANN sich die Aufsichts- bzw. Akkreditierungsstelle eines Mitgliedstaats dazu entschließen, das X.509v3-Zertifikat einer Root oder Upper Level CA (z. B. einer Zertifizierungsstelle, die nicht direkt Anwender-QC ausstellt, sondern eine CA-Hierarchie bis hinunter zu CAs, die QCs für Anwender ausstellen, zertifiziert) als „Sdi“ eines einzigen Eintrags in der Diensteliste eines gelisteten CSP zu verwenden. Die Konsequenzen (Vorteile und Nachteile) der Verwendung des X.509v3-Zertifikats einer Root oder Upper Level CA als „Sdi“-Wert von TL-Diensteeinträgen müssen von den Mitgliedstaaten gründlich erwogen und getragen werden ([1]). Außerdem MUSS der Mitgliedstaat im Falle dieser zulässigen Abweichung von der üblichen Vorgangsweise die erforderliche Dokumentation bereitstellen, um den Aufbau und die Verifizierung des Zertifizierungspfads zu ermöglichen.

Anmerkung: TSPs wie OCSP-Responder oder CRL-Aussteller, die Teil von CSP_{QC}-Zertifizierungsdiensten sind und separate Schlüsselpaare verwenden müssen, um OCSP-Responses bzw. CRLs zu signieren, KÖNNEN unter Verwendung der nachstehenden URI-Kombination ebenfalls in die vorliegende TSL-Vorlage aufgenommen werden:

— Wert für „Service type identifier“ (Abschnitt 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP

in Kombination mit dem nachstehenden Wert für „Service information extension“ (Abschnitt 5.5.9) additionalServiceInformation (Abschnitt 5.8.2):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/OCSP-QC

Beschreibung: ein Zertifikatstatusanbieter, der einen OCSP-Server betreibt, der Bestandteil eines Dienstes eines CSP ist, der qualifizierte Zertifikate ausstellt.

— Wert für „Service type identifier“ (Abschnitt 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL

in Kombination mit dem nachstehenden Wert für „Service information extension“ (Abschnitt 5.5.9) additionalServiceInformation (Abschnitt 5.8.2):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/CRL-QC

Beschreibung: ein Zertifikatstatusanbieter, der eine CRL führt, die Bestandteil eines Dienstes eines CSP ist, der qualifizierte Zertifikate ausstellt.

— Wert für „Service type identifier“ (Abschnitt 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

([1]) Die Verwendung eines X.509v3-Zertifikats einer RootCA als „Sdi“-Wert für einen gelisteten Dienst zwingt den „Scheme operator“ dazu, sämtliche Zertifizierungsdienste einer solchen Root CA im Hinblick auf den „Aufsichts- bzw. Akkreditierungsstatus“ als Ganzes zu betrachten. D. h. jeder für eine einzelne CA in der gelisteten Root-Hierarchie erforderliche Statuswechsel wird dazu führen, dass die gesamte Hierarchie diesen Statuswechsel übernimmt.

▼C1

in Kombination mit dem nachstehenden Wert für „Service information extension“ (Abschnitt 5.5.9) additionalServiceInformation (Abschnitt 5.8.2):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/RootCA-QC

Beschreibung: eine Root CA, ausgehend von welcher ein Zertifizierungspfad hinunter zur einer Zertifizierungsstelle hergestellt werden kann, die qualifizierte Zertifikate ausstellt.

— Wert für „Service type identifier“ (Abschnitt 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/TSA

in Kombination mit dem nachstehenden Wert für „Service information extension“ (Abschnitt 5.5.9) additionalServiceInformation (Abschnitt 5.8.2):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/TSS-QC

Beschreibung: ein Zeitstempeldienst als Bestandteil eines Dienstes eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt, die TST herausgeben, die bei der Verifizierung qualifizierter Signaturen verwendet werden können, um die Gültigkeit der Signatur sicherzustellen und zu verlängern, wenn das QC widerrufen wird oder abläuft.

Service name (Abschnitt 5.5.2)

Dieses Feld ist ERFORDERLICH und MUSS den Namen enthalten, unter welchem der im Feld „TSP name“ (Abschnitt 5.4.1) identifizierte CSP den im Feld „Service type identifier“ (Abschnitt 5.5.1) angegebenen Dienst erbringt. Es MUSS sich um eine Abfolge mehrsprachiger Zeichenketten handeln (wobei EN die obligatorische Sprache ist und potenziell eine oder mehrere Landessprachen verwendet werden können).

Service digital identity (Abschnitt 5.5.3)

Dieses Feld ist ERFORDERLICH und MUSS zumindest eine Darstellung eines digitalen Identifikators enthalten, der für den Dienst steht, dessen Typ im Feld „Service type identifier“ (Abschnitt 5.5.1) angegeben ist, und der eine eindeutige Identifizierung des Dienstes erlaubt.

In den vorliegenden Spezifikationen MUSS der in diesem Feld verwendete digitale Identifikator das entsprechende X.509v3-Zertifikat sein, das den bzw. die öffentlichen Schlüssel repräsentiert, den/die der CSP zur Erbringung des Dienstes verwendet, dessen Typ im Feld „Service type identifier“ (Abschnitt 5.5.1) angegeben ist (d. h. der von einer RootCA/QC verwendete Schlüssel bzw. der zum Signieren von Zertifikaten [1] oder alternativ zur Herausgabe von Zeitstempel-Tokens, zum Signieren von CRLs oder OCSP-Responses verwendete Schlüssel). Dieses entsprechende X.509v3-Zertifikat MUSS als minimaler erforderlicher digitaler Identifikator verwendet werden (als Repräsentation des/der öffentlichen Schlüssel(s), den/die der CSP zur Erbringung des gelisteten Dienstes nutzt). Weitere Identifikatoren KÖNNEN verwendet werden, wie nachstehend beschrieben, sie MÜSSEN jedoch alle auf dieselbe Identität (d. h. das entsprechende X.509v3-Zertifikat) verweisen:

[1] Dies kann das Zertifikat einer CA sein, die Nutzerzertifikate ausstellt (z. B. CA/PKC, CA/QC) oder das Zertifikat einer vertrauenswürdigen Root CA, von dem aus ein Pfad hinunter zu qualifizierten Anwenderzertifikaten hergestellt werden kann. Je nachdem, ob diese Angaben und die Informationen, die in jedem Anwenderzertifikat enthalten sind, das von dieser vertrauenswürdigen Root CA ausgestellt wird, dazu verwendet werden können, die angemessenen Eigenschaften eines qualifizierten Zertifikats eindeutig festzustellen, müssen diese Angaben („Service digital identity“) möglicherweise durch „Service information extensions“ (vgl. Abschnitt 5.5.9) ergänzt werden.

▼C1

a) Der eindeutige Name (Distinguished Name — DN) des Zertifikats, der zur Verifizierung elektronischer Signaturen des im Feld „Service type identifier“ (Abschnitt 5.5.1) angegebenen CSP-Dienstes verwendet werden kann;

b) Der entsprechende Identifikator des öffentlichen Schlüssels (d. h. X.509v3 SubjectKeyIdentifier oder SKI-Wert);

c) Der entsprechende öffentliche Schlüssel.

Generell DARF der digitale Identifikator (d. h. das entsprechende X.509v3-Zertifikat) NICHT mehr als einmal in der Vertrauensliste aufscheinen, d. h. es MUSS einen Eintrag für jedes einzelne X.509v3-Zertifikat für einen der gelisteten Zertifizierungsdienste eines in der Vertrauensliste enthaltenen CSP geben. Umgekehrt MUSS ein einziges X.509v3-Zertifikat in einem einzigen Diensteintrag als „Sdi“-Wert verwendet werden.

Anmerkung (1): Der einzige Fall, in dem der obige Grundsatz nicht gilt, ist, wenn ein einziges X.509v3-Zertifikat zur Ausstellung verschiedener Typen von Tokens für vertrauenswürdigen Dienste verwendet wird, für die unterschiedliche Aufsichts- bzw. Akkreditierungssysteme gelten; wenn z. B. von einem CSP ein einziges X.509v3-Zertifikat einerseits für die Ausstellung von QCs im Rahmen eines entsprechenden Aufsichtssystems und andererseits für die Ausstellung nicht qualifizierter Zertifikate im Rahmen eines anderen Aufsichts- bzw. Akkreditierungsstatus verwendet wird. In diesem Fall und Beispiel würden zwei Einträge mit unterschiedlichen „Sti“-Werten (z. B. CA/QC bzw. CA/PKC in diesem Beispiel) aber demselben „Sdi“-Wert (dem entsprechenden X.509v3-Zertifikat) verwendet werden.

Die Implementierungen sind ASN.1- oder XML-abhängig und MÜSSEN den Spezifikationen laut ETSI TS 102 231 entsprechen (für ASN.1 vgl. Anhang A von ETSI TS 102 231, für XML vgl. Anhang B von ETSI TS 102 231).

Anmerkung (2): Wenn im Hinblick auf den identifizierten Diensteintrag zusätzliche „Qualification“-Informationen angegeben werden müssen, MUSS der „Scheme operator“ gegebenenfalls die Verwendung der „additionalServiceInformation“-Erweiterung (Abschnitt 5.8.2) des Felds „Service information extension“ (Abschnitt 5.5.9) je nach dem Zweck der Bereitstellung weiterer „Qualification“-Informationen in Betracht ziehen. Zusätzlich kann der „Scheme operator“ optional Abschnitt 5.5.6 („Scheme service definition URI“) verwenden.

Service current status (Abschnitt 5.5.4)

Dieses Feld ist ERFORDERLICH und MUSS den Identifikator des Dienstestatus durch einen der nachstehenden URIs enthalten:

▼C2

— **Under Supervision (Beaufsichtigt)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/undersupervision);

— **Supervision of Service in Cessation (Aufsicht in Einstellung begriffen)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionincessation);

— **Supervision Ceased (Aufsicht beendet)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionceased);

— **Supervision Revoked (Aufsicht widerrufen)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionrevoked);

— **Accredited (Akkreditiert)** (http://uri.etsi.org/TrstSvc/Svcstatus/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited);

— **Accreditation Ceased (Akkreditierung beendet)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationceased);

— **Accreditation Revoked (Akkreditierung widerrufen)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationrevoked).

▼C1

Die obigen Statusangaben MÜSSEN im Zusammenhang mit den vorliegenden Spezifikationen für die vertrauenswürdige Liste folgendermaßen interpretiert werden:

— ***Beaufsichtigt:*** Der unter „Service digital identity“ (Abschnitt 5.5.3) angegebene Dienst, der vom unter „TSP name“ (Abschnitt 5.4.1) angeführten Zertifizierungsdiensteanbieter (CSP) erbracht wird, wird gegenwärtig vom unter „Scheme territory“ (Abschnitt 5.3.10) genannten Mitgliedstaat, in dem der CSP ansässig ist, im Hinblick auf die Einhaltung der Bestimmungen der Richtlinie 1999/93/EG beaufsichtigt.

▼M1

— ***Aufsicht in Einstellung begriffen:*** Die Beaufsichtigung des unter „Service digital identity“ (Abschnitt 5.5.3) angegebenen Dienstes, der vom unter „TSP name“ (Abschnitt 5.4.1) angeführten CSP erbracht wird, befindet sich derzeit in der Einstellungsphase; die Aufsicht dauert jedoch noch an, bis sie beendet oder widerrufen wird. Hat eine andere juristische Person als die unter „TSP name“ genannte die Verantwortung für die Abwicklung dieser Einstellungsphase übernommen, MUSS die Identität dieser neuen oder ersatzweisen juristischen Person (Ersatz-CSP) in „Scheme service definition URI“ (Abschnitt 5.5.6) und in der Erweiterung „TakenOverBy“ (Abschnitt L.3.2) des Diensteintrags angegeben werden.

▼C1

— ***Aufsicht beendet:*** Die Gültigkeit der Aufsichtsbewertung ist abgelaufen, ohne dass der unter „Service digital identity“ (Abschnitt 5.5.3) angegebene Dienst neuerlich bewertet wurde. Der Dienst wird seit dem Datum des gegenwärtigen Status nicht mehr beaufsichtigt, da davon auszugehen ist, dass der Dienst eingestellt wurde.

— ***Aufsicht widerrufen:*** Der unter „Scheme territory“ (Abschnitt 5.3.10) angegebene Mitgliedstaat, in dem der CSP ansässig ist, hat festgestellt, dass der früher beaufsichtigte Dienst des CSP und möglicherweise der CSP selbst nicht mehr den Bestimmungen der Richtlinie 1999/93/EG entsprechen. Dementsprechend wurde aus dem oben genannten Grund eine Einstellung des Dienstes veranlasst.

Anmerkung (1): Der Statuswert „Aufsicht widerrufen“ kann ein endgültiger Status sein. Selbst wenn der CSP seine Aktivitäten vollständig einstellt, ist es nicht erforderlich, seinen Status auf „Aufsicht in Einstellung begriffen“ oder „Aufsicht beendet“ zu setzen. Die einzige Möglichkeit, den Status „Aufsicht widerrufen“ zu ändern, besteht darin, die Bestimmungen der Richtlinie 1999/93/EG im Hinblick auf das entsprechende Aufsichtssystem des Mitgliedstaats, der die TL führt, wieder einzuhalten und damit erneut ►C2 den Status „Beaufsichtigt“ zu erhalten ◄. Der Status „Aufsicht in Einstellung begriffen“ bzw. „Aufsicht beendet“ kommt nur zur Anwendung, wenn ein CSP seine beaufsichtigten Dienste unmittelbar einstellt, nicht wenn die Aufsicht widerrufen wird.

— ***Akkreditiert:*** Im Auftrag des unter „Scheme territory“ (Abschnitt 5.3.10) genannten Mitgliedstaats hat die Akkreditierungsstelle eine Akkreditierungsbewertung durchgeführt. Dabei wurde festgestellt, dass der unter „Service digital identity“ (Abschnitt 5.5.3) genannte Dienst, der von dem unter „TSP name“ (Abschnitt 5.4.1) genannten CSP ([1]) erbracht wird, den Bestimmungen der Richtlinie 1999/93/EG entspricht.

([1]) Dieser akkreditierte CSP kann in einem anderen Mitgliedstaat als jenem, der im Feld „Scheme territory“ der TSL-Implementierung der TL genannt ist, oder in einem Drittland ansässig sein (vgl. Artikel 7 Absatz 1 Buchstabe a der Richtlinie 1999/93/EG).

▼C1

Anmerkung (2): Im Zusammenhang mit einem CSP, der QCs ausstellt, und im „Scheme territory“ (Abschnitt 5.3.10) ansässig ist, MÜSSEN „Akkreditierung widerrufen“ und „Akkreditierung beendet“ als „Übergangsstatus“-Werte betrachtet werden und DÜRFEN NICHT als Werte für den „Service current status“ dienen. Werden sie nämlich verwendet, MUSS ihnen in der „Service approval history information“ oder im „Service current status“ unmittelbar ein ►C2 „Beaufsichtigt“-Status ◄ und potenziell ein weiterer oben definierter und in Abbildung 1 dargestellter Aufsichtsstatus folgen. Im Zusammenhang mit einem CSP, der keine QCs ausstellt, wenn nur ein „freiwilliges Akkreditierungssystem“ ohne zugehöriges Aufsichtssystem existiert, oder bei einem CSP, der QCs ausstellt, aber nicht in dem unter „Scheme territory“ (Abschnitt 5.3.10) genannten Land angesiedelt ist (sondern z. B. in einem Drittland), KÖNNEN die Statuswerte „Akkreditierung widerrufen“ und „Akkreditierung beendet“ als Werte für „Service current status“ verwendet werden:

— ***Akkreditierung beendet:*** Die Gültigkeit der Akkreditierungsbewertung ist abgelaufen, ohne dass der unter „Service digital identity“ (Abschnitt 5.5.3) angegebene Dienst neuerlich bewertet wurde.

— ***Akkreditierung widerrufen:*** Der unter „Service digital identity“ (Abschnitt 5.5.3) angegebene Dienst, der von dem unter „TSP name“ (Abschnitt 5.4.1) genannten Zertifizierungsdiensteanbieter (CSP) erbracht wird, und möglicherweise der CSP selbst, entsprechen nicht mehr den Bedingungen der Richtlinie 1999/93/EG, obwohl dies früher der Fall war.

Anmerkung (3): Für CSPs, die QCs ausstellen, und für CSPs, die keine QCs ausstellen (z. B. Zeitstempel-Diensteanbieter, die TSTs ausstellen oder CSPs, die nicht qualifizierte Zertifikate ausstellen usw.), müssen exakt dieselben Statuswerte verwendet werden. Der „Service Type identifier“ (Abschnitt 5.5.1) dient zur Unterscheidung zwischen den anwendbaren Aufsichts- bzw. Akkreditierungssystemen.

Anmerkung (4): Zusätzliche statusbezogene „Qualification“-Informationen auf der Ebene der einzelstaatlichen Aufsichts- bzw. Akkreditierungssysteme für CSPs, die keine QCs ausstellen, KÖNNEN ggf. und wenn erforderlich (z. B. zur Unterscheidung zwischen verschiedenen Qualitäts-/Sicherheitsstufen) auf der Dienstebene bereitgestellt werden. Je nach dem Zweck der Bereitstellung solcher weiterer „Qualification“-Informationen MÜSSEN die „Scheme operators“ die „additionalServiceInformation“-Erweiterung (Abschnitt 5.8.2) des Felds „Service information extension“ (Abschnitt 5.5.9) verwenden. Zusätzlich kann der „Scheme operator“ optional Abschnitt 5.5.6 („Scheme service definition URI“) verwenden.

Current status starting date and time (Abschnitt 5.5.5)

Dieses Feld ist ERFORDERLICH und MUSS das Datum und den Zeitpunkt enthalten, seit welchem der aktuelle Genehmigungsstatus wirksam ist (Datums- und Zeitwert wie in ETSI TS 102 231, Abschnitt 5.1.4, definiert).

Scheme service definition URI (Abschnitt 5.5.6)

Dieses Feld ist OPTIONAL und MUSS, wenn vorhanden, den/die URI(s) enthalten, unter denen auf das Zertifikat vertrauende Parteien vom „Scheme operator“ dienstespezifische Informationen in Form einer Abfolge mehrsprachiger Zeiger erhalten (wobei EN die obligatorische Sprache ist und potenziell eine oder mehrere Landessprachen verwendet werden können).

Wird dieses Feld verwendet, MUSS/MÜSSEN der/die angegebene(n) URI(s) einen Pfad zu Informationen enthalten, die den Dienst beschreiben, wie im System vorgesehen. Dazu KÖNNEN ggf. insbesondere folgende URIs zählen:

a) URI zur Angabe der Identität des Ersatz-CSP bei einer in Einstellung begriffenen Aufsicht eines Dienstes, für den ein Ersatz-CSP vorhanden ist (vgl. „Service current status“ — Abschnitt 5.5.4);

▼C1

b) URI zur Angabe von Dokumenten, die Zusatzinformationen in Bezug auf die Verwendung einer einzelstaatlich festgelegten speziellen Qualifizierung für einen beaufsichtigten bzw. akkreditierten Dienst, der Tokens für vertrauenswürdige Dienste ausstellt, enthalten. Dabei wird vorgegangen, wie im Hinblick auf die Verwendung des Felds „Service information extension“ (Abschnitt 5.5.9) mit einer „additionalServiceInformation“-Erweiterung (Abschnitt 5.8.2) definiert.

Service supply points (Abschnitt 5.5.7)

Dieses Feld ist OPTIONAL und MUSS, wenn vorhanden, den/die URI(s) enthalten, unter denen auf das Zertifikat vertrauende Parteien über eine Abfolge von Zeichenketten, deren Syntax RFC 3986 entsprechen MUSS, auf den Dienst zugreifen können.

TSP service definition URI (Abschnitt 5.5.8)

Dieses Feld ist OPTIONAL und MUSS, wenn vorhanden, den/die URI(s) enthalten, unter denen auf das Zertifikat vertrauende Parteien vom TSP bereitgestellte dienstespezifische Informationen in Form einer Abfolge mehrsprachiger Zeiger erhalten (wobei EN die obligatorische Sprache ist und potenziell eine oder mehrere Landessprachen verwendet werden können). Der/die angegebene(n) URI(s) MUSS/MÜSSEN einen Pfad zu Informationen enthalten, die den Dienst beschreiben, wie vom TSP vorgesehen.

Service information extensions (Abschnitt 5.5.9)

Im Zusammenhang mit den vorliegenden Spezifikationen ist dieses Feld OPTIONAL, MUSS jedoch vorhanden sein, wenn die unter „Service digital identity“ (Abschnitt 5.5.3) enthaltenen Informationen zur eindeutigen Identifikation der von diesem Dienst ausgestellten qualifizierten Zertifikate nicht ausreichen und/oder die in den entsprechenden qualifizierten Zertifikaten angegebenen Informationen keine maschinenlesbaren Angaben darüber enthalten, ob das QC von einer SSCD ([1]) unterstützt wird.

Wenn die Verwendung vor dem Hintergrund der vorliegenden Spezifikationen ERFORDERLICH ist, z. B. für CA/QC-Dienste, MUSS ein optionales „Service information extensions“-(„Sie“)-Informationsfeld verwendet werden. Es ist unter Berücksichtigung der in ETSI TS 102 231, Anhang L.3.1, definierten „Qualifications“-Erweiterung als Abfolge eines oder mehrerer Tupel zu gestalten. Dabei enthält jedes Tupel:

— (Filter-)Informationen zur näheren Identifikation des Dienstes (d. h. die Gruppe qualifizierter Zertifikate), für welchen im Hinblick auf das Vorhandensein oder Fehlen der SSCD-Unterstützung (bzw. der Ausstellung für juristische Personen) Zusatzinformationen erforderlich sind/angegeben werden, aus dem durch die „Sdi“ identifizierten Zertifizierungsdienst;

— Verknüpfte „Kennzeichner“ informieren darüber, ob diese näher identifizierte Dienstegruppe qualifizierter Zertifikate von einer SSCD unterstützt wird (wenn diese Informationen „QCSSCDStatusAsInCert“ sind, d. h., dass die entsprechenden Informationen in einer ETSI-genormten, maschinenlesbaren Form Bestandteil des QC sind ([2])) und/oder ob solche QCs juristischen Personen ausgestellt werden (standardmäßig ist davon auszugehen, dass sie nur natürlichen Personen ausgestellt werden).

— QCWithSSCD (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCWithSSCD) bedeutet, dass vom CSP sichergestellt und vom Mitgliedstaat (bzw. seiner Aufsichts- oder Akkreditierungsstelle) kontrolliert (Aufsichtsmodell) bzw. geprüft (Akkreditierungsmodell) wird, dass alle von dem unter „Service digital identity“ (Abschnitt 5.5.3) genannten Dienst (QCA) ausgestellten QCs von einer SSCD unterstützt WERDEN (d. h., dass der zum öffentlichen Schlüssel im Zertifikat gehörige private Schlüssel in einer sicheren Signaturerstellungseinheit gespeichert wird, die Anhang III der Richtlinie 1999/93/EG entspricht). Die QCs werden durch die obigen (Filter-) Informationen näher bestimmt, die im Rahmen des unter „Sdi“ identifizierten Zertifizierungsdienstes jene exakte Gruppe qualifizierter Zertifikate benennen, für die diese Zusatzinformationen im Hinblick auf das Vorhandensein oder Fehlen von SSCD erforderlich sind;

([1]) Vgl. Abschnitt 2.2 des vorliegenden Dokuments.

([2]) D. h. eine entsprechende Kombination aus ETSI-definierter QcCompliance-Erklärung, QcSSCD-Erklärungen [ETSI TS 101 862] oder QCP/QCP + ETSI-definierter OID [ETSI TS 101 456].

▼C1

— QCNoSSCD (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCNoSSCD) bedeutet, dass vom CSP sichergestellt und vom Mitgliedstaat (bzw. seiner Aufsichts- oder Akkreditierungsstelle) kontrolliert (Aufsichtsmodell) bzw. geprüft (Akkreditierungsmodell) wird, dass alle von dem unter „Service digital identity“ (Abschnitt 5.5.3) genannten Dienst (RootCA/QC oder CA/QC) ausgestellten QCs NICHT von einer SSCD unterstützt WERDEN (d. h., dass der zum öffentlichen Schlüssel im Zertifikat gehörige private Schlüssel nicht in einer sicheren Signaturerstellungseinheit gespeichert wird, die Anhang III der Richtlinie 1999/93/EG entspricht). Die QCs werden durch die obigen (Filter-)Informationen näher bestimmt, die im Rahmen des unter „Sdi“ identifizierten Zertifizierungsdienstes jene exakte Gruppe qualifizierter Zertifikate benennen, für die diese Zusatzinformationen im Hinblick auf das Vorhandensein oder Fehlen von SSCD erforderlich sind;

— QCSSCDStatusAsInCert (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert) bedeutet, dass vom CSP sichergestellt und vom Mitgliedstaat (bzw. seiner Aufsichts- oder Akkreditierungsstelle) kontrolliert (Aufsichtsmodell) bzw. geprüft (Akkreditierungsmodell) wird, dass alle von dem unter „Service digital identity“ (Abschnitt 5.5.3) genannten Dienst (CA/QC) ausgestellten QCs maschinenlesbare Informationen über das Vorhandensein bzw. Fehlen von SSCD-Unterstützung enthalten MÜSSEN. Die QCs werden durch die obigen (Filter-)Informationen näher bestimmt, die im Rahmen des unter „Sdi“ identifizierten Zertifizierungsdienstes jene exakte Gruppe qualifizierter Zertifikate benennen, für die diese Zusatzinformationen im Hinblick auf das Vorhandensein oder Fehlen von SSCD erforderlich sind;

— QCForLegalPerson (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson) bedeutet, dass vom CSP sichergestellt und vom Mitgliedstaat (bzw. seiner Aufsichts- oder Akkreditierungsstelle) kontrolliert (Aufsichtsmodell) bzw. geprüft (Akkreditierungsmodell) wird, dass alle von dem unter „Service digital identity“ (Abschnitt 5.5.3) genannten Dienst (QCA) ausgestellten QCs juristischen Personen ausgestellt WERDEN. Die QCs werden durch die obigen (Filter-)Informationen näher bestimmt, die im Rahmen des unter „Sdi“ identifizierten Zertifizierungsdienstes jene exakte Gruppe qualifizierter Zertifikate benennen, für die diese Zusatzinformationen im Hinblick auf die Ausstellung für juristische Personen erforderlich sind;

Diese Kennzeichner dürfen nur als Erweiterung verwendet werden, wenn der Diensttyp http://uri.etsi.org/TrstSvc/Svctype/CA/QC ist.

Dieses Feld ist implementierungsspezifisch (ASN.1 oder XML) und MUSS den Spezifikationen laut ETSI TS 102 231, Anhang L.3.1 entsprechen.

▼M1

Im Zusammenhang mit einer XML-Implementierung muss der spezifische Inhalt solcher Zusatzinformationen unter Verwendung der in Anhang C der ETSI TS 102231 enthaltenen xsd-Datei codiert werden.

▼C1

Service Approval History

Dieses Feld ist OPTIONAL, MUSS aber vorhanden sein, wenn die „Historical information period“ (Abschnitt 5.3.12) nicht gleich null ist. Somit MUSS das System im Zusammenhang mit den vorliegenden Spezifikationen historische Informationen enthalten. In Fällen, in denen historische Informationen gespeichert werden sollen, der Dienst jedoch keinen anderen als den gegenwärtigen Status besitzt (d. h. es handelt sich um den ersten aufgezeichneten Status oder historische Informationen wurden vom „Scheme operator“ bisher nicht aufbewahrt) MUSS dieses Feld leer sein. Andernfalls MÜSSEN für jede Änderung des TSP „Service current status“, der innerhalb des historischen Informationszeitraums laut ETSI TS 102 231, Abschnitt 5.3.12 erfolgt, Angaben zum vorherigen Genehmigungsstatus, in absteigender Reihenfolge geordnet nach Datum und Zeit der Statusänderung (d. h. das Datum und der Zeitpunkt, zu dem der nachfolgende Genehmigungsstatus Wirksamkeit erlangte) gespeichert werden.

▼C1

Dabei MUSS es sich um die nachstehend definierte Abfolge historischer Informationen handeln.

TSP(1) Service(1) History(1)

Service type identifier (Abschnitt 5.6.1)

Dieses Feld ist ERFORDERLICH und MUSS den Identifikator des Diensttyps in dem im Feld „TSP Service Information — Service type identifier“ (Abschnitt 5.5.1) genannten Format und mit der entsprechenden Bedeutung enthalten.

Service name (Abschnitt 5.6.2)

Dieses Feld ist ERFORDERLICH und MUSS den Namen enthalten, unter welchem der CSP den im Feld „TSP Service Information — Service type identifier“ (Abschnitt 5.5.1) genannten Dienst erbringt. Dabei müssen Format und Bedeutung dem Feld „TSP Service Information — Service name“ (Abschnitt 5.5.2) entsprechen. Dieser Abschnitt verlangt nicht, dass der Name mit dem in Abschnitt 5.5.2 angegebenen identisch ist. Eine Namensänderung KANN einer der Umstände sein, die einen neuen Status erfordern.

▼M1

Service digital identity (Abschnitt 5.6.3)

Dieses Feld ist ERFORDERLICH und MUSS zumindest eine Darstellung eines digitalen Identifikators (d. h. das X.509v3-Zertifikat) enthalten, der im Feld „TSP Service Information — Service digital identity“ (Abschnitt 5.5.3) angegeben ist, wobei Format und Bedeutung ETSI TS 102231, Abschnitt 5.5.3, entsprechen.

Erläuterung: Bei einem X.509v3-Zertifikatwert, der im „Sdi“-Abschnitt 5.5.3 eines Dienstes verwendet wird, darf es pro Wert „Sti:Sie/additionalServiceInformation“ nur einen einzigen Diensteintrag in der vertrauenswürdigen Liste geben. Die „Sdi“-Informationen (Abschnitt 5.6.3), die in den Informationen zur Service Approval History verwendet werden, die mit einem Dienst verbunden sind, und die „Sdi“-Informationen (Abschnitt 5.5.3), die in diesem Diensteintrag verwendet werden, MÜSSEN sich auf denselben X.509v3-Zertifikatwert beziehen. Wenn sich die „Sdi“ eines aufgeführten Dienstes ändert (d. h. Erneuerung oder Änderung des Schlüssels eines X.509v3-Zertifikats z. B. für eine CA/PKC oder CA/QC) oder eine neue „Sdi“ für einen solchen Dienst erstellt wird (auch mit identischen Werten für die damit verbundenen „Sti“, „Sn“, und [„Sie“]), MUSS der Scheme Operator einen anderen Diensteintrag als zuvor vornehmen.

▼C1

Service previous status (Abschnitt 5.6.4)

Dieses Feld ist ERFORDERLICH und MUSS den Identifikator des vorhergehenden Status des Dienstes in dem im Feld „TSP Service Information — Service current status“ (Abschnitt 5.5.4) genannten Format und mit der entsprechenden Bedeutung enthalten.

Previous status starting date and time (Abschnitt 5.6.5)

Dieses Feld ist ERFORDERLICH und MUSS das Datum und den Zeitpunkt enthalten, zu dem der vorhergehende Status des Dienstes wirksam wurde. Datum und Zeit müssen in dem im Feld „TSP Service Information — Service current status starting date and time“ (Abschnitt 5.5.5) genannten Format und mit der entsprechenden Bedeutung angeführt werden.

Service information extensions (Abschnitt 5.6.6)

Dieses Feld ist OPTIONAL und KANN von den „Scheme operators“ zur Angabe spezieller dienstespezifischer Informationen in dem im Feld „TSP Service Information — Service information extensions“ (Abschnitt 5.5.9) genannten Format und mit der entsprechenden Bedeutung verwendet werden.

▼C1

TSP(1) Service(1) History(2)

Idem für TSP(1) Service(1) History(2) (vor History 1)

…

TSP(1) Service(2)

Idem für TSP(1) Service 2 (ggf.)

TSP(1)Service(2)History(1)

…

TSP(2) Information

Idem für TSP 2 (ggf.)

Idem für TSP 2 Service 1

Idem für TSP 2 Service 1 History 1

…

▼M1

Signed TSL

Die anhand der vorliegenden Spezifikationen und insbesondere anhand von Kapitel IV erstellte, vom Menschen unmittelbar lesbare TSL SOLLTE mit dem „Scheme operator name“ (Abschnitt 5.3.4) signiert werden, um ihre Authentizität und Integrität zu gewährleisten ([1]). Das Format der Signatur SOLLTE PAdES Teil 3 (ETSI TS 102 778-3 ([2])) entsprechen, KANN jedoch im Rahmen des spezifischen vertrauenswürdigen Modells, das mit der Veröffentlichung der Zertifikate zur Signatur der vertrauenswürdigen Liste eingerichtet wurde, auch PAdES Teil 2 (ETSI TS 102 778-2 ([3])) entsprechen.

Die anhand der vorliegenden Spezifikationen erstellte maschinenlesbare TSL-Implementierung der vertrauenswürdigen Liste MUSS mit dem „Scheme operator name“ (Abschnitt 5.3.4) signiert werden, um ihre Authentizität und Integrität zu gewährleisten. Die anhand der vorliegenden Spezifikationen erstellte maschinenlesbare TSL-Implementierung der vertrauenswürdigen Liste MUSS das Format XML haben, das den Spezifikationen aus Anhang B und C aus ETSI TS 102231 entsprechen MUSS.

Bei dem Format der Signatur MUSS es sich um XAdES BES oder EPES gemäß den Spezifikationen von ETSI TS 101903 für XML-Implementierungen handeln. Diese Implementierung der elektronischen Signatur MUSS den Anforderungen aus Anhang B von ETSI TS 102231 ([4]) entsprechen. Die nachstehenden Abschnitte enthalten weitere allgemeine Anforderungen im Zusammenhang mit dieser Signatur.

▼C1

Scheme identification (Abschnitt 5.7.2)

Dieses Feld ist ERFORDERLICH und MUSS einen vom „Scheme operator“ zugewiesenen Verweis enthalten, der das in den vorliegenden Spezifikationen und der erstellten TSL beschriebene System eindeutig identifiziert und in der Berechnung der Signatur enthalten sein MUSS. Dabei soll es sich um eine Zeichenkette oder eine Bitfolge handeln.

([1]) Falls die vom Menschen unmittelbar lesbare TSL-Implementierung der vertrauenswürdigen Liste nicht signiert ist, MÜSSEN ihre Authentizität und Integrität durch Verwendung eines angemessenen Kommunikationskanals mit einem gleichwertigen Sicherheitsniveau gewährleistet werden. Dazu wird der Einsatz von TLS (IETF RFC 5246: „The Transport Layer Security (TLS) Protocol Version 1.2“) empfohlen, und der Fingerprint des Zertifikats des TLS-Kanals MUSS den TSL-Nutzern von den Mitgliedstaaten über ein anderes Band zur Verfügung gestellt werden.

([2]) ETSI TS 102 778-3 — Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Teil 3: PAdES Enhanced — PAdES-BES and PAdES-EPES Profiles.

([3]) ETSI TS 102 778-2 — Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Teil 2: PAdES Basic — Profile based on ISO 32000-1.

([4]) Das Signaturzertifikat des „Scheme operator“ muss auf eine der in ETSI TS 101903 angegebenen Arten mit der Signatur geschützt werden, und das ds:keyInfo sollte gegebenenfalls die relevante Zertifikatkette enthalten.

▼M1

Im Zusammenhang mit den vorliegenden Spezifikationen MUSS der zugeordnete Verweis den „TSL type“ (Abschnitt 5.3.3), den „Scheme name“ (Abschnitt 5.3.6) und den Wert der „SubjectKeyIdentifier“-Erweiterung des Zertifikats enthalten, das vom „Scheme operator“ zur elektronischen Signierung der TSL verwendet wird.

▼C1

Signature algorithm identifier (Abschnitt 5.7.3)

Dieses Feld ist ERFORDERLICH und MUSS den kryptografischen Algorithmus enthalten, der zur Erstellung der Signatur verwendet wurde. Je nach verwendetem Algorithmus KANN dieses Feld weitere Parameter erfordern. Dieses Feld MUSS in der Berechnung der Signatur enthalten sein.

Signature value (Abschnitt 5.7.4)

Dieses Feld ist ERFORDERLICH und MUSS den tatsächlichen Wert der digitalen Signatur enthalten. Alle Felder der TSL (mit Ausnahme des Signaturwerts selbst) MÜSSEN in der Berechnung der Signatur enthalten sein.

TSL extensions (Abschnitt 5.8)

expiredCertsRevocationInfo-Erweiterung (Abschnitt 5.8.1)

Diese Erweiterung ist OPTIONAL. Wird sie verwendet, MUSS sie den Spezifikationen laut ETSI TS 102 231, Abschnitt 5.8.1, entsprechen.

additionalServiceInformation-Erweiterung (Abschnitt 5.8.2)

Diese OPTIONALE Erweiterung MUSS, wenn sie genutzt wird, ausschließlich auf Dienstebene und nur in dem in Abschnitt 5.5.9 („Service information extension“) genannten Feld verwendet werden. Sie dient zur Bereitstellung von Zusatzinformationen über einen Dienst. Bei dieser Erweiterung MUSS es sich um eine Abfolge eines oder mehrerer Tupel handeln. Dabei enthält jedes Tupel:

a) ein URI zur Angabe der Zusatzinformationen, z. B.:

   — ein URI, der Angaben über eine einzelstaatlich festgelegte spezielle Qualifizierung für einen beaufsichtigten bzw. akkreditierten Dienst, der Token für vertrauenswürdige Dienste ausstellt, enthält, z. B.

      — einen speziellen Granularitätsgrad in Bezug auf Sicherheit/Qualität im Zusammenhang mit einem einzelstaatlichen Aufsichts- bzw. Akkreditierungssystem für CSPs, die keine QCs ausstellen, (z. B. RGS */**/*** in FR oder ein spezieller „Aufsichtsstatus“, der durch die einzelstaatliche Gesetzgebung für spezielle CSPs eingerichtet wurde, die QCs ausstellen, in DE), vgl. Anmerkung(4) zu „Service current status“ — Abschnitt 5.5.4;

      — oder einen speziellen Rechtsstatus für einen beaufsichtigten bzw. akkreditierten Dienst, der Tokens für vertrauenswürdige Dienste ausstellt (z. B. einzelstaatlich definierte „qualifizierte TST“ wie in DE oder HU);

      — oder die Bedeutung eines speziellen Richtlinienidentifikators, der in einem im „Sdi“-Feld enthaltenen X.509v3-Zertifikat aufscheint;

   — oder ein registrierter URI, wie unter „Service type identifier“, Abschnitt 5.5.1, angegeben, zur näheren Bestimmung der Beteiligung des mit „Sti“ identifizierten Dienstes als Komponentendienst eines Zertifizierungsdiensteanbieters, der QCs ausstellt (z. B. OCSP-QC, CRL-QC und RootCA-QC);

b) eine optionale Zeichenkette, die den serviceInformation-Wert in der im System festgelegten Bedeutung (z. B. *, ** oder ***) enthält;

c) alle optionalen Zusatzinformationen, die in einem systemspezifischen Format bereitgestellt werden.

▼M1

Durch die Dereferenzierung des URI SOLLTEN menschenlesbare Informationen entstehen (mindestens in EN sowie möglicherweise in einer oder mehreren Landessprachen), die für das Verständnis der Erweiterung durch eine auf das Zertifikat vertrauende Person angemessen und ausreichend sind und insbesondere die Bedeutung der jeweiligen URIs erläutern sowie die möglichen Werte für service-Information und die Bedeutung jedes Werts angeben.

Qualifications Extension (Abschnitt L.3.1)

Beschreibung: Dieses Feld ist OPTIONAL, MUSS aber vorhanden sein, wenn seine Verwendung ERFORDERLICH ist, z. B. für RootCA/QC- oder CA/QC-Dienste, und wenn

— die unter „Service digital identity“ angegebenen Informationen zur eindeutigen Identifikation der von diesem Dienst ausgestellten qualifizierten Zertifikate nicht ausreichen;

— die in den entsprechenden qualifizierten Zertifikaten vorhandenen Informationen keine maschinenlesbare Identifikation der Angaben darüber, ob das QC von einer SSCD unterstützt wird, zulässt.

Falls sie zum Einsatz kommt, DARF diese Erweiterung der Dienstebene nur in dem unter „Service information extension“ (Abschnitt 5.5.9) definierten Feld verwendet werden und MUSS den in Anhang L.3.1 von ETSI TS 102231 festgelegten Spezifikationen entsprechen.

TakenOverBy Extension (Abschnitt L.3.2)

Beschreibung: Diese Erweiterung ist OPTIONAL, MUSS jedoch vorhanden sein, wenn ein zuvor unter der rechtlichen Verantwortung eines CSP stehender Dienst von einem anderen TSP übernommen wird und dazu dient, die rechtliche Verantwortung für einen Dienst formell anzugeben und es der Verifizierungssoftware ermöglichen soll, dem Anwender rechtliche Informationen zu übermitteln. Die mit dieser Erweiterung bereitgestellten Informationen MÜSSEN mit der entsprechenden Nutzung von Abschnitt 5.5.6 im Einklang stehen, und sie MÜSSEN den in Anhang L.3.2 von ETSI TS 102231 festgelegten Spezifikationen entsprechen.

▼M1

KAPITEL II

Bei der Erstellung der vertrauenswürdigen Listen verwenden die Mitgliedstaaten:

Sprachencodes in Kleinbuchstaben und Ländercodes in Großbuchstaben;

Sprachen- und Ländercodes gemäß der nachstehenden Tabelle;

wenn lateinische Schrift (mit dem entsprechenden Sprachencode) verwendet wird, fügen sie eine Transliteration in lateinischer Schrift mit den in der nachstehenden Tabelle aufgeführten Sprachencodes hinzu.

Kurzbezeichnung (Ausgangssprache)	Kurzbezeichnung (Englisch)	Länder-Code	Sprachen-Code	Anmerkungen	Transliteration in lateinischer Schrift
Belgique/België	Belgium	BE	nl, fr, de		
България (*)	Bulgaria	BG	bg		bg-Latn
Česká republika	Czech Republic	CZ	cs		
Danmark	Denmark	DK	da		
Deutschland	Germany	DE	de		
Eesti	Estonia	EE	et		
Éire/Ireland	Ireland	IE	ga, en		
Ελλάδα (*)	Greece	EL	el	von der EU empfohlener Länder- Code	el-Latn
España	Spain	ES	es	außerdem Katalonisch (ca), Baskisch (eu), Galizisch (gl)	
France	France	FR	fr		
▼M2 Hrvatska	Kroatien	HR	hr		
▼M1 Italia	Italy	IT	it		
Κύπρος/Kıbrıs (*)	Cyprus	CY	el, tr		el-Latn
Latvija	Latvia	LV	lv		
Lietuva	Lithuania	LT	lt		
Luxembourg	Luxembourg	LU	fr, de, lb		
Magyarország	Hungary	HU	hu		
Malta	Malta	MT	mt, en		
Nederland	Netherlands	NL	nl		
Österreich	Austria	AT	de		
Polska	Poland	PL	pl		
Portugal	Portugal	PT	pt		
România	Romania	RO	ro		

▼M1

Kurzbezeichnung (Ausgangssprache)	Kurzbezeichnung (Englisch)	Länder-Code	Sprachen-Code	Anmerkungen	Transliteration in lateinischer Schrift
Slovenija	Slovenia	SI	sl		
Slovensko	Slovakia	SK	sk		
Suomi/Finland	Finland	FI	fi, sv		
Sverige	Sweden	SE	sv		
United Kingdom	United Kingdom	UK	en	von der EU empfohlener Länder- Code	
Ísland	Iceland	IS	is		
Liechtenstein	Liechtenstein	LI	de		
Norge/Noreg	Norway	NO	no, nb, nn		

(*) Transliteration in lateinischen Buchstaben: България = Bulgaria; Ελλάδα = Elláda; Κύπρος = Kýpros.

———————

▼C1

KAPITEL IV

SPEZIFIKATIONEN FÜR DIE MENSCHENLESBARE FORM DER TSL-IMPLEMENTIERUNG DER VERTRAUENSWÜRDIGEN LISTE

Eine menschenlesbare Form der TSL-Implementierung der vertrauenswürdigen Liste MUSS öffentlich verfügbar und elektronisch zugänglich sein. Die Bereitstellung SOLLTE im PDF-Format gemäß ISO 32000 erfolgen. Die Formatierung MUSS dem Profil PDF/A (ISO 19005) entsprechen.

Der Inhalt der PDF/A-basierten menschenlesbaren Form der TSL-Implementierung der vertrauenswürdigen Liste SOLLTE folgende Anforderungen erfüllen:

▼M1

— Der Titel der menschenlesbaren Form der vertrauenswürdigen Listen ist eine Verkettung der folgenden Elemente:

  — optionale Abbildung der Nationalflagge des Mitgliedstaats;

  — Leerstelle;

  — Länderkurzbezeichnung in der/den Ausgangssprache(n) (siehe Spalte 1 der Tabelle in Kapitel II);

  — Leerstelle;

  — „(“;

  — Länderkurzbezeichnung auf Englisch (siehe Spalte 2 der Tabelle in Kapitel II) innerhalb der Klammer;

  — „):“ als schließende Klammer und Trennungszeichen;

  — Leerstelle;

  — „Trusted List“;

  — optional: Logo des Scheme Operators des Mitgliedstaats;

▼C1

— Die Struktur des menschenlesbaren Dokuments SOLLTE das in Abschnitt 5.1.2 von ETSI TS 102 231 beschriebene logische Modell reflektieren;

— Jedes vorhandene Feld SOLLTE angezeigt werden und Folgendes enthalten:

  — Die Bezeichnung des Felds (z. B. „Service type identifier“);

  — Den Wert des Felds (z. B. „CA/QC“);

  — Ggf. die Bedeutung (Beschreibung) des Werts des Felds wie in Anhang D von ETSI TS 102 231 oder in den vorliegenden Spezifikationen für registrierte URIs vorgesehen (z. B. „A Certification authority issuing public key certificates.“);

  — Ggf. mehrere Fassungen in natürlichen Sprachen, wie in der TSL-Implementierung der vertrauenswürdigen Liste vorgesehen.

— Zumindest die nachstehenden Felder und dazugehörigen Werte der digitalen Zertifikate, die sich im Feld „Service digital identity“ befinden, SOLLTEN in der menschenlesbaren Form angezeigt werden:

  — Version (Version)

  — Seriennummer (Serial number)

  — Signaturalgorithmus (Signature algorithm)

  — Aussteller (Issuer)

  — Gültig ab (Valid from)

  — Gültig bis (Valid to)

  — Gegenstand (Subject)

▼C1

— Öffentlicher Schlüssel (Public key)

— Zertifikatrichtlinien (Certificate Policies)

— Inhaberschlüssel-Identifikator (Subject Key Identifier)

— CRL-Verteilungspunkte (CRL Distribution Points)

— Ausstellerschlüssel-Identifikator (Authority Key Identifier)

— Schlüsselverwendung (Key Usage)

— Grundlegende Beschränkungen (Basic constraints)

— Daumenabdruck-Algorithmus (Thumbprint algorithm)

— Daumenabdruck (Thumbprint)

— Die menschenlesbare Form SOLLTE einfach gedruckt werden können;

— Die menschenlesbare Form KANN elektronisch signiert werden. In diesem Fall MUSS sie vom „Scheme operator“ anhand derselben Signaturspezifikationen signiert werden, wie sie für die TSL-Implementierung der vertrauenswürdigen Liste gelten.