eCH-0048 PKI-Zertifikatsklassen

Name	PKI-Zertifikatsklassen
eCH-Nummer	eCH-0048
Kategorie	Standard
Reifegrad	Definiert
Version	2.0
Status	Genehmigt
Beschluss am	2018-11-28
Ausgabedatum	2018-11-30
Ersetzt Version	1.0 < Major Change>
Voraussetzungen	-
Beilagen	-
Sprachen	Deutsch (Original), Französisch (Übersetzung)
Autoren	Fachgruppe IAM Adrian Müller, ID Cyber-Identity AG adrian.mueller@cyber-identity.com Michael von Niederhäusern, BIT Daniel Stich, BIT
Herausgeber / Vertrieb	Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Zusammenfassung

Der vorliegende Standard definiert Zertifikatsklassen (bzw. Certificate Policies oder Zertifizierungspolitiken) als verschiedene Vertrauensniveaus für X.509-Zertifikate im schweizerischen eGovernement. Diese Zertifikatsklassen basieren auf

- dem „Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, ZertES)“ und
- der Europäischen Norm (EN) ETSI EN 319 411 „Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates”.

Der Standard dient sowohl als Entscheidungshilfe für Verantwortliche für eGovernment-Applikationen hinsichtlich der (abhängig vom jeweiligen Schutzbedarf) benötigten Zertifikatsklassen, als auch zur Information der Anbieterinnen von Zertifizierungsdiensten.

Inhaltsverzeichnis

1 Einleitung 6
1.1 Status 6
1.2 Überblick 6
1.3 Inhalt und Ziel des Standards 6
1.4 Abgrenzung 11
1.5 Nutzer des Standards 11
1.6 Verwendung von Schlüsselwörtern 11
1.7 Erweiterte Übersicht der Zertifikatsklassen 13
2 Anforderungsprofile 17
2.1 Einleitung 17
2.2 Übergreifende Anforderungen 17
2.2.1 Erfüllung aller Anforderungen 17
2.2.2 Zertifikatsinhaber „Subject“ (informativ) 17
2.2.3 Identitätsnachweis 18
2.2.4 Algorithmen und Schlüssellängen (informativ) 18
2.2.5 Softtoken 19
2.2.6 Zertifikatszweck / Key Usage 19
2.2.7 Schlüsselhinterlegung 20
2.2.8 Laufzeit der Registrierung 20
2.3 Klasse 1 (LCP) 20
2.3.1 Einleitung 20
2.3.2 Archivierung der Antragsdokumente und/oder -daten 20
2.3.3 Referenzierte Certificate Policy 21
2.3.4 Beschreibung (informativ) 21
2.3.4.1 Kryptografisches Token 21
2.3.4.2 Registrierung 21
2.3.4.2.1 Registrierungsstärke 21
2.3.4.2.2 Identitätsnachweis 21
2.3.4.2.3 Erlaubte Zertifikats-Inhaber (Subject) 21
2.3.4.2.4 Identifikator 21
2.3.4.2.5 Archivierung der Antragsdokumente und/oder -daten 21
2.3.4.3 Steuerung 22
2.3.4.3.1 Anforderungen an CA (Betrieb, Personal, Prozesse) 22
2.3.4.3.2 Haftung 22
2.3.4.3.3 Bereitstellung von Widerrufs-Informationen 22
2.4 Klasse 2 (NCP) 22

2.4.1 Einleitung 22
2.4.2 Registrierung 22
2.4.3 Archivierung der Antragsdokumente und/oder -daten 22
2.4.4 Referenzierte Certificate Policy 22
2.4.5 Beschreibung (informativ) 23
2.4.5.1 Kryptografisches Token 23
2.4.5.2 Registrierung 23
2.4.5.2.1 Registrierungsstärke 23
2.4.5.2.2 Identitätsnachweis 23
2.4.5.2.3 Erlaubte Zertifikatsinhaber (Subject) 23
2.4.5.2.4 Identifikator 23
2.4.5.2.5 Archivierung der Antragsdokumente und/oder -daten 23
2.4.5.3 Steuerung 23
2.4.5.3.1 Anforderungen an CA (Betrieb, Personal, Prozesse) 23
2.4.5.3.2 Haftung 24
2.4.5.3.3 Bereitstellung von Widerrufs-Informationen 24
2.5 Klasse 2+ (NCP+) 24
2.5.1 Referenzierte Certificate Policy 24
2.6 Klasse 3 (geregelt) 25
2.6.1 Einleitung 25
2.6.2 Referenzierte Certificate Policy (analog QCP-n und QCP-l oder QCP-w) 25
2.6.3 Beschreibung (informativ) 26
2.6.3.1 Kryptografisches Token 26
2.6.3.2 Registrierung 26
2.6.3.2.1 Registrierungsstärke 26
2.6.3.2.2 Identitätsnachweis 26
2.6.3.2.3 Erlaubte Zertifikatsinhaber (Subject) 26
2.6.3.2.4 Identifikator 27
2.6.3.2.5 Archivierung der Antragsdokumente und/oder -daten 27
2.6.3.3 Steuerung 27
2.6.3.3.1 Anforderungen an CA (Betrieb, Personal, Prozesse) 27
2.6.3.3.2 Haftung 27
2.6.3.3.3 Bereitstellung von Widerrufs-Informationen 27
2.7 Klasse 3+ (geregelt+) 28
2.7.1 Einleitung 28
2.7.2 Signatur und Siegel 28
2.7.3 Zertifikate für Nicht-Signatur-Anwendungen 28
2.7.4 Referenzierte Certificate Policy 28

3 Object Identifier (OID) 29
4 Erläuterungen (informativ) 31
4.1 Erläuterungen zu ZertES 31
4.2 Erläuterungen zu eIDAS 33
4.3 Erläuterungen zu eCH-0170 33
4.4 Erläuterungen zum UID-System 34
4.5 Erläuterungen zu Attributzertifikaten 34
4.6 Erläuterungen zu ElDI-V 35
4.7 Extended-Validation-SSL-Zertifikate 35
5 Sicherheitsüberlegungen 35
6 Haftungsausschluss/Hinweise auf Rechte Dritter 36
7 Urheberrechte 36
Anhang A – Referenzen & Bibliographie 37
Anhang B – Mitarbeit & Überprüfung 40
Anhang C – Abkürzungen 40
Anhang D – Glossar 42
Anhang E – Änderungen gegenüber Vorversion 42
Anhang F – Abbildungsverzeichnis 42
Anhang G – Tabellenverzeichnis 42
Anhang H – Mapping auf bestehende Angebote 42

Hinweis

Aus Gründen der besseren Lesbarkeit und Verständlichkeit wird im vorliegenden Dokument bei der Bezeichnung von Personen ausschliesslich die maskuline Form verwendet. Diese Formulierung schliesst Frauen in ihrer jeweiligen Funktion ausdrücklich mit ein.

1 Einleitung

1.1 Status

Genehmigt: Das Dokument wurde vom Expertenausschuss genehmigt. Es hat für das definierte Einsatzgebiet im festgelegten Gültigkeitsbereich normative Kraft.

1.2 Überblick

Im eGovernment (und im eBusiness im Allgemeinen) werden zur Absicherung der Kommunikation bzw. des Geschäftsverkehrs Public Key Infrastrukturen (PKI) eingesetzt, in welchen digitale Zertifikate (gemäss der technischen Norm X.509) ausgestellt werden. Die Anwendungsbereiche umfassen dabei die Authentisierung von Teilnehmern, Integrität und Authentizität von Daten (Signaturen) oder Verschlüsselung.

Abhängig vom jeweiligen Anwendungsfall (Use Case), dem Schadenspotential und den rechtlichen Vorgaben ergibt sich der erforderliche Schutzbedarf einer Anwendung. Davon abgeleitet ergibt sich das benötigte *Vertrauensniveau* (bzw. *Vertrauensstufe*) der dabei eingesetzten digitalen Zertifikate, also die „*Zertifikatsklasse*“.

Der vorliegende Standard richtet sich an Anbieterinnen von Zertifizierungsdiensten und an eGovernment-Verantwortliche (siehe auch Kap. 1.5 „Nutzer des Standards“) und dient diesen als Vorgabe bzw. als Entscheidungshilfe, welches Vertrauensniveau für eine bestimmte Anwendung verlangt werden muss.

In der Umsetzung ergibt sich die Zertifikatsklasse aus

- dem verwendeten kryptographischen Token, also dem Schutz des zum digitalen Zertifikat gehörenden privaten Schlüssels (z.B. Speicherung in zertifizierter Hardware),
- der Stärke der Registrierung (z.B. persönliche Registrierung mit Pass oder Identitätskarte) und
- der Steuerung seitens der Anbieterin von Zertifizierungsdiensten, auch „Certification Service Provider“ oder „Trust Service Provider“ (TSP) genannt:
  Technische und organisatorische Massnahmen zum Schutz des Betriebs, Aufsicht, Prozessmaturität und Haftungsregelungen.

Die entsprechenden Vorgaben werden „Zertifizierungspolitik“ oder „Certificate Policy“ (CP) genannt. Eine Anbieterin von Zertifizierungsdiensten beschreibt neben der Zertifizierungspolitik auch die Art der Umsetzung in der „Zertifizierungspraxis“, auch „Certification Practice Statement“ (CPS) genannt. Aufgrund der thematischen Überlappung werden CP und CPS oft auch als kombiniertes Dokument erstellt.

1.3 Inhalt und Ziel des Standards

Das vorliegende Dokument beschreibt Vertrauensniveaus für digitale Zertifikate basierend auf den folgenden beiden Regularien:

- Das „Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, ZertES)“ vom 18. März 2016.
    - ZertES,
    - die zugehörige Verordnung (VZertES) sowie
    - die dafür erlassen Technischen und Administrativen Ausführungsbestimmungen (TAV-ZertES)

  legen die Anforderungen an gesetzlich „geregelte Zertifikate“ fest. Geregelte Zertifikate können dabei für beliebige Anwendungszwecke ausgestellt werden, bei Zertifikaten für die Anwendungen qualifizierte Signatur, geregelte Signatur und geregeltes Siegel gelten aber zusätzliche Anforderungen. Auch für geregelte Website-Zertifikate gelten spezifische Format-Vorschriften.
- Die Europäische Norm (EN) ETSI EN 319 411 „Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates”, welche Zertifizierungspolitiken für verschieden starke Vertrauensniveaus im Detail spezifiziert. Diese Norm wurde in zwei[1] Teilen publiziert:
    - ETSI EN 319 411-1 „Part 1: General requirements“
    - ETSI EN 319 411-2 „Part 2: Requirements for trust service providers issuing EU qualified certificates“

ETSI EN 319 411-1 „Part 1: General requirements“ definiert die Zertifizierungspolitiken bzw. Vertrauensniveaus

- Lightweight Certificate Policy (LCP) als schwaches Vertrauensniveau,
- Normalized Certificate Policy (NCP) als starkes Vertrauensniveau,
- Extended Normalized Certificate Policy (NCP+), welches zusätzlich zu NCP Hardware als Zertifikatstoken verlangt, sowie
- weitere (darauf aufbauende) Zertifizierungspolitiken, welche spezifisch auf TLS-Server-Zertifikate ausgerichtet sind.

ETSI EN 319 411-2 „Part 2: Requirements for trust service providers issuing EU qualified certificates“ wird von TAV-ZertES (weitgehend) referenziert, die entsprechenden Anforderungen müssen deshalb für geregelte Zertifikate eingehalten werden. Es werden die folgenden Vertrauensniveaus definiert:

- QCP-n (Policy for EU qualified certificate issued to a natural person): Zertifizierungspolitik zur Ausstellung von qualifizierten (bzw. geregelten) Zertifikaten auf natürliche Personen
- QCP-l (Policy for EU qualified certificate issued to a legal person): Zertifizierungspolitik zur Ausstellung von qualifizierten Zertifikaten auf juristische Personen (bzw. von geregelten Zertifikaten auf UID-Einheiten)
- QCP-n-qscd (Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a Qualified Signature Creation Device):

[1] Der ursprünglich vorgesehene (und in den ETSI-Normen referenzierte) dritte Teil „Policy requirements for Certification Authorities issuing public key certificates“ wurde in den ersten Teil integriert.

Zertifizierungspolitik gemäss QCP-n mit obligatorischer Verwendung einer “Sicheren Signaturerstellungseinheit”

- QCP-l-qscd (Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a Qualified Seal Creation Device): Zertifizierungspolitik gemäss QCP-n mit obligatorischer Verwendung einer “Sicheren Siegelerstellungseinheit”
- QCP-w (Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person): Zertifizierungspolitik zur Ausstellung von qualifizierten (bzw. geregelten) Website-Zertifikaten

ETSI EN 319 411-2 „Part 2: Requirements for trust service providers issuing EU qualified certificates“ ist als technische Norm für die Ausgabe qualifizierter Zertifikate gemäss der EU-Verordnung “über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG” (eIDAS) ausgelegt, sie lässt sich sinngemäss aber auch auf geregelte Zertifikate gemäss ZertES anwenden. Sie wird deshalb durch TAV-ZertES referenziert, d.h. sie muss auch für geregelte Zertifikate gemäss ZertES eingehalten werden.

Basierend auf ZertES und ETSI EN 319 411 „Policy and Security Requirements for Trust Service Providers issuing certificates” werden die unten aufgelisteten Zertifikatsklassen definiert. Dazu werden einige Präzisierungen zu ETSI EN 319 411 angebracht, um die schweizerische Rechtslage abzubilden. Auch werden zusätzlich zu den beiden Regelwerken wenige Anforderungen gestellt, um den Bedürfnissen des schweizerischen eGovernment gerecht zu werden.

Zusammengefasst werden die Zertifikatsklassen bzw. Vertrauensniveaus des vorliegenden Standards anhand der folgenden Kriterien festgelegt:

- Wird der zum Zertifikat zugehörige private Schlüssel in einem sicheren kryptografischen Gerät („Secure Cryptographic Device“) vorgehalten, welches gemäss einem internationalen Standard zertifiziert ist?
- Gemäss welcher Zertifizierungspolitik wurde das Zertifikat ausgestellt?
- Handelt es sich um ein geregeltes Zertifikat gemäss ZertES?
- Falls nein, wurde das Zertifikat gemäss einer in ETSI EN 319 411-1 beschriebenen Zertifizierungspolitik ausgestellt?

Der vorliegende Standard definiert somit die folgenden Zertifikatsklassen:

- Klasse 1 als schwächste Klasse basiert auf der „Lightweight Certificate Policy (LCP)“ gemäss ETSI EN 319 411-1
- Klasse 2 basiert auf der „Normalized Certificate Policy (NCP)“ gemäss ETSI EN 319 411-1
- Klasse 2+ basiert auf der „Extended Normalized Certificate Policy (NCP+)“ gemäss ETSI EN 319 411-1, also auf NCP mit Hardware-Token
- Klasse 3 basiert auf den Vorgaben für geregelte Zertifikate gemäss ZertES
- Klasse 3+ basiert auf
    - den Vorgaben für geregelte Zertifikate gemäss ZertES sowie

- der „Extended Normalized Certificate Policy (NCP+)“ gemäss ETSI EN 319 411-1

Die Klasse 3+ enthält auch die Zertifikate für geregelte und qualifizierte Signaturen sowie für geregelte Siegel, sie ist aber nicht auf diese Anwendungsfälle beschränkt.

Die untenstehende Tabelle zeigt die entsprechenden Vertrauensniveaus auf und fasst die einzuhaltenden Kriterien[2] zusammen:

[2] Die Einteilung der Kriterien lehnt sich dabei an diejenige von eCH-0170 “Qualitätsmodell zur Authentifizierung von Subjekten“ an.

Klasse	Bezeichnung	Token	Registrierung	Steuerung	Grundlagen
3+	Geregelt+ (geregelt und NCP+)	Zertifizierte Hardware	Gemäss ZertES: Staatlich anerkannte Beweismittel, Dokumentation der Anwesenheit gem. TAV-ZertES 2.3.1 a)	Gemäss ZertES: Haftung d. Anbieterin gem. ZertES Art. 17 (Halter gem. OR 59a für Signatur und Siegel) Aufsicht/Audit durch Anerkennungsstelle Prozessmaturität gem. Vorgaben TAV-ZertES	ZertES ETSI EN 319 411-2 ISO/IEC 15408 EAL 4+, ISO/IEC 19790, FIPS PUB 140-2 level 3
3	Geregelt (erfüllt NCP und weitere Anforderungen)	Softtoken möglich	Gemäss ZertES (s.o.)	Gemäss ZertES (s.o.)	ZertES ETSI EN 319 411-2
2+	NCP+	Zertifizierte Hardware	Staatlich anerkannte Beweismittel, Dokumentation der Anwesenheit (bzw. d. äquivalenten Registrierung)	Haftungsumfang definiert Audit durch Konformitätsbewertungsstelle gem. ETSI EN 319 403	ETSI EN 319 411-1: NCP+ ISO/IEC 15408 EAL 4+, ISO/IEC 19790, FIPS PUB 140-2 level 3
2	NCP	Softtoken möglich	Wie NCP+, s.o.	Wie NCP+, s.o.	ETSI EN 319 411-1: NCP
1	LCP	Softtoken möglich	Verifizierte eMail-Adresse	Wie NCP+, s.o.	ETSI EN 319 411-1: LCP

Tabelle 1: Überblick

1.4 Abgrenzung

Der vorliegende Standard definiert ausschliesslich „Zertifikatsklassen“, also Vertrauensniveaus für X.509-Public-Key-Zertifikate im eGovernment. X.509-Attribut-Zertifikate werden aufgrund ihrer geringen Verbreitung nicht betrachtet; auch entsprechen diese nicht der Definition eines Zertifikats gemäss ZertES.
Die Einteilung von Daten hinsichtlich Schutzbedarf ist nicht Thema des vorliegenden Standards.
Vertrauensniveaus für Authentisierungsmittel sind in „eCH-0170: Qualitätsmodell zur Authentifizierung von Subjekten“ spezifiziert, wobei es möglich ist, als Authentisierungs-Credentials Client-Zertifikate gemäss eCH-0048 einzusetzen.

1.5 Nutzer des Standards

Der Standard richtet sich an Verantwortliche für eGovernment-Applikationen, deren Kommunikation bzw. deren Schnittstellen mit digitalen Zertifikaten abgesichert werden. Der Fokus liegt dabei auf Government-To-Government (G2G), also auf der Interaktion zwischen Verwaltungsstellen und mit verwaltungsnahen Betrieben sowie zwischen den föderalen Ebenen Bund, Kantone und Gemeinden. Auch eine Anwendung in der Kommunikation mit privatwirtschaftlichen Unternehmen und mit Bürgern ist möglich, sofern dabei digitale Zertifikate eingesetzt werden.

Des Weiteren richtet sich der Standard an Anbieterinnen von Zertifizierungsdiensten und dient zur Information, welche Zertifikatsklassen im eGovernment eingesetzt werden sollen.

1.6 Verwendung von Schlüsselwörtern

Zur präziseren Qualifizierung der aufgeführten Anforderungen werden die folgenden Modalverben als Schlüsselwörter (in Grossbuchstaben) gemäss RFC 2119 verwendet:

- **MUSS** bedeutet, dass es sich um die normative Festlegung einer Eigenschaft handelt (MUST, REQUIRED, SHALL).
- **DARF NICHT** bezeichnet den normativen Ausschluss einer Eigenschaft. (MUST NOT, SHALL NOT)
- **SOLL** beschreibt eine dringende Empfehlung. Abweichungen hiervon sind in begründeten Fällen möglich, müssen jedoch hinsichtlich Funktionalität und Interoperabilität analysiert, bewertet und dokumentiert werden. (SHOULD, RECOMMENDED)
- **SOLL NICHT** bezeichnet die dringende Empfehlung zum Ausschluss einer Eigenschaft. Abweichungen hiervon sind in begründeten Fällen möglich, müssen jedoch hinsichtlich Funktionalität und Interoperabilität analysiert, bewertet und dokumentiert werden. (SHOULD NOT, NOT RECOMMENDED)
- **KANN** bedeutet, dass die Eigenschaften optional sind. Hierbei handelt es sich also nicht um normative Festlegungen, sondern eher um unverbindliche Anregungen hinsichtlich bestimmter Eigenschaften, an die somit auch keine Anforderungen zur

Interoperabilität mit Eigenschaften der vorgenannten Kategorien gestellt werden. (MAY, OPTIONAL)

1.7 Erweiterte Übersicht der Zertifikatsklassen

		Klasse 1	Klasse 2	Klasse 2+	Klasse 3	Klasse 3+
	Vertrau-ensniveau	Niedrig: Lightweight Certificate Policy (LCP)	Mittel: Normalized Certificate Policy (NCP)	Hoch: Extended Normalized Certificate Policy (NCP+)	Hoch: Geregelt gemäss ZertES	Sehr hoch: Geregelt+ bzw. Geregelt gemäss ZertES & Extended Normalized Certificate Policy (NCP+) oder Vorgaben für Signatur-/Siegel-Zertifikate gemäss ZertES
	Bezug	MUSS: ETSI EN 319 411-1: LCP	MUSS: ETSI EN 319 411-1: NCP	MUSS: ETSI EN 319 411-1: NCP+ (Hardware-Token)	MUSS: Geregeltes Zertifikat gemäss ZertES (inkl. ETSI EN 319 411-2: QCP-n, QCP-l, QCP-w)	MUSS: - Geregeltes Zertifikat gemäss ZertES (inkl. ETSI EN 319 411-2: QCP-n, QCP-l, QCP-w) - Zusätzlich: ETSI EN 319 411-1: NCP+ (Hardware-Token) oder - Geregeltes/qualifiziertes Zertifikat gemäss ZertES für Signatur/Siegel - ETSI EN 319 411-2: QCP-n-qscd (natürliche Personen) bzw. ETSI EN 319 411-2: QCP-l-qscd (UID-Einheiten)

		Klasse 1	Klasse 2	Klasse 2+	Klasse 3	Klasse 3+
Token	*Krypto-graphi-sches Token*	Gemäss ETSI EN 319 411-1: Softtoken möglich SOLL: Dokumentierter Installationsprozess	Gemäss ETSI EN 319 411-1: Softtoken möglich SOLL: Dokumentierter Installationsprozess	Gemäss ETSI EN 319 411-1: Hardtoken MUSS: Zertifizierte Hardware gemäss - ISO/IEC 15408 EAL 4+, - ISO/IEC 19790 oder FIPS PUB 140-2 level 3	Keine Vorgaben durch ZertES: Softtoken somit möglich SOLL: Dokumentierter Installationsprozess	MUSS: Zertifizierte Hardware gemäss - ISO/IEC 15408 EAL 4+, - ISO/IEC 19790 oder FIPS PUB 140-2 level 3 - Signatur/Siegel (zusätzlich, gemäss ZertES): Sichere Signatur- oder Siegelerstellungseinheit gemäss TAV-ZertES, Kap. 2.2.3
	Zertifikats zweck / Key Usage	SOLL: Separate Zertifikate für Signatur, Authentisierung und Verschlüsselung KANN: Kombination von Authentisierung und Verschlüsselung bei Zertifikaten für TLS, IPsec etc. MUSS: ETSI EN 319 412-2, Kap. 4.3.2			Gemäss ZertES: TAV-ZertES, Kap. 2.3.2/2.3.3 SOLL: Separate Zertifikate für Signatur, Authentisierung und Verschlüsselung KANN: Kombination von Authentisierung und Verschlüsselung bei Zertifikaten für TLS, IPsec etc. MUSS: ETSI EN 319 412-2, Kap. 4.3.2	
	Schlüssel-hinterle-gung (key escrow)	Gemäss ETSI EN 319 411-1, Kap. 6.3.12: - Signatur-/Siegelschlüssel dürfen nicht hinterlegt werden. - (Instanz-)Authentisierungsschlüssel sollen nicht hinterlegt werden. - Entschlüsselungsschlüssel können hinterlegt werden. MUSS: Information des Kunden über die Schlüsselhinterlegungs-Praxis				
Registrierung	Registrierungsstärke	Gemäss ETSI EN 319 411-1, Kap. 6.2.2: Überprüfen der Registrierungsdaten	Gemäss ETSI EN 319 411-1, Kap. 6.2.2: Persönliche Antragstellung oder gleichwertig; Überprüfen der Registrierungsdaten		Gemäss ZertES: Persönliche Antragstellung bei anerkannten Registrierungsstellen oder gleichwertig	
	Erlaubte Zertifikats Inhaber (Subject)	Gemäss ETSI EN 319 411-1: - Natürliche Person (ggf. als Vertreter einer Organisation) - Organisation bzw. Organisationseinheit - Gerät oder System			Gemäss ZertES: - Natürliche Person gemäss Identitätsnachweis. Das Zertifikat kann auch auf ein Pseudonym ausgestellt werden. Format gemäss ETSI EN 319 412-2 - UID-Einheit: Registrierter Name gemäss UID-Register. Format gemäss ETSI EN 319 412-3	

		Klasse 1	Klasse 2	Klasse 2+	Klasse 3	Klasse 3+
g	Identitätsnachweis	Mindestens eine verifizierte eMail-Adresse als MUSS	Gemäss ETSI EN 319 411-1, Kap. 6.2.2: - Natürliche Person: Basierend auf national anerkanntem Ausweisdokument. - Organisation, Organisationseinheit etc.: Vertretungsbefugnis Zusätzlich: Verifizierte eMail-Adresse als MUSS		Gemäss ZertES: - Natürliche Person: Hoheitliches Dokument (Reisepass, Identitätskarte) - UID-Einheit: Schriftliche Vertretungsbefugnis, Handelsregisterauszug (sofern im HR eingetragen) Zusätzlich: Verifizierte eMail-Adresse als MUSS	
	Identifikator	Eindeutiger Subject Distinguished Name (gemäss RFC 5280), ggf. spezifische oder technische Identifikatoren			- Natürliche Person: Pro Anbieter und Person eindeutiger Subject Distinguished Name (gemäss RFC 5280); die Verwendung spezifischer eindeutiger Identifikatoren ist möglich. - UID-Einheit: UID in „organizationIdentifier“ des Subject Distinguished Name (gemäss ZertES);	
	Archivierung Antragsdokumente und -daten	SOLL: Laufzeit plus 2 Jahre	SOLL: Laufzeit plus 5 Jahre (Verjährungsfrist gem. OR)		Gemäss ZertES: Laufzeit plus 11 Jahre	
	Laufzeit der Registrierung	Keine Vorgabe	Keine Vorgabe		Keine Vorgabe	
Steuerung	Anforderungen an CA (Betrieb, Personal, Prozesse)	Gemäss ETSI EN 319 411-1, analog ZertES	Gemäss ETSI EN 319 411-1, analog ZertES		Gemäss TAV-ZertES, Kap. 2.1„Organisation und operative Grundsätze“ bzw. gemäss ETSI EN 319 411-2 Kap. 5 General provisions on Certificate Practice Statement and Certificate Policies und 7 Framework for the definition of other certificate policies; 6.4 Facility, Management, and Operational Controls, 6.5.5 Computer Security Controls, 6.5.6 Life Cycle Security Controls und 6.5.7 Network Security Controls; 6.8 Other Business and Legal Matters; 6.9 Other Provisions	

	Klasse 1	Klasse 2	Klasse 2+	Klasse 3	Klasse 3+
Haftung	Gemäss ETSI EN 319 411-1: Haftungsumfang / Haftungsbeschränkungen definiert			Anbieter: Gemäss ZertES Art. 17 und VZertES Art. 2: Versicherung von mind. 2 Mio CHF pro Versicherungsfall und 8 Mio CHF jährlich (od. gleichwertig)	- Anbieter: Gemäss ZertES Art. 17 und VZertES Art. 2: Versicherung von mind. 2 Mio CHF pro Versicherungsfall und 8 Mio CHF jährlich (od. gleichwertig) - Halter bei Signatur oder Siegel: Gemäss OR 59a
Einsatz	Keine qualifizierten Signaturen, keine geregelten Signaturen und keine geregelten Siegel gemäss ZertES; ansonsten alle Anwendungen möglich			Keine Signaturen bzw. Siegel; ansonsten alle Anwendungen möglich	Alle Anwendungen möglich, aber besondere Anforderungen für qualifizierte Signatur, geregelte Signatur und geregelte Siegel gemäss ZertES
Widerrufs-Informationen	Gemäss ETSI EN 319 411-1: Per OCSP (zwingend) und CRL Mindestens bis Ende der Gültigkeitsdauer			Gemäss ZertES bzw. ETSI EN 319 411-2: Per OCSP (zwingend) und CRL Über das Ende der Gültigkeitsdauer hinaus	
Policy-Referenzen	SOLL: {lcp} KANN: {eCH0048V2Policies class1}	SOLL: {ncp} KANN: {eCH0048V2Policies class2}	SOLL: {ncpplus} KANN: {eCH0048V2Policies class2plus}	Gemäss ZertES: TAV-ZertES, Kap. 2.3.2 *„regulated certificate“* KANN: {QCP-web} für Website-Zertifikate KANN: {eCH0048V2Policies class3}	Gemäss ZertES: TAV-ZertES, Kap. 2.3.2/2.3.3 *„regulated certificate“/”qualified certificate”* Erweiterung qcStatements gemäss TAV-ZertES 2.3.2 g) für Signatur- / Siegel-Zertifikate KANN: {QCP-natural-qscd} / {QCP-legal-qscd} für Signatur- / Siegel-Zertifikate KANN: {ncpplus} (zeigt Verwendung eines Hardware-Tokens an) KANN: {eCH0048V2Policies class3plus}

Tabelle 2: Detaillierte Darstellung

Erläuterungen zur Tabelle 2:

- Die Angabe der Modalverben MUSS/DARF NICHT/SOLL/SOLL NICHT/KANN beziehen sich auf die eCH-0048-spezifische Anforderungen und werden gemäss Kapitel 1.6 «Verwendung von Schlüsselwörtern» bzw. gemäss RFC 2119 verwendet.
- Die Referenzierung eines ETSI-Standards oder von ZertES bzw. eines entsprechenden Kapitels (z.B. «Gemäss ETSI EN 319 411-1, Kap. 6.2.2») bedeutet, dass die Anforderungen des entsprechenden Regelwerks (bzw. des erwähnten Kapitels) gelten und eingehalten werden müssen.
- Sämtliche Vorgaben werden im folgenden Kapitel 2 «Anforderungsprofile» ausführlicher erläutert.

2 Anforderungsprofile

2.1 Einleitung

Mit der Einstufung in eine ‚Zertifikatsklasse' wird das Ausmass an Verbindlichkeit definiert, mit dem ein Dritter sich auf die im Zertifikat enthaltenen Daten und auf die damit abgesicherte Kommunikation verlassen kann.

Die Abstufung in fünf (bzw. drei plus zwei) derartige Klassen korrespondiert einerseits mit Geschäfts- und Verwaltungsprozessen unterschiedlichen Schutzbedarfes und folgt andererseits den am Markt etablierten Schemata.

2.2 Übergreifende Anforderungen

Die folgenden Anforderungen gelten übergreifend für mehrere Zertifikatsklassen, für die spezifisch angegebenen oder – sofern keine vermerkt sind – für alle Klassen.

2.2.1 Erfüllung aller Anforderungen

Es MÜSSEN jeweils restlos alle Anforderungen an eine Zertifikatsklasse erfüllt werden. Eine Übererfüllung ist dabei statthaft.

2.2.2 Zertifikatsinhaber „Subject" (informativ)

Ein geregeltes Zertifikat muss gemäss ZertES Art. 7 auf „natürliche Personen und UID-Einheiten ausgestellt werden". UID steht für Unternehmens-Identifikationsnummer, siehe auch Kap. 4.4 „Erläuterungen zum UID-System". Ein geregeltes Zertifikat muss deshalb immer die folgenden Angaben enthalten (nicht abschliessend):

- Natürliche Person: Vor- und Nachnamen oder ein Pseudonym
- UID-Einheit: UID-Nummer und registrierter Name der UID-Einheit

Auch die Angabe des Landes und des Allgemeinnamens („Common Name") sind zwingend erforderlich, die Angabe weiterer Attribute (z.B. Organisationseinheit) ist zulässig.

(Für Website-Zertifikate gelten besondere Vorgaben gemäss ETSI EN 319 412-4 „Certificate

Profiles; Part 4: Certificate profile for web site certificates“.)

Für nicht-geregelte Zertifikate gilt ETSI EN 319 411-1 „Part 1: General requirements“ Kap. 5.4.2. Dort werden die folgenden Varianten hinsichtlich Zertifikatsinhaber aufgelistet:

“In the framework of the present policies, the subject can be:
a) a natural person;
b) a natural person identified in association with a legal person;
c) a legal person (that can be an Organization or a unit or a department identified in association with an Organization); or
d) a device or system operated by or on behalf of a natural or legal person.”

Erläuterung zu a): Auch hier kann die natürliche Person im Zertifikat durch ein Pseudonym bezeichnet werden. Die Verwendung von Pseudonymen in eGovernment-Prozessen ist für den Grossteil der möglichen Anwendungsfälle nicht sinnvoll, solche Fälle sind aber theoretisch denkbar (z.B. „Bürgerbeteiligungsforum“).

Erläuterung zu b): Wenn eine natürliche Person mit einer Organisation assoziiert ist (z.B. Mitarbeiter), wird diese auch im „Subject“ des Zertifikats aufgeführt.

Erläuterung zu c): Die Definition der „legal person“ ist sehr breit gefasst und kann auch auf Organisationen oder Organisationseinheiten angewendet werden, welche keine juristischen Personen im engeren Sinne sind.

Erläuterung zu d): Bei den genannten Geräten oder Systemen („device or system“) kann es sich z.B. um einen Webserver, Router oder einen technischen Account handeln. Diese befinden sich immer im Besitz einer natürlichen Person oder einer Organisation. Die Aufführung des Besitzers im Subject ist aber nicht zwingend notwendig.

2.2.3 Identitätsnachweis

Als Mindestanforderung MUSS die Anbieterin vom Antragsteller die Angabe einer eMail-Adresse verlangen, unter der dieser erreichbar ist. Die Anbieterin MUSS diese eMail-Adresse verifizieren.

Dadurch wird sichergestellt, dass der Zertifikatsantrag auf die antragstellende Person zurückführbar ist, und dass diese kontaktierbar ist. Die Angabe einer persönlichen eMail-Adresse ist dabei aber nicht obligatorisch, es kann z.B. die Adresse eines Funktionspostfachs angegeben werden.

2.2.4 Algorithmen und Schlüssellängen (informativ)

Ein Public-Key-Zertifikat bindet einen Inhaber an einen öffentlichen Schlüssel. Dabei muss eine Anbieterin die Qualität und Sicherheit der verwendeten Algorithmen und Schlüssellängen gewährleisten, die Entwicklung diesbezüglich fortlaufend beobachten und wenn nötig entsprechend reagieren (s. auch ZertES Art. 6 und VZertES Art. 3). Eine wichtige Referenz diesbezüglich ist die ETSI-Norm ETSI TS 119 312 „Cryptographic Suites“. ETSI TS 119 312 bezieht sich auf den Anwendungsfall Signatur/Siegel, für andere Zertifikats-basierte Anwendungen gelten entsprechende Anforderungen[3].

Hervorzuheben sind die beiden folgenden Public-Key-Verfahren:

[3] Weiteres Beispiel einer Referenz: BSI TR-02102-1 „BSI Technische Richtlinie; Kryptographische Verfahren: Empfehlungen und Schlüssellängen“

- Rivest, Shamir and Adleman (RSA) und
- Elliptic Curve Cryptography (ECC)

Während der RSA-Algorithmus in der Vergangenheit der de-facto-Standard für Public-Key-Kryptografie war, sind heute auch vermehrt ECC-basierte Verfahren im Einsatz. ECC bietet gewisse Vorteile, so kann z.B. bei deutlich geringerer Schlüssellänge dieselbe Verschlüsselungsstärke erzielt werden.

Ein ECC-basierter Schlüssel besteht neben dem eigentlichen kryptografischen Wert auch aus der elliptischen Kurve, auf der dieser Wert basiert. Bei der Auswahl der entsprechenden Kurve muss neben Sicherheitsabwägungen auch die Unterstützung durch die verwendeten Systeme in Betracht gezogen werden.

Zu beachten ist auch, dass Schlüssellängen zeitabhängig gewählt werden müssen, d.h. für Zertifikate mit langer Laufzeit gelten höhere Anforderungen diesbezüglich.

2.2.5 Softtoken

Dieser Abschnitt gilt für die Klassen 1, 2 und 3.

ETSI EN 319 411-1 „Part 1: General requirements“ gibt bezüglich der Pflichten des „Subscriber“ (Entität, welche das Zertifikat bezieht) bzw. des „Subject“ (Zertifikatshalter) vor, dass unbefugter Zugriff auf den privaten Schlüssel verhindert werden muss („unauthorized use of the subject's private key is avoided“). Diese Vorgabe wird wie folgt präzisiert:

Die Geheimhaltung des zu einem Zertifikat gehörenden privaten Schlüssels ist über dessen ganzen Lebenszyklus hinweg sicherzustellen. Insbesondere SOLL der für die Installation bzw. Erzeugung des Schlüssels Verantwortliche diese Installation gemäss einem dokumentierten Prozess vornehmen, um sicherzustellen, dass der private Schlüssel nur im dafür vorgesehenen (geschützten) Speicherbereich vorgehalten wird.
Die Hinterlegung von Entschlüsselungs-Schlüsseln bleibt dabei erlaubt. Siehe Kapitel 2.2.6.

2.2.6 Zertifikatszweck / Key Usage

Bei Zertifikaten können grundsätzlich die folgenden Anwendungszwecke unterschieden werden:

- Signatur (von Dokumenten),
- Authentisierung (eines Teilnehmers oder Geräts/Systems) und
- Ver- bzw. Entschlüsselung

Diese drei Anwendungen SOLLEN nicht vermischt werden, d.h. es SOLLEN für diese Zwecke separate Zertifikate ausgestellt werden. Eine Ausnahme stellen dabei Zertifikate für sichere Netzwerk-Protokolle (bzw. Protokoll-Suiten) wie z.B. Transport Layer Security (TLS) oder Internet Protocol Security (IPsec) dar: Die dabei verwendeten Zertifikate werden teilweise nicht nur für Authentisierung, sondern auch für Verschlüsselung verwendet. Somit KANN bei diesen neben Authentisierung der Zertifikatszweck Verschlüsselung eingestellt werden.

In Bezug auf die Zertifikatserweiterung „Key Usage“ MÜSSEN dabei die Anforderungen in ETSI EN 319 412-2 „Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons“, Kapitel 4.3.2 eingehalten werden. (Hinweis: Dies gilt für alle Zertifikate, nicht nur für solche, welche auf natürliche Personen ausgestellt werden.)

(Bei geregelten und qualifizierten Zertifikaten gelten diesbezüglich ausserdem die Vorschriften in den Kapiteln 2.3.2 und 2.3.3 der TAV-ZertES.)

2.2.7 Schlüsselhinterlegung

Bei geregelten Zertifikaten ist die Schlüsselhinterlegung (Kopieren und Aufbewahren im Doppel, englisch „key escrow“) von privaten Signatur- und Siegelschlüsseln verboten, für andere Anwendungen ist die Hinterlegung privater Schlüssel beim Anbieter erlaubt (s. VZertES, Art. 8).

Konform dazu ist die Anforderung bezüglich Schlüsselhinterlegung für nicht-geregelte Zertifikate in ETSI EN 319 411-1 „Part 1: General requirements“, Kap. 6.3.12 „Key escrow and recovery“ formuliert. Eine Schlüsselhinterlegung

- DARF NICHT bei Signaturschlüsseln,
- KANN bei Entschlüsselungsschlüsseln und
- SOLL NICHT bei Authentisierungschlüsseln

erfolgen.

Der Hauptmotivation für die obige Differenzierung ist, dass bei der Verwendung von Zertifikaten für die verschlüsselte Ablage das Vorhalten eines Doppels des Entschlüsselungsschlüssels die Verfügbarkeit der Daten sicherstellt. Sowohl Schlüsselhinterlegung als auch eine allfällige neue Herausgabe eines privaten Schlüssels müssen natürlich hohe Sicherheitsanforderungen erfüllen.

Im vorliegenden Dokument wird die folgende Zusatzanforderung gestellt:
Eine Anbieterin von Zertifizierungsdiensten MUSS den Kunden informieren, ob eine Schlüsselhinterlegung erfolgt.
Die Anbieterin MUSS den Kunden auf die Konsequenzen ihrer Schlüsselhinterlegungs-Praxis und eines möglichen „key escrow“ hinweisen.

2.2.8 Laufzeit der Registrierung

Es gibt keine spezifische Vorgabe für die Laufzeit der Registrierung der für die Zertifikatsausstellung verwendete Identität. D.h. die maximale Zeitspanne, innerhalb derer der Registrierungsprozess erneut durchlaufen werden muss, ist nicht vorgegeben.

2.3 Klasse 1 (LCP)

2.3.1 Einleitung

Ein Zertifikat der Klasse 1 MUSS die Anforderungen der Zertifizierungspolitik „Lightweight Certificate Policy” (LCP) gemäss ETSI EN 319 411-1 „Part 1: General requirements“ erfüllen.

Es gelten dabei die unten folgenden Präzisierungen und Erläuterungen.

2.3.2 Archivierung der Antragsdokumente und/oder -daten

Die Anbieterin SOLL die Antragsdokumente und/oder –daten mindestens für die Laufzeit eines Zertifikats plus zwei Jahre aufbewahren.

2.3.3 Referenzierte Certificate Policy

ETSI EN 319 411-1 „Part 1: General requirements“ legt den Object Identifier (OID) *{lcp}* zur Verwendung in der Erweiterung „certificatePolicies“ fest, um die Konformität mit der Zertifizierungspolitik „Lightweight Certificate Policy” (LCP) anzuzeigen.

Im vorliegenden Dokument werden die folgenden Anforderungen diesbezüglich gestellt:

Eine Anbieterin SOLL den OID *{lcp}* gemäss ETSI EN 319 411-1 in der Erweiterung „certificatePolicies“ von Klasse-1-Zertifikaten einfügen.

Zusätzlich KANN eine Anbieterin den OID *{eCH0048V2Policies class1}* verwenden, um die Konformität mit der Klasse 1 gemäss eCH-0048 V2.0 anzuzeigen.

Das Einfügen weiterer OIDs in der Erweiterung „certificatePolicies“ ist möglich, z.B. zur Referenzierung der Zertifizierungspraxis (CPS) der Anbieterin.

2.3.4 Beschreibung (informativ)

Im Folgenden werden einige wichtige Anforderungen dargestellt, welche Zertifikate der Klasse 1, also Zertifikate gemäss „Lightweight Certificate Policy (LCP)“ erfüllen müssen.

2.3.4.1 Kryptografisches Token

Softtoken sind zulässig. Siehe auch Kap. 2.2.5.

2.3.4.2 Registrierung

2.3.4.2.1 Registrierungsstärke

Für LCP-konforme Zertifikate muss gemäss EN 319 411-1 „Part 1: General requirements“, Kap. 6.2.2 eine angemessenere Überprüfung der Identität (und Berechtigung) des Antragstellers erfolgen. („Verification of the subject's identity shall be at time of registration by appropriate means.“)

2.3.4.2.2 Identitätsnachweis

S. Kap. 2.2.3 bezüglich verifizierter eMail-Adresse.

2.3.4.2.3 Erlaubte Zertifikats-Inhaber (Subject)

S. Kap. 2.2.2.

2.3.4.2.4 Identifikator

S. Kap. 2.4.5.2.4.

2.3.4.2.5 Archivierung der Antragsdokumente und/oder -daten

Siehe Kap. 2.3.2.

2.3.4.3 Steuerung

2.3.4.3.1 Anforderungen an CA (Betrieb, Personal, Prozesse)

S. Kap. 2.4.5.3.1.

2.3.4.3.2 Haftung

S. Kap. 2.4.5.3.2.

2.3.4.3.3 Bereitstellung von Widerrufs-Informationen

S. Kap. 2.4.5.3.3.

2.4 Klasse 2 (NCP)

2.4.1 Einleitung

Ein Zertifikat der Klasse 2 MUSS die Anforderungen der Zertifizierungspolitik „Normalized Certificate Policy“ (NCP) gemäss ETSI EN 319 411-1 „Part 1: General requirements“ erfüllen.

Es gelten dabei die unten folgenden Präzisierungen und Erläuterungen.

2.4.2 Registrierung

Bei natürlichen Personen, welche Schweizer Staatsangehörige sind, KANN anstelle des Geburtsorts der (im Ausweisdokument vermerkte) Bürgerort als Registrierungs-Attribut verwendet werden.

2.4.3 Archivierung der Antragsdokumente und/oder -daten

Die Anbieterin SOLL die Antragsdokumente und/oder –daten mindestens für die Laufzeit eines Zertifikats plus fünf Jahre aufbewahren. Somit ist auch die Aufbewahrungsfrist gemäss Obligationenrecht (OR) gewährleistet.

2.4.4 Referenzierte Certificate Policy

ETSI EN 319 411-1 „Part 1: General requirements“ legt den Object Identifier (OID) *{ncp}* zur Verwendung in der Erweiterung „certificatePolicies“ fest, um die Konformität mit der Zertifizierungspolitik „Normalized Certificate Policy” (NCP) anzuzeigen.

Im vorliegenden Dokument werden die folgenden Anforderungen diesbezüglich gestellt:

Eine Anbieterin SOLL den OID *{ncp}* gemäss ETSI EN 319 411-1 in der Erweiterung „certificatePolicies“ von Klasse-2-Zertifikaten einfügen.

Zusätzlich KANN eine Anbieterin den OID *{eCH0048V2Policies class2}* verwenden, um die Konformität mit der Klasse 2 gemäss eCH-0048 V2.0 anzuzeigen.

Das Einfügen weiterer OIDs in der Erweiterung „certificatePolicies“ ist zulässig, z.B. zur Referenzierung der Zertifizierungspraxis (CPS) der Anbieterin.

2.4.5 Beschreibung (informativ)

Im Folgenden werden einige wichtige Anforderungen dargestellt, welche Zertifikate der Klasse 2, also Zertifikate gemäss „Normalized Certificate Policy“ (NCP) erfüllen müssen.

2.4.5.1 Kryptografisches Token

Softtoken sind zulässig. Siehe auch Kap. 2.2.5.

2.4.5.2 Registrierung

Siehe auch Kap. 2.4.2.

2.4.5.2.1 Registrierungsstärke

Gemäss ETSI EN 319 411-1 „Part 1: General requirements“, Kap. 6.2.2 muss entweder eine persönliche Antragstellung stattfinden oder ein Registrierungsprozess auf einem gleichwertigen Niveau erfolgen. Die Registrierungsdaten sind angemessen zu überprüfen.

2.4.5.2.2 Identitätsnachweis

Der Identitätsnachweis natürlicher Personen muss basierend auf einem national anerkannten Ausweisdokument erfolgen.

Für Organisationen und Organisationseinheiten ist die Vertretungsbefugnis des Antragstellers gemäss nationalen Vorschriften oder anderen angemessenen Identifikationsprozesse nachzuweisen, also z.B. mittels Handelsregisterauszug.

Es gilt ausserdem Kap. 2.2.3 bezüglich verifizierter eMail-Adresse.

2.4.5.2.3 Erlaubte Zertifikatsinhaber (Subject)

S. Kap. 2.2.2.

2.4.5.2.4 Identifikator

Es gelten keine spezifischen Vorgaben. Gemäss RFC 5280, Kap. 4.1.2.6. Subject darf aber ein Subject-Name nur für dieselbe Person oder Entität wiederverwendet werden. Für Systeme und Geräte können technische Identifikatoren verwendet werden (z.B. „Fully Qualified Domain Name“). Auch ist die Verwendung spezifischer Identifikatoren möglich (z.B. im Attribut „serialNumber“), sofern diese Datenschutz-konform sind.

Siehe auch Kap. 2.2.2 Zertifikatsinhaber „Subject“ (informativ).

2.4.5.2.5 Archivierung der Antragsdokumente und/oder -daten

Siehe Kap. 2.4.3.

2.4.5.3 Steuerung

2.4.5.3.1 Anforderungen an CA (Betrieb, Personal, Prozesse)

Es sind detaillierte Vorgaben bezüglich Zertifizierungspolitik und Aussagen über

Zertifizierungspraxen, das Sicherheitsmanagement sowie die Praxis hinsichtlich finanzieller, rechtlicher und weiterer organisatorischer und operativer Aspekte zu erfüllen. Diese werden in den entsprechenden Kapiteln in ETSI EN 319 411-1 „Part 1: General requirements“ beschrieben und sind in etwa mit den Anforderungen gemäss ZertES (bzw. TAV-ZertES) vergleichbar.

Ein Compliance Audit muss mindestens alle zwei Jahre stattfinden (s. ETSI EN 319 403 „Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers“, Kap. 7.4.6)

2.4.5.3.2 Haftung

Die Anbieterin muss Haftungsumfang bzw. Haftungsbeschränkungen beschreiben (s. ETSI EN 319 401 “General Policy Requirements for Trust Service Providers”, Kap. 6.2)

2.4.5.3.3 Bereitstellung von Widerrufs-Informationen

Widerrufs-Informationen müssen rund um die Uhr öffentlich zur Verfügung gestellt werden. Die Integrität und Authentizität dieser Informationen müssen gewährleistet werden.

Das Online Certificate Status Protocol (OCSP) muss dabei unterstützt werden, ausserdem soll eine Zertifikatssperrliste (Certificate Revocation List – CRL) publiziert werden.

Für ein Zertifikat muss die Widerrufs-Information mindestens bis zu seinem ursprünglich vorgesehenen Gültigkeitsende bereitgestellt werden.

2.5 Klasse 2+ (NCP+)

Ein Zertifikat der Klasse 2+ MUSS die Anforderungen der Zertifizierungspolitik „Extended Normalized Certificate Policy“ (NCP+) gemäss ETSI EN 319 411-1 „Part 1: General requirements“ erfüllen.

Es gelten also

- alle Anforderungen der Zertifizierungspolitik „Normalized Certificate Policy“ (NCP) sowie
- zusätzlich die Anforderungen für das Vorhalten des privaten Schlüssels in Hardware („secure cryptographic device“).

Zulässig (MUSS) ist hierbei Hardware, welche gemäss

- ISO/IEC 15408 EAL 4+ (gegen ein geeignetes Schutzprofil bzw. „Protection Profile“) oder
- ISO/IEC 19790 oder FIPS PUB 140-2 level 3

zertifiziert wurde (vgl. auch ETSI EN 319 411-1 „Part 1: General requirements“ Kap. 6.5.2).

(Hardware, welche den Anforderungen gemäss TAV-ZertES, Kap. 2.2.3 entspricht, ist dabei eingeschlossen.)

2.5.1 Referenzierte Certificate Policy

ETSI EN 319 411-1 „Part 1: General requirements“ legt den Object Identifier (OID) *{ncpplus}*

zur Verwendung in der Erweiterung „certificatePolicies“ fest, um die Konformität mit der Zertifizierungspolitik „Extended Normalized Certificate Policy” (NCP+) anzuzeigen.

Im vorliegenden Dokument werden die folgenden Anforderungen diesbezüglich gestellt:

Eine Anbieterin SOLL den OID *{ncpplus}* gemäss ETSI EN 319 411-1 in der Erweiterung „certificatePolicies“ von Zertifikaten der Klasse 2+ einfügen.

Zusätzlich KANN eine Anbieterin den OID *{eCH0048V2Policies class2plus}* verwenden, um die Konformität mit der Klasse 2+ gemäss eCH-0048 V2.0 anzuzeigen.

Das Einfügen weiterer OIDs in der Erweiterung „certificatePolicies“ ist möglich, z.B. zur Referenzierung der Zertifizierungspraxis (CPS) der Anbieterin.

2.6 Klasse 3 (geregelt)

2.6.1 Einleitung

Zur Klasse 3 gehören die gemäss ZertES, VZertES und TAV-ZertES geregelten Softtoken-basierten Zertifikate. Es MUSS sich also um geregelte Zertifikate gemäss ZertES handeln. Gemäss TAV-ZertES müssen dabei auch die Vorgaben in ETSI EN 319 411-2 „Part 2: Requirements for trust service providers issuing EU qualified certificates“, Kap. 5 bis Kap. 6.5.7 sowie Kap. 6.8 bis und mit Kap. 7 eingehalten werden.

Zu beachten sind die unten folgenden Punkte sowie die Erläuterungen zu ZertES in Kap. 4.1 „Erläuterungen zu ZertES“.

2.6.2 Referenzierte Certificate Policy (analog QCP-n und QCP-l oder QCP-w)

Für natürliche Personen gelten die in TAV-ZertES in ETSI EN 319 411-2 „Part 2: Requirements for trust service providers issuing EU qualified certificates“ referenzierten Vorgaben gemäss der Zertifizierungspolitik QCP-n (Policy for EU qualified certificate issued to a natural person) und für UID-Einheiten diejenige für QCP-l (Policy for EU qualified certificate issued to a legal person). Für die Ausgabe geregelter Website-Zertifikate ist ausserdem die Zertifizierungspolitik QCP-w (Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person) einzuhalten.

Zu beachten ist aber der folgende Umstand:

Im Kap. 5.5 “Certificate Usage” der ETSI EN 319 411-2 „Part 2: Requirements for trust service providers issuing EU qualified certificates“ werden die Anwendungsbereiche der gemäss jeweiliger Zertifizierungspolitik ausgestellten Zertifikate beschrieben. In den Kapiteln 5.5.1 (für QCP-n) und 5.5.2 (für QCP-l) wird der Anwendungsbereich auf die fortgeschrittene elektronische Signatur (bzw. Siegel) eingeschränkt („are aimed to support the advanced electronic signatures/seals […]“).

Diese Einschränkung gilt aber für geregelte Zertifikate gemäss ZertES NICHT. Es sind beliebige Zertifikatszwecke möglich. (Für Zertifikate für qualifizierte Signatur, geregelte Signatur und geregeltes Siegel gelten gemäss ZertES, VZertES und TAV-ZertES besondere Vorschriften, siehe auch Kap. 2.7.2 „Signatur und Siegel“). Die QCP-n und QCP-l zugeordneten Object Identifier (OID) *{QCP-natural}* und *{QCP-legal}* eignen sich somit nur bedingt, um Konformität mit ZertES anzuzeigen.

In geregelten Zertifikaten muss aber gemäss TAV-ZertES sowieso zwingend der Text

‚*regulated certificate*' im Feld „explicitText" der Erweiterung „certificatePolicies" eingefügt werden. Sie sind also eindeutig als geregelte Zertifikate markiert und erkennbar.

In ETSI EN 319 411-2 „Part 2: Requirements for trust service providers issuing EU qualified certificates" wird ausserdem der folgende standardisierte Object Identifier (OID) zur Verwendung in der Erweiterung „certificatePolicies" für Website-Zertifikate spezifiziert:

- *{QCP-web}*: Dieser OID zeigt an, dass die Zertifizierungspolitik zur Ausgabe von (geregelten) Website-Zertifikaten eingehalten wird.

Eine Anbieterin KANN den OID *{QCP-web}* gemäss ETSI EN 319 411-2 in der Erweiterung „certificatePolicies" von Klasse-3-Website-Zertifikaten einfügen.

Eine Anbieterin KANN den OID *{eCH0048V2Policies class3}* verwenden, um die Konformität eines geregelten Zertifikats mit der Klasse 3 gemäss eCH-0048 V2.0 anzuzeigen.

Das Einfügen weiterer OIDs in der Erweiterung „certificatePolicies" ist möglich, z.B. zur Referenzierung der Zertifizierungspraxis (CPS) der Anbieterin.

2.6.3 Beschreibung (informativ)

Im Folgenden werden einige wichtige Anforderungen dargestellt, welche Zertifikate der Klasse 3, also geregelte Zertifikate gemäss ZertES, VZertES und TAV-ZertES erfüllen müssen.

2.6.3.1 Kryptografisches Token

Softtoken sind zulässig. Siehe auch Kap. 2.2.5.

2.6.3.2 Registrierung

2.6.3.2.1 Registrierungsstärke

Generell ist eine persönliche Antragstellung gefordert, unter gewissen Umständen kann aber ein Registrierungsverfahren auf Distanz angewendet werden, wenn dieses zur Personenidentifikation eine gleichwertige Sicherheit zum persönlichen Erscheinen bietet.

2.6.3.2.2 Identitätsnachweis

Gemäss VZertES, Art. 5:

Natürliche Personen müssen sich mit Pass oder Identitätskarte ausweisen.

Gemäss VZertES, Art. 6:

Nachweis der Vertretungsbefugnis für eine UID-Einheit gemäss Handelsregister oder Begründung durch schriftliche Vollmacht.

Es gilt ausserdem Kap. 2.2.3 bezüglich verifizierter eMail-Adresse.

2.6.3.2.3 Erlaubte Zertifikatsinhaber (Subject)

S. Kap. 2.2.2.

2.6.3.2.4 Identifikator

Für UID-Einheiten ist zwingend die Unternehmens-Identifikationsnummer (UID) im Attribut „organizationIdentifier“ des Subject anzugeben.

Für natürliche Personen gelten keine spezifischen Vorgaben, gemäss RFC 5280, Kap. 4.1.2.6. Subject darf aber ein Subject-Name nur für dieselbe Person wiederverwendet werden. Auch ist die Verwendung spezifischer Identifikatoren möglich (z.B. im Attribut „serialNumber“), sofern diese Datenschutz-konform sind.

Siehe auch Kap. 2.2.2 Zertifikatsinhaber „Subject“ (informativ).

2.6.3.2.5 Archivierung der Antragsdokumente und/oder -daten

Es besteht eine Aufbewahrungsfrist von elf Jahren nach Ablauf der Zertifikate.

2.6.3.3 Steuerung

2.6.3.3.1 Anforderungen an CA (Betrieb, Personal, Prozesse)

Es sind detaillierte Vorgaben bezüglich Zertifizierungspolitik und Aussagen über Zertifizierungspraxen, das Sicherheitsmanagement sowie die Praxis hinsichtlich finanzieller, rechtlicher und weiterer organisatorischer und operativer Aspekte zu erfüllen. Diese werden in TAV-ZertES, Kap. 2.1 bzw. in den referenzierten Kapiteln in ETSI EN 319 411-2 „Part 2: Requirements for trust service providers issuing EU qualified certificates“ aufgeführt:

- 5 General provisions on Certificate Practice Statement and Certificate Policies und 7 Framework for the definition of other certificate policies;
- 6.4 Facility, Management, and Operational Controls, 6.5.5 Computer Security Controls, 6.5.6 Life Cycle Security Controls und 6.5.7 Network Security Controls;
- 6.8 Other Business and Legal Matters und
- 6.9 Other Provisions.

Es findet ein jährliches Compliance Audit durch die Anerkennungsstelle statt.

2.6.3.3.2 Haftung

Die Anbieterin haftet für Schäden, wenn sie ihre Pflichten gemäss ZertES nicht erfüllt hat (ZertES Art. 17). Gemäss VZertES Art. 2 gilt eine Versicherungs- bzw. Garantiesumme von mindesten 2 Millionen Franken pro Versicherungsfall und 8 Millionen Franken pro Versicherungsjahr.

2.6.3.3.3 Bereitstellung von Widerrufs-Informationen

Widerrufs-Informationen müssen rund um die Uhr öffentlich und kostenlos zur Verfügung gestellt werden. Die Integrität und Authentizität dieser Informationen müssen gewährleistet werden.

Das Online Certificate Status Protocol (OCSP) muss dabei unterstützt werden, ausserdem soll eine Zertifikatssperrliste (Certificate Revocation List – CRL) publiziert werden.

Für ein Zertifikat muss die Widerrufs-Information über sein ursprünglich vorgesehenes

Gültigkeitsende hinaus bereitgestellt werden (allerdings nicht zwingend mittels OCSP). Die Anbieterin muss präzise dokumentieren, wie dies bewerkstelligt wird und dabei auch den Fall einer Einstellung des Betriebs berücksichtigen.
Zu beachten: Diese Anforderung gilt für alle geregelten Zertifikate, also nicht nur für solche zur Erstellung von Signaturen und Siegeln (s. Kap. 2.7.2).

2.7 Klasse 3+ (geregelt+)

2.7.1 Einleitung

Zur Klasse 3+ als höchste Zertifikatsklasse gehören die geregelten Zertifikate, deren zugehöriger privater Schlüssel in zertifizierter Hardware vorgehalten werden MUSS.

2.7.2 Signatur und Siegel

Zur Erstellung qualifizierter Signaturen, geregelter Signaturen oder geregelter Siegel müssen „sichere Signaturerstellungseinheiten“ bzw. „sichere Siegelerstellungseinheiten“ zum Einsatz kommen. Die Anforderungen werden in ZertES, VZertES und TAV-ZertES abschliessend vorgegeben, siehe TAV-ZertES, Kap. 2.2 für Details bezüglich Signatur- und Siegelerstellungseinheiten.

Es gelten gemäss ETSI EN 319 411-2 „Part 2: Requirements for trust service providers issuing EU qualified certificates“ die Zertifizierungspolitiken

- QCP-n-qscd (Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD) für natürliche Personen, also bei den Zertifikatsanwendungen qualifizierte Signatur und geregelte Signatur sowie
- QCP-l-qscd (Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD) für UID-Einheiten, also bei der Zertifikatsanwendung geregeltes Siegel.

2.7.3 Zertifikate für Nicht-Signatur-Anwendungen

Zusätzlich zu den Anforderungen an geregelte Zertifikate gemäss ZertES, VZertES und TAV-ZertES gilt:

- Zertifikate für Nicht-Signatur-Anwendungen der Klasse 3+ MÜSSEN der Zertifizierungspolitik „Extended Normalized Certificate Policy” (NCP+) entsprechen und sie müssen die Anforderungen gemäss Kap. 2.5 „Klasse 2+“ erfüllen (d.h. beim Zertifikatstoken handelt es sich um zertifizierte Hardware).

2.7.4 Referenzierte Certificate Policy

In ETSI EN 319 411-2 „Part 2: Requirements for trust service providers issuing EU qualified certificates“ werden die folgenden standardisierten Object Identifier (OID) zur Verwendung in der Erweiterung „certificatePolicies“ von Signatur- und Siegel-Zertifikaten spezifiziert:

- *{QCP-natural-qscd}*: Dieser OID zeigt an, dass das Zertifikat gemäss gesetzlichen Vorgaben auf eine natürliche Person ausgestellt wurde und dass der private Schlüssel in einer sicheren Signaturerstellungseinheit vorgehalten wird. Dieser OID findet also Verwendung in Zertifikaten für die geregelte oder qualifizierte Signatur.
- *{QCP-legal-qscd}*: Dieser OID zeigt an, dass das Zertifikat gemäss gesetzlichen Vorgaben auf eine UID-Einheit ausgestellt wurde und dass der private Schlüssel in einer sicheren Siegelerstellungseinheit vorgehalten wird. Dieser OID findet also Verwendung in Zertifikaten für das geregelte Siegel.

Eine Anbieterin KANN den entsprechenden OID gemäss obiger Aufzählung bzw. gemäss ETSI EN 319 411-2 in der Erweiterung „certificatePolicies“ von Klasse-3+-Signatur- bzw. Siegel-Zertifikaten einfügen.

Zusätzlich KANN eine Anbieterin den OID *{eCH0048V2Policies class3plus}* verwenden, um die Konformität mit der Klasse 3+ gemäss eCH-0048 V2.0 anzuzeigen.

Das Einfügen weiterer OIDs in der Erweiterung „certificatePolicies“ ist möglich, z.B. zur Referenzierung der Zertifizierungspraxis (CPS) der Anbieterin.

(Daneben sind auch die Vorgaben in TAV-ZertES bezüglich der Erweiterung „qcStatements“ zwingend zu beachten.)

Für die Nicht-Signatur-Zertifikate ist der folgende OID gemäss ETSI-Normen massgeblich:

- *{ncpplus}*, um anzuzeigen, dass der zugehörige private Schlüssel in zertifizierter Hardware vorgehalten wird (siehe Kap. 2.5.1).

Eine Anbieterin SOLL den OID *{ncpplus}* gemäss ETSI EN 319 411-1 in der Erweiterung „certificatePolicies“ von Klasse-3+-Zertifikaten einfügen, welche keine Signatur- bzw. Siegel-Zertifikate sind.

Zusätzlich KANN eine Anbieterin den OID *{eCH0048V2Policies class3plus}* verwenden, um die Konformität mit der Klasse 3+ gemäss eCH-0048 V2.0 anzuzeigen.

In geregelte Zertifikate muss ausserdem gemäss TAV-ZertES zwingend der Text ‚*regulated certificate*‘ im Feld „explicitText“ der Erweiterung „certificatePolicies“ eingefügt werden. Für qualifizierte Zertifikate lautet der Text ‚*qualified certificate*’. Sie sind also eindeutig als geregelte oder qualifizierte Zertifikate markiert und erkennbar.

3 Object Identifier (OID)

Der Verein eCH hat den folgenden Object Identifier (OID) bei der Internet Assigned Numbers Authority (IANA) registriert, siehe https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers:

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) 51948} (ASN.1 notation) bzw.
1.3.6.1.4.1.51948 (dot notation)

Zur Identifizierung der Zertifizierungspolitiken bzw. Klassen gemäss eCH-0048 wurde der

Object Identifier (OID) *{eCH0048V2Policies}* registriert. Es handelt sich um den OID:

{*certificate-policies* (1) *eCH0048V2Policies* (1)}
(dot notation: 1.3.6.1.4.1.51948.1.1)

Bei den OIDs zur Bezeichnung der Klassen handelt es sich um die darunter liegenden OIDs

- *{eCH0048V2Policies class1 (1)}* für Klasse 1
  (dot notation: 1.3.6.1.4.1.51948.1.1.1)
- *{eCH0048V2Policies class2 (2)}* für Klasse 2
  (dot notation: 1.3.6.1.4.1.51948.1.1.2)
- *{eCH0048V2Policies class3 (3)}* für Klasse 3
  (dot notation: 1.3.6.1.4.1.51948.1.1.3)
- *{eCH0048V2Policies class2plus (4)}* für Klasse 2+
  (dot notation: 1.3.6.1.4.1.51948.1.1.4)
- *{eCH0048V2Policies class3plus (5)}* für Klasse 3+
  (dot notation: 1.3.6.1.4.1.51948.1.1.5)

Für ETSI EN 319 411-1 „Part 1: General requirements“ gilt der OID

{itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1)}

bzw. gelten die darunterliegenden OIDs:

- *{ncp (1)}*
- *{ncpplus (2)}*
- *{lcp (3)}*

Für ETSI EN 319 411-2 „Part 2: Requirements for trust service providers issuing EU qualified certificates“ gilt der OID

{itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1)}

bzw. gelten die darunterliegenden OIDs

- *{qcp-natural (0)}*
- *{qcp-legal (1)}*
- *{qcp-natural-qscd (2)}*
- *{qcp-legal-qscd (3)}*
- *{qcp-web (4)}*

4 Erläuterungen (informativ)

4.1 Erläuterungen zu ZertES

ZertES definiert die folgenden drei Typen von Zertifikaten:

- digitales Zertifikat
- geregeltes Zertifikat
- qualifiziertes Zertifikat

Das *digitale Zertifikat* ist „eine digitale Bescheinigung, die den öffentlichen Schlüssel eines asymmetrischen kryptografischen Schlüsselpaars seinem Inhaber oder seiner Inhaberin zuordnet". Ein solches Zertifikat kann auf eine beliebige *Entität* oder ein beliebiges *Objekt* ausgestellt werden, also z.B. auf eine *natürliche Person, juristische Person, eine UID*[4]*-Einheit*, auf eine Website, auf einem Server oder auf eine sonstige Maschine. Mit Ausnahme der unten folgenden Zertifikatstypen sind *digitale Zertifikate* nicht gesetzlich geregelt. ZertES-anerkannte wie auch nicht-anerkannte Anbieterinnen können somit beliebige nicht-geregelte *digitale Zertifikate* ausstellen.

Das geregelte Zertifikat ist „*ein digitales Zertifikat, das die Anforderungen nach Artikel 7* [des ZertES] *erfüllt und von einer nach diesem Gesetz anerkannten Anbieterin von Zertifizierungsdiensten ausgestellt wurde*". Das geregelte Zertifikat stellt somit eine besondere Ausprägung des digitalen Zertifikats dar. Es wird auf eine *natürliche Person* oder auf eine *UID-Einheit* (s. Kap. 4.4) ausgestellt. Ein geregeltes Zertifikat muss den Anforderungen an Inhalt und Format gemäss ZertES, VZertES, TAV und ETSI-Normen genügen.

Das qualifizierte Zertifikat ist „*ein geregeltes Zertifikat, das die Anforderungen nach Artikel 8* [des ZertES] *erfüllt*". Es ist somit ein Spezialfall des geregelten Zertifikats. Es wird nur auf eine *natürliche Person* ausgestellt und nur für den Einsatzzweck der *qualifizierten elektronischen Signatur* verwendet wird.

ZertES behandelt auch die folgenden Zertifikats-basierten Anwendungsfälle[5]:

- „*Geregelte elektronische Signatur*": Eine elektronische Signatur, welche durch eine natürliche Person erstellt wird und den Vorgaben des ZertES entspricht.
- „G*eregeltes elektronisches Siegel*": Eine elektronische Signatur, welche durch eine UID-Einheit erstellt wird und den Vorgaben des ZertES entspricht.
  Geregelte Siegel können automatisiert erstellt werden, z.B. zur Erstellung kryptografischer Zeitstempel oder bei der Signatur von elektronischen Rechnungen.
- „*Qualifizierte elektronische Signatur*": Ein Spezialfall der geregelten elektronischen Signatur, welche auf einem qualifizierten Zertifikat beruht. Sie wird durch eine natürliche Person erstellt, und nur eine (mit einem qualifizierten Zeitstempel verbundene) qualifizierte Signatur ist gemäss Obligationenrecht (OR) Art. 14, 2bis einer eigenhändigen Unterschrift gesetzlich gleichgestellt.

[4] Unternehmens-Identifikationsnummer

[5] S. auch ZertES, Art. 2 „Begriffe"

Grafisch lassen sich diese Anwendungsfälle, also die Signaturtypen gemäss ZertES, Artikel 2 «Begriffe» wie folgt darstellen:

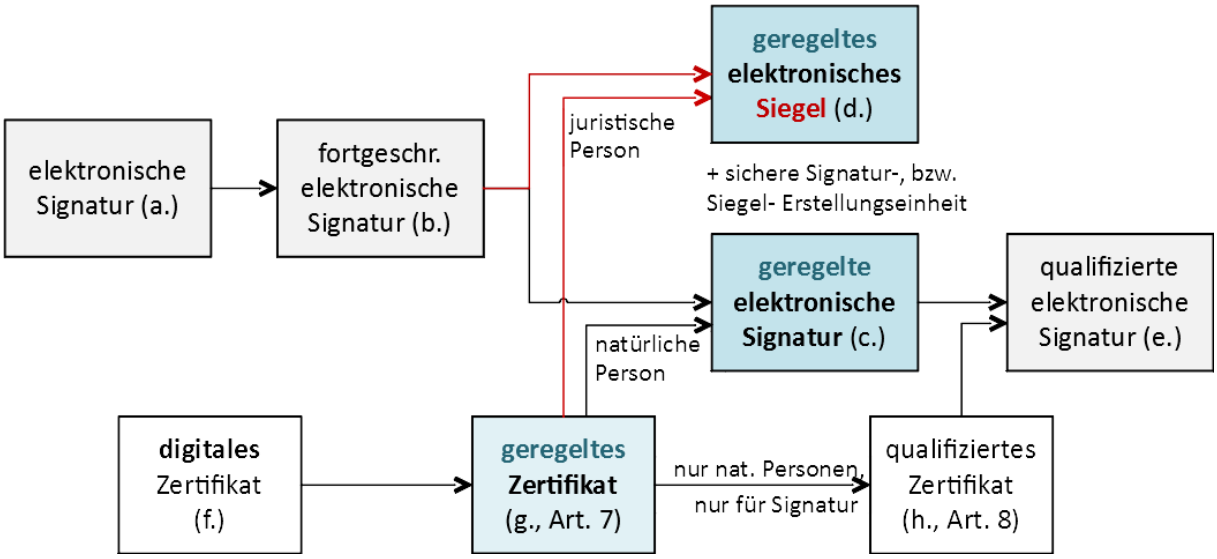

Abbildung 1: Zertifikats-basierte Anwendungsfälle gemäss ZertES Art. 2

Diese Signaturen können auch als Fernsignaturen angebracht werden. Das heisst, dass die “Sichere Signaturerstellungseinheit” sich nicht im physischen Besitz eines Anwenders befinden muss, sie kann auch in der Manier eines Cloud-Dienstes remote mittels Multi-Faktor-Authentisierung angesprochen werden. Dabei besteht auch die Möglichkeit, bei Bedarf pro Signaturvorgang ein Schlüsselpaar mit zugehörigem kurzlebigem Zertifikat zu erzeugen (z.B. mit einer Gültigkeitsdauer von 10 Minuten). Zu beachten ist bei diesen kurzlebigen Zertifikaten, dass für sie dieselben Anforderungen hinsichtlich Ungültigerklärung, Bereitstellung von Widerrufsinformationen (mittels OCSP bzw. CRL) und qualifiziertem Zeitstempel (vgl. auch OR Art. 14 2bis) gelten wie bei Zertifikaten mit langer Gültigkeitsdauer.

Zu erwähnen ist für diese Anwendungsfälle ausserdem, dass bei diesen für den Zertifikatshalter die Haftungsbestimmungen gemäss OR Art. 59a bezüglich „Haftung für kryptografische Schlüssel“ gelten:

„Art. 59a

1 Der Inhaber eines kryptografischen Schlüssels, der zur Erzeugung elektronischer Signaturen oder Siegel eingesetzt wird, haftet Drittpersonen für Schäden, die diese erleiden, weil sie sich auf ein gültiges geregeltes Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes vom 18. März 2016 über die elektronische Signatur verlassen haben.

2 Die Haftung entfällt, wenn der Inhaber glaubhaft darlegen kann, dass er die nach den Umständen notwendigen und zumutbaren Sicherheitsvorkehrungen getroffen hat, um den Missbrauch des kryptografischen Schlüssels zu verhindern.

3 Der Bundesrat umschreibt die Sicherheitsvorkehrungen im Sinne von Absatz 2.“

4.2 Erläuterungen zu eIDAS

eIDAS ist eine Verordnung der Europäischen Union (EU), welche in der EU und im Europäischen Wirtschaftsraum (EWR) als direkt anwendbares Recht gültig ist. Für die Schweiz gilt eIDAS nicht, da diesbezüglich kein Staatsvertrag besteht. eIDAS steht für „VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG“.

eIDAS regelt im Wesentlichen

- „Elektronische Identifizierung“ (Kapitel II), also die eID und
- „Vertrauensdienste“ (Kapitel III).

Im Kapitel III werden (neben anderen „Vertrauensdiensten“) auch die Voraussetzungen zur Ausgabe von Zertifikaten für

- elektronische Signaturen,
- elektronische Siegel und
- Website-Authentifizierung

geregelt.

Zu beachten ist dabei die von ZertES abweichende Terminologie:

Gemäss ZertES kann das „qualifizierte Zertifikat“ nur für den Zweck „qualifizierte elektronische Signatur“ ausgestellt und verwendet werden. Bei ZertES-konformen Zertifikaten für andere Verwendungszwecke handelt es sich um „geregelte Zertifikate“. eIDAS hingegen unterscheidet nur zwischen „qualifiziert“ und „fortgeschritten“ (bezüglich der Anwendungen Signatur und Siegel).

4.3 Erläuterungen zu eCH-0170

Der eCH-Standard „eCH-0170 Qualitätsmodell zur Authentifizierung von Subjekten“ dient der qualitativen Einstufung und dem Vergleich von Authentifizierung. Er definiert vier Vertrauensstufen für Authentisierung und stellt diesbezüglich detaillierte Vorgaben zu Authentisierungsmittel, Registrierung, Steuerung und Föderierung.

eCH-0170 ist Technologie-neutral formuliert, die Verwendung eCH-0048-konformer Client-Zertifikaten als Authentisierungs-Credentials gemäss eCH-0170 ist somit möglich.

Die Gegenüberstellung der Zertifikatsklassen gemäss eCH-0048 mit den Vertrauensniveaus gemäss eCH-0170 ergibt das folgende Bild bezüglich *ungefährer* Übereinstimmung:

eCH-0170 Vertrauensstufe	eCH-0170 Bezeichnung	eCH-0048 Klasse
4	Hohes Vertrauen	Klasse 3+
3	Beträchtliches Vertrauen	Klasse 2+
2	Geringes Vertrauen	Klasse 1
1	Kein oder minimales Vertrauen	-

Tabelle 3: Mapping auf eCH-0170

Entsprechende Client-Zertifikate einer eCH-0048-Zertifikatsklasse können somit als Authentisierungs-Credentials gemäss eCH-0170 verwendet werden.

4.4 Erläuterungen zum UID-System

Bei einer UID-Einheit handelt es sich um ein Unternehmen im weiteren Sinne, dem für Behördenkontakte eine Unternehmens-Identifikationsnummer (UID) gemäss Bundesgesetz über die Unternehmens-Identifikationsnummer (UIDG) zugeteilt wurde und welches somit im UID-Register eingetragen ist. UID-Einheiten sind

- eingetragene juristische Personen (z.B. GmbHs oder AHV-abrechnende Vereine),
- unternehmerisch tätige natürliche Personen (z.B. im Handelsregister eingetragene Einzelfirmen oder freie Berufe),
- Behördenstellen (von Bund, Kantonen und Gemeinden) sowie auch
- wirtschaftlich aktive Entitäten ohne eigene Rechtspersönlichkeit

(Aufzählung nicht abschliessend).

Hinsichtlich UID-Einheiten ist der folgenden Punkt zu beachten: Nicht jede juristische Person ist eine UID-Einheit. Jeder rechtsgültig gegründete Verein stellt eine juristische Person dar, auch ohne behördlichen Registereintrag und somit ohne Zuteilung einer UID. Ein nicht-eingetragener Verein ist somit durch das obige Konzept nicht abgedeckt; da er keine Behördenkontakte pflegt, ist dieser Fall im Kontext eGovernment aber nicht relevant.

4.5 Erläuterungen zu Attributzertifikaten

Im X.509-Standard werden neben den Public-Key-Zertifikaten auch „Attribut-Zertifikate“ spezifiziert. Attribut-Zertifikate zeichnen sich dadurch aus, dass sie selbst keinen öffentlichen Schlüssel enthalten, sondern eine Referenz auf ein Public-Key-Zertifikat bzw. auf dessen Inhaber. Sie entsprechen somit nicht der Definition eines digitalen Zertifikats gemäss ZertES; auch sind sie in der Praxis wenig verbreitet. Aus diesen Gründen wird auf eine tiefergehende Behandlung der Attribut-Zertifikate im vorliegenden Standard verzichtet.

4.6 Erläuterungen zu ElDI-V

Die Verordnung des EFD über elektronische Daten und Informationen (ElDI-V) regelt die Anforderungen an die Beweiskraft und die Kontrolle elektronischer Rechnungen (und verwandter relevanter Daten), welche die Konformität zur Gesetzgebung bezüglich Mehrwertsteuer (MWST) sicherstellen. Nur diese Konformität berechtigt zum MWST-Vorsteuer-Abzug.

Zur Gewährleistung des Ursprungs und der Unversehrtheit der elektronischen Rechnungen **können** elektronische Signaturen verwendet werden. Da Rechnungen normalerweise von *Organisationen* bzw. *juristischen Personen* oder UID-Einheiten ausgestellt werden, ist es sinnvoll, dass das für die Signatur verwendete Zertifikat auf das entsprechende Wirtschaftssubjekt ausgestellt wird und nicht unbedingt auf eine *natürliche Person*. ElDI-V verweist deshalb in Artikel 2, Absatz 2 auf die erweiterte Definition einer elektronischen Signatur gemäss ZertES:
„Als elektronische Signaturen im Sinn dieser Verordnung gelten Signaturen nach Artikel 2 Buchstaben c-e des Bundesgesetzes vom 18. März 2016 über die elektronische Signatur, sofern sie keine Einschränkungen enthalten, die die Verwendung zu Zwecken dieser Verordnung ausschliessen.“

Konkret bedeutet dies, dass neben qualifizierten und geregelten Signatur-Zertifikaten für *natürliche Personen* auch geregelte Siegel-Zertifikate eingesetzt werden können.

4.7 Extended-Validation-SSL-Zertifikate

In ETSI EN 319 411 „Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates” wird auf die “Extended Validation Certificate Policy” (EVCP) bzw. auf die “Guidelines for The Issuance and Management of Extended Validation Certificates” verwiesen. Diese werden vom “CA/Browser Forum” erstellt und verwaltet, einer Kooperation von Browser-Herstellern und Anbieterinnen von Zertifizierungsdiensten (http://cabforum.org).

Der Zweck ist hauptsächlich die Ausstellung von EV-SSL-Zertifikaten. Wesentliches Merkmal ist das hohe Anforderungsprofil für den Registrierungsprozess (https://cabforum.org/extended-validation-2/) sowie Art und Umfang der Validierung der eingereichten Registrierungsdaten. Hierdurch soll sichergestellt werden, dass die ausgegebenen Zertifikate eindeutig den juristisch Berechtigten zugeordnet werden.

Zur vereinfachten Wahrnehmung dieses Vertrauensniveaus durch die Benutzer wurde von den Browser-Herstellern die Anzeige eines „Grünen Balkens“ in der Adressleiste des Browsers mit Namen des Zertifikatsinhabers implementiert.

Hinsichtlich eCH-0048 entsprechen diese Zertifikate der Klasse 2.

5 Sicherheitsüberlegungen

Keine

6 Haftungsausschluss/Hinweise auf Rechte Dritter

eCH-Standards, welche der Verein **eCH** dem Benutzer zur unentgeltlichen Nutzung zur Verfügung stellen oder welche **eCH** referenzieren, haben nur den Status von Empfehlungen. Der Verein **eCH** haftet in keinem Fall für Entscheidungen oder Massnahmen, welche der Benutzer auf Grund dieser Dokumente trifft und / oder ergreift. Der Benutzer ist verpflichtet, die Dokumente vor deren Nutzung selbst zu überprüfen und sich gegebenenfalls beraten zu lassen. **eCH**-Standards können und sollen die technische, organisatorische oder juristische Beratung im konkreten Einzelfall nicht ersetzen.

In **eCH**-Standards referenzierte Dokumente, Verfahren, Methoden, Produkte und Standards sind unter Umständen markenrechtlich, urheberrechtlich oder patentrechtlich geschützt. Es liegt in der ausschliesslichen Verantwortlichkeit des Benutzers, sich die allenfalls erforderlichen Rechte bei den jeweils berechtigten Personen und/oder Organisationen zu beschaffen.

Obwohl der Verein **eCH** all seine Sorgfalt darauf verwendet, die **eCH**-Standards sorgfältig auszuarbeiten, kann keine Zusicherung oder Garantie auf Aktualität, Vollständigkeit, Richtigkeit bzw. Fehlerfreiheit der zur Verfügung gestellten Informationen und Dokumente gegeben werden. Der Inhalt von **eCH**-Standards kann jederzeit und ohne Ankündigung geändert werden.

Jede Haftung für Schäden, welche dem Benutzer aus dem Gebrauch der **eCH**-Standards entstehen ist, soweit gesetzlich zulässig, wegbedungen.

7 Urheberrechte

Wer **eCH**-Standards erarbeitet, behält das geistige Eigentum an diesen. Allerdings verpflichtet sich der Erarbeitende, sein betreffendes geistiges Eigentum oder seine Rechte an geistigem Eigentum anderer, sofern möglich, den jeweiligen Fachgruppen und dem Verein **eCH** kostenlos zur uneingeschränkten Nutzung und Weiterentwicklung im Rahmen des Vereinszweckes zur Verfügung zu stellen.

Die von den Fachgruppen erarbeiteten Standards können unter Nennung der jeweiligen Urheber von **eCH** unentgeltlich und uneingeschränkt genutzt, weiterverbreitet und weiterentwickelt werden.

eCH-Standards sind vollständig dokumentiert und frei von lizenz- und/oder patentrechtlichen Einschränkungen. Die dazugehörige Dokumentation kann unentgeltlich bezogen werden.

Diese Bestimmungen gelten ausschliesslich für die von **eCH** erarbeiteten Standards, nicht jedoch für Standards oder Produkte Dritter, auf welche in den **eCH**-Standards Bezug genommen wird. Die Standards enthalten die entsprechenden Hinweise auf die Rechte Dritter.

Anhang A – Referenzen & Bibliographie

CH Rechtsgrundlagen

(s.a. Übersicht unter: https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/digitale-kommunikation/elektronische-signatur.html)

SR 943.03 ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (18. März 2016, in Kraft seit 1. Januar 2017)
SR 942.032 VZertES	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (23. November 2016, Stand am 1. Januar 2017)
SR 943.032.1 TAV-ZertES	„Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate anderer Anwendungen digitaler Zertifikate“, Ausgabe 1 (BAKOM 13. November 2016, in Kraft seit 1. Januar 2017)
SR 641.20 MWSTG	Bundesgesetz über die Mehrwertsteuer (12. Juni 2009)
SR 641.201 MWSTV	Mehrwertsteuerverordnung (27. November 2009)
SR 641.201.511 ElDI-V	Verordnung des EFD über elektronisch übermittelte Daten und Informationen vom 11. Dezember 2009 (Stand am 1. Januar 2017)
SR 641.201.511.1	Verordnung der ESTV über Zertifizierungsdienste im Bereich der ElDI-V
SR 221.431 GeBüV	Verordnung vom 24. April 2002 über die Führung und Aufbewahrung der Geschäftsbücher
SR 221.415 Verordnung SHAB	Verordnung über das Schweizerische Handelsamtsblatt (21.2.2006)
SR 431.02	Bundesgesetz vom 23. Juni 2006 über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister (Registerharmonisierungsgesetz, RHG)
	Botschaft zur Totalrevision des Bundesgesetzes über die elektronische Signatur (ZertES)
SR 431.03	Bundesgesetz über die Unternehmens-Identifikationsnummer (UIDG) vom 18. Juni 2010 (Stand am 1. Januar 2011)
SR 431.031	Verordnung über die Unternehmens-Identifikationsnummer (UIDV) vom 26. Januar 2011 (Stand am 1. Dezember 2015)

EU Rechtsakte (Anwendung in EU und EWR, nicht in der Schweiz)

eIDAS	VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

ETSI-Publikationen zu „Electronic Signatures and Infrastructures (ESI)“

Zu beachten: Hier werden die durch TAV-ZertES (direkt oder indirekt) referenzierten Versionen der ETSI-Normen zum Thema aufgeführt. Es handelt sich dabei nicht zwingend um die aktuellsten Versionen dieser Normen.

(S. auch Übersicht unter: https://portal.etsi.org//TBSiteMap/ESI/ESIActivities.aspx oder https://portal.etsi.org/tbsitemap/esi/trustserviceproviders.aspx bezüglich der gültigen ETSI-Normen und deren jeweiliger aktueller Version zu den Themen „Electronic Signatures and Infrastructures (ESI)“ und „Trust Service Provider (TSP)“)

ETSI EN 319 401 V2.1.1 (2016-02)	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI EN 319 403 V2.2.2 (2015-08)	Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers
ETSI EN 319 411-1 V1.1.1 (2016-02)	Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates; Part 1: General requirements
ETSI EN 319 411-2 V2.1.1 (2016-02)	Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
ETSI EN 319 412-1 V1.1.1 (2016-02)	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
ETSI EN 319 412-2 V2.1.1 (2016-02)	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates
ETSI EN 319 412-3 V1.1.1 (2016-02)	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
ETSI TS 119 312 V1.2.1 (2017-05)	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

CEN Workshop Agreements

CWA 14169 (2004)	Secure Signature-Creation Devices "EAL 4+"

CWA 24272-5	EESSI Conformity Assessment Guidance - Part 5: Secure signature-creation devices
CWA 24272-6	EESSI Conformity Assessment Guidance - Part 6: Signature-creation device supporting signatures other than qualified

ISO Standards

ISO/IEC 15408:2005	Information technology – Security techniques. Evaluation criteria for IT security (Alternative Bezeichnung: “Common Criteria for Information Technology Security Evaluation”)
ISO/IEC 19790:2012	Information technology -- Security techniques -- Security requirements for cryptographic modules

ITSEC

ITSEC	Information Technology Security Evaluation Criteria

ITU-T Recommendation

X.509	X.509: Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks (03-2000) http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-X.509

NIST Federal Information Processing Standards (FIPS)

FIPS 140-2 (2001)	Security requirements for Cryptographic Modules

PKIX RFCs

RFC 2119	Key words for use in RFCs to Indicate Requirement Levels
RFC 3279	Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 5280	PKI Certificate and CRL Profile
RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
RFC 3739	PKI Qualified Certificates Profile

eCH-Dokumente

eCH-0170	eCH-0170 Qualitätsmodell zur Authentifizierung von Subjekten V2.0
eCH-0219	eCH-0219 IAM Glossar V1.0

Deutsches Bundesamt für Sicherheit in der Informationstechnik – BSI

BSI TR-02102-1	BSI Technische Richtlinie; Kryptographische Verfahren: Empfehlungen und Schlüssellängen; Version 2018-01

Anhang B – Mitarbeit & Überprüfung

Mitarbeit	Cornelia Enke, BIT
	Simon Günter, Swiss Open Systems User Group
	Urs Paul Holenstein, EJPD
	Christian Bütler, EJPD
	Peter von Dach, ISB
	Urs Bürge, Urs Bürge Beratung
	Gerhard Hassenstein, Berner Fachhochschule
	Christian Jenny, BAKOM
	Michael von Niederhäusern, BIT
	Daniel Stich, BIT
	Andreas Zürcher, BIT
	Reinhard Dietrich, Swisssign
	Mario Voge, Swisssign
	eCH Fachgruppe Identity and Access Management

Anhang C – Abkürzungen

BIT	Bundesamt für Informatik und Telekommunikation (http://www.bit.admin.ch/)
BSI	Deutsches Bundesamt für Sicherheit in der Informationstechnik
CA	Certificate Authority – Zertifizierungsbehörde
CEN	Comité Européen de Normalisation – Europäisches Komitee für Normung (https://www.cen.eu/)
CN	Common Name – X.509 Zertifikatsfeld für den Namen des Zertifikatsinhabers
CP	Certificate Policy – Zertifizierungspolitik
CPS	Certification Practice Statement - Zertifizierungspraxis
CRL	Certificate Revocation List – Liste mit Sperrinformationen zu herausgegebenen Zertifikaten einer Anbieterin von Zertifizierungsdiensten.

CSP	Certification Service Provider – Anbieterin von Zertifizierungsdiensten
CWA	CEN Workshop Agreement – CWAs sind Konsens-basierte Spezifikationen, die durch „CEN Workshops“ erarbeitet werden.
EFD	Eidgenössisches Finanzdepartement
ElDI-V	Verordnung des EFD über elektronische Daten und Informationen
ETSI	European Telecommunications Standards Institute (http://www.etsi.org/)
EV-SSL	Extended Validation-Secure Socket Layer (Zertifikat)
FIPS	Federal Information Processing Standard – Von NIST ausgegebene IT-Standards (Schwerpunkt Sicherheit)
HSM	Hardware Security Module Komponente zur sicheren Erzeugung und Speicherung von Private Keys sowie für alle PKI-Funktionalitäten (dig. Signatur, Hash, Ver- und Entschlüsselung, etc.). Diese HSM werden in Form von Crypto-Adaptern in CA- oder Signaturserver eingebaut oder als Netzwerk-Appliance mehreren CA- oder Signaturservern zur Verfügung gestellt. HSM-eigene Verfahren ermöglichen Backup und Recovery von Keys und Zertifikaten in einem gesicherten Verfahren.
IAC	Identification and Authentication Certificate
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
IPsec	Internet Protocol Security
ISO	International Standardization Organisation
ITU	International Telecommunication Union
LRA	*Local Registration Authority*
MWST	Mehrwertsteuer
NIST	National Institute of Standards and Technology (http://csrc.nist.gov/publications)
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OR	Obligationenrecht
RFC	Request for Comment (Art Internetstandard)
SAN	Subject Alternative Name – optionales X.509 Zertifikatsfeld für weitere Namenseinträge
TAV	Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur; s.o. unter „CH-Rechtsgrundlagen“
TLS	Transport Layer Security
TSP	Trust Service Provider
UID	Unternehmens-Identifikationsnummer

URL	Uniform Resource Locator
VZertES	Verordnung zum Bundesgesetz über die elektronische Signatur
ZertES	Bundesgesetz über die elektronische Signatur

Anhang D – Glossar

Es gelten die Begriffsdefinitionen gemäss eCH-0219 IAM Glossar V1.0.

Anhang E – Änderungen gegenüber Vorversion

Die Version 2.0 des Standards „eCH-0048 Zertifikatsklassen“ wurde gegenüber der Vorversion 1.1 vollständig überarbeitet.

Es besteht keine Rückwärtskompatibilität, d.h. die Zertifikatsklassen gemäss eCH-0048 Version 2.0 sind nicht kompatibel mit den Klassen eCH-0048 Version 1.1.

Anhang F – Abbildungsverzeichnis

Abbildung 1: Zertifikats-basierte Anwendungsfälle gemäss ZertES Art. 2 32

Anhang G – Tabellenverzeichnis

Tabelle 1: Überblick 10
Tabelle 2: Detaillierte Darstellung 16
Tabelle 3: Mapping auf eCH-0170 34

Anhang H – Mapping auf bestehende Angebote

Im Folgenden werden die Zertifikatsklassen gemäss eCH-0048 Version 2.0 dem Angebot der gemäss ZertES anerkannten Anbieterinnen gegenübergestellt (Stand Ende 2017).

Zu beachten: Es handelt sich dabei um eine rein informative Gegenüberstellung bzw. um eine Annäherung ohne Anspruch auf Vollständigkeit oder Exaktheit, d.h. es wurde kein Assessment der Konformität der entsprechenden Zertifikate zu den Zertifikatsklassen gemäss eCH-0048 durchgeführt.

Klasse		BIT	Swisssign	Swisscom	QuoVadis
3+	Geregelt+	Klasse A (qualifiziert)	Platinum Qualified (qualifiziert)	„Diamant“ (qualifiziert)	Qualifizierte Zertifikate Zertifikate für geregelte Siegel
3	Geregelt	-	-	-	-
2+	NCP+	Klasse B	Platinum	Saphir	Fortgeschritte-ne Zertifikate
2	NCP	Klasse C Code-Signing	Gold Silver	Smaragd	EV SSL Zertifikate etc.
1	LCP	Klasse E		Rubin	

Tabelle 4: Mapping auf bestehende Angebote

Die Gegenüberstellung zeigt, dass der Markt im Bereich der geregelten Zertifikate noch in der Entwicklung begriffen ist. Neben qualifizierten Zertifikaten, welche schon gemäss altem ZertES ausgestellt werden konnten, besteht bisher ein kleines Angebot an geregelten Zertifikaten.