DURCHFÜHRUNGSBESCHLUSS DER KOMMISSION

vom 14. Oktober 2013

zur Änderung der Entscheidung 2009/767/EG in Bezug auf die Erstellung, Führung und Veröffentlichung von vertrauenswürdigen Listen der von den Mitgliedstaaten beaufsichtigten bzw. akkreditierten Zertifizierungsdiensteanbieter

(Bekanntgegeben unter Aktenzeichen C(2013) 6543)

(Text von Bedeutung für den EWR)

(2013/662/EU)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

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) Durch die Entscheidung 2009/767/EG 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 ([2]) werden die Mitgliedstaaten dazu verpflichtet, die Informationen bereitzustellen, die für die Prüfung von auf einem qualifizierten Zertifikat beruhenden fortgeschrittenen elektronischen Signaturen erforderlich sind. Die Informationen sind in einheitlicher Form unter Verwendung der so genannten „vertrauenswürdigen Listen" bereitzustellen; diese Listen enthalten Angaben zu Zertifizierungsdiensteanbietern, die öffentlich qualifizierte Zertifikate gemäß der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen ([3]) ausstellen und von den Mitgliedstaaten beaufsichtigt werden bzw. akkreditiert wurden.

(2) Die in der Praxis gewonnene Erfahrung mit der Durchführung der Entscheidung 2009/767/EG durch die Mitgliedstaaten hat gezeigt, dass gewisse Verbesserungen vonnöten sind, wenn ein größtmöglicher Nutzen der vertrauenswürdigen Listen gewährleistet werden soll. Zudem hat das Europäische Institut für Telekommunikationsnormen (European Telecommunications Standards Institute — ETSI) neue technische Spezifikationen für vertrauenswürdige Listen (TS 119 612) veröffentlicht, die auf den Spezifikationen im Anhang der Entscheidung basieren, aber gleichzeitig einige Verbesserungen gegenüber den derzeit geltenden Spezifikationen beinhalten.

(3) Die Entscheidung 2009/767/EG sollte deshalb dahin gehend geändert werden, dass auf die technischen Spezifikationen 119 612 des ETSI Bezug genommen wird und die Änderungen vorgenommen werden, die für eine bessere und leichtere Implementierung und Verwendung der vertrauenswürdigen Listen notwendig sind.

(4) Damit die Mitgliedstaaten ausreichend Zeit haben, um die erforderlichen technischen Änderungen an ihren derzeitigen vertrauenswürdigen Listen vorzunehmen, sollte dieser Beschluss ab dem 1. Februar 2014 gelten.

(5) Die in diesem Beschluss vorgesehenen Maßnahmen entsprechen der Stellungnahme des für die Dienstleistungsrichtlinie eingesetzten Ausschusses —

BESCHLIESST:

Artikel 1

Änderung der Entscheidung 2009/767/EG

Die Entscheidung 2009/767/EG wird wie folgt geändert:

1. Artikel 2 wird wie folgt geändert:

a) Die Absätze 1, 2 und 2a erhalten folgende Fassung:

„(1) Jeder Mitgliedstaat sorgt entsprechend den im Anhang festgelegten technischen Spezifikationen für die Erstellung, Führung und Veröffentlichung einer „vertrauenswürdigen Liste", die mindestens Angaben zu den von ihm beaufsichtigten bzw. akkreditierten Zertifizierungsdiensteanbietern enthält, die öffentlich qualifizierte Zertifikate ausstellen."

„(2) Die Mitgliedstaaten erstellen und veröffentlichen die vertrauenswürdige Liste entsprechend den im Anhang festgelegten Spezifikationen in maschinenlesbarer Form. Entscheidet sich ein Mitgliedstaat dafür, seine vertrauenswürdige Liste in menschenlesbarer Form zu veröffentlichen, hat diese Fassung der Liste den im Anhang festgelegten Spezifikationen zu entsprechen."

„(2a) Die Mitgliedstaaten versehen die maschinenlesbare Fassung ihrer vertrauenswürdigen Liste mit einer elektronischen Signatur, um ihre Authentizität und Integrität zu gewährleisten. Veröffentlicht ein Mitgliedstaat die vertrauenswürdige Liste in menschenlesbarer Form, stellt er sicher, dass diese Fassung der Liste dieselben Angaben enthält wie die Liste in maschinenlesbarer Form, und versieht sie mit einer elektronischen Signatur auf der Grundlage desselben Zertifikats, das bei der maschinenlesbaren Fassung verwendet wird."

([1]) ABl. L 376 vom 27.12.2006, S. 36.
([2]) ABl. L 274 vom 20.10.2009, S. 36.
([3]) ABl. L 13 vom 19.1.2000, S. 12.

b) Folgender Absatz 2b wird eingefügt:

„(2b) Die Mitgliedstaaten stellen sicher, dass die maschinenlesbare Fassung ihrer vertrauenswürdigen Liste jederzeit und ohne Unterbrechungen — ausgenommen aus Wartungsgründen — an ihrem Veröffentlichungsort zugänglich ist."

c) Absatz 3 erhält folgende Fassung:

„(3) Die Mitgliedstaaten teilen der Kommission Folgendes mit:

a) die Stelle(n), die für die Erstellung, Führung und Veröffentlichung der vertrauenswürdigen Liste in maschinenlesbarer Form zuständig ist (sind);

b) den Veröffentlichungsort der maschinenlesbaren Fassung der vertrauenswürdigen Liste;

c) zwei oder mehrere Public-Key-Zertifikate eines „Scheme operator" mit einer um mindestens drei Monate zeitversetzten Gültigkeitsdauer, die den privaten Schlüsseln entsprechen, welche für die elektronische Signatur der maschinenlesbaren Fassung der vertrauenswürdigen Liste verwendet werden können;

d) jegliche Änderungen in Bezug auf die Buchstaben a, b und c."

d) Folgender Absatz 3a wird eingefügt:

„(3a) Veröffentlicht ein Mitgliedstaat die vertrauenswürdige Liste in menschenlesbarer Form, sind die in Absatz 3 genannten Informationen auch für die menschenlesbare Fassung zu übermitteln."

2. Der Anhang wird durch den Anhang dieses Beschlusses ersetzt.

Artikel 2

Anwendung

Dieser Beschluss gilt ab dem 1. Februar 2014.

Artikel 3

Adressaten

Dieser Beschluss ist an die Mitgliedstaaten gerichtet.

Brüssel, den 14. Oktober 2013

Für die Kommission

Michel BARNIER

Mitglied der Kommission

ANHANG

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

ALLGEMEINE ANFORDERUNGEN

1. **Einleitung**

Zweck der gemeinsamen Vorlage für die „vertrauenswürdige Liste der beaufsichtigten bzw. akkreditierten Zertifizierungsdiensteanbieter“ der Mitgliedstaaten ist die Festlegung einer gemeinsamen Vorgehensweise, die alle Mitgliedstaaten anwenden, um Informationen über den Aufsichts- bzw. Akkreditierungsstatus der Zertifizierungsdienste von Zertifizierungsdiensteanbietern ([1]) (Certification Service Providers — CSPs) bereitzustellen, die im Hinblick auf die Einhaltung der einschlägigen Bestimmungen der Richtlinie 1999/93/EG von den betreffenden Mitgliedstaaten beaufsichtigt werden bzw. akkreditiert wurden. Dies beinhaltet auch die Bereitstellung historischer Informationen über den Aufsichts- bzw. Akkreditierungsstatus der beaufsichtigten bzw. akkreditierten Zertifizierungsdienste.

Diese Informationen dienen vor allem zur Validierung qualifizierter elektronischer Signaturen (Qualified Electronic Signatures — QES) und fortgeschrittener elektronischer Signaturen (Advanced Electronic Signatures — AdES) ([2]), die auf einem qualifizierten Zertifikat (Qualified Certificate — QC) beruhen ([3]) ([4]).

Zu den für die vertrauenswürdige Liste zwingend erforderlichen Angaben zählen mindestens Informationen über beaufsichtigte bzw. akkreditierte CSPs, die qualifizierte Zertifikate (QCs) ([5]) gemäß den Bestimmungen der Richtlinie 1999/93/EG (Artikel 3 Absatz 2, Artikel 3 Absatz 3 und Artikel 7 Absatz 1 Buchstabe a) ausstellen, einschließlich — sofern dies nicht Bestandteil der QCs ist — Informationen über QCs zur Unterstützung einer elektronischen Signatur und Informationen darüber, ob die Signatur von einer sicheren Signaturerstellungseinheit (Secure Signature Creation Device — SSCD) ([6]) erzeugt wurde.

Zusatzinformationen über andere CSPs, die keine QCs ausstellen, aber Dienste im Zusammenhang mit elektronischen Signaturen anbieten (z. B. CSPs, die Zeitstempel, Zeitstempel-Tokens oder nicht qualifizierte Zertifikate ausstellen), können auf einzelstaatlicher Basis freiwillig in die vertrauenswürdige Liste aufgenommen werden, sofern sie entweder auf vergleichbare Weise wie die CSPs, die QCs ausstellen, beaufsichtigt werden bzw. akkreditiert wurden oder nach einem anderen einzelstaatlichen Genehmigungssystem zugelassen wurden. In einigen Mitgliedstaaten können sich die einzelstaatlichen Genehmigungssysteme in Bezug auf die geltenden Anforderungen und/oder die zuständige Organisation von den Aufsichts- oder freiwilligen Akkreditierungssystemen für QCs ausstellende CSPs unterscheiden. Die in den vorliegenden Spezifikationen verwendeten Begriffe „akkreditiert“ und/oder „beaufsichtigt“ decken auch die einzelstaatlichen Genehmigungssysteme ab, doch müssen die Mitgliedstaaten in ihrer vertrauenswürdigen Liste Zusatzinformationen zur Art der einzelstaatlichen Regelungen geben, einschließlich präziser Angaben zu den etwaigen Unterschieden gegenüber den Akkreditierungs- bzw. Aufsichtssystemen, denen QCs ausstellende CSPs unterliegen.

Die gemeinsame Vorlage stützt sich auf ETSI TS 119 612 v1.1.1 ([7]) (im Folgenden „ETSI TS 119 612“), die Erstellung, Veröffentlichung, Fundstellen, Zugänglichkeit, Authentifizierung und Integrität solcher Listen regelt.

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

Die gemeinsame Vorlage für die vertrauenswürdige Liste der Mitgliedstaaten ist gemäß ETSI TS 119 612 in folgende Kategorien von Informationen untergliedert:

1. Tag zur Identifikation der vertrauenswürdigen Liste (Trusted list tag) bei elektronischen Suchvorgängen;

2. Informationen über die vertrauenswürdige Liste und ihre Ausstellungsmodalitäten;

3. eine Abfolge von Feldern, die eindeutige Informationen zur Identifizierung jedes im Rahmen des Systems beaufsichtigten bzw. akkreditierten CSP enthalten (diese Abfolge ist optional; d. h. wenn sie nicht verwendet wird, wird die Liste als leer betrachtet, was bedeutet, dass es in dem betreffenden Mitgliedstaat keinen für die Zwecke der vertrauenswürdigen Liste in Betracht kommenden beaufsichtigten oder akkreditierten CSP gibt);

4. für jeden gelisteten CSP detaillierte Angaben zu den jeweiligen vertrauenswürdigen Diensten, deren aktueller Status in der vertrauenswürdigen Liste vermerkt ist, als eine Abfolge von Feldern zur eindeutigen Identifizierung der von dem CSP erbrachten beaufsichtigten bzw. akkreditierten Zertifizierungsdienste sowie ihres gegenwärtigen Status (diese Abfolge muss mindestens einen Eintrag haben);

([1]) Definition nach Artikel 2 Absatz 11 der Richtlinie 1999/93/EG.
([2]) Definition nach Artikel 2 Absatz 2 der Richtlinie 1999/93/EG.
([3]) Für auf einem QC beruhende AdES wird im vorliegenden Dokument die Kurzbezeichnung „$AdES_{QC}$“ verwendet.
([4]) 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.
([5]) Definition nach Artikel 2 Absatz 10 der Richtlinie 1999/93/EG.
([6]) Definition nach Artikel 2 Absatz 6 der Richtlinie 1999/93/EG.
([7]) ETSI TS 119 612 v1.1.1 (2013-06) — Electronic Signatures and Infrastructures (ESI); Trusted Lists.

5. für jeden gelisteten beaufsichtigten bzw. akkreditierten Zertifizierungsdienst etwaige historische Statusinformationen;

6. die für die vertrauenswürdige Liste geltende Signatur.

In Bezug auf einen QCs ausstellenden CSP müssen die Struktur der vertrauenswürdigen Liste und insbesondere die Informationen über die Dienste (siehe oben Punkt 4) es ermöglichen, im Feld „Service information extensions" ergänzende Angaben zu machen für den Fall, dass im qualifizierten Zertifikat keine ausreichenden (maschinenlesbaren) Angaben über dessen „qualifizierten" Status und eine mögliche SSCD-Unterstützung verfügbar sind, und insbesondere auch, um der Tatsache Rechnung zu tragen, dass der Großteil der (kommerziellen) CSPs nur eine einzige Zertifizierungsstelle (Certification Authority — CA) mit der Ausstellung verschiedener Typen qualifizierter und nicht qualifizierter Anwenderzertifikate betraut.

Im Kontext von Zertifikatserstellungsdiensten kann, wenn einer oder mehrere Upper-Level-CA-Dienste innerhalb der PKI des CSP existieren (z. B. bei einer Hierarchie von CAs, die von einer Root-CA hinunter bis zu verschiedenen Zertifikate ausstellenden CAs reicht), die Zahl der Diensteinträge für einen CSP in der Liste reduziert werden, indem solche Upper-Level-CA-Dienste und nicht die CA-Dienste, die die Anwenderzertifikate ausstellen, gelistet werden (z. B. ausschließliches Listen der Root-CA des CSP). Die Statusinformationen gelten in diesen Fällen jedoch für die gesamte Hierarchie der dem gelisteten Dienst nachgeordneten CA-Dienste; außerdem 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.

2.1. *Beschreibung der Informationen in den einzelnen Kategorien*

1. Tag zur Identifizierung der vertrauenswürdigen Liste

2. Informationen über die vertrauenswürdige Liste und ihre Ausstellungsmodalitäten

Die nachstehenden Informationen sind Teil dieser Kategorie:

— **Identifikator für die Formatversion** der vertrauenswürdigen Liste;

— **Abfolge- (oder Release-)Nummer;**

— **Angaben zum Typ** der vertrauenswürdigen Liste (z. B. Angabe der Tatsache, dass diese vertrauenswürdige Liste Informationen über den Aufsichts- bzw. Akkreditierungsstatus der Zertifizierungsdienste von CSPs enthält, die von dem betreffenden Mitgliedstaat im Hinblick auf die Einhaltung der Bestimmungen der Richtlinie 1999/93/EG beaufsichtigt werden bzw. akkreditiert wurden);

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

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

  — Land, für das die Liste gilt;

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

  — Aufbewahrungszeitraum von (historischen) Informationen;

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

— **Datum und Uhrzeit der Ausstellung;**

— **nächste geplante Aktualisierung.**

3. Eindeutige Informationen zur Identifizierung aller im Rahmen des Systems beaufsichtigten bzw. akkreditierten CSPs

Diese Informationen umfassen mindestens Folgendes:

— offizielle Bezeichnung der CSP-Einrichtung gemäß amtlicher Registrierung (je nach Praxis im jeweiligen Mitgliedstaat unter Angabe der UID der CSP-Einrichtung);

— Adresse und Kontaktdaten des CSP;

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

4. 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 wurde

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

— Service type identifier: 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);

— Service (trade) name: den (Handels-)Namen dieses Zertifizierungsdienstes;

— Service digital identity: einen eindeutigen, unverwechselbaren Identifikator des Zertifizierungsdienstes;

— Service current status: einen Identifikator des aktuellen Status des Dienstes;

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

— (ggf.) Service information extension: Zusatzinformationen über den Dienst (z. B. direkt angegeben oder mittels Verweis auf eine Download-Adresse): vom Scheme operator gegebene Informationen zur Definition des Dienstes, Zugangsinformationen in Bezug auf den Dienst, vom CSP gegebene Informationen zur Definition des Dienstes und Service information extensions; für CA/QC-Dienste beispielsweise eine optionale Abfolge von Informationstupeln, von denen jedes folgende Angaben enthält:

  — Kriterien zur näheren Identifikation (Filterung) innerhalb des identifizierten vertrauenswürdigen Dienstes der konkreten Outputs des Dienstes (z. B. Gruppe (qualifizierter) Zertifikate), für welche im Hinblick auf ihren Status, die Angabe zur SSCD-Unterstützung und/oder die Ausstellung für juristische Personen Zusatzinformationen erforderlich sind bzw. angegeben werden, und

  — verknüpfte „Kennzeichner", die darüber informieren, ob unter den Outputs des Dienstes Zertifikate identifiziert werden, die als qualifiziert zu betrachten sind, und/oder ob die identifizierten qualifizierten Zertifikate des Dienstes von einer SSCD unterstützt werden und/oder ob solche QCs juristischen Personen ausgestellt werden (standardmäßig ist davon auszugehen, dass sie natürlichen Personen ausgestellt werden).

5. Für jeden gelisteten Zertifizierungsdienst die historischen Informationen über seinen Status

6. Eine Signatur, in die für Authentifizierungszwecke alle Felder der vertrauenswürdigen Liste mit Ausnahme des Signaturwerts selbst eingehen

3. **Leitlinien für die Bearbeitung von Einträgen in der vertrauenswürdigen Liste**

3.1. *Statusinformationen über beaufsichtigte bzw. akkreditierte Zertifizierungsdienste und ihre Anbieter in einer einzigen Liste*

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

Eine solche vertrauenswürdige Liste ist das einzige Instrument, mit dem der betreffende Mitgliedstaat Informationen über den Aufsichts-/Akkreditierungsstatus der Zertifizierungsdienste und ihrer Anbieter bereitstellt, und zwar

— **aller Zertifizierungsdiensteanbieter** im Sinne der Definition von Artikel 2 Absatz 11 der Richtlinie 1999/93/EG („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 einschlägigen Bestimmungen der Richtlinie 1999/93/EG **beaufsichtigt werden bzw. akkreditiert wurden**.

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: 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, (sofern sie in einem Mitgliedstaat ansässig sind) beaufsichtigt werden und können im Hinblick auf die Einhaltung der Bestimmungen der Richtlinie 1999/93/EG, einschließlich der Anforderungen von 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 weiterhin 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 entsprechenden Anforderungen der Richtlinie 1999/93/EG, insbesondere Artikel 3 Absatz 3, Artikel 8 Absatz 1, Artikel 11 und Erwägungsgrund 13 (bzw. Artikel 2 Absatz 13, Artikel 3 Absatz 2, Artikel 7 Absatz 1 Buchstabe a, Artikel 8 Absatz 1, Artikel 11, Erwägungsgründe 4 sowie 11 bis 13) genügen.

— **CSPs, die keine QCs ausstellen**:

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

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

Jeder Mitgliedstaat erstellt und führt nur eine einzige vertrauenswürdige Liste, aus der der Aufsichts- und/oder Akkreditierungsstatus der Zertifizierungsdienste hervorgeht, die von den von diesem Mitgliedstaat beaufsichtigten bzw. akkreditierten CSPs erbracht werden. In der vertrauenswürdigen Liste werden mindestens die QCs ausstellenden CSPs aufgeführt. In der vertrauenswürdigen Liste kann auch der Status anderer Zertifizierungsdienste angegeben werden, die nach einem auf einzelstaatlicher Ebene festgelegten Genehmigungssystem beaufsichtigt werden oder akkreditiert wurden.

3.2. *Einheitliche Aufsichts- bzw. Akkreditierungsstatuswerte*

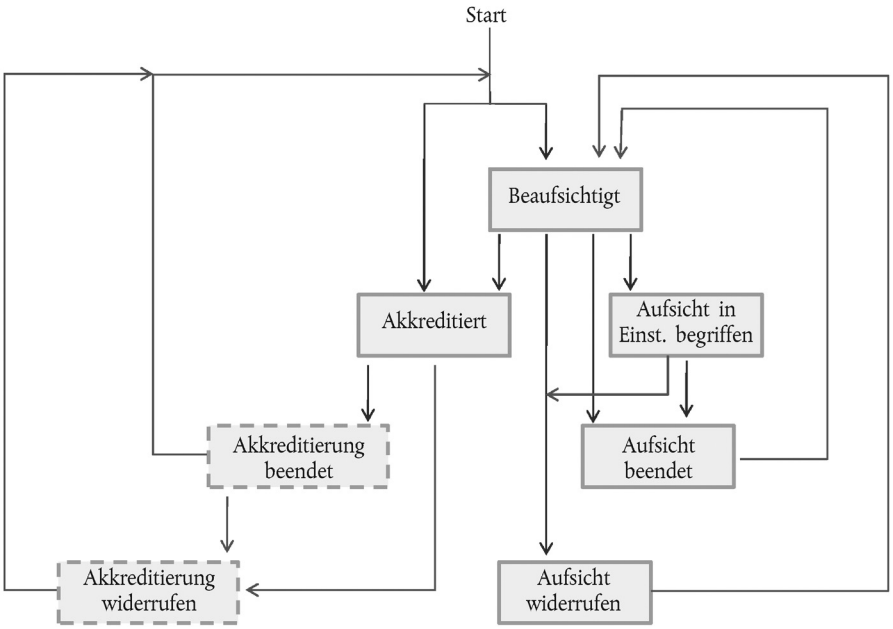
In der vertrauenswürdigen Liste wird die Tatsache, dass ein Dienst gegenwärtig entweder „beaufsichtigt“ wird oder „akkreditiert“ ist, durch den Wert seines aktuellen Status angegeben. Darüber hinaus kann ein Aufsichts- oder Akkreditierungsstatus positiv („beaufsichtigt“, „akkreditiert“, „Aufsicht in Einstellung begriffen“), beendet („Aufsicht beendet“, „Akkreditierung beendet“) oder gar widerrufen („Aufsicht widerrufen“, „Akkreditierung widerrufen“) sein und auf den entsprechenden Wert gesetzt werden. Während seiner gesamten Lebensdauer kann ein Zertifizierungsdienst zwischen Aufsichts- und Akkreditierungsstatus wechseln. ([1])

Die nachstehende Abbildung 1 beschreibt den zu erwartenden Wechsel des Aufsichts- bzw. Akkreditierungsstatus für einen einzelnen Zertifizierungsdienst:

([1]) Beispielsweise kann ein in einem Mitgliedstaat ansässiger Zertifizierungsdiensteanbieter, der einen Zertifizierungsdienst anbietet, der anfänglich von dem Mitgliedstaat (Aufsichtsbehörde) beaufsichtigt wird, 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.

Abbildung 1

Zu erwartender Wechsel des Aufsichts-/Akkreditierungsstatus für einen einzelnen CSP-Dienst



Legende:

Übergangsstatus bei entsprechendem Aufsichtsmodell (z. B. für einen QCs ausstellenden CSP, der in dem Mitgliedstaat, in dem er ansässig ist, akkreditiert ist und beaufsichtigt wird)
Möglicher gegenwärtiger Status, wenn kein entsprechendes Aufsichtsmodell existiert (z. B. für einen CSP, der in einem Mitgliedstaat, in dem er nicht ansässig ist, akkreditiert ist

Möglicher gegenwärtiger Status

Ein in einem Mitgliedstaat ansässiger Zertifizierungsdienst, der QCs ausstellt, muss einer Beaufsichtigung (durch den Mitgliedstaat, in dem er ansässig ist) unterliegen und kann auf freiwilliger Basis akkreditiert werden. Als gegenwärtiger Statuswert („Current status value") eines solchen in einer vertrauenswürdigen Liste aufgeführten Dienstes ist einer der oben angeführten Statuswerte anzugeben; dieser ist im Falle eines Statuswechsels entsprechend zu ändern. „Akkreditierung beendet" und „Akkreditierung widerrufen" müssen jedoch Werte mit „Übergangsstatus" sein, wenn der betreffende CSP_{QC}-Dienst in der vertrauenswürdigen Liste des Mitgliedstaats gelistet ist, in dem er ansässig ist, da ein solcher Dienst standardmäßig beaufsichtigt werden muss (selbst wenn er nicht oder nicht mehr akkreditiert ist). Ist der betreffende Dienst in einem anderen Mitgliedstaat als dem, in dem er ansässig ist, gelistet (akkreditiert), können diese Werte endgültige Werte sein.

Mitgliedstaaten, die ein einzelstaatlich definiertes „anerkanntes Genehmigungssystem" einrichten oder eingerichtet haben, das auf nationaler Ebene der Überwachung 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 (diese) Genehmigungssystem(e) in eine der beiden nachstehenden Kategorien einordnen:

— „freiwillige Akkreditierung" gemäß der Definition und den Bestimmungen 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, Erwägungsgründe 4 sowie 11 bis 13;

— „Aufsicht" wie in der Richtlinie 1999/93/EG vorgesehen und durch einzelstaatliche Bestimmungen und Anforderungen im Einklang mit den einzelstaatlichen gesetzlichen Vorschriften umgesetzt.

Dementsprechend kann ein Zertifizierungsdienst, der keine QCs ausstellt, beaufsichtigt oder freiwillig akkreditiert werden. Als gegenwärtiger Statuswert („Current status value") eines solchen in einer vertrauenswürdigen Liste aufgeführten Dienstes ist einer der oben angeführten Statuswerte (siehe Abbildung 1) anzugeben; dieser ist im Falle eines Statuswechsels entsprechend zu ändern.

Die vertrauenswürdige Liste muss Angaben zu dem (den) zugrunde liegenden Aufsichts- bzw. Akkreditierungssysteme(n) enthalten, 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 im Hinblick auf die Beurteilung des Qualitäts- und Sicherheitsgrads derartiger, auf einzelstaatlicher Ebene für CSPs, die keine QCs ausstellen, eingerichteter Aufsichts- bzw. Akkreditierungssysteme. Sind in der vertrauenswürdigen Liste in Bezug auf Dienste von CSPs, die keine QCs ausstellen, Informationen über den Aufsichts- bzw. Akkreditierungsstatus enthalten, sind die oben genannten Informationen auf der Ebene der vertrauenswürdigen Liste bereitzustellen 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 und den Mitgliedstaaten die Möglichkeit bietet, einen länderspezifischen Text bzw. länderspezifische Verweise hinzuzufügen).

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 „additionalServiceInformation Extension" (Abschnitt 5.5.9.4) als Teil der „Service information extensions" (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 Beaufsichtigung bzw. Akkreditierung von Zertifizierungsdiensten in diesem Mitgliedstaat zuständig sind, darf für einen Zertifizierungsdienst nur ein einziger Eintrag vorhanden sein und der Aufsichts- bzw. Akkreditierungsstatus muss entsprechend aktualisiert werden.

3.3. *In der vertrauenswürdigen Liste enthaltene Einträge zur Erleichterung der Validierung von QES und $AdES_{QC}$*

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

Bei den verlangten Informationen kann es sich um andere Informationen als die „Service digital identity" einer einzigen (Root-)CA handeln, insbesondere um Informationen zur Identifizierung des QC-Status der von einem solchen CA-Dienst ausgestellten Zertifikate und um Angaben dazu, ob die unterstützten Signaturen durch eine SSCD erzeugt wurden. Die für die Erstellung, Bearbeitung und Führung der vertrauenswürdigen Liste zuständige Stelle in einem Mitgliedstaat muss daher für jeden in der vertrauenswürdigen Liste erfassten 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 EN 319 411-2 [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.

[1] Vgl. ETSI EN 319 412-5 — Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile) for the definition of such a statement.

[2] ETSI EN 319 411-2 — Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.

Durch Ergänzung der Felder „Service type identifier“ („Sti“), „Service name“ („Sn“) und „Service digital identity“ („Sdi“) des Diensteintrags in der vertrauenswürdigen Liste mit den im Feld „Service information extensions“ („Sie“) enthaltenen Informationen kann ein spezieller Typ eines qualifizierten Zertifikats, das von einem gelisteten QCs ausstellenden CSP 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). Zu diesem Eintrag gehört auch eine spezielle Angabe zum „Service current status“ („Scs“). Dies wird in Abbildung 2 dargestellt.

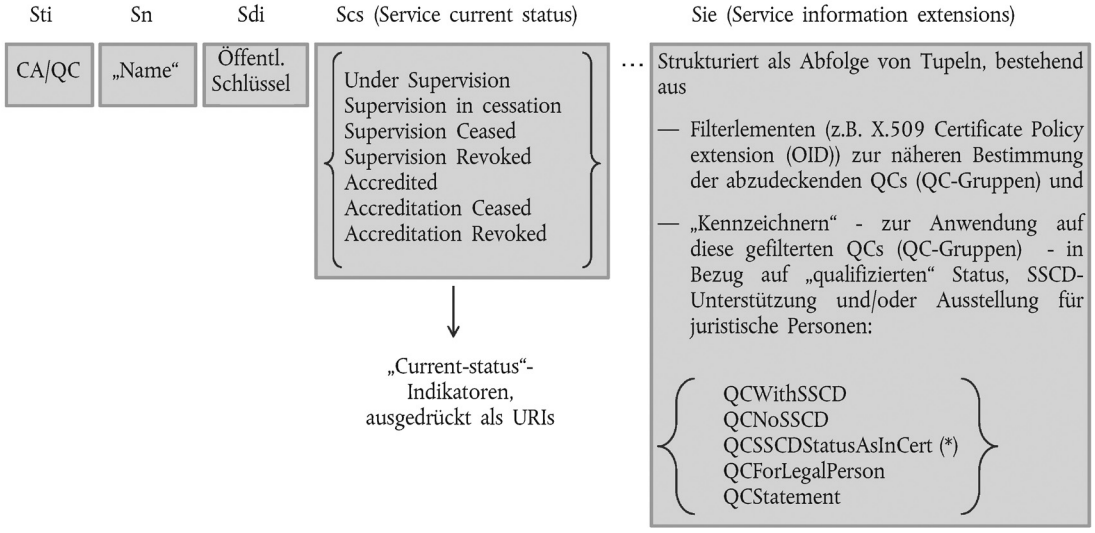
Durch die Aufnahme eines Dienstes in die Liste mit der Angabe der „Sdi“ einer (Root-)CA würde gewährleistet (durch den QCs ausstellenden CSP, aber auch durch die für diesen CSP zuständige Aufsichts- bzw. Akkreditierungsstelle), dass jedes von dieser (Root-)CA(-Hierarchie) ausgestellte Anwenderzertifikat 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 allein aufgrund der Angabe der „Sdi“ dieser (Root-)CA nur angenommen werden, dass über diese (Root-)CA-Hierarchie ausgestellte QCs nicht von einer SSCD unterstützt werden. Für den Hinweis, dass diese QCs als von einer SSCD unterstützt zu betrachten sind, sollte das „Sie“-Feld genutzt werden (dadurch wird auch angezeigt, dass diese Information vom QCs ausstellenden CSP gewährleistet wird und eine Aufsicht bzw. Akkreditierung durch die zuständige Stelle erfolgt).

Abbildung 2

Diensteintrag für einen gelisteten QCs ausstellenden CSP-Dienst in der vertrauenswürdigen Liste

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

Diensteintrag für einen gelisteten CSP_{QC}:



(*) bedeutet, dass entsprechende Angaben in jedem QC unter der von einer CA/QC definierten Sdi-[Sie] sichergestellt sind (keine Angaben im QC: NoSSCD)

Die vorliegenden Spezifikationen für eine gemeinsame Vorlage für die vertrauenswürdige Liste erlauben die Verwendung einer Kombination, bestehend aus fünf Hauptinformationsteilen, im Diensteintrag:

— „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) der öffentliche Schlüssel einer CA, die QCs ausstellt;

— für CA/QC-Dienste optionale Informationen als „Service information extension“ („Sie“), die es ermöglichen, verschiedene dienstespezifische Informationen bezüglich des Widerrufsstatus abgelaufener Zertifikate, zusätzlicher Merkmale von QCs, der Übernahme einer CSP durch eine andere CSP sowie sonstige zusätzliche Diensteinformationen aufzunehmen. Die zusätzlichen Merkmale von QCs werden beispielsweise durch eine Abfolge von einem oder mehreren Tupeln dargestellt, von denen jedes folgende Angaben enthält:

— Kriterien zur näheren Identifikation (Filterung) — innerhalb des durch die „Sdi“ identifizierten Zertifizierungsdienstes — der Gruppe qualifizierter Zertifikate, für die im Hinblick auf die Angabe des „qualifizierten“ Status, die SSCD-Unterstützung und/oder die Ausstellung für juristische Personen Zusatzinformationen erforderlich sind bzw. angegeben werden, und

— entsprechende Informationen („Qualifier“ — „Kennzeichner“) darüber, ob diese Gruppe qualifizierter Zertifikate als „qualifiziert“ zu betrachten ist und ob sie von einer SSCD unterstützt wird, oder Hinweis darauf, ob die entsprechenden Informationen in einer genormten, maschinenlesbaren Form Bestandteil des QC sind, und/oder Informationen darüber, dass solche QCs juristischen Personen ausgestellt werden (standardmäßig ist davon auszugehen, dass sie nur natürlichen Personen ausgestellt werden).

— 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.

3.4. *Leitlinien für die Bearbeitung und Nutzung von CSP_{QC}-Diensteinträgen*

Allgemeine Leitlinien für die Bearbeitung:

1. Wenn sichergestellt ist (aufgrund einer Garantie des CSP_{QC} und der Beaufsichtigung bzw. Akkreditierung durch die Aufsichtsstelle (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 zur SSCD-Unterstützung enthalten.

2. Wenn sichergestellt ist (aufgrund einer Garantie des CSP_{QC} und der Beaufsichtigung bzw. Akkreditierung 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/oder den 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 (aufgrund einer Garantie des CSP_{QC} und der Beaufsichtigung bzw. Akkreditierung 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), ein von einer SSCD unterstütztes Zertifikat 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, wenn das „Sie“-Feld verwendet wird.

4. Wenn sichergestellt ist (aufgrund einer Garantie des CSP_{QC} und der Beaufsichtigung bzw. Akkreditierung 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/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 Qualifikation verwendet werden. Infolgedessen wird wahrscheinlich die Aufnahme verschiedener „SSCD support information values“ für eine „Sdi“ erforderlich, wenn das „Sie“-Feld verwendet wird.

Generell kann für einen in der vertrauenswürdigen Liste enthaltenen CSP von einem Diensteintrag pro öffentlichen Schlüssel für einen CA/QC-Zertifizierungsdienst, d. h. pro Zertifizierungsstelle, die (direkt) QCs ausstellt, ausgegangen werden. Unter bestimmten außergewöhnlichen Umständen und bei sorgfältiger Verwaltung kann sich die Aufsichts- bzw.

Akkreditierungsstelle eines Mitgliedstaats dazu entschließen, den öffentlichen Schlüssel einer Root-CA oder Upper-Level-CA innerhalb der PKI des CSP (wenn z. B. bei einem CSP eine Hierarchie von CAs von einer Root-CA hinunter bis zu mehreren QCs ausstellenden CAs besteht) als „Sdi" eines einzigen Eintrags in der Diensteliste des gelisteten CSP zu verwenden, anstatt alle nachgeordneten CAs, die QCs ausstellen, zu listen (d. h. Listung einer CA, die nicht direkt Anwender-QCs ausstellt und Zertifizierung einer Hierarchie von CAs bis hinunter zu CAs, die Anwender-QCs ausstellen). Die Konsequenzen (Vorteile und Nachteile) der Verwendung des öffentlichen Schlüssels einer Root-CA oder einer Upper-Level-CA als „Sdi"-Wert in einer vertrauenswürdigen Liste müssen bei der Implementierung durch die Mitgliedstaaten gründlich erwogen werden. Im Falle dieser zulässigen Abweichung von der üblichen Vorgehensweise muss der Mitgliedstaat zudem die erforderliche Dokumentation bereitstellen, um den Aufbau und die Verifizierung des Zertifizierungspfads zu ermöglichen. Im Falle eines CSP_{QC}, der eine Root-CA verwendet, unter der mehrere CAs qualifizierte und nicht qualifizierte Zertifikate ausstellen, dessen QCs jedoch nur die Erklärung zur QcCompliance, aber keine Informationen über eine etwaige SSCD-Unterstützung enthalten, würde die alleinige Angabe der „Sdi" der Root-CA auf der Grundlage der oben ausgeführten Regeln beispielsweise bedeuten, dass keines der unter dieser Root-CA ausgestellten QCs von einer SSCD unterstützt wird. Im Falle von QCs, die zwar von einer SSCD unterstützt werden, aber keine maschinenlesbare Erklärung über eine solche Unterstützung enthalten, wäre dringend zu empfehlen, bei künftig ausgestellten QCs von der QcSSCD-Erklärung Gebrauch zu machen. Zwischenzeitlich (bis zum Ablauf des letzten QC, das diese Information nicht enthält) sollten in der vertrauenswürdigen Liste das Feld „Sie" und die entsprechende „Qualifications Extension" genutzt werden, z. B. für die Bereitstellung von Informationen 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 für die Ergänzung der identifizierten (gefilterten) (Gruppen von) Zertifikate(n) mit eindeutiger „SSCD support information" durch Anwendung von „Kennzeichnern".

Die **allgemeinen Leitlinien zur Nutzung** von Anwendungen und Diensten im Zusammenhang mit elektronischen Signaturen oder Produkten, die auf 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 Extension" näher als „Root-CA/QC" bestimmt wurde)

— bedeutet, dass alle durch die mit „Sdi" identifizierte CA (ebenso bei der CA-Hierarchie, die von der mit „Sdi" identifizierten Root-CA ausgeht) ausgestellten Anwenderzertifikate QCs sind, **vorausgesetzt**, dass dies im Zertifikat durch die Verwendung der entsprechenden maschinenlesbaren QC-Erklärung (d. h. QcCompliance) und/oder der vom ETSI definierten QCP(+) OIDs angegeben wird (und von der Aufsichts- bzw. Akkreditierungsstelle gewährleistet wird, siehe oben „Allgemeine Leitlinien für die Bearbeitung").

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

— **und WENN** „Sie"-„Qualifications Extension"-Informationen vorhanden sind, müssen — zusätzlich zur obigen Standard-Auslegungsregel — Zertifikate, die durch die Verwendung dieser „Sie"-„Qualifications Extension"-Informationen identifiziert werden, die auf dem Grundsatz einer Abfolge von „Filtern" zur näheren Identifikation einer Gruppe von Zertifikaten beruhen, anhand deren entsprechende Kennzeichner interpretiert werden, die Zusatzinformationen zum qualifizierten Status, zur „SSCD-Unterstützung" und/oder zur „Legal person as subject" enthalten (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, in einem eigenen Feld oder einer Erweiterung des Zertifikats angegebenen Werts, gefiltert werden usw.). Diese Kennzeichner gehören zu folgender Gruppe von „Kennzeichnern", die — bei Fehlen einschlägiger Informationen im entsprechenden QC-Zertifikat — verwendet werden zur

  — Angabe des qualifizierten Status: Bedeutung von „QCStatement": identifiziertes Zertifikat (identifizierte Zertifikate) ist (sind) qualifiziert;

  UND/ODER

  — Angabe der Art der 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 zur SSCD-Unterstützung in jedem QC im Rahmen der unter „Sdi"-„Sie" angegebenen Informationen in diesem CA/QC-Eintrag sichergestellt;

  UND/ODER

— Angabe zur Ausstellung für juristische Personen:

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

3.5. *Dienste, die „CA/QC“-Dienste unterstützen, aber nicht Bestandteil der „CA/QC“-„SdI“ sind*

Dienste im Zusammenhang mit dem Gültigkeitsstatus von qualifizierten Zertifikaten, bei denen die Angabe des Gültigkeitsstatus (z. B. CRLs und OCSP-Responses) von einer Stelle signiert wird, deren privater Schlüssel nicht über einen Zertifizierungspfad für gelistete, QCs ausstellende CAs („CA/QC“) zertifiziert wurde, werden in die vertrauenswürdige Liste aufgenommen; die betreffenden Dienste im Zusammenhang mit dem Gültigkeitsstatus von Zertifikaten werden als solche in der Liste aufgeführt (d. h. als Dienste des Typs „OCSP/QC“ bzw. „CRL/QC“), da sie als Bestandteil 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 innerhalb 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 auf Zertifizierungsdienste, die nicht qualifizierte Zertifikate ausstellen (Dienste des Typs „CA/PKC“), angewandt werden.

In der vertrauenswürdigen Liste müssen Dienste im Zusammenhang mit dem Gültigkeitsstatus von Zertifikaten aufgeführt sein, wenn die Anwenderzertifikate, auf die sich die Dienste beziehen, keine Angaben dazu enthalten, an welchem Ort Informationen über solche Dienste zu finden sind.

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	1. ein Zertifizierungsdiensteanbieter, der Public-Key-Zertifikate erstellt und zuweist, oder 2. ein technischer Zertifikatserstellungsdienst, der von einem Zertifizierungsdiensteanbieter genutzt wird, der Public-Key-Zertifikate erstellt und zuweist. *HINWEIS*: Weitere Erläuterungen zum Begriff der „Zertifizierungsstelle“ siehe EN 319 411-2 [1], Abschnitt 4.
Zertifizierungsstelle, die qualifizierte Zertifikate ausstellt	CA/QC	Eine CA, die die Anforderungen von Anhang II der Richtlinie 1999/93/EG erfüllt und qualifizierte Zertifikate gemäß Anhang I der Richtlinie 1999/93/EG ausstellt.
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	Unterzeichner	Definition nach Artikel 2 Absatz 3 der Richtlinie 1999/93/EG.
Aufsicht	Aufsicht	Betrifft die Aufsicht im Sinne von Artikel 3 Absatz 3 der Richtlinie 1999/93/EG. Die Richtlinie 1999/93 sieht vor, dass die Mitgliedstaaten ein angemessenes System zur Beaufsichtigung der auf ihrem Staatsgebiet ansässigen CSPs, die qualifizierte Zertifikate für die Öffentlichkeit ausstellen, einrichten, 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 wurden, hervorgeht, so dass den Bestimmungen der Richtlinie 1999/93/EG Genüge getan ist.

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 119 612 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 119 612). *HINWEIS*: Dieser Begriff ist umfassender als der Begriff „Zertifizierungsdiensteanbieter, der Zertifikate ausstellt oder andere Dienste im Zusammenhang mit elektronischen Signaturen erbringt“.
Anbieter von vertrauenswürdigen Diensten (Trust Service Provider)	TSP	Stelle, die einen oder mehrere (elektronische) vertrauenswürdige Dienste erbringt. (Dieser Begriff ist umfassender als der Begriff „CSP“.)
Token für vertrauenswürdigen Dienst (Trust Service Token)	TrST	Ein physisches oder binäres (logisches) Objekt, das bei Nutzung eines vertrauenswürdigen Dienstes erzeugt oder ausgestellt wird. Beispiele für binäre TrSTs sind Zertifikate, Certificate Revocation Lists (CRLs), Zeitstempel-Tokens (Time Stamp Tokens — TSTs) und Online Certificate Status Protocol responses (OCSP-Responses).
Qualifizierte elektronische Signatur (Qualified Electronic Signature)	QES	Eine von einem QC unterstützte AdES, die von einer sicheren Signaturerstellungseinheit (secure signature creation device — SSCD) gemäß der Definition in 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 Anforderungen an eine 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.

([1]) EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.

Die in den folgenden Kapiteln 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 wie in RFC 2119 ([1]) erläutert auszulegen.

KAPITEL I

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

Diese Spezifikationen beruhen auf den in ETSI TS 119 612 v1.1.1 (im Folgenden „ETSI TS 119 612“) enthaltenen Spezifikationen und Anforderungen.

Soweit die vorliegenden Spezifikationen keine speziellen Anforderungen enthalten, MÜSSEN die Anforderungen aus ETSI TS 119 612 Abschnitte 5 und 6 in ihrer Gesamtheit erfüllt werden. Soweit die vorliegenden Spezifikationen spezielle Anforderungen enthalten, haben diese Vorrang vor den entsprechenden Anforderungen aus ETSI TS 119 612. Bei Diskrepanzen zwischen den vorliegenden Spezifikationen und den Spezifikationen laut ETSI TS 119 612 MUSS den vorliegenden Spezifikationen normative Wirkung eingeräumt werden.

Scheme operator name (Abschnitt 5.3.4)

Dieses Feld MUSS vorhanden sein und MUSS den Spezifikationen laut TS 119 612 Abschnitt 5.3.4 entsprechen.

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

Ein Land KANN über separate Aufsichts- und Akkreditierungsstellen und sogar über zusätzliche Einrichtungen für beliebige operative Aktivitäten verfügen. Es obliegt den einzelnen Mitgliedstaaten, den Scheme operator ihrer vertrauenswürdigen Liste zu benennen. Es ist davon auszugehen, dass die Aufsichtsstelle, die Akkreditierungsstelle und der Scheme operator (wenn es sich um separate Stellen handelt) jeweils 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 vertrauenswürdigen Liste sowie in den systemspezifischen Informationen im „Scheme information URI" (Abschnitt 5.3.7) als solche identifiziert werden.

Scheme name (Abschnitt 5.3.6)

Dieses Feld MUSS vorhanden sein und MUSS den Spezifikationen laut TS 119 512 Abschnitt 5.3.6 entsprechen. Dabei MUSS der „Scheme name" wie folgt lauten:

„DE_name_value" = „Aufsichts- bzw. Akkreditierungsstatusliste der Zertifizierungsdienste von Zertifizierungsdiensteanbietern, die von dem Mitgliedstaat, in dem der betreffende Scheme operator ansässig ist, im Hinblick auf die Einhaltung der einschlägigen Bestimmungen der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen beaufsichtigt werden bzw. akkreditiert wurden".

Scheme information URI (Abschnitt 5.3.7)

Dieses Feld MUSS vorhanden sein und MUSS den Spezifikationen laut TS 119 512 Abschnitt 5.3.7 entsprechen. Dabei MÜSSEN die „angemessenen Informationen" über das System mindestens Folgendes umfassen:

— Für alle Mitgliedstaaten identische einleitende Informationen hinsichtlich Umfang und Hintergrund der vertrauenswürdigen Liste und der zugrunde liegenden Aufsichts- bzw. Akkreditierungssysteme. Nachstehend der zu verwendende gemeinsame Text, in dem die Zeichenkette „[*name of the relevant Member State*]" durch den Namen des betreffenden Mitgliedstaats ersetzt werden MUSS:

„The present list is the „Trusted List of Supervisor/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;

— allowing for a trusted validation of electronic signatures supported by those listed supervised/accredited certification services from the listed CSPs.

The Trusted List of a Member State provides, as a minimum, information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Article 3(2) and (3) and Article 7(1)(a)), including, when this is not part of the QCs, 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 compliance 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 Article 3(3), Article 8.(1), Article 11 (respectively, Article 2(13), Article 3(2), Article 7(1)(a), Article 8(1), Article 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 at a national level on a voluntary basis."

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

  — 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.

  Diese spezifischen Informationen MÜSSEN für jedes der oben genannten zugrunde liegenden Systeme zumindest Folgendes enthalten:

  — allgemeine Beschreibung;

  — Informationen über das von der Aufsichts- bzw. Akkreditierungsstelle einerseits und den CSPs andererseits angewandte Verfahren für die Beaufsichtigung bzw. Akkreditierung von CSPs;

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

— Ggf. spezielle Informationen über die besonderen „Qualifications", die einige der infolge der Bereitstellung eines Zertifizierungsdienstes generierten oder ausgestellten physischen oder binären (logischen) Objekte beanspruchen können, wenn sie den einzelstaatlichen Bestimmungen und Anforderungen entsprechen, unter anderem zur Bedeutung einer derartigen „Qualification" und der entsprechenden einzelstaatlichen Bestimmungen und Anforderungen.

Weitere länderspezifische Informationen über das System KÖNNEN auf freiwilliger Basis bereitgestellt werden:

— 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.

Scheme type/community/rules (Abschnitt 5.3.9)

Dieses Feld MUSS vorhanden sein, den Spezifikationen aus TS 119 612 Abschnitt 5.3.9 entsprechen und mindestens zwei URIs enthalten:

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

  URI: http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon

  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 implementation of such Trusted Lists is also to be referred to in the list of links (pointers) towards each Member State's 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, as a minimum, information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Article 3(2) and (3) and Article 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.

([1]) Die letzten beiden Informationsgruppen sind von entscheidender Bedeutung für die Beurteilung des Qualitäts- und Sicherheitsgrads solcher für CSPs, die keine QCs ausstellen, geltender Aufsichts- bzw. Akkreditierungssysteme durch die auf das Zertifikat vertrauenden Parteien. Diese Informationsgruppen werden auf der Ebene der vertrauenswürdigen Liste 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). Zusatzinformationen 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.

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 compliance 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 Article 3(3), Article 8)(1), Article 11 (respectively, Article2(13), Article 3(2), Article 7(1)(a), Article 8(1), Article 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 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 Article 2(11) of Directive 1999/93/EC). 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 Trusted List

The **general user guidelines** for electronic signature applications, services or products relying on a Trusted List according to the Annex of Commission Decision [reference to the present Decision] 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 EN 319 412-5 defined QcStatements (i.e. QcCompliance, QcSSCD usw.) and/or EN 319 411-2 defined QCP(+) OIDs (and this is guaranteed by the issuing CSP and ensured by the Member State Supervisory/Accreditation Body)

Note: if no „Sie" „Qualifications Extension" information is present or if an end-entity certificate that is claimed to be a QC is not further identified through a related „Sie" „Qualifications Extension" information, 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. QcCompliance, QcSSCD usw.) 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" „Qualifications Extension" information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this „Sie" „Qualifications Extension" information, 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 the qualified status, the „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:

— o to indicate the qualified status: „QCStatement" meaning the identified certificate(s) is(are) qualified;

AND/OR

— o 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

— o 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/EC for further details on the fields, description and meaning for the Member States' Trusted Lists.“

— einen für die jeweilige vertrauenswürdige Liste eines Mitgliedstaats spezifischen URI, der auf einen deskriptiven Text verweist, der für die vertrauenswürdige Liste dieses Mitgliedstaats gelten MUSS:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC; dabei ist CC der im Feld „Scheme territory“ (Abschnitt 5.3.10) verwendete ISO 3166-1 ([1]) Alpha-2-Ländercode.

— Angaben dazu, wo Benutzer länderspezifische Richtlinien/Vorschriften des betreffenden Mitgliedstaats finden, anhand deren die in die Liste aufgenommenen Dienste aufgrund des entsprechenden Aufsichtssystems und der freiwilligen Akkreditierungssysteme des Mitgliedstaats bewertet werden MÜSSEN.

— Angaben dazu, wo Benutzer eine länderspezifische Anleitung des betreffenden Mitgliedstaats zur Verwendung und Auslegung des Inhalts der vertrauenswürdigen Liste im Hinblick auf Zertifizierungsdienste finden, bei denen es sich nicht um die Ausstellung von QCs handelt. 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“ (Abschnitt 5.5.9) zu diesem Zweck verwendet werden.

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

TSL policy/legal notice (Abschnitt 5.3.11)

Dieses Feld MUSS vorhanden sein und MUSS den Spezifikationen laut TS 119 612 Abschnitt 5.3.11 entsprechen. Es muss die Richtlinien bzw. einen rechtlichen Hinweis („policy/legal notice“) zum Rechtsstatus des Systems bzw. die vom System in der Rechtsordnung, der es angehört, erfüllten rechtlichen Anforderungen und/oder alle Beschränkungen und Bedingungen enthalten, unter denen die vertrauenswürdige Liste veröffentlicht und gepflegt wird. Dabei MUSS es sich um eine Abfolge mehrsprachiger Zeichenketten (Klartext) handeln, die aus zwei Teilen besteht:

1. einem ersten obligatorischen Teil, der den vertrauenswürdigen Listen aller Mitgliedstaaten gemeinsam ist (obligatorische Sprache Englisch (UK), eine oder mehrere Landessprachen möglich) und aus dem hervorgeht, dass der anwendbare Rechtsrahmen die 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 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.“

([1]) ISO 3166-1/2006: Codes für die Namen von Ländern und deren Untereinheiten — Teil 1: Codes für Ländernamen.

Fassung des gemeinsamen Texts in deutscher Sprache: [amtliche Übersetzung(en) des vorstehenden englischen Texts].

2. einem zweiten optionalen Teil, der speziell auf die jeweilige vertrauenswürdige Liste zugeschnitten ist (obligatorische Sprache Englisch (UK), eine oder mehrere Landessprachen möglich) und der Verweise auf den spezifischen anwendbaren einzelstaatlichen Rechtsrahmen enthält (z. B. insbesondere im Zusammenhang mit einzelstaatlichen Aufsichts- bzw. Akkreditierungssystemen für CSPs, die keine QCs ausstellen).

KAPITEL II

KONTINUITÄT DER VERTRAUENSWÜRDIGEN LISTEN

Die der Kommission gemäß Artikel 3 Buchstabe c des vorliegenden Beschlusses zu übermittelnden Zertifikate MÜSSEN so ausgestellt werden,

— dass zwischen ihren Gültigkeitsdaten mindestens drei Monate liegen;

— dass sie mit neuen Schlüsselpaaren erzeugt werden, da bereits früher verwendete Schlüsselpaare nicht erneut zertifiziert werden dürfen.

Bei Kompromittierung oder Außerkraftsetzung EINES der privaten Schlüssel, die dem öffentlichen Schlüssel entsprechen, welcher zur Validierung der Signatur der vertrauenswürdigen Liste verwendet werden könnte und der Kommission übermittelt und in ihren zentralen Zeigerlisten veröffentlicht wurde, MÜSSEN die Mitgliedstaaten

— unverzüglich eine neue, mit einem nicht kompromittierten privaten Schlüssel signierte vertrauenswürdige Liste ausstellen, sofern die veröffentlichte Liste mit einem kompromittierten oder außer Kraft gesetzten privaten Schlüssel signiert wurde;

— der Kommission unverzüglich die neue Liste der den privaten Schlüsseln entsprechenden Public-Key-Zertifikate übermitteln, welche für die Signatur der vertrauenswürdigen Liste verwendet werden könnten.

Bei Kompromittierung oder Außerkraftsetzung ALLER privaten Schlüssel, die den öffentlichen Schlüsseln entsprechen, welche zur Validierung der Signatur der vertrauenswürdigen Liste verwendet werden könnten und der Kommission übermittelt und in ihren zentralen Zeigerlisten veröffentlicht wurden, MÜSSEN die Mitgliedstaaten

— neue Schlüsselpaare erstellen, die für die Signatur der vertrauenswürdige Liste und der entsprechenden Public-Key-Zertifikate verwendet werden könnten;

— unverzüglich eine neue, mit einem dieser neuen privaten Schlüssel signierte vertrauenswürdige Liste erstellen und das entsprechende Public-Key-Zertifikat übermitteln;

— der Kommission unverzüglich die neue Liste der den privaten Schlüsseln entsprechenden Public-Key-Zertifikate übermitteln, welche für die Signatur der vertrauenswürdigen Liste verwendet werden könnten.

KAPITEL III

SPEZIFIKATIONEN FÜR DIE MENSCHENLESBARE FASSUNG DER VERTRAUENSWÜRDIGEN LISTE

Wird eine menschenlesbare Fassung der vertrauenswürdigen Liste erstellt und veröffentlicht, SOLLTE die Bereitstellung im PDF-Format gemäß ISO 32000 [1] erfolgen. Die Formatierung MUSS dem Profil PDF/A (ISO 19005 [2]) entsprechen.

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

— Die Struktur der menschenlesbaren Fassung SOLLTE sich an dem in TS 119 612 beschriebenen logischen Modell orientieren.

— 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 Wert des Felds (z. B. „eine Zertifizierungsstelle, die Public-Key-Zertifikate ausstellt“);

  — ggf. mehrere Fassungen in natürlichen Sprachen, wie in der vertrauenswürdigen Liste vorgesehen.

[1] ISO 32000-1:2008: Document management — Portable document format — Part 1: PDF 1.7.
[2] ISO 19005-2:2011: Document management — Electronic document file format for long-term preservation — Part 2: Use of ISO 32000-1 (PDF/A-2).

— 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)

  — 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 Fassung SOLLTE leicht auszudrucken sein.

— Die menschenlesbare Fassung MUSS vom Scheme operator gemäß dem PAdES-Signaturen-Baseline-Profil signiert werden ([1]).

([1]) ETSI TS 103 172 (März 2012) — Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile.