eCH-0048 PKI-Zertifikatsklassen

Name	PKI Zertifikatsklassen
Standard-Nummer	eCH-0048
Kategorie	Standard
Reifegrad	Definiert
Version	1.10
Status	Aufgehoben
Genehmigt am	2018-11-28
Ausgabedatum	2012-04-10
Ersetzt Standard	eCH-0048 1.00
Sprachen	Deutsch
Autoren	**Fachgruppe Sicherheit** Gerold H. Werner, max. consult AG (Leiter), max.consult-ag@bluewin.ch Adrian Müller, ID Cyber-Identity AG adrian.mueller@cyber-identity.com
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

Seit der Verabschiedung der V1-0 Ende 2006 konnten eine Reihe von X.509 Zertifikatsprodukten am Markt etabliert werden, die eine Aktualisierung und Ergänzung des eCH-0048 Standards veranlasst haben. Die Änderungen beziehen sich dabei neben redaktionellen Anpassungen auf

- die Einführung normierter Schlüsselworte für Anforderungen
- inhaltliche Umstrukturierungen ohne fachliche Änderungen, wo dies zur besseren Klarheit angeraten schien
- Ergänzung um das Kapitel 4.5 mit der Beschreibung aktuell marktgängiger Zertifikatsformate sowie deren Einordnung in die vorliegende Klassifikation.

Die Kriterien zur Kategorisierung der jeweiligen Vertrauensniveaus sind unverändert.

Inhaltsverzeichnis

1 Status des Dokuments

Aufgehoben: Das Dokument wurde von eCH zurückgezogen. Er darf nicht mehr genutzt werden.

2 Einleitung

Wesentliche Grundlage zur Realisierung verbindlicher und vertrauenswürdiger eGovernment Geschäftsprozesse[1] ist die verlässliche Identifikation der beteiligten Partner. Als internationaler Standard hat sich in diesem Kontext der Einsatz von elektronischen Signaturen mittels X.509 Zertifikaten etabliert. Diesem technischen Standard ist zusätzlich ein organisatorisches und juristisches Regelwerk an die Seite zu stellen, damit die eindeutige Zuordnung von Dokumenten, Willenserklärungen, etc. zu ihren Urhebern in Form digitaler Signaturen sichergestellt werden kann und mit den von allen Beteiligten gewünschten Rechtsfolgen verbunden ist.

Das Einsatzgebiet von X.509 Zertifikaten ist nicht nur auf die Signatur von elektronischen Dokumenten beschränkt. Es umfasst weiterhin die Authentifizierung, Code-Signaturen, Verschlüsselung und weitere. Der vorliegende eCH-Standard adressiert sämtliche Einsatzbereiche.

2.1 Verwendung von Schlüsselworten

Zur präziseren Qualifizierung der aufgeführten Anforderungen werden die folgenden Schlüsselworte (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 In-

[1] Der Begriff ‚Geschäftsprozess' bezeichnet in diesem Dokument nicht nur Aktivitäten privatwirtschaftlichen Handelns, sondern ebenso die vielfältigen Auskunfts- und Verwaltungstätigkeiten der öffentlichen Verwaltung einschliesslich der Schnittstellen zur Privatwirtschaft.

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

2.2 Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.1	16.06.2011	4.5.1 4.5.2	Aufnahme folgender Zertifikatsformate (informativ): ElDI-V, SuisseID IAC	A. Müller
1.1	21.06.2011	4.5.3	Aufnahme folgender Zertifikatsformate (informativ): EV-SSL	G. Werner
1.1	26.06.2011	Alle	Präzisierung der Anforderungen gemäss RFC-2119	G. Werner
1.1	29.06.2011	Alle	Überprüfung und Detail-Korrektur	H. Graf D. Müller A. Müller

2.3 Zweck des Standards für Zertifikatsklassen

Im europäischen Wirtschaftsraum kann als Ausgangsbasis und Referenz die Richtlinie 93/1999 EU[2] gelten, die zwischenzeitlich in den meisten EU-Mitgliedsstaaten in nationales Recht umgesetzt ist. In dieser Richtlinie werden die Rahmenbedingungen für drei verschiedene Qualitätsstufen von digitalen Signaturen und Zertifikaten (in unterschiedlichem Detaillierungsgrad) angesprochen:

- Elektronische Signatur
  „elektronische Signatur" Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen. (Richtlinie, Art. 2, 1.)

- Fortgeschrittene elektronische Signatur
  „fortgeschrittene elektronische Signatur" eine elektronische Signatur, die folgende Anforderungen erfüllt:
  a) Sie ist ausschließlich dem Unterzeichner zugeordnet;
  b) sie ermöglicht die Identifizierung des Unterzeichners;
  c) sie wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann;
  d) sie ist so mit den Daten, auf die sie sich bezieht, verknüpft, daß eine nachträgliche Veränderung der Daten erkannt werden kann. (Richtlinie, Art. 2, 2.)

[2] RICHTLINIE 1999/93/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen

- Qualifizierte elektronische Signatur
  (Fortgeschrittene elektronische Signatur, die auf einem qualifizierten Zertifikat basiert)
  „qualifiziertes Zertifikat" ein Zertifikat, das die Anforderungen des Anhangs I erfüllt und von einem Zertifizierungsdiensteanbieter bereitgestellt wird, der die Anforderungen des Anhangs II erfüllt. (Richtlinie, Art. 2, 10.)

In den Erwägungsgründen[3] sowie in den inhaltlichen Ausführungen[4] dieser Richtlinie wird ausdrücklich auf die Förderung auch der grenzüberschreitenden elektronischen Kommunikation im gemeinsamen Wirtschaftraum abgestellt.

Ebenso sind die elektronischen Geschäftsprozesse in der öffentlichen Verwaltung zwischen Bürgern, Wirtschaft und staatlichen Einrichtungen adressiert.[5]

Die gesetzlichen Grundlagen und Rahmenbedingungen in der Schweiz (ZertES, VZertES, TAV und referenzierte Dokumente) für den Einsatz elektronischer Signaturen sowie die Ausgabe von digitalen Zertifikaten fokussieren dabei Regelungen für die Ausgabe von qualifizierten Zertifikaten an ausschliesslich **natürliche Personen** durch anerkannte Anbieter. Das Ziel hierbei ist die Bereitstellung eines elektronischen Äquivalents der handschriftlichen Unterschrift zur Dokumentierung einer Willenserklärung.

Die Akteure in elektronischen Geschäfts- und eGovernment-Prozessen sind – über die gesamte Prozesskette betrachtet – jedoch nicht nur natürliche Personen, sondern ebenso juristische Personen und Organisationen, Funktionseinheiten und Rollen sowie schliesslich auch technische Infrastrukturkomponenten (Server, Router, … allgemein Maschinen und Systemprozesse).

Die rechtsverbindliche Signatur durch natürliche Personen deckt somit nur einen Teilbereich der komplexen Prozessketten in Wirtschaft und eGovernment ab.

Weiterhin unterliegen die weitaus meisten Geschäftsprozesse nicht gesetzlichen Formvorschriften, die eine handschriftliche Unterschrift – oder deren elektronisches Äquivalent, die qualifizierte elektronische Signatur - tatsächlich erfordern. Wird sie dennoch eingesetzt, ergeben sich daraus gesetzliche Folgerungen hinsichtlich Gewährleistung und Haftung, die nicht in jedem Falle angemessen oder gewünscht sind.

- Zur sicheren Implementierung von eGovernment-Prozessketten bedarf es (u.a.) verschiedener ‚Digitaler Identitäten' in Form elektronischer Zertifikate, von denen eines das qualifizierte Signatur-Zertifikat gemäss ZertES ist, resp. sein kann.
- Neben der „qualifizierten Signatur" sind im ZertES ebenfalls die einfache "elektronischen Signatur" (ZertES Art. 2a) sowie die "fortgeschrittene elektronische Signatur" (ZertES Art.2b) angesprochen. Rahmenbedingungen und Rechtsfolgen sind hierzu jedoch in den weiteren Ausführungen nicht hinreichend detailliert.

[3] Siehe Erwägungsgründe 5, 7, 8, 10, 19 und 23
[4] RICHTLINIE Art 3 „Marktzugang" und Art. 4 „Binnenmarktgrundsätze"
[5] Siehe Erwägungsgrund 5

- Für die qualifizierte Signatur gilt gemäss OR Art. 59a die Beweislast-Umkehr. Dies bedeutet, dass im Gegensatz zu Regelungen für den papierschriftlichen Verkehr der (angebliche) Unterzeichner beweisen muss, dass er ein Dokument nicht signiert hat. Für Signaturen, die nicht auf einem qualifizierten Zertifikat beruhen, bestehen keine gesetzlichen Vorschriften.

2.4 Zielsetzung

Etablierung eines eCH Standards für digitale Zertifikate zur Unterstützung von verschiedenen Einsatzbereichen für Identity-Management, Signatur und Verschlüsselung in eGovernment-Geschäftsprozessen mit den korrespondierenden Sicherheitsniveaus.

Die Prämissen für einen eCH-Standard der Zertifikatsklassen sind:

- Ergänzende Regelungen für die im ZertES angesprochenen „elektronischen Signaturen“ und „fortgeschrittenen elektronischen Signaturen“
- Definition von 3 Zertifikatsklassen mit abgestuftem Vertrauensniveau
- Konkretisierung der Anforderungen zur Ausgabe von Zertifikaten
- Technische Parameter werden nicht spezifiziert. Nur die für Vertrauensniveaus relevanten Standards werden referenziert.
- Konformität zu
  - schweizerischer Gesetzgebung
  - Regularien internationaler Handelspartner (insbes. EU)

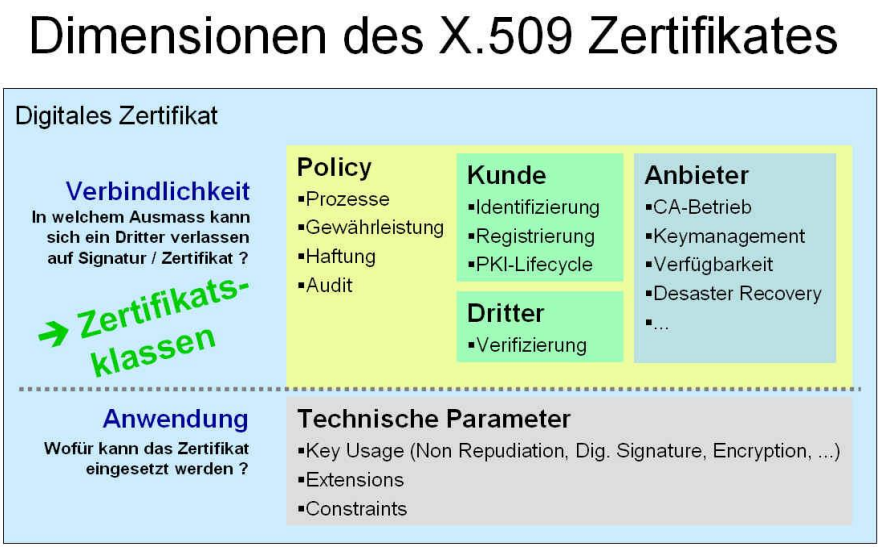
2.5 Klassifikation des Vertrauensniveaus

Im vorliegenden eCH-Standard wurde vor diesem Hintergrund zunächst eine Trennung der zwei wesentlichen Aspekte digitaler Zertifikate vorgenommen:

- **Vertrauensniveau**’[6]
  der im Zertifikat enthaltenen Angaben zum zertifizierten Subjekt (natürliche oder juristische Person, Organisation, Maschine, Prozess, Rolle). Dieser Aspekt bestimmt, in welchem Ausmass ein Geschäftspartner sich auf die Inhalte des Zertifikates verlassen kann. In Verbindung mit den Haftungsregelungen des Zertifizierungsdienste-Anbieters sowie ggf. ergänzenden vertragsrechtlichen Regelungen der Geschäftspartner resultiert hieraus die Verbindlichkeit der elektronisch signierten Vorgänge.
- **Funktion**
  des Zertifikates, die über das Setzen der technischen Parameter (gemäss X.509 Standard) gesteuert wird. Dieser Aspekt bestimmt, WOFÜR ein Zertifikat technisch genutzt werden kann (elektronische Signatur, Nicht-Abstreitbarkeit, Authentifizierung, eMail-Verschlüsselung, Server-Authentifizierung, Code-Signing, etc.).

[6] Vertrauensniveau zur Klassifikation des Ausmasses an Zuverlässigkeit der im Zertifikat enthaltenen Angaben. Dieses Zuverlässigkeit basiert einerseits auf den international anerkannten technischen Standards, andererseits aber vor allem auf der Güte der implementierten organisatorischen Prozesse zur Identifikation der zertifizierten Identitätsangaben, sowie der Verifizierung dieser Angaben.

Der vorliegende Standard geht davon aus, dass Vertrauenswürdigkeit und Funktion zwei unabhängige Dimensionen eines konkreten Zertifikat-Produktes sind. Da die Funktion über rein technische Parameter des Zertifikates gesetzt wird, konzentriert sich dieser Standard auf diejenigen **technischen und organisatorischen Kriterien zur Vertrauenswürdigkeit** der im Zertifikat enthaltenen Daten.



Ein konkretes Zertifikatsprodukt einer Anbieterin von Zertifizierungsdiensten (CSP)[7] setzt sich somit zusammen aus:

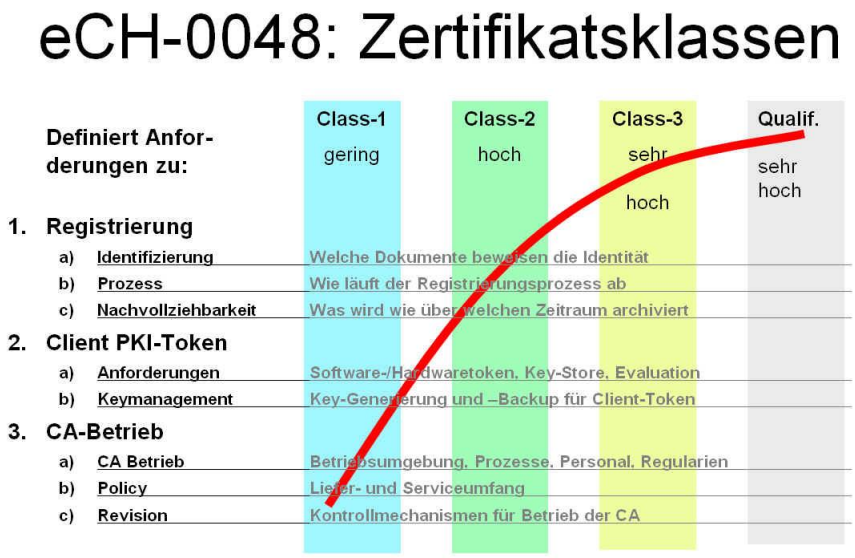
- Gewährleistung der Eigenschaften einer bestimmten Zertifikatsklasse für diese von ihm ausgegebenen Zertifikate
- Implementierung der technischen Parameter für den ausgewiesenen Einsatzbereich sowie die hierfür erforderlichen Verzeichnisdienste

Die Gruppierung von Anforderungsprofilen zu diesen Kriterien ergeben danach 3 „Zertifikatsklassen“. Zertifikate der höchsten Klasse **Class-3** werden danach in einem dem **ZertES** gleichwertigen Verfahren erstellt und ausgegeben - unterliegen dabei jedoch **vertragsrechtlich** vereinbarten Regelungen und sind nicht ausschliesslich an natürliche Personen gebunden. Auf diese Weise können über die gesamte Prozesskette auch juristische Personen, Maschinen und automatisierte Prozesse mit Zertifikaten eines hohen, klar definierten und verbindlichen Vertrauens-Niveaus ausgestattet werden.

Für unterschiedliche Schutzbedarfe der Geschäftsprozesse werden entsprechend abgestufte Anforderungen definiert, um einen optimalen und auch wirtschaftlichen Abgleich von Schutz-

[7] CSP, „Certification Service Provider“ oder in deutscher Terminologie gemäss ZertES „Anbieterin von Zertifizierungsdiensten“

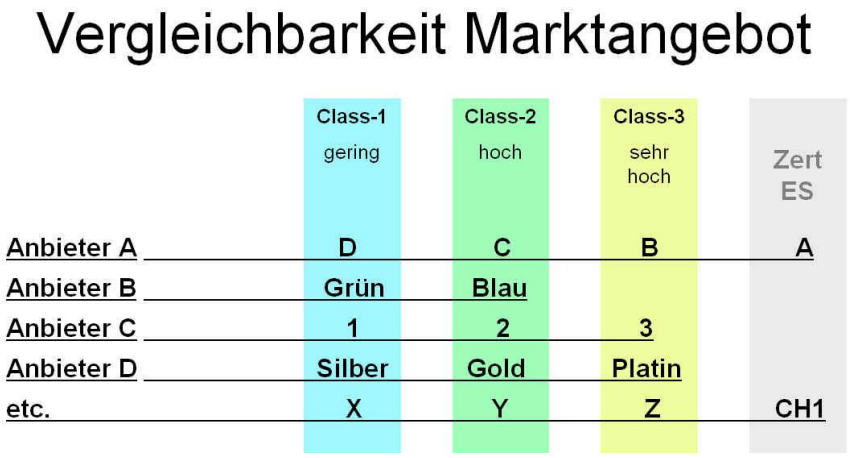
bedarf und kostenrelevanten Massnahmen im Zusammenspiel von eGovernment und Wirtschaft zu unterstützen.



Im Ergebnis entsteht eine Matrix, in der

- die Eigner eines Geschäftsprozesses gemäss Schutzbedarf von Daten und Anwendung die geforderte Zertifikatsklasse vorgeben, unter der eine Online-Interaktion mit Dritten erlaubt werden soll.
- die Anbieterinnen von Zertifizierungsdiensten (CSPs) ihr Angebot positionieren können - ungeachtet der eigenen Marken-Label ihrer Zertifikatsklassen.
  Über zulässige Ausstattungsvarianten erfolgt dabei die marktgerechte Differenzierung der Service-Angebote.

Ein Abgleich des Marktangebotes für Zertifikate anhand der klassifizierten Kriterien fördert die Vergleichbarkeit des Angebotes und unterstützt die Entscheidungsträger in Orientierung und Auswahl im Sinne sicherer und kosteneffizienter elektronischer Geschäftsprozesse.



2.6 Randbedingungen und Abgrenzung

Der Fokus liegt auf der Spezifizierung der Anforderungen, mit denen unterschiedliche Vertrauensniveaus (Verbindliche Zusicherung der im Zertifikat enthaltenen Angaben) realisiert werden können. In welchen Szenarien und mit welcher technischen Funktion diese Zertifikate zum Einsatz kommen, unterliegt dem Befinden der Geschäftsprozess-Eigner und ist - soweit hierdurch nicht das Vertrauensniveau betroffen ist - nicht Gegenstand des vorliegenden eCH-Standards.

2.6.1 Authentifizierung / Autorisierung

Der Standard bezieht sich ausdrücklich und ausschliesslich auf eine durch das Zertifikat bestätigte Identität resp. Identitätsrepräsentation des Inhabers des zugeordneten privaten Signaturschlüssels.

Auch wenn es generell möglich ist, in den Zertifikaten Attribute zu setzen, mit deren Hilfe deren Inhaber für die Nutzung bestimmter Applikationen oder Services autorisiert werden, ist dies aus folgendem Grund **ausdrücklich nicht Gegenstand** dieses Standards:

- Autorisierungsdaten sind keine originäre Eigenschaft des Zertifikatsinhabers, sondern werden diesem von dritter Seite (Geschäftsprozesseigner) zugewiesen.
- Art, Wirksamkeit und Prüfung von Autorisierungsdaten durch die entsprechenden Applikationen unterliegen keinen einheitlichen Standards und stehen somit generell ausserhalb der Definition einer Certificate-Policy und den Prüfmöglichkeiten eines Certificate Service Provider (CSP).
  Eine Haftung für diese Nutzung und darauf abgestellter Informationen kann somit nicht übernommen werden.
- Autorisierungsdaten ändern sich in aller Regel öfter als Authentifizierungsdaten. Zur Vermeidung häufiger Neuausstellung der Zertifikate hat sich in der Praxis die strikte Trennung beider Ebenen bewährt.

Gleichwohl steht es den Eignern der Geschäftsprozesse frei, Zertifikatsangaben, etwa OU-Inhalte (z.B. Abteilungskürzel o.ä.) zur Steuerung von Zugangsberechtigungen für z.B. Web-Applikationen zu nutzen – allerdings erfolgt dies dann ausserhalb der CA-Policy und unterliegt ggf. separaten Vereinbarungen.

2.6.2 ZertES

Die Klasse der *qualifizierten Zertifikate* ist explizit ausgenommen, da hier die gesetzliche Regelungen des ZertES und VZertES greifen, die keines zusätzlichen eCH-Standards bedürfen. Soweit Aspekte der *qualifizierten Zertifikate* in diesem Dokument erwähnt werden, erfolgt dies zur Orientierung hinsichtlich Abgrenzung zu den hier definierten ergänzenden Zertifikatsklassen.

Im ZertES sind – in Übereinstimmung auch mit der EU-Richtlinie – sowohl einfache „elektronische Signaturen“ wie auch „fortgeschrittene elektronische Signaturen“ erwähnt, für deren Erstellung jedoch keine Konkretisierung hinsichtlich der zugrunde liegenden Zertifikate im Gesetz erfolgt. Diese „Lücke“ durch ein ergänzendes Regelwerk zu füllen, und damit diese

Art der Signaturen als eine definierte Ergänzung zu den qualifizierten Zertifikaten in den eGovernment-Geschäftsprozessen einsetzen zu können, ist das Anliegen dieses Standards.

2.7 Zweck

Mit den vorgestellten Zertifikatsklassen Class-1, Class-2 und Class-3 steht ein Raster von elementaren Anforderungsprofilen für digitale Zertifikate zur Verfügung, die in Ergänzung zu den qualifizierten Zertifikaten gemäss ZertES eine wohldefinierte Identifikation der Akteure über die gesamten Prozessketten im eGovernment ermöglichen.

Weiterhin ermöglicht der Abgleich mit den vorgestellten Profilen eine Vergleichbarkeit des Marktangebotes von Certification Service Provider (CSPs) hinsichtlich Funktionalität, Qualität und Gewährleistung und bildet damit eine Grundlage für Markttransparenz und unterstützt damit letztlich auch Wettbewerb.

3 Übersicht der Zertifikatsklassen

	Klasse 1	Klasse 2	Klasse 3	Qualifiziertes Zertifikat
Vertrauensniveau	niedrig	hoch	sehr hoch	sehr hoch
Rechtsbezug	"Elektronische Signatur" ZertES 943.03, 1. Absch. Art. 2, Abs. a.	"Fortgeschrittene elektronische Signatur" ZertES 943.03, 1. Absch. Art. 2, Abs. b.	"Fortgeschrittene elektronische Signatur" ZertES 943.03, 1. Absch. Art. 2, Abs. b.	"Qualifizierte elektronische Signatur" ZertES 943.03, 1. Absch. Art. 2, Abs. c.
Identitätsnachweis	E-Mail Account / Domain-Account / technischer Account	---PERSON--- Personalisierte Dokumente ---ROLLE, GRUPPE, u. MASCHINE--- Auftrag des Verantwortlichen mit Berechtigungsnachweis.	---PERSON--- Hoheitliches Dokument (Reisepass, ID) ---ROLLE, GRUPPE, u. MASCHINE-- Auftrag des Verantwortlichen mit erweitertem Berechtigungsnachweis	---PERSON--- Hoheitliches Dokument (Reisepass, ID) ---ROLLE, GRUPPE, u. MASCHINE-- Nicht anwendbar
Namen	Name kann frei gewählt werden (CN) Name des eMail- oder technischen Accounts wird im Zertifikat aufgenommen.	Natürliche Person gemäss Identitätsnachweis. Das Zertifikat kann auf ein Pseudonym ausgestellt werden. Spezielle Attribute (geschützte Berufsbezeichnungen, akademische- und standesrechtliche Titel, etc.) erfordern gesonderten Berechtigungsnachweis zu deren Verwendung.		
Registrierung	Beliebiger Prozess mit faktischer Verifizierung der o.g. Account-Daten	Sicherer Prozess basierend auf eingereichten Ident-Unterlagen	Sicherer Prozess basierend auf einer persönlichen Antragstellung ggf. auch bei Dritten	Persönliche Antragstellung bei anerkannten Registrierungsstellen.
Archivierung der Antragsdokumente und/oder -daten	Laufzeit plus 2 Jahre	Laufzeit plus 5 Jahre (Verjährungsfrist gem. OR)	Laufzeit plus 11 Jahre	
Gültigkeit der Registrierung	wie Laufzeit Zertifikat	Maximal 6 Jahre.		
Laufzeit Zertifikat	Gemäss Anbieter-Policy			Keine Angabe

	Klasse 1	Klasse 2	Klasse 3	Qualifiziertes Zertifikat
Security-Token[8]	Soft- / Hardware	Soft- / Hardware	Hardware evaluiert gem. - FIPS 140-1/140-2 Level 2 oder - BAKOM TAV	Hardwaretoken gemäss BAKOM TAV SR 943.032.1
Keymanagement für Security-Token	Key-Backup und –Recovery seitens des CSP für: - Signaturschlüssel: DARF NICHT erfolgen - Verschlüsselungsschlüssel: KANN in sicheren und dokumentierten Infrastrukturen und Prozessen erfolgen			Hardwaretoken gemäss BAKOM TAV SR 943.032.1
Anforderungen an CA (Betrieb, Personal, Prozesse)	Dokumentiertes Betriebs- und Sicherheitskonzept	Dokumentiertes Betriebs- und Sicherheitskonzept; Zugangskontrolle zu CA-Systemen u. Backups etc.; jährl. Audit durch interne Verantwortliche.	Dokumentiertes Betriebs- und Sicherheitskonzept; Zugangskontrolle zu CA-Systemen u. Backups etc.; jährl. Audit durch ausgewiesen qualifizierte Revision (intern / extern).	Gemäss: ETSI TS 101 456, Kap. 6.1, 7.1, 7.4, 7.5, 8.1; jährliche Audits. Details siehe BAKOM TAV SR 943.032.1, Kap. 3.2 Organisation und operative Grundsätze
Anbieter-Policy (CP, CPS)	Aussagen gemäss RFC-3647 u.a. zu zugesicherten Eigenschaften, Leistungs- und Haftungsumfang			Haftung: 2 Mio Fr pro Versicherungsfall
Erlaubte ZertifikatsInhaber (Subject)	Keine Vorgaben	- natürliche Personen - juristische Personen, einfache Gesellschaften und Organisationen - Gruppen, Rollen - Maschinen (SSL, IPsec, etc.)		- natürliche Personen (Client-Zertifikate)
Einsatz	Alle Zwecke zugelassen			- Signatur elektronischer Dokumente (Willenserklärung)
Widerrufs-Informationen (per CRL und/oder OCSP)	MUSS publiziert werden	MUSS publiziert werden; mindestens tägliche Aktualisierung		MUSS per CRL angeboten werden; mindestens tägliche Aktualisierung.

[8] Software- oder Hardwaremedium zur Speicherung des/der privaten Schlüssel eines Zertifikates (Bsp. f. Software: Microsoft Certificate Manager im Windows OS; Bsp. f. Hardware: SmartCard, USB-Token, Hardware Security Module)

4 Anforderungsprofile

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

Die Abstufung in drei derartige Klassen korrespondiert einerseits mit Geschäftsprozessen unterschiedlichen Schutzbedarfes und folgt andererseits den am Markt etablierten Schemata.

Als technische Grundlagen gelten X.509v3 und PKIX.

4.1 Class-1

Zertifikate dieser Klasse dienen in aller Regel Geschäftsprozessen, bei denen die Authentizität der Teilnehmer insgesamt unkritisch oder auf andere Weise sichergestellt ist.

Eine Klassifizierung dieser "low level" Zertifikatsklasse im eCH Standard liegt in der Anforderung begründet, dass - wenn ein CSP derartige Zertifikate am Markt anbieten möchte - dies unter definierten Regularien erfolgen soll.

4.1.1 Registrierung

4.1.1.1 Identitätsnachweis

Als Identitätsnachweis genügt ein technischer Account, etwa ein E-Mail-Konto oder eine Domain-Registrierung. Der Name des eMail- oder technischen Accounts MUSS Bestandteil des Zertifikates sein.

Class-1 Zertifikate bestätigen somit die Existenz eines solchen Accounts zum Zeitpunkt der Ausstellung. Eine Zuordnung des Zertifikates zu einer Entität (natürliche oder juristische Person, Organisation etc.) kann daraus nicht abgeleitet werden.

4.1.1.2 Namen

Namen (CN, SAN) können frei gewählt werden, sofern sie nicht sittenwidrig sind oder gegen die Rechte Dritter verstossen. Die Benutzung standesrechtlich geschützter Titel und Berufsbezeichnungen ist wegen fehlender Nachweise unzulässig und DARF NICHT erfolgen.

Feldinhalte für Organisation (O:) und Organisationseinheit (OU:) MÜSSEN durch die CA gesetzt werden.

4.1.1.3 Registrierungsprozess

Ein beliebiger Prozess mit faktischer Verifizierung der o.g. Account-Daten (z.B. Mail-Zusendung von Zertifikat, Online-Abrufcode oder direkte Ausstellung auf einen Domain-Account oder Verzeichnis-Eintrag).

Beispiel
a) Mail-Zusendung des ausgestellten Zertifikates;
b) Mail-Zusendung eines Online-Abrufcodes;
c) direkte Ausstellung eines Zertifikates für einen Domain-Account oder Verzeichnis-Eintrag.

4.1.2 Gültigkeit der Registrierung

Registrierungsdaten werden nicht für Zertifikatserneuerungen vorgehalten und gelten nur für die einmalige Ausstellung des beantragten Zertifikates.

4.1.3 Securitytoken

Es können sowohl Software- als auch Hardwaretoken herausgegeben werden. Enthält ein vom CSP geliefertes Token ebenfalls den geheimen Schlüssel für das Zertifikat, MUSS ein geeigneter Zugriffschutz (Passwort, PIN) für den Transportweg die unberechtigte Nutzung zuverlässig verhindern.

4.1.4 Ausstellung und Übergabe

Der CSP hat durch technische und organisatorische Massnahmen sicherzustellen, dass geheime Schlüssel ausgestellter Zertifikate während Produktion und Auslieferung nicht durch Dritte einsehbar oder nutzbar werden. Nach Übergabe des Zertifikatstokens geht die Verantwortung für die vertrauliche Verwahrung von Token und PIN auf den Zertifikatsinhaber über.

4.1.5 Widerruf der Zertifikate

Informationen über widerrufene (gesperrte) Zertifikate müssen durch den CSP aktualisiert und veröffentlicht werden.

4.1.6 CA-Betrieb

Für Technik und Prozesse des CA-Betriebs MUSS der CSP einfache Dokumentationen vorhalten. Eine Archivierung der CA-Logfiles MUSS für Zwecke der Nachvollziehbarkeit über einen Zeitraum von 2 Jahren nach Ausstellung gesichert werden.

4.1.7 Anbieter Policy (CP / CPS)

Als rechtsverbindliche Rahmenvereinbarung zwischen CSP, Zertifikatsinhaber und einem auf das Zertifikat vertrauendem Dritten MUSS eine Anbieterpolicy des CSP publiziert werden, in der Leistungsumfang und zugesicherte Eigenschaften seiner Produkte und Services definiert sind. Zur Vergleichbarkeit und Transparenz des Angebotes SOLL diese Policy gemäss RFC-3647 strukturiert sein.

4.2 Class-2

In den Geschäfts- und Verwaltungsprozessen der realen Welt haben sich auch kulturell bestimmte Verfahren etabliert und über viele Jahrzehnte bewährt, die gleichwohl und bekanntermassen keine letztendliche Sicherheit über Identität und Berechtigung der Beteiligten oder die Integrität der Daten bieten. Als Beispiele seien hier genannt: Warenbestellungen per Telefon oder Fax; schriftliche Bestellungen oder Vereinbarungen mit Unterschriften, die vom Empfänger nicht eindeutig entsprechend berechtigten Personen zugeordnet werden können, etc..

Auch im eGovernment besteht die gängige Praxis, Auskünfte, Vereinbarungen und Anträge bis zu einem gewissen Grad an Sensibilität teils telefonisch oder aber schriftlich per Post, Fax oder eMail abzuwickeln – ohne letztlich prozessfeste Prüfung von Unterschrift oder Berechtigung.

Eine digitale Entsprechung dieser im Alltag verankerten Geschäftspraxis wird mit Zertifikaten gemäss **Class-2** definiert.

4.2.1 Registrierung

4.2.1.1 Identitätsnachweis

a) Natürliche Personen

Vorlage von personalisierten Dokumenten Dritter mit Foto u. Angaben zu Geschäfts- oder Dienstverhältnis; z.B.

- Führerausweis
- Gesundheitskarte
- Firmen- / Dienstausweis
- Halbtax-Abo oder GA

b) Juristische Personen, Organisationen, Rollen, Gruppen, Prozesse

Auftrag des wirtschaftlich oder organisatorisch Verantwortlichen unter Nachweis seiner Berechtigung und Identität (s.o.)

Beispiel
Zertifikatsbestellung durch Abteilungsleiter auf Firmenpapier mit zweiter Unterschrift; zur persönlichen Identifizierung des Auftraggebers gelten die oben unter a) aufgeführten Nachweise.

c) Maschinen, Hostnamen, öffentliche IP-Adressen

Zertifikate für Webserver, Router, etc. werden durch die wirtschaftlich oder organisatorisch Verantwortlichen unter Nachweis ihrer Berechtigung und Identität (s.o.) in Auftrag gegeben. Die Berechtigung zur Beauftragung von Zertifikaten für bestimmte Domains oder öffentliche IP-Nummern wird nachgewiesen über Auszüge der entsprechenden Register.

4.2.1.2 Namen

Sämtliche Eigennamen natürlicher Personen, die im Zertifikat aufgeführt werden, MÜSSEN mit den Angaben der vorgelegten ID-Dokumente zur Person übereinstimmen.

Für Pseudonyme natürlicher Personen sowie Nicht-Personennamen (Maschinen, Rollen, ...) MUSS eine Hinterlegung der tatsächlichen Namen der beantragenden Person so in den Registrierungsdaten erfolgen, dass eine Auflösung des Pseudonyms auf richterliche Anordnung möglich ist.

Eine Weitergabe von Realdaten zu Pseudonymen für andere Zwecke DARF NICHT erfolgen.

Die berechtigte Verwendung von Firmen- oder Organisationsbezeichnungen im Zertifikat MUSS durch anerkannte Registerauszüge (wie Handelsregister) oder durch Belege von vergleichbaren Bestätigungsstellen belegt werden.

Sollen standesrechtlich geschützte Berufs- oder akademische Titelbezeichnungen in das Zertifikat aufgenommen werden, MUSS die Berechtigung zur Verwendung in geeigneter

Weise (Verleihungsurkunde oder Bestätigung der Standesorganisation) nachgewiesen werden.

4.2.1.3 Registrierungsprozess

Der technische und organisatorische Ablauf liegt in der Gesamtverantwortung der Anbieterin von Zertifizierungsdiensten. Teilbereiche können auf vertraglich geregelter Grundlage an andere Stellen ausgelagert werden.

Die Übermittlung von Antrags-, Identitäts- und Berechtigungsunterlagen (Registrierungsdaten) kann persönlich, per Fax oder auch elektronisch erfolgen. Für die Übernahme elektronischer geführter Datenbestände Dritter (organisatorische Registrierung) MUSS eine Dokumentation der Prozessabläufe und Verantwortlichkeiten erstellt und vertraglich mit dem Dritten vereinbart werden.

In und mit den Registrierungsdaten MÜSSEN Kopien oder Referenzen auf die vorgelegten ID-Dokumente archiviert werden, um die eindeutige und nachvollziehbare Zuordnung der digitalen Identität zur verantwortlichen natürlichen Person zu ermöglichen.

Die Archivierungsfrist für Registrierungsdaten beträgt: Laufzeit des Zertifikates plus 5 Jahre gemäss Verjährungsfrist OR.

4.2.2 Gültigkeit der Registrierung

Die zum Zeitpunkt der Zertifikatsausstellung gültigen Dokumente gelten als Grundlage der Registrierung für die gesamte Laufzeit des Zertifikates. Bei unveränderten Registrierungsdaten KÖNNEN auf dieser Grundlage Zertifikatserneuerungen durchgeführt und weitere Zertifikate ausgestellt werden – limitiert auf einen Gesamtzeitraum von 6 Jahren. Mit Ablauf dieser Gültigkeitsfrist für Registrierungsdaten MUSS eine erneute Registrierung unter Vorlage aller Unterlagen erfolgen.

4.2.3 Zertifikatstoken

Für **Class-2** Zertifikate können sowohl Software- als auch Hardwaretoken herausgegeben werden. Enthält ein Token ebenfalls den geheimen Schlüssel für das Zertifikat, MUSS ein geeigneter Zugriffschutz (Passwort, PIN) die unberechtigte Nutzung zuverlässig verhindern.

4.2.4 Ausstellung und Übergabe

Die Anbieterin von Zertifizierungsdiensten MUSS durch technische und organisatorische Massnahmen sicherstellen, dass geheime Schlüssel ausgestellter Zertifikate während Produktion und Auslieferung nicht durch Dritte einsehbar oder nutzbar werden. Nach Übergabe des Zertifikatstokens geht die Verantwortung für die vertrauliche Verwahrung von Token und PIN auf den Zertifikatsinhaber über.

4.2.5 Widerruf der Zertifikate

Informationen über widerrufene (gesperrte) Zertifikate müssen täglich aktualisiert und veröffentlicht werden.

4.2.6 CA-Betrieb

Ein dokumentiertes Betriebs- und Sicherheitskonzept einschliesslich Zugangskontrollen zu CA-Systemen und weiteren Infrastruktur-Komponenten MUSS als nachvollziehbare Betriebsgrundlage für den PKI-Service geführt werden. Ein jährliches Audit (intern oder extern) prüft die Einhaltung aller definierten Anforderungen für technische Komponenten, Personal und Prozesse.

4.2.7 Anbieter Policy (CP / CPS)

Als rechtsverbindliche Rahmenvereinbarung zwischen CSP, Zertifikatsinhaber und einem auf das Zertifikat vertrauendem Dritten MUSS eine Anbieterpolicy des CSP publiziert werden, in der Leistungsumfang und zugesicherte Eigenschaften seiner Produkte und Services definiert sind. Zur Vergleichbarkeit und Transparenz des Angebotes SOLL diese Policy gemäss RFC-3647 strukturiert sein.

4.3 Class-3

Für Geschäfts- oder Verwaltungsprozesse mit hohen Anforderungen an die eindeutige Identifizierung der Beteiligten (Personen, Organisationen, Programmcode, Maschinen, ...) wurde ein entsprechendes Profil mit hohen Anforderungen definiert. Generell entsprechen diese Anforderungen denjenigen der qualifizierten Zertifikate gemäss ZertES, ohne jedoch auf die Ausstellung an ausschliesslich natürliche Personen und den eng gefassten Rechtsrahmen des ZertES (Haftung, Beweislastumkehr, etc.) limitiert zu sein.

Mit Zertifikaten nach **Class-3** lassen sich vielseitige und dem qualifizierten Niveau vergleichbar sichere Geschäftsprozesse etablieren.

4.3.1 Registrierung

4.3.1.1 Identitätsnachweis

a) Natürliche Personen

Vorlage eines hoheitlichen Dokumentes mit Foto bei der initialen Registrierung; z.B.

- Reisepass
- Amtlicher Identitätsausweis
- Ausländerausweis

Werden elektronische Datenbestände als Registrierungsdaten übernommen, MUSS sichergestellt und nachvollziehbar dokumentiert sein, dass die elektronischen Daten einer Person auf der Grundlage einer Identitätsprüfung im o.g. Sinne entstanden sind.

b) Juristische Personen, Organisationen, Rollen, Gruppen, Prozesse

Die Beauftragung eines unpersönlichen Zertifikates im Namen einer Firma oder Organisation MUSS durch einen wirtschaftlich oder organisatorisch Verantwortlichen unter Nachweis seiner Zeichnungsberechtigung gemäss eines anerkannten Registerauszuges erfolgen. Für Firmen ist dies ein Auszug des Handelsregisters. Ämter und Behörden bestätigen die Berechtigung des Auftraggebers in der Regel durch ein Dienstsiegel oder vergleichbare Nach-

weise. Für andere Organisationen und Vereine sind analoge Nachweise zu erbringen, die allgemein anerkannt sind.

Der Identitätsnachweis der beauftragenden Person erfolgt gemäss den o.g. Anforderungen für natürliche Personen.
In der Praxis werden derartige Zertifikatsaufträge eher selten durch die Zeichnungsberechtigten erteilt, sondern meist durch die IT-Verantwortlichen oder andere Funktionsträger ohne HR-Zeichnungsberechtigung. Um die Nachweiskette jedoch konsistent zu halten, MUSS in diesem Falle ausgehend vom HR-Auszug der Zeichnungsberechtigte den IT-Verantwortlichen schriftlich zur Auftragserteilung autorisieren. Die konkrete Bestellung erfolgt dann durch den IT-Verantwortlichen unter Nachweis seiner Identität gemäss den o.g. Regeln. Die Dokumente der gesamten Nachweiskette sind der Bestellung beizufügen.

> Beispiel-1
> Zertifikatsbestellung durch Abteilungsleiter auf Firmenpapier mit zweiter Unterschrift des Zeichnungsberechtigtem gemäss HR-Auszug. Ein HR-Auszug ist dem Auftrag beizufügen. Zur persönlichen Identifizierung des Auftraggebers gelten die oben unter a) aufgeführten Nachweise.
>
> Beispiel-2
> Zertifikatsbestellung durch IT-Leiter durch Übermittlung digital signierter Datensätze. Dem CSP liegt bereits die vom Zeichnungsberechtigten ausgestellte Bevollmächtigung des IT-Leiters vor. Ein HR-Auszug liegt bereits vor. Zur persönlichen Identifizierung des IT-Leiters liegen die gemäss a) geltenden Nachweise bereits vor.

c) Maschinen, Hostnamen, öffentliche IP-Adressen

Zertifikate für Webserver, Router, etc. werden durch die wirtschaftlich oder organisatorisch Verantwortlichen unter Nachweis seiner Berechtigung und Identität (s.o.) in Auftrag gegeben. Die Berechtigung zur Beauftragung von Zertifikaten für bestimmte Domains oder IP-Nummern wird in der Regel nachgewiesen über Auszüge der entsprechenden Register.

Ergänzend zu den geforderten Nachweisen aus b) sind für öffentlich zugängliche Systeme geeignete Nachweise zu erbringen, dass der Auftraggeber berechtigt über diese verfügen darf.

4.3.1.2 Namen

Sämtliche Eigennamen natürlicher Personen, die im Zertifikat aufgeführt werden, MÜSSEN mit den Angaben der vorgelegten ID-Dokumente zur Person übereinstimmen.

Für Pseudonyme natürlicher Personen sowie Nicht-Personennamen (Maschinen, Rollen, ...) MUSS eine Hinterlegung der tatsächlichen Namen der beantragenden Person so in den Registrierungsdaten erfolgen, dass eine Auflösung des Pseudonyms auf richterliche Anordnung möglich ist. Eine Weitergabe für andere Zwecke DARF NICHT erfolgen.

Die berechtigte Verwendung von Firmen- oder Organisationsbezeichnungen im Zertifikat MUSS durch anerkannte Registerauszüge (in der Regel: Handels- oder auch Vereinsregister) oder vergleichbare Bestätigungsstellen belegt werden.

Sollen standesrechtlich geschützte Berufs- oder akademische Titelbezeichnungen in das Zertifikat aufgenommen werden, MUSS die Berechtigung zur Verwendung durch geeignete Nachweise (Verleihungsurkunde oder Bestätigung der Standesorganisation) beigefügt werden.

4.3.1.3 Registrierungsprozess

Der technische und organisatorische Ablauf liegt in der Gesamtverantwortung der Anbieterin von Zertifizierungsdiensten. Teilbereiche können auf vertraglich geregelter Grundlage an andere Stellen ausgelagert werden.

Der Registrations-Prozess MUSS auf einer persönlichen Antragstellung - gegebenenfalls auch bei Dritten - beruhen.

Die Übermittlung von Antrags-, Identitäts- und Berechtigungsunterlagen (Registrierungsdaten) kann erfolgen über

- Persönliche Übergabe
- Briefpost
- Digital signierte Datensätze Dritter

Für die Übernahme elektronischer geführter Datenbestände Dritter (organisatorische Registrierung) MUSS eine Dokumentation der Prozessabläufe und Verantwortlichkeiten erstellt und vertraglich mit dem Dritten vereinbart werden.

Elektronisch übermittelte Registrierungsdaten MÜSSEN durch den Vertragspartner digital signiert werden mit einem Zertifikat mindestens der Güteklasse **Class-3**.

In und mit den Registrierungsdaten MÜSSEN Kopien oder Referenzen auf die vorgelegten ID-Dokumente archiviert werden, um die eindeutige und nachvollziehbare Zuordnung der digitalen Identität zur verantwortlichen natürlichen Person zu ermöglichen.

Die Archivierungsfrist für Registrierungsdaten beträgt: Laufzeit des Zertifikates plus 11 Jahre analog den Bestimmungen des ZertES.

4.3.2 Gültigkeit der Registrierung

Die zum Zeitpunkt der Zertifikatsausstellung gültigen Dokumente gelten als Grundlage der Registrierung für die gesamte Laufzeit des Zertifikates. Bei unveränderten Registrierungsdaten KÖNNEN auf dieser Grundlage Zertifikatserneuerungen durchgeführt und weitere Zertifikate ausgestellt werden – limitiert auf einen Gesamtzeitraum von 6 Jahren. Mit Ablauf dieser Gültigkeitsfrist für Registrierungsdaten MUSS eine erneute Registrierung unter Vorlage aller Unterlagen erfolgen.

4.3.3 Zertifikatstoken

Für **Class-3** Zertifikate MÜSSEN Hardwaretoken herausgegeben werden, die den enthaltenen geheimen Schlüssel mit Passwort oder PIN vor unberechtigte Nutzung zuverlässig schützen.

Die Hardwaretoken MÜSSEN mindestens den Anforderungen gemäss FIPS 140-1/140-2 Level 2 genügen. Eine gesicherte Grundlage für die Auswahl geeigneter Hardwaretoken bieten ebenfalls die TAV zu ZertES des BAKOM.

4.3.4 Ausstellung und Übergabe

Die Anbieterin von Zertifizierungsdiensten MUSS durch technische und organisatorische Massnahmen sicherstellen, dass geheime Schlüssel ausgestellter Zertifikate während Produktion und Auslieferung nicht durch Dritte einsehbar oder nutzbar werden.

Die Generierung des Schlüsselmaterials MUSS entweder in den Zertifikatstoken selbst oder in vergleichbar evaluierten Hardware-Devices erfolgen.

Die Übergabe des Zertifikatstokens sowie der zugehörigen PIN SOLL durch persönliche Übergabe oder via getrennter Versandwege, die eine protokollierte Übernahme durch den Zertifikatsinhaber ermöglichen.

Nach Übergabe des Zertifikatstokens geht die Verantwortung für die vertrauliche Verwahrung von Token und PIN auf den Zertifikatsinhaber über.

4.3.5 Widerruf der Zertifikate

Die Information über widerrufene (gesperrte) Zertifikate MUSS mindestens täglich aktualisiert und veröffentlicht werden.

4.3.6 CA-Betrieb

Ein dokumentiertes Betriebs- und Sicherheitskonzept einschliesslich Zugangskontrolle zu CA-Systemen und weiteren Infrastruktur-Komponenten MUSS als nachvollziehbare Betriebsgrundlage für den PKI-Service erstellt, dokumentiert und implementiert werden. Ein jährliches Audit durch ausgewiesen qualifizierte IT-Revisoren (intern oder extern) MUSS die Einhaltung aller definierten Anforderungen für technische Komponenten, Personal und Prozesse prüfen, die Ergebnisse dokumentieren und archivieren.

Eine Archivierung von CA-Logfiles sowie der Protokolle von Zutrittssystemen MUSS erfolgen. Die Archivierungsfrist entspricht derjenigen für Registrierungsdaten.

4.3.7 Anbieter Policy (CP / CPS)

Als rechtsverbindliche Rahmenvereinbarung zwischen CSP, Zertifikatsinhaber und einem auf das Zertifikat vertrauendem Dritten MUSS eine Anbieterpolicy des CSP publiziert werden, in der Leistungsumfang und zugesicherte Eigenschaften seiner Produkte und Services definiert sind. Zur Vergleichbarkeit und Transparenz des Angebotes SOLL diese Policy gemäss RFC-3647 strukturiert sein.

4.4 Testzertifikate

Aus folgenden Gründen wurde ausdrücklich keine Klasse für Testzertifikate definiert:

- Zertifikate zu Testzwecken werden grundsätzlich in allen PKI-fähigen Anwendungen und Prozessketten benötigt, um z.B. in der Einführungsphase die Funktionalität der Implementierung sowie die organisatorischen Prozesse zu prüfen.
- Testzertifikate dürfen sich in Struktur und Inhalt nicht von produktiven Zertifikaten unterscheiden - anderenfalls könnten sie ihre Testfunktion nicht erfüllen.

- Wenn eine systematische Ausgabe von Zertifikaten für Testzwecke eingerichtet wird, SOLL eine Unterscheidung von Test- und Produktionszertifikaten nicht auf Zertifikats- sondern auf CA-Ebene erfolgen.
  Für die Ausstellung von Testzertifikaten sind entsprechende TEST-CAs (mit separater TEST-RootCA) einzurichten, die ihren Testcharakter DEUTLICH in den CA-Namen hinterlegt haben. Falls unterstützt, SOLL auch der Policy-Link auf eine entsprechende Test-Policy verweisen. Weiterhin hat es sich als gute Praxis erwiesen, im Subject dieser CA-Zertifikate sowie der von ihnen ausgestellten Client-Zertifikate das Wort "TEST" aufzunehmen.

4.5 Konkrete Ausprägungen (informativ)

Die nachfolgenden Ausführungen bezüglich Zertifikatsformaten, die entweder durch gesetzliche Regularien (ElDI-V, SuisseID) oder Marktangebote (EV-SSL, …) definiert wurden, sind nicht Bestandteil des vorliegenden eCH-Standards, sondern haben rein informativen Charakter und dienen der Orientierung bei der Einordnung dieser Zertifikatsformate in die drei hier definierten Zertifikatsklassen.

Je nach Bedarf wird die Liste dieser Beispiele mit den nächsten Releases des eCH-0048 weiter ergänzt und aktualisiert.

4.5.1 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 werden elektronische Signaturen verwendet. Da Rechnungen normalerweise von Organisationen bzw. juristischen Personen ausgestellt werden, ist es sinnvoll, dass das für die Signatur verwendete Zertifikat auf das entsprechende Wirtschaftssubjekt ausgestellt wird und nicht auf eine natürliche Person. Zu diesem Zweck definiert die ElDI-V, beziehungsweise definieren die dazugehörigen „Technischen und administrativen Vorschriften“ (TAV) Zertifikate für die entsprechenden fortgeschrittenen Signaturen. Diese Zertifikate können z.B. auf juristischen Personen oder einfache Gesellschaften ausgestellt werden.

Die Anforderungen an die Registrierung und an die zu verwendende Technik sind hoch und weitgehend mit denjenigen für qualifizierte Zertifikate vergleichbar, bzw. identisch. Sie liegen deshalb innerhalb der hier definierten Anforderungen an **Class-3** Zertifikate.

Weitere Erläuterungen zum Thema lassen sich unter dem Link
http://www.estv.admin.ch/mwst/themen/00159/ finden.

4.5.2 SuisseID Authentisierungs-Zertifikat

Die SuisseID ist ein standardisierter elektronischer Identitätsnachweis der Schweiz, der

- sowohl eine qualifizierte elektronische Signatur
- als auch eine Zertifikats-basierte Authentisierung (Z.B. für Web-Login)

ermöglicht.

Für diese zwei Anwendungen/"Use Cases" enthält deshalb ein entsprechender Zertifikatsträger bzw. Security-Token zwei Schlüsselpaare und zugehörige Zertifikate. Neben dem qualifizierten Zertifikat befindet sich darauf ein Authentisierungs-Zertifikat, das „SuisseID IAC" (Identification and Authentication Certificate).

Dieses SuisseID IAC stellt kein qualifiziertes Zertifikat gemäss ZertES dar. Es wird aber zusammen mit einem solchen ausgegeben und der entsprechende private Schlüssel wird auf demselben Zertifikatsträger (Security-Token) gespeichert. Deshalb entspricht das SuisseID IAC einem **Class-3** Zertifikat.

Weitere Information zur SuisseID und dem SuisseID IAC befinden sich auf der SuisseID-Website (http://www.suisseid.ch/) und in den SuisseID-Spezifikationen (www.suisseid.ch/unternehmen/technik).

4.5.3 Extended-Validation-SSL-Zertifikate

Für Onlineprozesse mit hohem Schutzbedarf (insbesondere Online-Banking, etc.) wurde die Produktkategorie der EV-SSL-Zertifikate in Kooperation von Zertifizierungsdienstleistern und Browser-Herstellern definiert (http://cabforum.org).

Wesentliches Merkmal ist das gemeinsame und verbindliche Anforderungsprofil für den Registrierungsprozess (http://cabforum.org/EV_Certificate_Guidelines.pdf) sowie Art und Umfang der Validierung der eingereichten Registrierungsdaten. Hierdurch soll sichergestellt werden, dass die ausgegebenen Zertifikatsinhalte eindeutig und unzweifelhaft den juristisch- und wirtschaftlich Berechtigten zugeordnet werden können.

Zur vereinfachten Wahrnehmung dieses Vertrauensniveaus durch die Benutzer wurde von den Browser-Herstellern die Anzeige eines „Grünen Balkens" mit Name und Logo des Zertifikatsinhabers in der Browser-Software ergänzt. Diese Anzeige wird ausgelöst durch den Eintrag definierter Objektbezeichner (Object Identifier, OID), welche eine EV-SSL-konforme CPS bezeichnen.

Aus technischer Sicht handelt es sich um standardkonforme X.509 Zertifikate, deren extensions durch die hierzu kompatiblen Browser in definierter Weise ausgewertet werden und somit eine Produkt- und Servicedifferenzierung der Anbieter ermöglicht.

Hinsichtlich des eCH-0048 entsprechen diese Zertifikate dem Vertrauensniveau **Class-2**, sofern es sich um ein Software-Token handelt, respektive um ein **Class-3** bei Verwendung eines Hardware-Token.

5 Schlussbemerkung

Festzuhalten bleibt, dass auch unter Class-3 oder ZertES - ebenso wie in der realen Welt - keine absolute Sicherheit gewährt werden kann für die zertifizierten Identitätsdaten. Letztlich können durch hinreichend gut gefälschte Identitätsdokumente krimineller Antragsteller, fehlerhafte oder lückenhafte Prozesse in der Registrierung sowie schlecht geschulte oder kriminelle Mitarbeiter im RA- oder CA-Betrieb gefälschte digitale Identitäten entstehen.

Die Qualitätsklassen digitaler Identitäten sind dabei weniger von den eingesetzten kryptographischen Verfahren und Algorithmen abhängig, als vielmehr von einer durchgängig auf Sicherheit und Nachvollziehbarkeit ausgerichteten organisatorischen und technischen Prozesskette

- Auftragserteilung / Antragsdaten
- Identitätsprüfung / Protokollierung / Archivierung
- Datenübermittlung zur CA
- Operating und Schnittstellen der CA-Infrastruktur
- Zustellung resp. Versandlogistik für Zertifikate, Token, PIN
- Aktualität und Verfügbarkeit von Sperrinformationen

Ziel dieser eCH-Standardisierung ist somit auch über die Vereinheitlichung der Anforderungen und Transparenz der Prozesse die Sicherheit der Ausstellungsverfahren zu unterstützen.

6 Haftungsausschluss/Hinweise auf Rechte Dritter

eCH-Standards, welche der Verein **eCH** dem Benutzer zur unentgeltlichen Nutzung zur Verfügung stellt, oder welche **eCH** referenziert, 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 mittels spezieller, schriftlicher Vereinbarung, 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: http://www.bakom.ch/themen/internet/00467/index.html?lang=de)

SR 943.03, ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (19.12.2003, in Kraft seit 1.1.2005)
SR 942.032 VZertES	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (3.12.2004)
SR 943.032.1 TAV Version 3	„Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur" (BAKOM 13.11.2006, in Kraft seit 1.12.2006)
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 (11. Dezember 2009)
SR 641.201.511.1	Verordnung der ESTV über Zertifizierungsdienste im Bereich der ElDI-V (14. Dezember 2009)
SR 641.201.511.1 Anhang / TAV ElDI-V	Technische und administrative Vorschriften für Zertifizierungsdienste im Bereich der ElDI-V im Zusammenhang mit der Ausstellung von Zertifikaten basierend auf fortgeschrittenen Signaturen (Ausgabe 2, 4. Dezember 2009) http://www.estv.admin.ch/mwst/themen/00159/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDdIB_fmym162epYbg2c_JjKbNoKSn6A--
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)

EU Richtlinie

1999/93 EG	RICHTLINIE 1999/93/EU DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen http://europa.eu.int/scadplus/leg/de/lvb/124118.htm

ETSI Publikationen

ETSI TS 101 456	Policy requirements for certification authorities issuing qualified certificates
ETSI TS 101 862	Qualified Certificate Profile
ETSI TS 101 733	CMS Advanced Electronic Signatures (CAdES)
ETSI TS 101 903	XML Advanced Electronic Signatures (XAdES)
ETSI TR 102 040	International Harmonization of Policy Requirements for CAs issuing Certificates
ETSI TS 102 042	Policy requirements for certification authorities issuing public key certificates
ETSI TR 102 044	Requirements for role and attribute certificates

ETSI TR 102 045	Signature policy for extended business model
ETSI TS 102 176-1	Algorithms and Parameters for Secure Electronic Signatures;Part 1: Hash functions and asymmetric algorithms

CEN Workshop Agreements

CWA 14169	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	Information technology – Security techniques. Evaluation criteria for IT security

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 Standards

FIPS 140-1 / FIPS 140-2	Security requirements for Cryptographic Modules

pkix RFCs

Siehe auch: http://www.ietf.org/html.charters/pkix-charter.html

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

SuisseID Spezifikation

SuisseID	SuisseID Specification - Digital Certificates and Core Infrastructure Services (Version 1.3, 10. Juni 2010) http://www.suisseid.ch/unternehmen/technik/

Anhang B – Mitarbeit & Überprüfung

Mitarbeit eCH Fachgruppe Sicherheit

Anhang C – Abkürzungen

BIT	Bundesamt für Informatik und Telekommunikation (http://www.bit.admin.ch/)
CA	Certificate Authority – Zertifizierungsbehörde
CEN/ISSS	Comité Européen de Normalisation / Information Society Standardization System (http://www.cenorm.be/isss) – Standardisierungs-Initiative für IKT des Europäischen Komitees für Normung
CN	Common Name – X.509 Zertifikatsfeld für den Namen des Zertifikatsinhabers
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.
EESC	E-Europe SmartCard Initiative (http://www.eeurope-smartcards.org/); hier insbesondere die Arbeitsgruppen: • TB1 Electronic Identity (e-ID) • TB5 E&M Payments with SmartCards
EESSI	European Electronic Signature Standardization Initiative
EFD	Eidgenössisches Finanzdepartement
ElDI-V	Verordnung des EFD über elektronische Daten und Informationen
ETSI	European Telecommunications Standards Institute (http://www.etsi.org/)
EV-SSL	Extendend Validation-Secure Socket Layer (Zertifikat)
FIPS	Federal Information Processing Standards – 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 Entschlüsse-

	lung, 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
IETF	Internet Engineering Task Force
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
RFC	Request for Comment (Art Internetstandard)
SAN	Subject Alternate 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“
URL	Uniform Ressource Locator – Eindeutige Adresse einer Information im Internet
VZertES	Verordnung zum Bundesgesetz über die elektronische Signatur
ZertES	Bundesgesetz über die elektronische Signatur

Anhang D – Änderungen gegenüber Version 1.00

Kap. 2.1	Neu eingefügt:	Verwendung normierter Schlüsselworte zur Kategorisierung von Anforderungen. In diesem Kapitel wird RFC2119 referenziert und die Schlüsselworte eingeführt. Im gesamten Dokument wurden sämtliche Anforderungen unter Verwendung dieser Schlüsselworte umformuliert.
Kap 2.2	Neu eingefügt	Dokumentenhistorie
Kap 2.1	=> Kap 2.5	Ausführungen über Vertrauensniveau wurden in ein eigenes Unterkapitel 2.5 verschoben – nachdem in 2.3 Zweck und 2.4 Zielsetzung des Standards ausgeführt ist. Aus den 3 identifizier-

		ten Vertrauensniveaus werden sodann die 3 Zertifikatsklassen entwickelt.
Kap 4.1.3	Umbenennung	„Client-Zertifikatstoken“ in „Securitytoken“
Kap 4.2.3	Umbenennung	„Client-Zertifikatstoken“ in „Securitytoken“
Kap 4.3.3	Umbenennung	„Client-Zertifikatstoken“ in „Securitytoken“
Kap 4.5	Neu eingefügt	Kapitel „Konktrete Ausprägungen (informativ); hier werden konkret am Markt eingeführte Zertifikatsprodukte kurz beschrieben und gemäss der im vorliegenden Standard etablierten Klassifikation eingeordnet.
Kap 4.5.1	Neu eingefügt	Kapitel „ElDI-V“; siehe Kap 4.5
Kap 4.5.2	Neu eingefügt	Kapitel „SuisseID Authentisierungs-Zertifikat“; siehe Kap 4.5
Kap 4.5.3	Neu eingefügt	Kapitel „Extended-Validation-SSL-Zertifikat“; siehe Kap 4.5
Anh. A	Ergänzt	Tabelle „CH Rechtsgrundlagen“ ergänzt um die Referenzen auf MwSTG, ElDI-V und GeBüV
Anh. A	Ergänzt	Tabelle “SuisseID Spezifikation“
Anh. C	Ergänzt	Tabelle „Abkürzungen“
Ende		