Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation UVEK

Bundesamt für Kommunikation BAKOM

Abteilung Telecomdienste und Post

Richtlinien bezüglich des Verfahrens bei Einstellung der Geschäftstätigkeit einer anerkannten CSP

Ausgabe 2, Dezember 2017

Inhaltsverzeichnis

1 Allgemeines

1.1 Geltungsbereich

Diese Richtlinien haben Empfehlungsstatus. Sie bezwecken die Harmonisierung der Verfahren zur Übertragung und Übernahme der Aufgaben im Fall einer Einstellung der Geschäftstätigkeit einer anerkannten Anbieterin von Zertifizierungsdiensten (CSP) im Sinne von Artikel 14 des Bundesgesetzes vom 18. März 2016 über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (ZertES) [1] und Artikel 12 der Verordnung vom 23. November 2016 über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (VZertES) [2]. Damit können diese Verfahren bei Bedarf rasch und reibungslos umgesetzt werden.

Die anerkannten CSPs sowie die Anerkennungsstelle haben an der Ausarbeitung dieser Richtlinien mitgewirkt.

1.2 Referenzen

[1] SR 943.03, ZertES
Bundesgesetz vom 18. März 2016 über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate

[2] SR 943.032, VZertES
Verordnung vom 23. November 2016 über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate

[3] SR 943.032.1, TAV
Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate

1.3 Abkürzungen und Definitionen

Es gelten die Abkürzungen und Definitionen der TAV [3].

2 Vorbereitungsmassnahmen

Die anerkannten Anbieterinnen schliessen die notwendigen Versicherungen zur Deckung der Kosten, welche aus den im Fall einer Einstellung der Geschäftstätigkeit vorgesehenen Massnahmen erwachsen könnten, ab (vgl. Art. 3 Abs. 1 Bst. f ZertES [1]).

Die Anerkennungsstelle sollte regelmässig überprüfen, welche anerkannte CSP beauftragt werden sollte, falls eine anerkannte Anbieterin von Zertifizierungsdiensten ihre Tätigkeit einstellen sollte. Die Anerkennungsstelle sollte diese Information der SAS mitteilen. Die SAS sollte eine aktualisierte Liste führen, auf der für jede anerkannte CSP angegeben ist, welche andere anerkannte CSP bei einer Einstellung der Geschäftstätigkeit beauftragt werden könnte.

3 Verfahren im Fall einer Einstellung der Geschäftstätigkeit

3.1 Information an die Betroffenen

Die anerkannte CSP, die ihre Geschäftstätigkeit aufgibt, muss gemäss Art. 12 Abs. 1 VZertES [2] die Einstellung ihrer Tätigkeit unverzüglich und spätestens 30 Tage, bevor sie die Zertifizierungsdienste nach ZertES [1] nicht mehr anbietet, der SAS und der Anerkennungsstelle mitteilen.

Die anerkannte CSP, die ihre Geschäftstätigkeit aufgibt, sollte spätestens 20 Tage, bevor sie die Zertifizierungsdienste nach ZertES [1] nicht mehr anbietet, Kontakt mit der Nachfolge-CSP aufnehmen.

Die anerkannte CSP, die ihre Geschäftstätigkeit aufgibt, sollte die Zertifikatsinhaber spätestens 20 Tage, bevor sie die Zertifizierungsdienste nach ZertES [1] nicht mehr anbietet, informieren.

Folgende Informationen sollten den Zertifikatsinhabern mitgeteilt werden:
- das geplante Datum der Einstellung der Geschäftstätigkeit;
- das geplante Datum für die Ungültigkeitserklärung der geregelten Zertifikate;
- dass einzig die Publikation der CRL und die Aufbewahrung des Tätigkeitsjournals sowie der dazugehörenden Belege nach der Einstellung der Geschäftstätigkeit gewährleistet werden;
- der Name der Nachfolge-CSP, die diese beschränkten Aufgaben übernehmen wird;
- die Kontaktperson, die Telefonnummer und die E-Mail-Adresse der anerkannten CSP, die ihre Geschäftstätigkeit aufgibt, und der Nachfolge-CSP.

Die Zertifikatsinhaber können sowohl auf elektronischem Weg (E-Mail) wie auch mit traditionellen Mitteln (Post) informiert werden.

Bevor sie die Zertifizierungsdienste nach ZertES [1] nicht mehr anbietet, sollte die anerkannte CSP, die ihre Geschäftstätigkeit aufgibt, die Signaturüberprüfer durch eine Pressemitteilung über die Einstellung der Geschäftstätigkeit informieren. Folgende Informationen sollten den Signaturüberprüfern mitgeteilt werden:

- das geplante Datum der Einstellung der Geschäftstätigkeit;
- dass die geregelten Zertifikate für ungültig erklärt werden;

- dass einzig die Publikation der CRL und die Aufbewahrung des Tätigkeitsjournals sowie der dazugehörenden Belege nach der Einstellung der Geschäftstätigkeit gewährleistet werden;
- der Name der Nachfolge-CSP, die diese beschränkten Aufgaben übernimmt;
- die Kontaktinformationen der Nachfolge-CSP.

3.2 Verwaltung der geregelten Zertifikate

Die anerkannte CSP, die ihre Geschäftstätigkeit aufgibt, sollte spätestens 5 Tage, bevor sie die Zertifizierungsdienste nach ZertES [1] nicht mehr anbietet, die noch gültigen geregelten Zertifikate für ungültig erklären und die letzte CRL erstellen, signieren und online veröffentlichen.

Die Veröffentlichung einer einzigen CRL genügt. Die Gültigkeitsdauer der CRL muss so gewählt werden, dass sie die Gültigkeitsdauer aller revozierten Zertifikate abdeckt. Nach Ablauf der Gültigkeit eines für ungültig erklärten geregelten Zertifikats erübrigt sich die Veröffentlichung einer neuen CRL. Das geregelte Zertifikat bleibt in der letzten CRL aufgeführt.

Die Nachfolge-CSP sollte überprüfen, ob sie die übertragenen Daten interpretieren kann. Datenzugang und -auswertung sollten während der Mindestaufbewahrungszeit von 11 Jahren nach Ablauf der Gültigkeitsdauer aller geregelten Zertifikate sichergestellt werden (vgl. Art. 11 VZertES [2]).

Der Domain-Name einer anerkannten CSP, die ihre Geschäftstätigkeit aufgibt, sollte beibehalten werden, damit die Signaturüberprüfer auf die letzte CRL und die übrigen zur Überprüfung der geregelten Zertifikate nützlichen Informationen zugreifen können.

Folgende Fälle sind beispielsweise vorstellbar, um die Publikation der CRL und der übrigen zur Überprüfung der geregelten Zertifikate nützlichen Informationen sicherzustellen:
- behält die anerkannte CSP, die ihre Geschäftstätigkeit aufgibt, ihren Internet-Domain-Namen der zweiten Ebene, sollte sie die CRL und die übrigen zur Überprüfung der geregelten Zertifikate nützlichen Informationen veröffentlichen;
- behält die anerkannte CSP, die ihre Geschäftstätigkeit aufgibt, ihren Internet-Domain-Namen der zweiten Ebene nicht, sollte sie diesen an die Nachfolge-CSP übertragen. In diesem Fall dürfte der Internet-Domain-Name der zweiten Ebene einzig benutzt werden, um Informationen bezüglich der für ungültig erklärten geregelten Zertifikate zu publizieren.

3.3 Verwaltung der Schlüssel der anerkannten CSP

Bevor die anerkannte CSP, die ihre Geschäftstätigkeit aufgibt, die Zertifizierungsdienste nach ZertES [1] nicht mehr anbietet, sollte sie ihr eigenes Zertifikat für ungültig erklären und die ARL (Authority Revocation List) aktualisieren. Die Nachfolge-CSP sollte überprüfen, ob sie die übertragenen Daten interpretieren kann. Datenzugang und -auswertung sollten während der Mindestaufbewahrungszeit von 11 Jahren nach Ablauf der Gültigkeitsdauer aller geregelten Zertifikate sichergestellt werden.

Gibt die anerkannte CSP alle ihre Zertifizierungstätigkeiten auf, sollte sie auch das Root-CA-Zertifikat für ungültig erklären.

Die anerkannte CSP, die ihre Geschäftstätigkeit aufgibt, sollte ihren privaten Schlüssel vernichten oder unbrauchbar machen, bevor sie die Zertifizierungsdienste nach ZertES [1] nicht mehr anbietet.

3.4 Tätigkeitsjournal

Die anerkannte CSP, die ihre Geschäftstätigkeit aufgibt, sollte der Nachfolge-CSP das

Tätigkeitsjournal sowie die entsprechenden Belege über den Lebenszyklus der geregelten Zertifikate spätestens 5 Tage, bevor sie die Zertifizierungsdienste nach ZertES [1] nicht mehr anbietet, übertragen. Die Daten über die Funktionsweise der Systeme, die im Rahmen der Infrastruktur der CSP eingerichtet wurden, sollten nicht unbedingt weitergeleitet werden.

Die Daten sollten in einem lesbaren Format und auf einem lesbaren Datenträger übergeben werden.

Wenn die anerkannte CSP, die ihre Geschäftstätigkeit aufgibt, und die Nachfolge-CSP sich nicht einigen können, sollten Text- oder XML-Dateien mit einer ISO-8859-1 oder UTF-8 Codierung benutzt werden, um Umlaute oder Sonderzeichen darstellen zu können. Wenn in Englisch protokolliert wurde, sollten ASCII-Dateien ausreichend sein. Als Datenträger sollten CDs oder DVDs benutzt werden.

Die anerkannte CSP, die ihre Geschäftstätigkeit aufgibt, sollte der Nachfolge-CSP eine Dokumentation abgeben, mit deren Hilfe die Systeme identifiziert werden können und aus welcher das Zusammenspiel der verschiedenen Komponenten ersichtlich ist.

Die Nachfolge-CSP sollte überprüfen, ob sie die übertragenen Daten interpretieren kann. Datenzugang und -auswertung sollten während der Mindestaufbewahrungszeit von 11 Jahren sichergestellt werden.

3.5 CP, CPS und weitere öffentliche Informationen

Eine Anpassung der CP und CPS ist nicht erforderlich.

CP und CPS sollten bis Ablauf der Gültigkeit aller Zertifikate online veröffentlicht werden. Der Domain-Name einer anerkannten CSP, die ihre Geschäftstätigkeit aufgibt, sollte gemäss Kapitel 3.2 beibehalten werden, damit die Signaturüberprüfer auf die CP und CPS zugreifen können.

Die CP und die CPS sollten Informationen zu den Massnahmen enthalten, die zwecks Sicherstellung der Überprüfung nach Aufgabe der Geschäftstätigkeit getroffen werden.

In den Kapiteln über die Aufgabe der Geschäftstätigkeit sollten die CP und die CPS aufzeigen, wie die Nachfolge-CSP bestimmt werden kann. Man kann zum Beispiel auf den Link der SAS-Webseite hinweisen, auf der sich die Liste der anerkannten CSP befindet.

In den Kapiteln über die Aufgabe der Geschäftstätigkeit sollten die CP und die CPS darauf hinweisen, dass einzig die Publikation der CRL und die Aufbewahrung des Tätigkeitsjournals sowie der dazugehörenden Belege nach der Einstellung der Geschäftstätigkeit gewährleistet werden.

Biel, den 6. Dezember 2017

BUNDESAMT FÜR KOMMUNIKATION

Der Direktor

Philipp Metzger

Anhang
Zeitlicher Ablauf der verschiedenen Etappen