Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Wirtschaft, Bildung und Forschung WBF

Staatssekretariat für Wirtschaft SECO
Schweizerische Akkreditierungsstelle SAS

Interpretationen zu Fragen im Zusammenhang mit der Anerkennung von CSPs im Bereich der elektronischen Signatur

Dokument Nr. 522.dw

Ausgabe Februar 2013, Rev. 01

Einleitung

Dieses Dokument soll bei der Interpretation und Umsetzung der Anforderungen im Zusammenhang mit der Anerkennung von Certification Service Provider (CSP) im Bereich der elektronischen Signaturen als Leitfaden dienen.

Bemerkung zum Dokument:

Anbieterinnen von Zertifizierungsdiensten (CSP), deren Systeme diesem BAKOM-SAS Dokument (Dok. Nr. 522.d) nicht folgen, sind nur dann anerkennungsfähig, wenn sie der Anerkennungsstelle (Zertifizierungsstelle) nachweisen können, dass ihre Verfahren den relevanten Abschnitten der angewendeten Normen, Gesetze oder Verordnungen in gleicher Weise entsprechen.

	Frage / Kommentar	Stellungnahme BAKOM und SAS
1.	**Angabe bezüglich Quantität:** Wie viele Zertifikate muss die CSP während der Anerkennung ausstellen, um nachzuweisen, dass eine Anerkennung der CSP durchführbar ist?	Im Minimum müssen zwei digitale Zertifikate für Audit-Zwecke erstellt werden. Mit diesen zwei digitalen Zertifikaten soll die CSP der Anerkennungsstelle aufzeigen können, dass alle Schritte des Zertifikats-Lebenszyklus bei der CSP konform zu der TAV 943.032.1 und den referenzierten Dokumenten umgesetzt werden können. Eine rückwirkende Anerkennung für früher ausgestellte digitale Zertifikate wird nicht toleriert. Der Hinweis, dass die CSP anerkannt ist sowie der Name der Anerkennungsstelle dürfen nicht auf den vor der Anerkennung ausgestellten Inhaberzertifikaten erscheinen.
2.	**Schlüsselpaar-Generierung:** Muss das Schlüsselpaar vor den Augen der RAO (Registration Authority Operation) auf dem SSCD generiert werden?	Wenn die CSP das Schlüsselpaar der Antragstellerin oder des Antragstellers generiert, kann die Schlüsselpaar-Generierung ohne Mitarbeit und ohne Anwesenheit der Antragstellerin oder des Antragstellers erstellt werden. Die CSP muss der Anerkennungsstelle aufzeigen können, dass ein sicherer und vertraulicher Prozess für die Schlüsselpaar-Generierung stattfindet. Wenn die Antragstellerin oder der Antragsteller eines Zertifikats sein Schlüsselpaar selber generiert, gelten folgende Anforderungen der ETSI TS 101 456- Spezifikation: • Kapitel: 6.2.d.) Subscriber obligations • Kapitel: 7.3.1. Bst. k und l.) Subscriber registration In diesem Fall ist die Antragstellerin oder der Antragsteller nicht verpflichtet, das Key Pair vor den Augen der RA zu generieren.

3.	**Benutzung der SSCD:** Wie (technisch) muss die CSP feststellen können, ob ein Schlüsselpaar auf einem zertifizierten SSCD generiert wurde? Falls die CSP nicht selbst SSCD abgeben möchte: Reicht es aus, wenn die CSP Verfahren festlegt, die sicherstellen, dass z. B.: • die eingesetzte SSCD den Anforderungen entspricht; • die Generierung des Schlüssels gemäss Kap. 3.3.2 der TAV SR 943.032.1 durchgeführt wurde; • Algorithmus und Schlüssellänge gemäss CSP verwendet wurde; • ein Signaturprüfschlüssel publiziert wird; • die Freischaltung nach Überschreiten der max. Anzahl Fehlversuche nur durch Einbindung der CSP möglich ist. Oder sind zusätzliche Massnahmen nötig?	Kap. 3.3.2 der TAV 943.032.1 regelt den Fall, wenn die CSP selber das Schlüsselpaar der Antragstellerin oder des Antragstellers generiert. Wenn der Antragsteller eines Zertifikats sein Schlüsselpaar selber generiert, muss die CSP sicherstellen, dass das Schlüsselpaar in einer SSCD generiert wurde, so wie es im Kapitel 7.3.1, Bst. k und l der ETSI 101 456-Spezikation definiert ist. Die CSP soll eine Vereinbarung zwischen ihr und dem Antragsteller des Zertifikats erstellen. Dieser Prozess muss durch die Anerkennungsstelle auditiert werden (Kapitel 6.2. d und e der ETSI TS 101 456-Spezifikation, regeln den Fall, wenn die Antragstellerin oder der Antragsteller eines Zertifikats ihr/sein Schlüsselpaar selber generiert.) Eine rein technische Lösung ist nicht gefordert. Mit dem Dokument CWA 14169 wird die Konformität mit den Anforderungen von Art. 6, Abs. 2 ZertES sichergestellt. Es liegt in der Verantwortung der CSP sicherzustellen, dass bei Adaptionen der SSCD, deren EAL 4+ Zertifizierung bestehen bleibt.
4.	**Schlüssel-Grösse:** Die Schlüssel-Grösse 1024 Bits kann in wenigen Wochen gebrochen (oder geknackt) werden. 2048 Bits Crypto-Devices sind vorhanden, jedoch noch nicht FIPS 140-2 Security Level 3 geprüft. (siehe auch Art. 3 VZertES, Signatur- und Signaturprüf-Schlüssel).	Die Produkte für die Verwaltung der Schlüssel der CSP müssen den Anforderungen des Kap. 7.2.1 der ETSI TS 101 456 Spezifikation erfüllen. Die CSP ist verpflichtet, ausreichende Sicherheit für die ausgehändigten qualifizierten Zertifikate zur Verfügung zu stellen. Es wird empfohlen, sich für die Auswahl der zulässigen Signaturalgorithmen, der Mindestgrösse der für diese Algorithmen zu verwendenden Schlüssel, der Merkmale der Zufalls-zahlengeneratoren und der Hash-Funktionen an der ETSI TS 102 176-1 – Spezifikation zu orientieren.

	Wie kann jetzt die CSP dieses Produkt ohne Produkt-Zertifizierung einführen (FIPS Produkt Zertifizierung oder Schlüssel-/Datensicherheit?	Die CSP muss den Markt aktiv beobachten, insbesondere auf Technologieänderungen, Verwundbarkeiten und entsprechende Attacken. Die CSP muss seine eigene PKI Infrastruktur (Prozess & Technik) kontinuierlich auf Verwundbarkeiten analysieren, angemessene Schutzmassnahmen aufrechthalten und die Prozesse an die neuen Anforderungen im Technologieumfeld fortwährend anpassen.
5.	**Audit der Registration Authorities (RA):** Wie prüft die Anerkennungsstelle die ZertES-konformen RAs der CSP? Wie oft? Nach welchen Kriterien? (Wenn eine RA dazu kommt, wie ist dann der Prozess des Audits?)	Falls die CSP eine kleine Anzahl von Registration Authorities (RA: 1-5) betreibt, wird die Anerkennungsstelle jede RA überprüfen. Wird von der CSP eine grössere Anzahl von RA betrieben, werden von der Anerkennungsstelle mit einem ausgewählten "Spot-Check" Verfahren die einzelnen RAs auditiert. Die CSP darf Aktivitäten an Dritte delegieren, wenn sie die Voraussetzungen gemäss ZertES erfüllen und sie die daraus resultierenden Pflichten einhalten. Die CSP kann ihre Haftung aus dem Gesetz weder für sich noch für Hilfspersonen weg bedingen (Art. 16 ZertES)**.** Die folgenden Kapitel der ETSI TS 101 456-Spezifikation sind u. a. für das Audit der RA relevant und müssen standardkonform umgesetzt werden: Kap.7.3.1; Kap. 7.4.11; Kap. 7.3.4; Kap. 7.3.3.; Kap. 7.4.6. Auf der Basis der RA-Aktivitäten bestimmt die Anerkennungsstelle, welche Bereiche überprüft werden.
6.	**Kontrollen, welche nicht in der Verantwortung der CSP liegen:** Wie behandelt eine CSP die Gesetzes-anforderungen, die nicht in ihrer Kontrolle in Obhut stehen? z.B. Art. 6, Abs. 3, Bst. a bis g ZertES	Die Bestimmungen des Art. 6, Abs. 3, Bst. a bis g ZertES liegen nicht in der Verantwortung der CSPs. Die CSP sollte für den Endbenutzer einen Pflichten-Katalog erstellen, damit die Arbeitsweise und die Handhabung von Passwörtern und SW & HW Komponenten für den End-Benutzer nicht zum Risiko werden. Für die Signaturverifizierung wurden folgende Richtlinien entwickelt: CWA 14171 General Guidelines for Electronic Signature Verification (abrufbar unter http://www.cen.eu/cenorm/businessdomains/businessdomains/isss/cen+workshop+agreements/cwa_listing.asp)

7.	**Haftpflicht-Versicherung:** Wann soll die Haftpflicht-Versicherung abgeschlossen werden?	Die Haftpflicht-Versicherung muss durch die CSP vor dem Abschluss des Audit-Berichtes eines Anerkennungsaudits rechtskräftig abgeschlossen werden. Die Anforderungen für die Versicherungen sind im Art. 2, Abs.1 und 2 VZertES beschrieben.
8.	**Issuer-Feld (Kap. 3.4.2, TAV 943.032.1) :** Es kann nicht sein, dass das System der Anerkennung (siehe Kapitel 2) im Issuer-Feld statisch wiedergegeben ist. Dies ist aus folgenden Gründen nicht praktikabel: - die Festlegung des Issuer-Feldes impliziert das Erstellen einer neuen CSP, wenn immer diese CSP mit SR 943.032.1 kompatibel sein will (die bestehenden CSPs haben schon einen Namen (der "O=" Eintrag) und Zertifikat und können diesen nicht ändern!). Die Anerkennung sollte, wie das Wort schon sagt, keine neuen CSPs forcieren, sondern bestehende anerkennen. - mit der statischen Festlegung der Anerkennungsstelle wird ein Wechsel schwierig (zumindest dessen Widerspiegelung im Issuer), denn das Root-Zertifikat kann nicht nach Belieben neu ausgestellt und verteilt werden. Es müsste doch, eventuell in Zukunft, möglich sein, die Dienstleistungen einer anderen akkreditierten Anerkennungsstelle zu beanspruchen und dies im Zertifikat korrekt zu erwähnen. Die Gesetzesanforderung, im Zertifikat die Anerkennungskette darzustellen, muss unbedingt auf anderem Wege, natürlich ohne die internationale Kompatibilität zu gefährden, realisiert werden.	Gemäss Art. 7, Abs. 1, Bst g. ZertES muss der Name der Anerkennungsstelle statisch im Zertifikat wiedergegeben werden. Man will die vor und nach der Anerkennung ausgestellten Inhaberzertifikate unterscheiden. Eine rückwirkende Zertifizierung für früher ausgestellte digitale Zertifikate wird nicht toleriert. Der Hinweis, dass die CSP anerkannt ist, sowie der Name der Anerkennungsstelle dürfen nicht auf den vor der Anerkennung ausgestellten Inhaberzertifikaten erscheinen. Nach einem Wechsel der Anerkennungsstelle werden die neu erstellten Inhaberzertifikate den Namen der neuen Anerkennungsstelle enthalten. Wichtig ist der Stand bei der Zertifikatsausstellung.

9.	**„Certificate Policies“-Erweiterung, (Kap. 3.4.2, TAV 943.032.1):** Aus Kap. 4.2.1.5 RFC 3280 (Certificate Policies): The certificate policies extension contains a sequence of one or more policy information terms, each of which consists of an object identifier (OID) and optional qualifiers. Optional qualifiers, which MAY be present, are not expected to change the definition of the policy. Dies bedeutet: es muss eine OID geben. Die Frage ist nur welche? Es wäre sinnvoll (eigentlich ein Muss) für anerkannte CAs, in der Schweiz, eine einheitliche OID zu verwenden. Dies ist die normale und übrigens sehr flexible PKI-Methode, um Policies, Spielregeln und Gesetzeskonformität darzustellen bzw. nachzuweisen.	Die CSP soll die CP und CPS mit einem OID kennzeichnen (ETSI TS 101 456 Kap. 8.1, Bst. i). Eine einheitliche OID für anerkannte CSPs in der Schweiz ist nicht vorgesehen. Eine Referenzierung der „QCP-Public-with-SSCD“-Policy gemäss Kap. 5 der ETSI 101 456-Spezifikation ist möglich. Für die Bestellung eines OID beim BAKOM soll das Formular „Zuteilungsgesuch für Kommunikationsparameter“ unter http://www.bakom.admin.ch/themen/telekom/00458/00614/index.html?lang=de ausgefüllt werden (Seite 1 ausfüllen, „RDN“ und „Object Id“ auf Seite 2 ankreuzen und Beilage B ausfüllen).
10.	**“Authority Information Access”-Erweiterung (Kap. 3.4.2, Bst. C, TAV 943.032.1):** Welche OID wird als Extension in Bezug auf die Authority Information Access Definition genau angewendet? (ad-caIssuers, OCSP)? Der RFC 3280 schreibt keine Muss-Kriterien für die OID in dieser Extension vor.	Im Kap. 3.4.2, Bst. c der TAV 943.032.1 handelt es sich für die „Authority Information Access“-Erweiterung um den id-ad-caIssuers gemäss Kap. 4.2.2.1 RFC 3280
11.	**„Certificate Policies“-Erweiterung (Kap. 3.4.3, Bst. D, TAV 943.032.1):** Welche OID? Bei dieser Extension im CA-Zertifikat ist die Bedeutung anders: Es sagt aus, welche OIDs unter dieser CA vorkommen können: z. B. anyPolicy = { 2 5 29 32 0 }.	Es gibt keine Anforderungen für die „certificate-Policies“-Erweiterung im CA-Zertifikat.

	Diese Frage ist sehr wichtig, denn falls die CA nur genau die OID der 'ZertES policy' haben kann, würde dies bedeuten, dass die CSP keine Chiffrierung und Authentication für Zertifikate unter dieser CA haben kann. Falls nun nur die "Subscriber-Zertifikate" die "ZertES policy" hätten (+ qc extension) und die CA "anyPolicy" hätte, könnte man unter der anerkannten CA auch mittels ein sub-CA Chiffrierung und eventuell Authentication für die Zertifikate ausgeben und dies immer mit der gleichen DN. Ist dies nicht die Flexibilität, die der Gesetzgeber eigentlich will? Das Signatur-Zertifikat sollte vollumfänglich der ZertES entsprechen, aber viele Berufsgattungen (z. B Ärzte, Anwälte, gewisse Bundesbehörden) müssen die Vertraulichkeit gewährleisten, und dies ist mit dem jetzigen ZertES ohne weiteres möglich, wenn eben nur die Subscriber-Zertifikate die 'ZertES policy' haben und die CA anyPolicy hat.	
12.	**Root-Key Generierung/Zeremonie:** Welche "Must"-Kriterien (Trust Anker Zeremonie) müssen minimal umgesetzt werden? Was muss für eine CSP im Minimum umgesetzt werden? - Vorgaben - Umsetzung - Witness-Personen - Dokumentation	Die Root-Key-Zeremonie für qualifizierte Zertifikate beinhaltet folgende minimale Anforderungen für eine Zertifizierung für qualifizierte Zertifikate: Die folgenden Teilnehmer müssen bei einer Root-Key-Generierung partizipieren, oder das Vorgehen muss in diesem Detaillierungsgrad aufgezeigt werden können, damit Klarheit besteht, dass die Root-Key-Generierung sicher und vertraulich verlaufen ist: • Operation Manager • Key Manager • Key Administrators • Zeugen

		Die Aufzeichnung einer Root-Key-Zeremonie muss "aufzeichnungssicher" und in jedem detaillierten Schritt nachvollziehbar sein. Für die technische Infrastruktur und organisatorischen Abläufe ist Folgendes umzusetzen: • Personen-Liste und Verantwortlichkeiten (Funktion, Firma, Telefon) • Detaillierte Beschreibung der Installation der PKI-Komponenten, welche für die Root-Key Zeremonie wichtig sind • Prozessbeschreibung "Zeugen" und Record-Aufbewahrung der CSPs • Initialisierung, Aufsetzen der Hardware Encryption Module (Beschreibung) • Key-Generierung Prozeduren, detaillierte Checkliste mit Datum und Beschreibung des Vorgehens • Ort, Datum, Unterschriften für die Beglaubigung vor Ort (während der Root-Key- Zeremonie) Hinweis: Für manche hochgesicherte Anwendungen, wie zum Beispiel für eine Root CA, kann die Geräteinstallation und der Initialisierungsprozess von einem Auditor und/oder anderen Zeugen überwacht und/oder aufgenommen werden.
13.	**Anzahl Mitarbeiter:** Wie viele Personen müssen im Betrieb eines PKI Trust Centers (CSP) Arbeit leisten. - Aufteilung der Funktionen: - Funktionentrennung - Dual Control - Administration/Verkauf - Operation - Integr./Implementation - Konzeption - Beratung/Dokumentation - Policy/Direktiven - Kommunikation (intern/extern) - Audit/Überwachung	Eine CSP für digitale qualifizierte Zertifikate soll einen Betrieb für 24h/7Tage zur Verfügung stellen können. Um den Betrieb einer CSP aufrechterhalten zu können, ist die Verfügbarkeit der PKI-Komponenten und der zur Verfügung zu stellenden Arbeitskräfte essentiell. Die folgende Zusammenstellung zeigt die minimalen Ressourcen in Bezug auf "Human Capital Ressources" auf (Dies sind CSP intern angestellte Mitarbeiter): • 100 % Anstellung, Full-Time Equivalent, Function: Geschäftsführer, Executive Management (diese Person kann eine weitere Funktion im Folgenden übernehmen) • 100 % Anstellung, Full-Time Equivalent, Function: Verantwortlicher Betriebs-Management

		• 100 % Anstellung, Full-Time Equivalent, Function: Verantwortlicher Betriebs-Management Stellvertretung • 30 % Anstellung, Part-Time Equivalent, Function: Security Officer • 20% Anstellung, Part-Time Equivalent, Function: Administration, Verwaltung, Dok., RA-Admin., Geschäftsleitung • 20% Anstellung, Part-Time Equivalent, Function: Konfiguration und Implementation (Folgende Ressourcen können als CSP-externe Fachpersonen eingesetzt werden) • 50% Prozessverantwortung und Dokumentation sowie Prozessüberwachung (Möglichkeit: externer Berater) • 10% Audit-Verantwortlicher (Möglichkeit: externer Auditor) Eine 100%-ige Anstellung entspricht einer Vollzeitanstellung (FTE) bei der CSP. Dieser Anstellungsvertrag toleriert keine Arbeitsverhältnisse ausserhalb der Firma bzw. der CSPs (Grund: Unabhängigkeit, Verfügbarkeit Betrieb, Katastrophenfall, Risiko-Management). Die Exklusiv-Arbeits-Verträge müssen bei der CSP schriftlich vorliegen. Die minimalen Ressourcenzusammenstellung ist im Zusammenhang mit den folgenden Anforderungen der PKI Standards SR 943.032.1, ETSI TS 101 456, ANSI X9.79 definiert: • Funktionentrennung (Administration, Konzeption, Konfiguration, Überwachung) • Dual Control im Normal- und Katastrophenfall • Krankheit, Militär, Ferienabwesenheiten, Pikett-Dienst für Support & Service • Verfügbarkeit im Betriebsmanagement • Verfügbarkeit der Ressourcen im Schadenereignis oder Katastrophenfall.

		Diese Anforderungen stützen sich auch auf die Verordnung 1 des Arbeitsgesetzes (Art. 14, Abs. a ArGV1,) Pikettdienst Grundsatz: Ausschnitt Art. 14 Abs. 2 ArGV1: Der einzelne Arbeitnehmer oder die einzelne Arbeitnehmerin darf im Zeitraum von vier Wochen an höchstens sieben Tagen auf Pikett sein oder Piketteinsätze leisten. Nach Beendigung des letzten Pikettdienstes darf der Arbeitnehmer oder die Arbeitnehmerin während den zwei darauf folgenden Wochen nicht mehr zum Pikettdienst aufgeboten werden. Abschnitt Art.14. Absatz 3: Ausnahmsweise kann ein Arbeitnehmer oder eine Arbeitnehmerin im Zeitraum von vier Wochen an höchstens 14 Tagen auf Pikett sein, sofern a.) auf Grund der betrieblichen Grösse und Struktur keine genügenden Personalressourcen für einen Pikettdienst nach Absatz 2 zur Verfügung stehen; und b.) die Anzahl der tatsächlichen Piketteinsätze im Durchschnitt eines Kalenderjahres nicht mehr als fünf Einsätze pro Monat ausmacht. Die Zuständigkeiten und Volumen-Prozente für das Arbeitspensum von Mitarbeitern bei einer CSP werden durch die Anerkennungsstelle (Zertifizierungsstelle) beurteilt. Grundsätzlich sind diese Definitionen in Bezug auf die Grösse und Komplexität des Geschäfts einer CSP zu relativieren, jedoch gibt es keinen Unterschied in der Einschätzung der "Human Capital Ressources" in Bezug auf die internationalen PKI Standards, mit welchem die CSP anerkannt wird. Diese Vorgaben gelten als Minimal-Anforderungen und sind zwingend umzusetzen.
14.	**Re-Engineering-Prozess für die Einstellung der CSP-Geschäftstätigkeit:** Dieser Prozess muss mit dem BAKOM definiert werden. Alle CAs mit qualifizierten Zertifikaten werden mit dem BAKOM Kontakt aufnehmen. Muss für den Prozess bei einer Auflösung der CSPs resp. des Zertifizierungsgeschäftes eine Absichts-erklärung vom Bund (BAKOM) vorhanden sein?	Bei der Einstellung der Geschäftstätigkeit beauftragt die SAS eine andere CSP, Verzeichnisse zu führen sowie Tätigkeitsjournal und entsprechenden Belege aufzubewahren (Art. 13 ZertES). Die CSP muss einen Phasenplan für die Übergabe ihrer Aktivitäten (Einstellung der Geschäftstätigkeit) und einem Phasenplan für die Übernahme der Aktivitäten einer anderen CSP aufzeigen können.

		Der Phasenplan für die Einstellung der Geschäftstätigkeit muss folgende Definitionen und Beschreibungen beinhalten: ▸ Asset Liste der CSP (Auflistung der HW & SW Komponenten, Standort, Eigenschaften über das Format der aufbewahrten Daten ▸ Bestimmung des Geltungsbereiches ▸ Telefon-Kontakte und Funktionen der Hauptansprechpartner ▸ Re-Engineering-Plan (Ablaufplan/Phasenplan, mit welchen Schritten eine Migration der qualifizierten Zertifikate zur neuen CSP gemacht wird) ▸ Konzeptioneller Zeitplan: Daraus muss ersichtlich sein (Wochen, Monate), in welchen Zeitphasen welche Migrationen zwischen der neuen CSP und der terminierten CSP durchgeführt werden ▸ Detaillierte Beschreibung über die Informationsverteilung an den Endkunden (Subscriber), Behörden (Brief, Presse Mitteilung) ▸ Kommunikationskanal darstellen (wer wird intern und extern offiziell informiert?) Die CSP müsste sich auf die Richtlinien des BAKOMs, bezüglich des Verfahrens bei Einstellung der Geschäftstätigkeit einer anerkannten CSP, beziehen (erhältlich unter http://www.bakom.admin.ch/themen/internet/00467/index.html?lang=de).
15.	**Zuständigkeit beim BAKOM:** Wer ist beim BAKOM zuständig für das Gespräch "Termination Prozess/Re-Engineering" und die Sitzung mit der CSP?	BAKOM, C. Jenny, christian.jenny@bakom.admin.ch, Tel. 032 327 59 75

16.	**Akkreditierte Anerkennungsstelle (Certification Body):** Wer ist in der Schweiz akkreditiert, d.h. beglaubigt, Anerkennungsaudits für PKI Trust Centers (CSPs) durchzuführen?	Die Anerkennung nach den folgenden Standards/Richtlinien ist abhängig vom definierten Geltungsbereich und Standard des CB: • SR 932.03 (ZertES), SR 932.032 (VZertES) und SR 932.032.1 (TAV) über die Zertifizierungsdienste im Bereich der elektronischen Signatur • ETSI TS 101 456 (Policy requirements for certification authorities issuing qualified certificates) • ANSI X9.79 (PKI Practices and Policy Framework) Die Liste der akkreditierten Anerkennungsstellen ist unter http://www.seco.admin.ch/sas/index.html?lang=de publiziert. Im Moment gibt es nur die KPMG (Akkr. Nr. SCESm 071) als akkreditierte Anerkennungsstelle (CB).
17.	**Sicherheit über Signaturerstellungseinheiten:** Was gilt als „hinreichend“ bzw. „verlässlich“ gemäss ZertES für sichere Signaturerstellungseinheiten? Text Bundesgesetz, Art. 6, Abs. 2 ZertES: 2 Die Signaturerstellungseinheiten müssen zumindest gewährleisten, dass die für die Erzeugung der Signatur verwendeten Signaturschlüssel: a. praktisch nur einmal auftreten können und ihre Geheimhaltung ***hinreichend*** gewährleistet ist; b. mit hinreichender Sicherheit nicht abgeleitet werden können und die Signatur bei Verwendung der jeweils verfügbaren Technologie vor Fälschungen geschützt ist; c. von der rechtmässigen Inhaberin oder vom rechtmässigen Inhaber vor der missbräuchlichen Verwendung durch andere ***verlässlich*** geschützt werden können.	In der TAV SR 943.032.1 Kapitel 3.3.3 a) heisst es: Die CSP muss den Antragstellerinnen und Antragstellern eines Zertifikats sichere Signaturerstellungseinheiten liefern, die den Mindestanforderungen von Artikel 6 Absatz 2 ZertES [1] entsprechen, oder sicherstellen, dass diese solche verwenden. Mit dem Dokument CWA 14169 wird die Konformität mit den Anforderungen von Art. 6, Abs. 2 ZertES sichergestellt. Diese Forderung basiert auf den Sicherheitsanforderungen (CWA 14169) des europäischen-Raumes und soll somit auch die Anerkennung der schweizerischen qualifizierten Signatur im Ausland fördern, wie es von der ZertES beabsichtigt wird. Gemäss Kap. 2.1, 2.2, 4.2, 5.1.6.2 CWA 14169, Annexe B, wird ein Trusted Path/channel für die Eingabe des PINs mittels der PC-Tastatur angefordert.

	Konkret: Wenn eine CSP annimmt, dass sie in einer SmartCard/USB Token mehrere Schlüssel abgespeichert hat und den Signaturschlüssel nur und ausschliesslich zum Signieren verwendet, aber z. B. in derselben SmartCard einen Schlüssel für Single Sign On (SSO) und/oder VPN Encryption hat, was gilt als „hinreichend“ für den Schutz dieses Schlüssels? - Kann der PIN Code zur Aktivierung einer Signatur grundsätzlich über die PC Tastatur eingegeben werden? - Kann der PIN Code bei der Generierung des Schlüssels für den Zugriff das erste Mal über die Tastatur eines PC eingegeben werden? - Wenn ja, was gilt als „verlässlicher“ Schutz, dass der PIN Code nicht "gecashed", von einem Trojaner gespeichert oder durch einen "keylogger" aufgefangen wird? - Wenn nein, wie sonst muss/kann der Freigabe-PIN eingegeben werden?	Damit der Forderung nach einem Trusted Path/channel genüge getan wird, muss eine sichere Software/Applikation eingesetzt werden, die diesen trusted Path/channel garantiert. Dies bedeutet für die CSP, dass sie der Anerkennungsstelle nachvollziehbar darlegen muss, wie die oben genannten Forderungen nach einem trusted Path/Channel umgesetzt wurden.
18.	**Heimatort oder Geburtsort:** Im Kap. 3.4.1 der TAV 943.032.1 und im Kap. 7.3 der ETSI TS 101 456-Spezifikation, sind die Verfahren für eine Registrierung einer natürlichen Person definiert. Dort wird unter Kap. 7.3.1 Bst. e „Place of birth“ verlangt. In der Schweiz ist meines Wissens in keinem offiziellen Dokument der Geburtsort geführt. Doch wird der Heimatort geführt. Würde nicht der Heimatort genügen?	Beide Einträge (Geburtsort oder Heimatort) sind für die Registrierung akzeptiert. Es ist von der CSP sicherzustellen, dass nicht beide Einträge auf dem gleichen Zertifikat definiert werden. Grundsätzlich hat die CSP den Prozess so aufzusetzen, dass im Falle einer Verwechslungsmöglichkeit der Name des Zertifikatinhabers mit einem unterscheidenden Zusatz zu versehen ist (Art. 7 Abs. 1, Bst c ZertES). In diesem Fall könnte der Eintrag des Heimatortes nicht sehr nützlich sein.

19.	**Zusätzliche Felder und Erweiterungen im Zertifikat:** In Kap. 3.4.2 der TAV 943.032.1 wird aufgeführt, welche Felder hinzugefügt werden müssen. Kann die CSP zusätzliche kritische/nicht kritische Erweiterung im Zertifikat anbringen (z. B. Zeichnungsberechtigung nach Handelsregister)?	Zusätzliche Felder oder Erweiterungen können angebracht werden, sobald die Konformität mit anderen ZertES-Anforderungen gewährleistet ist. Zertifikatinhaber-Attribute müssen vor der Zertifikat-Generierung verifiziert werden. Die CSP ist für die Zuverlässigkeit der Zertifikatsdaten verantwortlich. Attribute sind grundsätzlich für qualifizierte Zertifikate tolerierbar (siehe auch Art. 5, Abs.2 a und b VZertES). Wichtig ist: Jede neue Unterschriftsberechtigung muss durch die CSP gemäss Art. 8 ZertES und Art. 5 VZertES validiert werden.
20.	**Zeitstempel:** Kap. 3.5, TAV 943.032.1: Der Wortlaut deutet darauf hin, dass es optional ist (d.h. dass das Erzeugen von Zertifikaten mit Beginn- und Endzeit nicht unter diese Klausel fällt). Um anerkennt zu werden, muss nun eine CSP ein Zeitstempel einführen oder ist diese Forderung optional? Zertifikat mit formellen ETSI TS 102 023-Spezifikation (= RFC 3161 = Patent Streit) Zeitstempel ausstellen. Jede Schweizer CSP würde sich den Patentstreit gerne sparen.	Art. 12 ZertES verpflichtet die CSP, einen Zeitstempeldienst einzurichten. Dies wiederum heisst, dass die CSP einen operativen Time Stamping Authority (TSA) Service installieren muss. Die CSP muss die „Server“ Lösung anbieten. Die Bereitstellung einer „Client“-Lösung ist nicht angefordert. Dieser TSA Service muss aktiv von einer CSP an ihre Kunden zur Verfügung gestellt werden. Die Benutzung des TSA Services (Zeitstempeln auf Zertifikaten) ist jedoch nur optional von CSP Kunden anzuwenden.
21.	**PIN-Code:** In welcher Art und Güte muss der PIN-Code für den Zugriff auf die Subscriber SSCD’s resp. Hard-Tokens (z.B. Smardcards, USB Token) ausgestattet sein?	Der PIN-Code muss im Minimum 6 Zeichen enthalten. Die CEN –Dokumente CWA 14169 (Signature Creation Devices „EAL4+“) und CWA 14170 (security requirements for signature creation application) informieren über die PIN-Sicherheit.

22.	**Revokations-Dienst:** Zu welchen Betriebszeiten muss ein Revokations-Service zur Verfügung gestellt werden? Wie schnell und in welcher Arbeits-Durchlaufzeit muss ein kompromittiertes Zertifikat gesperrt werden? Muss der Revokations-Service (Antrag-Annahme) elektronisch / automatisch zur Verfügung stehen? Es stellt sich hier die Frage, ob mit einem Web-Interface dieser Anforderung genüge getan ist oder eine 24 Stunden-Hotline gefordert ist. Ist ein Web-Interface, welches auf einer starken Identifikation basiert, ausreichend?	Dieser Revokations-Service muss sicherstellen, dass ein Zertifikatsinhaber jederzeit die Möglichkeit hat, einen Antrag für die Revokation seines Zertifikates 24h/7Tage zu stellen und dass der Zeitpunkt und die Rechtmässigkeit dieses Antrages rechtsverbindlich festgehalten wird. Es ist keine Lösung für den Revokations-Service vorgeschrieben. Die Annahmen müssen mit geeigneten Mitteln und Massnahmen erfolgen, welche den Zeitpunkt und die Rechtmässigkeit dieses Antrages rechtsverbindlich festhalten, z.B. Help Desk mit Telefon oder Fax. Eine webbasierende Lösung ist sicher eine mögliche Lösung. Als gutes und vergleichbares Beispiel kann der Swiss Card AECS SOS-Service für Kreditkarten empfohlen werden.
23.	**Einschränkung des Kundenkreises:** Kann die CSP ihren Kundenkreis einschränken? Beispiele: Qualifizierte Zertifikate nur für Kantone (Kantonsangestellte), nur für Apotheker, nur für Mitarbeiter, etc. Können Sie diese Meinung teilen?	Die CSP kann ihren Kundenkreis einschränken.
24.	**Verfügbarkeit des Revokations-Dienstes:** Gemäss ETSI 101 456 Kapitel 7.3.6 h) muss der Revokations-Dienst 7x24 Stunden verfügbar sein. Ob diese Verfügbarkeit nun 80% oder 99.999% sein muss, ist nicht definiert. Gibt es seitens BAKOM diesbezüglich Vorstellungen? In den ersten Versionen/Entwürfe der TAV (SR 784.103.01) wurde noch die Verfügbarkeitsanforderungen definiert, sollen wir diese als Richtwerte benutzen?	Beispiel: Die CSP bietet ein Revokations-Dienst mittels einer telefonischen "Hotline" an. In diesem Fall muss das Personal Anfragen 24Std/Tag und 7 Tagen/Woche beantworten. Die technische Lösung und ihre Verfügbarkeit sollten jedoch in der CSP beschrieben werden. Die folgende Grundlage scheint uns in diesem Fall für die Anerkennung ausreichend zu sein: Art. 7, Abs. 1 VZertES: "Die anerkannten Anbieterinnen informieren ihre Kundinnen und Kunden darüber, wie sie die Ungültigerklärung von qualifizierten Zertifikaten verlangen können. Sie müssen in der Lage sein, die Anträge zur Ungültigkeitserklärung jederzeit entgegenzunehmen." ETSI TS101 456 Kap. 7.3.6, Bst. h)"Revocation management services shall be available 24 hours per day, 7 days per week. Upon system failure, service

		or other factors which are not under the control of the CA, the CA shall make best endeavours to ensure that this service is not unavailable for longer than a maximum period of time as denoted in the certification practice statement." ISO 21188 (B4.7) und ANSI X9.79 (B3.6): "CA provides a means of rapid communication to facilitate the secure and authenticated revocation." Die Definition der Verfügbarkeit des Revokations-Service muss sich nach Best Practice Definitionen richten und darf nicht schlechter sein als dies bei Credit Card Services, z.B. bei Swiss Card AECS SOS-Service definiert ist. Der Verlust oder die Kompromittierung der digitalen Identität hat für den Zertifikats-Inhaber eine ähnliche emotionale Bindung wie der Umgang mit Kreditkarten.
25.	**Tätigkeitsjournal:** Gibt es eine Liste der Tätigkeiten und Belege?	Folgende Dokumente könnten zur Ausarbeitung einer vollständigen Liste beitragen: Art. 5 VZertES ETSI TS 101 456, Kap. 7.3.1, 7.4.6, 7.4.11 ETSI TS 102 023, Kap. 7.3.1, 7.4.6, 7.4.11 ISO 21188 B1.11 Die Grundlage ist somit genügend. BAKOM/SAS verzichten auf die Bearbeitung einer Liste.
26.	**Übergabe des Tätigkeitsjournals:** Gemäss der ZertES Art.13 müssen die Verzeichnisse, das Tätigkeitsjournal, sowie die entsprechenden Belege an einen anderen anerkannten Anbieter von Zertifizierungsdiensten übergeben werden. Die CSP fragen sich nun, ob das ganze Tätigkeitsjournal inklusive aller Belege stattfinden muss, oder aber, ob Teile davon ausreichen. Unsere Kunden begründen dies damit, dass nach einem Konkursfall nicht mehr alle Belege für das Fortführen der Verzeichnisse notwendig sind. Als Gegenargument sehen wir, dass die	Die Belege und das Tätigkeitsjournal sollen im Gerichtsfall helfen, die Nachvollziehbarkeit zu garantieren. (ETSI 101456, 7.4.11, c: « [...]for the purpose of providing evidence of certification for the purposes of legal proceedings »).

	Belege und das Tätigkeitsjournal im Gerichtsfall helfen sollen, die Nachvollziehbarkeit zu garantieren. Die CSP haben nun den Wunsch geäussert, dass das BAKOM/SAS eine Liste der Tätigkeiten und Belege veröffentlicht, in der geklärt ist, was grundsätzlich zu behalten und aufzuzeichnen und im Terminierungsfall weiterzugeben ist. Ist so was möglich? Übergabe der CSP-Tätigkeiten im Falle der Einstellung der Geschäftstätigkeiten In der Botschaft 01.044 Artikel 13 wird von der Übergabe der Aufgaben gesprochen, in der ZertES Art. 13 werden diese Aufgaben einzeln genannt (Führen der Verzeichnis der gültigen, der abgelaufenen, und für ungültig erklärten qualifizierten Zertifikate, Tätigkeitsjournal). So weit so gut, in der Botschaft steht nun, dass die Zertifikate nicht für ungültig erklärt werden müssen, aber im ETSI 101 456 7.4.9 CA termination steht " the CA shall destroy,...,its private key. Wenn dies nun die CSP tut, kann die CSP, welche die Tätigkeiten übernimmt, die Verzeichnisse nicht mehr führen, sondern nur noch publizieren - Wir gehen davon aus, dass die CSP alle ihre Zertifikate revozieren soll (nicht muss), und dann die CRL unterschreibt, diese übergibt und dann die Private-Keys zerstört. Alle anderen Lösungen erzeugen meiner Ansicht nach Widersprüche und Probleme mit den verwendeten Produkten.	Folgende Dokumente könnten zur Ausarbeitung einer Liste beitragen: Art. 5 VZertES ETSI TS 101 456, Kap. 7.3.1, 7.4.6, 7.4.11 ETSI TS 102 023, Kap. 7.3.1, 7.4.6, 7.4.11 ISO 21188 B1.11 Die Grundlage ist somit genügend. BAKOM/SAS verzichten auf die Bearbeitung einer Liste. Bei Einstellung der Geschäftstätigkeiten, ist die Ungültigerklärung der noch gültigen qualifizierten Zertifikate die beste Lösung. Die CSP müsste sich auf die Richtlinien des BAKOMs, bezüglich des Verfahrens bei Einstellung der Geschäftstätigkeit einer anerkannten CSP, beziehen (erhältlich unter http://www.bakom.admin.ch/themen/internet/00467/index.html?lang=de)

27.	**Konkursfall:** Geht eine CSP Konkurs, muss diese ebenfalls die Kosten für das Führen der Verzeichnisse und des Tätigkeitsjournal tragen. • Muss für diese Kosten eine Versicherung abgeschlossen sein, oder sind diese Kosten im ersten Rang? • Wer zahlt, wenn kein Geld mehr da ist? • Wie werden diese Kosten berechnet? • Müssen im worst-case-Szenario nun die Verzeichnisse 11 Jahre lang geführt werden? • Wer bestimmt was die Kosten hierfür sind? Ein Web-Service kostet heute zwischen 10 Franken bis 2'500 Franken pro Monat ohne Berücksichtigung der Sicherheitsan-forderungen aus der ZertES und den davon abgeleiteten Verordnungen und Standards. Da im Zertifikat eine URL eingetragen ist, muss diese auch transferiert werden. Wie der Konkurs der Swissair zeigt, sind Namen/URL auch Werte, an denen der Konkursverwalter Verwertungsrechte gelten machen kann. Wie ist nun gewährleistet, dass die Bedürfnisse des Konkursrechtes und der ZertES adäquat berücksichtigt werden?	**Grundlage: Art. 3, Abs. 1 ZertES** "Als Anbieterinnen von Zertifizierungsdiensten anerkannt werden können natürliche oder juristische Personen, die: [...] f. die notwendigen Versicherungen zur Deckung allfälliger Haftungsansprüche aus Artikel 16 und der Kosten, welche aus den in Artikel 13 Absätze 2 und 3 vorgesehenen Massnahmen erwachsen könnten, abschliessen;" **Art. 13 ZertES** "2 Die Akkreditierungsstelle beauftragt eine andere anerkannte Anbieterin von Zertifizierungsdiensten, das Verzeichnis der gültigen, der abgelaufenen und der für ungültig erklärten qualifizierten Zertifikate zu führen und das Tätigkeitsjournal sowie die entsprechenden Belege aufzubewahren. Der Bundesrat bezeichnet eine geeignete Stelle zur Übernahme der Aufgabe, wenn es an einer anerkannten Anbieterin von Zertifizierungsdiensten fehlt. Die anerkannte Anbieterin von Zertifizierungsdiensten, die ihre Tätigkeit aufgibt, trägt die daraus entstehenden Kosten. Art. 13 Absatz 2 gilt auch dann, wenn eine anerkannte Anbieterin von Zertifizierungsdiensten in Konkurs fällt." **Art. 2 VZertES** "1 Eine Anbieterin von Zertifizierungsdiensten, die anerkannt werden will, muss zur Deckung ihrer Haftung eine Versicherung von mindestens 2 Millionen Franken pro Versicherungsfall und 8 Millionen Franken pro Versicherungsjahr abschliessen. 2 Sie kann anstelle einer Versicherung eine gleichwertige Garantie vorlegen." Für die Anerkennung sollte überprüft werden, ob die CSP die minimale Versicherung gemäss Art. 2 VZertES abgeschlossen hat oder eine gleichwertige Garantie vorlegen kann. Alle anderen Probleme müssen erst dann gelöst werden, wenn sie auftauchen. Wir können im Voraus leider keine Lösung geben, da diese Probleme mit dem Privatrecht, dem Versicherungsrecht und dem Konkursrecht zu tun haben.

28.	**Auswahl der CSP:** Gemäss ZertES Art. 13 bestimmt die SAS (Akkreditierungsstelle), welche CSP die Tätigkeiten übernehmen soll. Nun fragen sich einige unserer Kunden, auf Grund welcher Kriterien diese Beauftragung stattfindet. Es gibt Kunden, die nicht von allen anderen Mitbewerbern die CSP-Tätigkeiten übernehmen möchten oder übergeben müssen. Können und wollen Sie respektive die SAS diese Kriterien bekannt geben?	Es gibt dazu keine Kriterien. Die Situation wird in jedem Fall untersucht und die CSPs werden sicher die Möglichkeit haben Stellung zu nehmen. Gemäss Art. 13, Abs. 2 wird die Akkreditierungsstelle (SAS) schließlich entscheiden.
29.	**Übertragung der Anerkennung im Rahmen einer Fusion:** Wie soll im Rahmen einer Fusion, wo Rechte und Pflichten an eine andere Organisation übergehen, vorgegangen werden?	Für Änderungen an einem der unten aufgeführten Bereiche im Rahmen einer Fusion soll die CSP mittels einer Risikoanalyse mögliche Auswirkungen auf den Betrieb der CA, den Zertifikatsinhaber oder die "Relying Party" aufzeigen: • Veränderung der Garantieerklärung für Versicherungsanforderungen (VZertES) • Änderungen an der Ablauforganisation der CSP (Prozesse) • Standortänderung der Registration Authority (RA) • Änderung an der technischen Infrastruktur (ausserhalb Change Management) • Änderung des Geltungsbereiches der Anerkennung • Personelle Änderungen, Anpassung von Verantwortlichkeiten • Profiländerungen am Issuing-, Subscriber- oder TimeStamping Zertifikat bezüglich der Legal Entity (Issuer Feld). Aufgrund der Risikoanalyse wird die Zertifizierungsstelle entscheiden, allenfalls in Absprache mit der SAS, ob punktuelle Konformitätsprüfungen im Rahmen eines zusätzlichen Audits durchzuführen sind.

30.	**Änderung des Firmennamens:** Eine allfällige Änderung des Firmennamens im Rahmen einer Fusion hat Auswirkungen auf bereits ausgestellte Zertifikate, weil der Firmenname Bestandteil des Zertifikates ist und dadurch die Aktualität der Zertifikatsattribute nicht mehr gewährleistet ist. Wie ist in diesem Fall mit dem Issuing und den ausgestellten Zertifikaten umzugehen?	Der Firmenname ist ein integraler Bestandteil des „issuer Feldes“ und kann nicht so ohne weiteres geändert werden. Wird der Firmenname geändert, so müssen die Punkte im ETSI TS 101 456, Kapitel 7.4.9 CA termination durchgeführt werden. Gemäss Punkt c) ist auch der „transfer of its obligations to other parties“ geregelt und statthaft. Der Name, der im „issuer“- Feld der Zertifikate der Kunden erwähnt wird und der Name, der im „subject“- Feld der Zertifikate der CA erwähnt wird, müssen mit dem offiziellen Namen der Gesellschaft übereinstimmen, um diesen identifizieren zu können. Es ist notwendig, ein neues Zertifikat und einen neuen Schlüssel zur Unterschrift der CRL und der Kundenzertifikate nach der Namensänderung zu erzeugen. Die vor der Organisationsänderung ausgestellten Zertifikate müssen nicht ungültig erklärt werden. Es ist möglich, die Schlüssel der alten CA zu benutzen, um CRL zu unterzeichnen, die Kunden-Zertifikate mit dem „issuer“ Name der alten Gesellschaft erwähnen. In diesem Fall kann die alte CA dieselbe Infrastruktur benutzen wie die neue CA.

Definitionen und Abkürzungen:

Die Definitionen und Abkürzungen der technischen und administrativen Vorschriften SR 943.032.1 sind anwendbar.