Zertifizierungsprogramm eIDAS der Zertifizierungsstelle (KBS) (akkreditierter Bereich) der SRC Security Research & Consulting GmbH

Version 2.0 / 11.11.2022

Inhaltsverzeichnis

1	Zweck	3
2	Anwendungsbereich und erfasste Produkte	5
3	Ablauf der Zertifizierung	10
4	Beschwerden und Einsprüche	20
5	Normen	21
6	Anlagen	22
7	Glossar	23

1 Zweck

Die Zertifizierungsstelle der SRC Research & Consulting GmbH – kurz SRC – bietet anderen Unternehmen die Zertifizierung von Produkten, Systemen, Dienstleistungen und Prozessen aus dem Bereich Informationstechnik an. Im Folgenden wird vereinfachend von der Zertifizierung von Produkten gesprochen. Die Zertifizierung erfolgt auf der Grundlage von normativen Dokumenten wie Rechtsvorschriften, Normen oder technischen Spezifikationen, welche Anforderungen an Produkte festlegen. Die beauftragenden Unternehmen (Kunden) haben mit einer Zertifizierung durch einen unabhängigen Dritten die Möglichkeit zu dokumentieren, dass ihre Produkte die festgelegten Anforderungen erfüllen.

Die Zertifizierungsstelle der SRC ist auf Basis der DIN EN ISO/IEC 17065 für die Zertifizierung von Produkten in den Bereichen IT-Sicherheit und Sicherheitstechnik akkreditiert. Das vorliegende Dokument beschreibt das Zertifizierungsprogramm für die Vergabe der SRC-Zertifikate für qualifizierte Vertrauensdiensteanbieter und die von ihnen erbrachten qualifizierten Vertrauensdienste im Anwendungsbereich der Verordnung (EU) Nr. 910/2014 des europäischen Parlamentes und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Verordnung).

Das Zertifizierungsprogramm eIDAS enthält die folgenden Teilprogramme für die Zertifizierung von qualifizierten Vertrauensdiensten und Vertrauensdienst-Komponenten:

1) Qualifizierter Dienst für die Erstellung von qualifizierten Zertifikaten für elektronische Signaturen – ohne die Notwendigkeit, dass sich die elektronischen Signaturerstellungsdaten in einer qualifizierten elektronischen Signaturerstellungseinheit (QSCD) befinden – gemäß Art. 28 der eIDAS-Verordnung,

    1a. Qualifizierter Dienst für die Erstellung von qualifizierten Zertifikaten für elektronische Signaturen – ohne die Notwendigkeit, dass sich die elektronischen Signaturerstellungsdaten in einer qualifizierten elektronischen Signaturerstellungseinheit (QSCD) befinden – mit der Option zur Verwaltung der Signaturerstellungsdaten im Auftrag des Unterzeichners (Fernsignatur)

2) Qualifizierter Dienst für die Erstellung von qualifizierten Zertifikaten für elektronische Signaturen – mit der Notwendigkeit, dass sich die elektronischen Signaturerstellungsdaten in einer qualifizierten elektronischen Signaturerstellungseinheit (QSCD) befinden – gemäß Art. 28 und 29 der eIDAS-Verordnung,

    2a. Qualifizierter Dienst für die Erstellung von qualifizierten Zertifikaten für elektronische Signaturen – mit der Notwendigkeit, dass sich die elektronischen Signaturerstellungsdaten in einer qualifizierten elektronischen Signaturerstellungseinheit (QSCD) befinden – mit der Option zur Verwaltung der Signaturerstellungsdaten im Auftrag des Unterzeichners (Fernsignatur)

3) Qualifizierter Dienst für die Erstellung von qualifizierten Zertifikaten für elektronische Siegel – ohne die Notwendigkeit, dass sich die elektronischen Siegelerstellungsdaten in einer qualifizierten elektronischen Siegelerstellungseinheit (QSCD) befinden – gemäß Art. 38 der eIDAS-Verordnung,

3a. Qualifizierter Dienst für die Erstellung von qualifizierten Zertifikaten für elektronische Siegel – ohne die Notwendigkeit, dass sich die elektronischen Siegelerstellungsdaten in einer qualifizierten elektronischen Siegelerstellungseinheit (QSCD) befinden – mit der Option zur Verwaltung der Siegelerstellungsdaten im Auftrag des Unterzeichners (Fernsiegel)

4) Qualifizierter Dienst für die Erstellung von qualifizierten Zertifikaten für elektronische Siegel – mit der Notwendigkeit, dass sich die elektronischen Siegelerstellungsdaten in einer qualifizierten elektronischen Siegelerstellungseinheit (QSCD) befinden – gemäß Art. 38 und 39 der eIDAS-Verordnung,

4a. Qualifizierter Dienst für die Erstellung von qualifizierten Zertifikaten für elektronische Siegel – mit der Notwendigkeit, dass sich die elektronischen Siegelerstellungsdaten in einer qualifizierten elektronischen Siegelerstellungseinheit (QSCD) befinden – mit der Option zur Verwaltung der Siegelerstellungsdaten im Auftrag des Unterzeichners (Fernsiegel),

5) Qualifizierter Dienst für die Erstellung von qualifizierten Zertifikaten für die Website-Authentifizierung, gemäß Art. 45 der eIDAS-Verordnung,

6) Qualifizierter Dienst für die Erstellung von qualifizierten elektronischen Zeitstempeln gemäß Art. 42 der eIDAS-Verordnung,

7) Qualifizierter Validierungsdienst für qualifizierte elektronische Signaturen gemäß Art. 33 der eIDAS-Verordnung und / oder qualifizierte elektronische Siegel gemäß Artikel 40 der eIDAS-Verordnung,

8) Qualifizierter Bewahrungsdienst für qualifizierte elektronische Signaturen gemäß Art. 34 der eIDAS-Verordnung und / oder qualifizierte elektronische Siegel gemäß Art. 40 der eIDAS-Verordnung,

9) Qualifizierter Dienst für die Zustellung elektronischer Einschreiben gemäß Art. 44 der eIDAS-Verordnung,

10) Vertrauensdienst-Komponente zur Identitätsfeststellung von natürlichen Personen und / oder juristischen Personen gemäß Art. 24, Abs. 1 der eIDAS-Verordnung.

Alle Angaben dieses Zertifizierungsprogrammes gelten gleichermaßen für alle Teilprogramme, es sei denn es ist ausdrücklich anders beschrieben.

Das Zertifizierungsprogramm eIDAS mit seinen Teilprogrammen 1) – 10) soll Unternehmen, die eine Zertifizierung bei SRC durchführen lassen wollen, einen Überblick über das Verfahren geben. Das Zertifizierungsprogramm wird Kunden und anderen Parteien mit berechtigtem Interesse auf Anfrage zur Verfügung gestellt und zudem in der jeweils gültigen Fassung auf der Website der Zertifizierungsstelle (https://src-zert.de) veröffentlicht. Falls darüber hinaus Fragen zum Zertifizierungsverfahren bestehen, kann die Zertifizierungsstelle wie folgt erreicht werden:

SRC Security Research & Consulting GmbH

Zertifizierungsstelle (KBS)

Emil-Nolde-Str. 7
53113 Bonn

E-Mail: info@src-gmbh.de
Telefon: +49(0)228 2806-0

2 Anwendungsbereich und erfasste Produkte

Die Zertifizierungsstelle der SRC bietet qualifizierten Vertrauensdiensteanbietern oder bisher nicht-qualifizierten Vertrauensdiensteanbietern, die den Status eines qualifizierten Vertrauensdiensteanbieters im Sinne der eIDAS-Verordnung anstreben, die Bewertung und Zertifizierung der genannten (qualifizierten) Vertrauensdienste oder Vertrauensdienst-Komponenten gemäß der Teilprogramme 1) – 10) (wo relevant, samt Unterprogrammen a.) an.

Die Bewertung erfolgt auf der Grundlage relevanter Normen oder technischer Spezifikationen der Normierungsgremien ETSI und CEN. Die zu berücksichtigenden Produktanforderungen für die Teilprogramme werden im Folgenden aufgeführt:

2.1 Qualifizierte Dienste für die Erstellung von qualifizierten Zertifikaten für elektronische Signaturen ohne QSCD gemäß Art. 28 eIDAS, gemäß Teilprogramm 1):

Für alle Anbieter:

- Verordnung (EU) Nr. 910/2014 vom 23.07.2014 (eIDAS)

sowie

- ETSI EN 319 411-2 V2.3.1 (2021-05), Richtlinie QCP-n, einschließlich der referenzierten Anforderungen aus
    - ETSI EN 319 411-1 V1.3.1 (2021-05), Richtlinie NCP und
    - ETSI EN 319 401 V2.3.1 (2021-05)

Für Anbieter aus der Bundesrepublik Deutschland zusätzlich:

- Vertrauensdienstegesetz vom 18. Juli 2017 (VDG) und
- Vertrauensdiensteverordnung vom 15. Februar 2019 (VDV)

Falls der Anbieter die Signaturerstellungsdaten im Auftrag des Unterzeichners verwaltet (Unterprogramm a.) zusätzlich:

- CEN EN 419 241:2018 (2018-09)

Falls der Anbieter Antragssteller (natürliche Personen) über video-gestützte Verfahren oder (teilweise) automatisierte video-gestützte Verfahren identifiziert, die er im eigenen Verantwortungsbereich betreibt (keine Einbindung einer Vertrauensdienste-Komponente), so sind zusätzlich die Produktanforderungen für Teilprogramm 10) zu erfüllen.

2.2 Qualifizierte Dienste für die Erstellung von qualifizierten Zertifikaten für elektronische Signaturen mit QSCD gemäß Art. 28 und 29 eIDAS, gemäß Teilprogramm 2):

Für alle Anbieter:

- Verordnung (EU) Nr. 910/2014 vom 23.07.2014 (eIDAS)

sowie

- ETSI EN 319 411-2 V2.3.1 (2021-05), Richtlinie QCP-n-qscd, einschließlich der referenzierten Anforderungen aus
    - ETSI EN 319 411-1 V1.3.1 (2021-05), Richtlinie NCP+ und
    - ETSI EN 319 401 V2.3.1 (2021-05)

Für Anbieter aus der Bundesrepublik Deutschland zusätzlich:

- Vertrauensdienstegesetz vom 18. Juli 2017 (VDG) und
- Vertrauensdiensteverordnung vom 15. Februar 2019 (VDV)

Falls der Anbieter die Signaturerstellungsdaten im Auftrag des Unterzeichners verwaltet (Unterprogramm a.) zusätzlich:

- CEN EN 419 241:2018 (2018-09)

Falls der Anbieter Antragssteller (natürliche Personen) über video-gestützte Verfahren oder (teilweise) automatisierte video-gestützte Verfahren identifiziert, die er im eigenen Verantwortungsbereich betreibt (keine Einbindung einer Vertrauensdienste-Komponente), so sind zusätzlich die Produktanforderungen für Teilprogramm 10) zu erfüllen.

2.3 Qualifizierte Dienste für die Erstellung von qualifizierten Zertifikaten für elektronische Siegel ohne QSCD gemäß Art. 38 eIDAS, gemäß Teilprogramm 3):

Für alle Anbieter:

- Verordnung (EU) Nr. 910/2014 vom 23.07.2014 (eIDAS)

sowie

- ETSI EN 319 411-2 V2.3.1 (2021-05), Richtlinie QCP-l, einschließlich der referenzierten Anforderungen aus
  - ETSI EN 319 411-1 V1.3.1 (2021-05), Richtlinie NCP und
  - ETSI EN 319 401 V2.3.1 (2021-05)

Für Anbieter aus der Bundesrepublik Deutschland zusätzlich:

- Vertrauensdienstegesetz vom 18. Juli 2017 (VDG) und
- Vertrauensdiensteverordnung vom 15. Februar 2019 (VDV)

Falls der Anbieter die Siegelerstellungsdaten im Auftrag des Unterzeichners verwaltet (Unterprogramm a.) zusätzlich:

- CEN EN 419 241:2018 (2018-09)

Für Anbieter, die qualifizierte Zertifikate für elektronische Siegel ausstellen, welche durch Zahlungsdienstleister im Sinne der Richtlinie (EU) 2015/2366 des europäischen Parlamentes und des Rates vom 25. November 2015 verwendet werden, zusätzlich:

- ETSI TS 119 495 V1.5.1 (2021-04)

Falls der Anbieter Antragssteller (gesetzliche Vertreter der juristischen Personen) über video-gestützte Verfahren oder (teilweise) automatisierte video-gestützte Verfahren identifiziert, die er im eigenen Verantwortungsbereich betreibt (keine Einbindung einer Vertrauensdienste-Komponente), so sind zusätzlich die Produktanforderungen für Teilprogramm 10) zu erfüllen.

2.4 Qualifizierte Dienste für die Erstellung von qualifizierten Zertifikaten für elektronische Siegel mit QSCD gemäß Art. 38 und 39 eIDAS, gemäß Teilprogramm 4):

Für alle Anbieter:

- Verordnung (EU) Nr. 910/2014 vom 23.07.2014 (eIDAS)

sowie

- ETSI EN 319 411-2 V2.3.1 (2021-05), Richtlinie QCP-l-qscd, einschließlich der referenzierten Anforderungen aus
    - ETSI EN 319 411-1 V1.3.1 (2021-05), Richtlinie NCP+ und
    - ETSI EN 319 401 V2.3.1 (2021-05)

Für Anbieter aus der Bundesrepublik Deutschland zusätzlich:

- Vertrauensdienstegesetz vom 18. Juli 2017 (VDG) und
- Vertrauensdiensteverordnung vom 15. Februar 2019 (VDV)

Falls der Anbieter die Siegelerstellungsdaten im Auftrag des Unterzeichners verwaltet (Unterprogramm a.) zusätzlich:

- CEN EN 419 241:2018 (2018-09)

Für Anbieter, die qualifizierte Zertifikate für elektronische Siegel ausstellen, welche durch Zahlungsdienstleister im Sinne der Richtlinie (EU) 2015/2366 des europäischen Parlamentes und des Rates vom 25. November 2015 verwendet werden, zusätzlich:

- ETSI TS 119 495 V1.5.1 (2021-04)

Falls der Anbieter Antragssteller (gesetzliche Vertreter der juristischen Personen) über video-gestützte Verfahren oder (teilweise) automatisierte video-gestützte Verfahren identifiziert, die er im eigenen Verantwortungsbereich betreibt (keine Einbindung einer Vertrauensdienste-Komponente), so sind zusätzlich die Produktanforderungen für Teilprogramm 10) zu erfüllen.

2.5 Qualifizierte Dienste für die Erstellung von qualifizierten Zertifikaten für die Website-Authentifizierung gemäß Art. 45 eIDAS, gemäß Teilprogramm 5):

Für alle Anbieter:

- Verordnung (EU) Nr. 910/2014 vom 23.07.2014 (eIDAS)

sowie

- ETSI EN 319 411-2 V2.3.1 (2021-05), Richtlinie QCP-w, einschließlich der referenzierten Anforderungen aus
    - ETSI EN 319 411-1 V1.3.1 (2021-05), Richtlinie NCP+ und
    - ETSI EN 319 401 V2.3.1 (2021-05)

Für Anbieter aus der Bundesrepublik Deutschland zusätzlich:

- Vertrauensdienstegesetz vom 18. Juli 2017 (VDG) und
- Vertrauensdiensteverordnung vom 15. Februar 2019 (VDV)

Für Anbieter, die qualifizierte Zertifikate für die Website Authentisierung ausstellen, welche durch Zahlungsdienstleister im Sinne der Richtlinie (EU) 2015/2366 des europäischen Parlamentes und des Rates vom 25. November 2015 verwendet werden, zusätzlich:

- ETSI TS 119 495 V1.5.1 (2021-04)

Falls der Anbieter Antragssteller (natürliche Personen oder gesetzliche Vertreter der juristischen Personen) über video-gestützte Verfahren oder (teilweise) automatisierte video-gestützte Verfahren identifiziert, die er im eigenen Verantwortungsbereich betreibt (keine Einbindung einer Vertrauensdienste-Komponente), so sind zusätzlich die Produktanforderungen für Teilprogramm 10) zu erfüllen.

2.6 Qualifizierte Dienste für die Erstellung von qualifizierten elektronischen Zeitstempeln gemäß Art. 42 eIDAS, gemäß Teilprogramm 6):

Für alle Anbieter:

- Verordnung (EU) Nr. 910/2014 vom 23.07.2014 (eIDAS)

sowie

- ETSI EN 319 421 V1.1.1 (2016-03), einschließlich der referenzierten Anforderungen aus
    - ETSI EN 319 401 V2.3.1 (2021-05)

Für Anbieter aus der Bundesrepublik Deutschland zusätzlich:

- Vertrauensdienstegesetz vom 18. Juli 2017 (VDG) und
- Vertrauensdiensteverordnung vom 15. Februar 2019 (VDV)

2.7 Qualifizierte Validierungsdienste für qualifizierte elektronische Signaturen gemäß Art. 33 eIDAS und / oder qualifizierte elektronische Siegel gemäß Art. 40 eIDAS, gemäß Teilprogramm 7):

Für alle Anbieter:

- Verordnung (EU) Nr. 910/2014 vom 23.07.2014 (eIDAS)

sowie

- ETSI TS 119 441 V1.1.1 (2018-08), Richtlinie QSVSP, einschließlich der referenzierten Anforderungen aus
    - ETSI EN 319 401 V2.3.1 (2021-05)

ETSI TS 119 441 zielt darauf ab, die allgemein gültigen Anforderungen der Verordnung (EU) Nr. 910/2014 an die Validierung von elektronischen Signaturen und Siegeln zu erfüllen. Das Dokument enthält zusätzliche Anforderungen für EU-qualifizierte Validierungsdienste (QSVSP), die die Anforderungen an einen qualifizierten Validierungsdienst für qualifizierte elektronische Signaturen oder für qualifizierte elektronische Siegel gemäß Artikel 33 der Verordnung (EU) Nr. 910/2014 erfüllen wollen.

Für Anbieter aus der Bundesrepublik Deutschland zusätzlich:

- Vertrauensdienstegesetz vom 18. Juli 2017 (VDG) und
- Vertrauensdiensteverordnung vom 15. Februar 2019 (VDV)

2.8 Qualifizierte Bewahrungsdienste für qualifizierte elektronische Signaturen gemäß Art. 34 eIDAS und / oder qualifizierte elektronische Siegel gemäß Art. 40 eIDAS, gemäß Teilprogramm 8):

Für alle Anbieter:

- Verordnung (EU) Nr. 910/2014 vom 23.07.2014 (eIDAS)

sowie

- ETSI TS 119 511 V1.1.1 (2019-06), Bewahrungsmodell WST, WTS oder WOS, einschließlich der referenzierten Anforderungen aus
    - ETSI EN 319 401 V2.3.1 (2021-05)

ETSI TS 119 511 zielt darauf ab, die Anforderungen der Artikel 34 und 40 der Verordnung (EU) Nr. 910/2014 zu erfüllen, um Vertrauen in Bewahrungsdienste zu schaffen, die zur Bewahrung des Gültigkeitsstatus digitaler Signaturen oder zum Nachweis der Existenz digitaler Objekte unter Verwendung digitaler Signaturtechniken verwendet werden können.

Für Anbieter aus der Bundesrepublik Deutschland zusätzlich:

- Vertrauensdienstegesetz vom 18. Juli 2017 (VDG) und
- Vertrauensdiensteverordnung vom 15. Februar 2019 (VDV)

2.9 Qualifizierte Dienste für die Zustellung elektronischer Einschreiben gemäß Art. 44 eIDAS, gemäß Teilprogramm 9):

Für alle Anbieter:

- Verordnung (EU) Nr. 910/2014 vom 23.07.2014 (eIDAS)

sowie

- ETSI EN 319 521 V1.1.1 (2019-02), Richtlinie QERDS, einschließlich der referenzierten Anforderungen aus
    - ETSI EN 319 401 V2.3.1 (2021-05)

oder

- ETSI EN 319 531 V1.1.1 (2019-01), Richtlinie QREMS, einschließlich der referenzierten Anforderungen aus
    - ETSI EN 319 401 V2.3.1 (2021-05)
    - ETSI EN 319 521 V1.1.1 (2019-02)

Für Anbieter aus der Bundesrepublik Deutschland zusätzlich:

- Vertrauensdienstegesetz vom 18. Juli 2017 (VDG) und
- Vertrauensdiensteverordnung vom 15. Februar 2019 (VDV)

Falls der Anbieter Sender bzw. Empfänger (natürliche Personen oder gesetzliche Vertreter der juristischen Personen) über video-gestützte Verfahren oder (teilweise) automatisierte video-gestützte Verfahren identifiziert, die er im eigenen Verantwortungsbereich betreibt (keine Einbindung einer Vertrauensdienste-Komponente), so sind zusätzlich die Produktanforderungen für Teilprogramm 10) zu erfüllen.

2.10 Vertrauensdienste-Komponenten zur Identitätsfeststellung von natürlichen Personen und / oder juristischen Personen gemäß Art. 24 (1) eIDAS, gemäß Teilprogramm 10):

Für alle Anbieter:

- Verordnung (EU) Nr. 910/2014 vom 23.07.2014 (eIDAS)

sowie

- ETSI EN 319 411-2 V2.3.1 (2021-05), Anforderungen an Registrierungsstellen aus den Richtlinien QCP-n und / oder QCP-l, einschließlich der referenzierten Anforderungen aus
    - ETSI EN 319 411-1 V1.3.1 (2021-05), Richtlinie NCP und
    - ETSI EN 319 401 V2.3.1 (2021-05)

Für Anbieter aus der Bundesrepublik Deutschland zusätzlich:

- Vertrauensdienstegesetz vom 18. Juli 2017 (VDG) und
- Vertrauensdiensteverordnung vom 15. Februar 2019 (VDV) und
- Für video-gestützte Identifizierungsverfahren: Verfügung Nr. 118/2021 der Bundesnetzagentur "Verlängerung der befristeten Anerkennung der Methode der Videoidentifizierung als „sonstige Identifizierungsmethode" gemäß § 11 Absatz 1 VDG" (Videoident-Verfügung) und
- Für automatisierte video-gestützte Identifizierungsverfahren: Mitteilung Nr. 340/2021 der Bundesnetzagentur „Verlängerung der befristeten Anerkennung der Methode der Videoidentifizierung als „sonstige Identifizierungsmethode" gemäß § 11 Absatz 1 VDG"(Autoident-Verfügung)
- Für Smart-eID-Verfahren: Mitteilung Nr. 341/2021 der Bundesnetzagentur „Vorläufige Anerkennung einer innovativen Identifizierungsmethode gemäß § 11 Absatz 3 VDG" (Smart-eID-Verfügung)

Für Anbieter, welche eine Identifizierung über notifizierte elektronische Identifizierungsmittel (gemäß eIDAS-Verordnung, Artikel 24.1 b)) oder eine Identifizierung mittels eines Zertifikates einer qualifizierten elektronischen Signatur bzw. eines qualifizierten elektronischen Siegels (gemäß eIDAS-Verordnung Artikel 24 c)) anbieten oder für Anbieter aus anderen Mitgliedstaaten der europäischen Union, die ein video-gestütztes Identifizierungsverfahren bzw. ein teilweise oder vollständig automatisiertes video-gestütztes Identifizierungsverfahren anbieten und dabei nicht freiwillig eine Prüfung nach den Anforderungen der Verfügung der Bundesnetzagentur (s.o.) anstreben, zusätzlich:

- ETSI TS 119 461, passender Use Case der Richtlinie Baseline LoIP.

Eine Abbildung der gesetzlichen Anforderungen aus der eIDAS-Verordnung, dem Vertrauensdienstegesetz und der Vertrauensdiensteverordnung auf die Produktanforderungen aus den relevanten Normen und technischen Spezifikationen findet sich in Anlage 2 des Zertifizierungsprogrammes.

Die anzuwendenden Ermittlungsmethoden und Verfahren für die Produktanforderungen aus den relevanten Normen und technischen Spezifikationen können den entsprechenden Anlagen 3.* des Zertifizierungsprogrammes entnommen werden.

3 Ablauf der Zertifizierung

Die Konformitätsbewertung von Produkten erfolgt auf der Grundlage relevanter Normen oder technischer Spezifikationen der Normierungsgremien ETSI und CEN (siehe Kapitel 2). Die Konformitätsbewertung umfasst die Bewertung des Produktes anhand aller mit der Evaluierung im Zusammenhang stehender Informationen und Ergebnissen

sowie die Zertifizierungsentscheidung. Die Durchführung der Konformitätsbewertung erfolgt auf Basis der DIN EN ISO/IEC 17065 in Verbindung mit ETSI EN 319 403-1.

3.1 Angebotsanfrage und Zertifizierungsvereinbarung

Der Kunde für die Zertifizierung richtet seine Anfrage zum Zertifizierungsvorgang an die Zertifizierungsstelle. Für die Angebotserstellung liefert der Kunde eine Beschreibung des Zertifizierungsgegenstandes (Geltungsbereich) auf Basis dessen der Aufwand der Zertifizierung kalkuliert und ein individuelles Angebot erstellt wird. Hierfür müssen durch den Kunden mindestens die folgenden Informationen bereitgestellt werden:

- Die Art des zu zertifizierenden Vertrauensdienstes (1) – 10)) und die zugehörigen Produktanforderungen, nach denen der Kunde eine Zertifizierung wünscht,
- relevante Einzelheiten über den antragstellenden Vertrauensdiensteanbieter, insbesondere den Namen, die Anschrift und die Angabe verantwortlicher Ansprechpartner,
- die Art und die Anschriften aller für die Erbringung des zu zertifizierenden Vertrauensdienstes relevanter Standorte, sowie
- ggf. die für den zu zertifizierenden Vertrauensdienst relevanten Dienste-Zertifikate (sofern bereits vorhanden).

Durch die Leitung der Zertifizierungsstelle oder einen erfahrenen Evaluator erfolgt eine Bewertung des Zertifizierungsantrages. Hierbei wird insbesondere geprüft, ob die vorliegenden Informationen für die Durchführung des Zertifizierungsprozesses ausreichend sind und alle Unklarheiten geklärt wurden, ob der Geltungsbereich festgelegt ist, ob alle für die Evaluierungstätigkeiten erforderlichen Mittel verfügbar sind und ob die Zertifizierungsstelle über die nötigen Fähigkeiten und Kompetenzen verfügt.

Nach positiver Antragsbewertung informiert die Zertifizierungsstelle den Interessenten über das weitere Zertifizierungsverfahren und der Kunde erhält auf Wunsch ein Zertifizierungsangebot, das die Zertifizierungsvereinbarung mit den Zertifizierungsbedingungen enthält.

Der Kunde erteilt auf der Grundlage des Angebotes der Zertifizierungsstelle den Auftrag zur Zertifizierung und erkennt durch die Unterzeichnung der Zertifizierungsvereinbarung die Zertifizierungsbedingungen an.

Nach Auftragseingang für die Zertifizierung vergibt die Zertifizierungsstelle eine Registrierungsnummer für die Zertifizierung und benennt dem Kunden einen für das Verfahren verantwortlichen Ansprechpartner.

Die Evaluierung wird von einem Evaluierungsteam unter Verantwortung des Teamleiters gemäß den Anforderungen und Vorgaben der Zertifizierungsstelle durchgeführt. Der verantwortliche Absprechpartner (Teamleiter) plant mit dem Kunden und dem Evaluierungsteam den zeitlichen Ablauf des Evaluierungsvorgangs und räumt bei Bedarf in Vorgesprächen letzte Unklarheiten bezüglich des Evaluierungs- und Zertifizierungsablaufs aus.

3.2 Evaluierung

Die Evaluierung umfasst alle Tätigkeiten, um zu vollständigen Informationen über die Erfüllung der festgelegten Anforderungen durch den Zertifizierungsgegenstand zu ge-

langen. Dies schließt planende und vorbereitendende Tätigkeiten sowie Dokumentenprüfungen, Ermittlung von Produktmerkmalen nach festgelegten Verfahren, Prüfungen, Inspektionen und Audits mit ein.

Die Evaluierung wird von Evaluatoren durchgeführt, die Mitarbeiter der Zertifizierungsstelle sind oder durch die Zertifizierungsstelle zugelassen sind. Die Zertifizierungsstelle stellt sicher, dass nur Evaluatoren eingesetzt werden, die über die notwendige Kompetenz und Unparteilichkeit verfügen. Die Evaluatoren untersuchen den Vertrauensdiensteanbieter bzgl. der Konformität zu den für den qualifizierten Vertrauensdienst relevanten Anforderungen der eIDAS-Verordnung unter Berücksichtigung der relevanten Produktanforderungen.

Um die Durchführung der Evaluierung sicherzustellen, muss der Kunde die geforderte Dokumentation zur Verfügung stellen, den Evaluatoren den Zugang zu allen für die Erbringung der zu zertifizierenden Vertrauensdienste relevanten Standorten ermöglichen sowie einen verantwortlichen Ansprechpartner benennen.

Im Rahmen der Evaluierung wird festgestellt, ob die organisatorischen und technischen Maßnahmen des Vertrauensdiensteanbieters den Anforderungen genügen. Die Evaluierung des Vertrauensdienstes unterteilt sich in zwei Phasen:

- die Dokumentationsprüfung und die daran anschließende
- Evaluierung vor Ort[1].

In der ersten Phase der Evaluierung des Vertrauensdiensteanbieters wird die in den Produktanforderungen geforderte Dokumentation durch die Evaluatoren analysiert und auf ihre Konformität überprüft. Die Dokumentation muss für alle Vertrauensdienste mindestens die folgenden Dokumente umfassen:

- Die Trust Service Policy,
- das Trust Service Practice Statement,
- das Sicherheitskonzept,
- Dokumente zum Risikomanagement, inkl. einer dokumentierten Risikoanalyse,
- Prozessbeschreibungen sowie relevante Arbeitsanweisungen und technische Dokumentationen,
- die für die Nutzung des Vertrauensdienstes geltenden Geschäftsbedingungen,
- Unterlagen für die Schulung der Mitarbeiter,
- Dienstleistungsverträge (bei Auslagerung von Tätigkeiten) und
- den Beendigungsplan (Termination Plan) für den Vertrauensdienst.

[1] In spezifischen Situationen, die eine Evaluierung vor Ort aus wesentlichen Gründen nicht zulässt (z.B. Schutzmaßnahmen aufgrund der Covid-19 Pandemie), kann die Evaluierung in Form eines Remote-Audits vorgenommen werden.

Falls die Dokumentationsprüfung zeigt, dass der Vertrauensdienst die Produktanforderungen nicht erfüllt, wird keine Evaluierung vor Ort durchgeführt. Der Kunde hat Gelegenheit die Dokumentation des Vertrauensdienstes an die Anforderungen anzupassen und erneut durch die Evaluatoren prüfen zu lassen.

Kommen die Evaluatoren nach der Bewertung der Dokumentation des Vertrauensdiensteanbieters zu dem Schluss, dass die Dokumentation die Anforderungen der Produktanforderungen erfüllt, so folgt die zweite Phase, die Evaluierung vor Ort. Ziel dieser Evaluierung ist es festzustellen, ob der Vertrauensdienst gemäß den Angaben in der Dokumentation implementiert ist und ob die Implementierung den normativen Produktanforderungen entspricht. Die Evaluierung vor Ort wird im Rahmen eines vorher mit dem Kunden abgestimmten Termins beim Vertrauensdiensteanbieter durchgeführt.

Die Evaluierung vor Ort umfasst die Überprüfung der organisatorischen, baulichen und technischen Umsetzung der in der Dokumentation beschriebenen Maßnahmen zur Erfüllung der Anforderungen.

Dabei werden von den Evaluatoren stichprobenhaft Nachweise durch Befragungen von Mitarbeitern, Prüfungen von Unterlagen, Beobachtungen von Tätigkeiten und Bedingungen sowie durch technische Tests gesammelt. Soweit vorhanden können auch Bewertungen anderer unabhängiger Stellen zu einzelnen Teilen des zu beurteilenden Dienstes herangezogen werden. Zum Beispiel ist es nicht notwendig, dass die Evaluatoren eigene Evaluierungen von technischen Komponenten durchführen. Sie können für ihre Beurteilung Prüfberichte und Zertifikate anderer unabhängiger Stellen heranziehen. Dabei ist sicherzustellen, dass die verwendeten Ergebnisse für die Zertifizierung des qualifizierten Vertrauensdiensteanbieters und der von ihm erbrachten Vertrauensdienste nach eIDAS anwendbar sind.

Werden im Rahmen der Evaluierung Nichtkonformitäten festgestellt, wird der Kunde hierüber informiert. Entscheidet sich der Kunde für eine Fortsetzung des Zertifizierungsprozesses, stimmen die Evaluatoren die zusätzlichen Evaluierungsaufgaben mit dem Kunden ab, welche notwendig sind, um die Korrektur der Nichtkonformitäten zu verifizieren. Für diese Evaluierungsaufgaben werden erneut die zuvor beschriebenen Phasen der Evaluierung durchlaufen.

Nach erfolgter Evaluierung erstellen die Auditoren einen Evaluierungsbericht (Konformitätsbewertungsbericht gemäß Artikel 20 Absatz 1 eIDAS), der die Grundlage für die Zertifizierungsentscheidung darstellt.

3.3 Bewertung und Zertifizierungsentscheidung

Seitens der Zertifizierungsstelle erfolgen eine Bewertung der Evaluierung anhand des erstellten Evaluierungsberichts und eine Überwachung der Einhaltung der Verfahrensvorgaben auf Basis der DIN EN ISO/IEC 17065. Die Entscheidung über die Zertifizierung wird von der Leitung der Zertifizierungsstelle oder einem anderen erfahrenen Mitarbeiter der Zertifizierungsstelle, dem Zertifizierungsentscheider, unter Berücksichtigung der Zertifizierungsentscheidungskriterien getroffen.

Voraussetzung für eine positive Zertifizierungsentscheidung sind die folgenden Bedingungen:

- Die Unparteilichkeit der Evaluatoren und des Zertifizierungsentscheiders im Evaluierungs- und Zertifizierungsvorgang war und ist gegeben[2],
- der Zertifizierungsentscheider war am Evaluierungsprozess nicht beteiligt,
- eine Zertifizierungsvereinbarung mit Anerkennung der Zertifizierungsbedingungen ist mit dem Kunden getroffen,
- das Evaluierungs- und Zertifizierungsverfahren ist gemäß dem Zertifizierungsprogramm und den Regeln der Zertifizierungsstelle durchgeführt worden,
- der Evaluierungsbericht liegt vor und weist keine kritischen Nichtkonformitäten aus,
- die Evaluierung ist auf Basis der für den Dienst festlegten Normen, Gesetzen und Richtlinien durchgeführt worden und
- das Zertifikat weist ein Ergebnis in Übereinstimmung mit den Evaluierungsergebnissen aus.

Die Zertifizierungsentscheidung wird protokolliert und vom Zertifizierungsentscheider unterzeichnet[3]. Der Kunde wird über die Zertifizierungsentscheidung informiert.

Bei positiver Zertifizierungsentscheidung wird das Zertifikat ausgestellt, das den Geltungsbereich der Zertifizierung und eine Gültigkeit von maximal 2 Jahren wiedergibt sowie das Prüfzeichen darstellt. Ein gültiges Zertifikat berechtigt zur öffentlichen Nutzung des Prüfzeichens im Zusammenhang mit dem zertifizierten qualifizierten Vertrauensdienst gemäß den Nutzungsbedingungen des SRC-Zertifikats und des SRC-Prüfsiegels.

Wurden im Rahmen der Evaluierung nicht-kritische Nicht-Konformitäten identifiziert, so wird, falls die Kriterien für eine positive Zertifizierungsentscheidung erfüllt sind, ebenfalls eine positive Zertifizierungsentscheidung getroffen. In diesem Fall erfolgt eine Zertifizierung mit Auflagen und dem Vertrauensdiensteanbieter wird eine Frist von 3 Monaten, in begründeten Fällen eine Frist von 6 Monaten, nach Bekanntgabe im Evaluierungsbericht (Konformitätsbewertungsbericht) zur Behebung der Nicht-Konformitäten gewährt. Die Behebung wird durch ein aktualisiertes Zertifikat bzw. durch einen Nachtrag zur Konformitätsbewertung bestätigt. Dabei wird die ursprüngliche Gültigkeitsdauer des Zertifikates nicht verlängert. Kommt der Vertrauensdiensteanbieter der fristgerechten Behebung nicht nach, wird das unter Auflagen erteilte Zertifikat entzogen.

Bei negativer Zertifizierungsentscheidung wird der Kunde unter Nennung der Gründe schriftlich hierüber informiert. In diesem Fall kann der Kunde die Evaluierung wiederaufnehmen, sofern gewünscht.

Die Arbeiten der Zertifizierungsstelle werden überwiegend in den Geschäftsräumen von SRC in Bonn und/oder Wiesbaden durchgeführt. Darüber hinaus werden Prüfungen, Audits und Inspektionen auch bei Kunden durchgeführt.

---

[2] Für jeden Zertifizierungsvorgang wird eine projektspezifische Risikoanalyse vorgenommen und im Formular Risikoanalyse zur Unparteilichkeit dokumentiert.

[3] Die Zertifizierungsentscheidung wird im Formular Zertifizierungsentscheidung dokumentiert.

Alle im Rahmen der Evaluierung und Zertifizierung erstellten Dokumente, Aufzeichnungen und erhobene Nachweise werden durch die Zertifizierungsstelle für die Dauer von mindestens 10 Jahren nach Ablauf der Gültigkeit des Zertifikates aufbewahrt.

Die Übergabe des Zertifikats erfolgt grundsätzlich in den Räumlichkeiten der Zertifizierungsstelle. Auf Wunsch kann das Zertifikat auch an anderen Orten übergeben oder postalisch bzw. per E-Mail zugestellt werden.

3.4 Überwachung

Innerhalb des Gültigkeitszeitraums des Zertifikats muss eine Überwachung erfolgen, um die Zertifikatsgültigkeit zu erhalten. Das Datum der Überwachung soll im letzten Halbjahr des ersten Jahres nach Zertifikatsausstellung liegen. Bei dieser Überwachung wird in Form einer Stichprobe überprüft, ob die Konformität des Vertrauensdienstes zu den relevanten Produktanforderungen weiterhin gegeben ist. Der Umfang der jeweiligen Stichprobe beträgt bei Überwachungen mindestens 50% des Stichprobenumfangs der Erstevaluierung. Dabei soll die Stichprobe alle seit der Erstevaluierung durchgeführten Änderungen umfassen. Nach erfolgter Überwachung erstellen die Evaluatoren einen entsprechenden Evaluierungsbericht, der dem Kunden zur Verfügung gestellt wird.

Im Gültigkeitszeitraum eines Zertifikates wird maximal ein Überwachungsaudit durchgeführt, um die Gültigkeit des Zertifikates zu erhalten. Spätestens 2 Jahre nach Ausstellung des Zertifikates ist gemäß Artikel 20 Absatz 1 der eIDAS-Verordnung ein eine vollständige Re-Zertifizierung notwendig, um das Zertifikat zu erneuern (bzw. zu verlängern).

Zusätzlich zur Überwachung muss der Vertrauensdiensteanbieter die Zertifizierungsstelle unverzüglich über sämtliche Änderungen, die Auswirkung auf die Zertifizierung haben könnten, informieren und eine Beschreibung der Änderungen zur Verfügung stellen. Die Zertifizierungsstelle entscheidet anhand der Beschreibung, ob eine erneute Dokumentenprüfung oder eine erneute Evaluierung vor Ort notwendig ist oder ob die Änderungen im Rahmen der nächsten Überwachung bzw. Re-Zertifizierung überprüft werden können. Im Falle einer erneuten Dokumentenprüfung oder Evaluierung vor Ort erstellen die Evaluatoren einen entsprechenden Evaluierungsbericht, der dem Kunden zur Verfügung gestellt wird.

Sofern im Rahmen der Überwachung oder der Prüfung von Änderungen Nichtkonformitäten festgestellt werden, so ist mit dem Kunden ein Plan zur Behebung dieser Nichtkonformitäten innerhalb einer gesetzten Frist zu vereinbaren. Diese Frist soll im Regelfall 3 Monate nach Bekanntgabe der Nichtkonformität im Evaluierungsbericht nicht überschreiten. Sofern die Komplexität der vorgesehenen Behebungsmaßnahme dies erfordert, kann die Frist auf bis zu 6 Monate nach Bekanntgabe der Nichtkonformität im Evaluierungsbericht verlängert werden.

Der Evaluierungsbericht der Überwachung oder der Prüfung von Änderungen dient als Grundlage für eine Zertifizierungsentscheidung analog zu Abschnitt 3.3. Bei positiver Zertifizierungsentscheidung wird ein Nachtrag zum Konformitätsbewertungsbericht und ein aktualisiertes Zertifikat unter Beibehaltung der ursprünglichen Gültigkeitsdauer ausgestellt. Auf die Ausstellung eines aktualisierten Zertifikates bzw. eines Nachtrages zum Konformitätsbewertungsbericht kann verzichtet werden, wenn keine Änderungen an der Zertifizierungsdokumentation nötig sind.

3.5 Zertifikatsveröffentlichung und Prüfzeichennutzung

Zur Unterstützung der Transparenz der Zertifizierungen führt die Zertifizierungsstelle eine Liste der zertifizierten Produkte, die der Öffentlichkeit zur Verfügung gestellt wird. Neue Zertifikate werden kurzfristig nach positiver Zertifizierungsentscheidung unter Angabe einer kurzen Beschreibung des zertifizierten Produktes auf der Webseite der Zertifizierungsstelle (www.src-zert.de) veröffentlicht.

Der Kunde ist berechtigt, das Zertifikat und das Prüfzeichen in Verbindung mit dem zertifizierten Produkt in Veröffentlichungen, Katalogen etc. entsprechend der Vorgaben der Nutzungsbedingungen des SRC-Zertifikats und des SRC-Prüfsiegels zu verwenden. Bei inkorrekter Bezugnahme oder irreführender Verwendung des Zertifikates oder des Prüfzeichens durch den Kunden ist die Zertifizierungsstelle berechtigt, das Zertifikat zu entziehen.

Mitarbeiter der Zertifizierungsstelle überwachen regelmäßig, dass der Kunde bei der Nutzung der Zertifikate und Prüfzeichen die Zertifizierungsbedingungen einhält. Bei Feststellung von inkorrekter Bezugnahme oder irreführender Verwendung des Zertifikates oder des Prüfzeichens wird der Kunde aufgefordert, dies unverzüglich zu korrigieren. Es erfolgt eine Wiederholungskontrolle auf korrekte Nutzung durch die Zertifizierungsstelle innerhalb von drei Monaten.

3.6 Multizertifizierung

Wenn ein Vertrauensdiensteanbieter mehrere Vertrauensdienste betreibt, können diese Vertrauensdienste im Rahmen eines gemeinsamen Zertifizierungsverfahrens evaluiert werden. Dabei werden die Produktanforderungen der betroffenen Teilprogramme berücksichtigt.

Anforderungen, die in den Teilprogrammen identisch sind und für alle betriebenen Vertrauensdienste identisch umgesetzt sind, müssen nur einmal evaluiert werden. Die Ergebnisse dieser Evaluierung können in allen betroffenen Zertifizierungen genutzt werden.

Der Zertifizierungsprozess für alle bei der Multizertifizierung betrachteten Vertrauensdienste folgt dabei den Vorgaben aus den Kapiteln 3.1 bis 3.4. Für jeden Vertrauensdienst wird ein eigener Konformitätsbewertungsbericht und ein eigenes Zertifikat ausgestellt.

3.7 Zertifizierungsaufwände

Die Kosten der Aufwände für

- die Durchführung der Zertifizierung,
- die Durchführung von Evaluierungen,
- die Übergabe von Zertifikate an anderen Orten als den Räumlichkeiten der Zertifizierungsstelle

3.8 sowie ggf. weitere Tätigkeiten der Zertifizierungsstelle sind der Preisliste (Anlage 1) zu entnehmen.**Ermittlungsmethoden**

Im Rahmen der Evaluierung werden neben vor Ort Audits und Inspektionen die folgenden Ermittlungsmethoden eingesetzt:

- Dokumentenprüfung,
- Anerkennung von Zertifikaten für Hardware Security Modules (HSMs) und Qualifizierten Signatur- bzw. Siegelerstellungseinheiten (QSCDs),
- Anerkennung von Zertifizierungen von Teilkomponenten und
- Anerkennung von Berichten von unabhängigen Dritten.

Diese werden nachfolgend genauer beschrieben:

3.8.1 Dokumentenprüfung

Im Rahmen der Dokumentenprüfung wird überprüft, ob die durch den Vertrauensdiensteanbieter vorzuhaltende Dokumentation (insbesondere Trust Service Policy, Trust Service Practice Statement und Termination Plan) nachvollziehbar die Erfüllung der jeweiligen Produktanforderungen darlegt.

3.8.2 Anerkennung von Zertifikaten für HSMs und QSCDs

Soweit in Einzelanforderungen gefordert wird, dass vom Vertrauensdiensteanbieter eingesetzte Komponenten, beispielsweise HSMs oder QSCDs, über bestimmte Zertifizierungen verfügen müssen, so ist dies wie folgt zu verifizieren.

Zertifizierung nach FIPS PUB 140-2

Über die Webseite des NIST Cryptographic Module Validation Program[4] ist das Zertifikat der eingesetzten Komponente abzufragen und der Status (Feld „Validation Status“) der Zertifizierung zu überprüfen. Zertifikate sollen im Status „Active“ sein, um akzeptiert zu werden. Zertifikate im Status „Historical“ dürfen ebenfalls akzeptiert werden, wenn der Vertrauensdiensteanbieter darlegen kann, dass der Umstand der zu dieser Einstufung geführt hat (Feld „Historical Reason“) für das zu betrachtende Einsatzszenario nicht relevant ist oder zu keinem Sicherheitsverlust führt. Zertifikate für die der Status „Revoked“ ausgegeben wird, dürfen nicht akzeptiert werden.

Es muss verifiziert werden, dass die auf der Komponente eingesetzte Firmware mit der im Zertifikat angegebenen übereinstimmt.

Evaluierung und Zertifizierung nach Common Criteria (ISO/IEC 15408)

Zertifizierungen nach Common Criteria (CC) müssen von einer dafür akkreditierten Stelle ausgestellt worden sein. Die aktuelle Gültigkeit des CC-Zertifikats ist zu prüfen. Dies kann beispielsweise durch Abruf des Verzeichnisses zertifizierter Produkte der jeweiligen Zertifizierungsstelle erfolgen.

Es muss verifiziert werden, dass die vom Vertrauensdiensteanbieter verwendeten Komponenten entsprechend der Identifizierung und den Bedingungen aus der CC-Zertifizierung betrieben werden.

Sofern eine Evaluierung der technischen Komponente nach den Vorgaben der Common Criteria ausreicht und keine Zertifizierung gefordert ist, ist die erfolgreich abge-

[4] https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search

schlossene Evaluierung zu verifizieren. Hierzu können Informationen vom Common Criteria Portal (https://www.commoncriteriaportal.org/) herangezogen werden oder es liegt ein Nachweis der Common Criteria Prüfstelle über die erfolgreiche Evaluierung vor (z.B. der Evaluation Technical Report (ETR), Summary zur Evaluierung).

Zertifizierung als QSCD

Qualifizierte Signatur- / Siegelerstellungseinheiten müssen von einer dafür zugelassenen Stelle als QSCD zertifiziert sein. Diese sollen im Regelfall auf der QSCD-Liste der EU gemäß Artikel 31 Nr. 2 eIDAS[5] gelistet sein. Es können auch QSCDs akzeptiert werden die nicht auf der EU-Liste stehen, sofern für diese ein gültiges Zertifikat einer gemäß Artikel 30, Absatz 1 eIDAS zugelassenen Stelle[6] vorgelegt werden kann. Darüber hinaus werden SSCDs akzeptiert, die unter die Übergangsregel nach Artikel 51, Absatz 1 eIDAS fallen.

Es muss verifiziert werden, dass die vom Vertrauensdiensteanbieter verwendeten QSCDs entsprechend den Bedingungen aus der QSCD-Zertifizierung behandelt werden.

3.8.3 Anerkennung von Zertifizierungen von Teilkomponenten

Bestehen für den im Rahmen der Evaluierung betrachteten Vertrauensdienst bereits gültige Zertifizierungen für bestimmte (Teil-)Komponenten (z.B. Identifizierung des Antragsstellers) gemäß den Vorgaben der eIDAS-Verordnung, so können diese für die Zertifizierung des qualifizierten Vertrauensdiensteanbieters und der von ihm erbrachten qualifizierten Vertrauensdienste wiederverwendet werden. Die Wiederverwendung ist aufgrund der gesetzlichen Anforderungen gemäß Art. 20 Abs. 1 eIDAS-Verordnung, nach denen der Vertrauensdiensteanbieter alle 24 Monate von einer Konformitätsbewertungsstelle geprüft werden muss, grundsätzlich möglich.

Der Umfang der Wiederverwendung wird zwischen dem verantwortlichen Ansprechpartner des Kunden und den Evaluatoren abgestimmt. Dabei ist sicherzustellen, dass die wiederverwendeten Ergebnisse für die Zertifizierung des qualifizierten Vertrauensdiensteanbieters und der von ihm erbrachten qualifizierten Vertrauensdienste anwendbar sind. Insbesondere ist zu überprüfen, dass der Konformitätsbewertungsbericht und das zugehörige Zertifikat von einer Zertifizierungsstelle ausgestellt worden sind, die durch eine nationale Akkreditierungsstelle zur Durchführung entsprechender Zertifizierungen und zur Ausstellung entsprechender Zertifikate ermächtigt worden ist. Zudem ist zu prüfen, dass das Zertifikat gültig ist und dass der Geltungsbereich der Zertifizierung die relevanten Produktanforderungen, für deren Erfüllung die Ergebnisse wiederverwendet werden sollen, abdeckt.

Enthält der Konformitätsbewertungsbericht der zertifizierten Komponente Angaben, die die Evaluatoren zu Zweifeln über die Erfüllung einzelner Produktanforderungen veranlassen, müssen die Evaluatoren die Erfüllung der betroffenen Anforderungen selbst durch entsprechende Ermittlungsmethoden nachprüfen.

---

[5] Informative EU-Liste zertifizierter QSCDs: https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD

[6] Informative EU-Liste über „Designates Bodies für die Zertifizierung von QSCDs: https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/BODIES_QSCD_SSCD

Bezieht sich die bestehende Zertifizierung auf eine Vertrauensdienst-Komponente, die durch eine Dritte Partei betrieben wird und die in den betrachteten Vertrauensdienst eingebunden werden soll, müssen die Evaluatoren nachprüfen, dass die Produktanforderungen auch durch die entsprechenden Schnittstellen zwischen dem Vertrauensdienst und der angebundenen Komponente erfüllt werden.

3.8.4 Anerkennung von Berichten von unabhängigen Dritten

Grundsätzlich kann jeder Vertrauensdiensteanbieter Dritte Parteien mit der Erfüllung einzelner Produktanforderungen in seinem Namen beauftragen (Auslagerung). Macht der Vertrauensdiensteanbieter von dieser Möglichkeit Gebrauch, muss verifiziert werden, dass die relevanten Produktanforderungen durch den beauftragen Dritten erfüllt werden.

Dies kann je nach Umfang der Auslagerung und der betroffenen Produktanforderungen erfolgen durch:

- vor Ort Audits oder Inspektionen bei der Dritten Partei oder
- die Sichtung von Berichten über durchgeführte Tätigkeiten (z.B. Berichte von Penetrationstest oder Schwachstellentests) oder von Zertifizierungen bestimmter Eigenschaften eines Produktes (z.B. Angaben zur Falsch-Akzeptanz Rate von automatisierten, video-gestützten Identifizierungsverfahren).

Falls vor Ort Audits oder Inspektionen bei Dritten Parteien durchgeführt werden, werden diese im gleichen Umfang durchgeführt, als wenn die Erfüllung der Produktanforderungen durch den Vertrauensdiensteanbieter selbst gewährleistet werden würde.

Falls die Prüfung der Erfüllung der Produktanforderungen durch Sichtung von Berichten bzw. Zertifizierungsurkunden erfolgt, die eine Dritte Partei zur Verfügung stellt, müssen sich die Evaluatoren davon überzeugen, dass die Ermittlungsmethoden, die dem Bericht bzw. der Zertifizierung zugrunde liegen, geeignet sind, die Erfüllung der Produktanforderung zweifelsfrei nachzuweisen. Insbesondere müssen die Evaluatoren prüfen, dass die jeweiligen Berichte bzw. Zertifizierungen von einer Dritten Partei ausgestellt wurden, die über eine hinreichende Unabhängigkeit zum Vertrauensdiensteanbieter und über entsprechende Qualifikationen und Ermächtigungen zur Durchführung der Prüfung bzw. Zertifizierung verfügt. Zudem muss verifiziert werden, dass der Geltungsbereich und die Gültigkeitsfrist des Berichtes bzw. der Zertifizierung geeignet sind, die Erfüllung der jeweiligen Produktanforderung nachzuweisen. Durch Sichtung der dokumentierten Ergebnisse der Prüfung (z.B. eines Penetrationstest Berichtes) bzw. der Zertifizierung müssen die Evaluatoren in der Lage sein, die Erfüllung der Produktanforderung zweifelsfrei als gegeben ansehen zu können.

3.9 Beendigung, Einschränkung oder Zurückziehung der Zertifizierung

Eine positive Zertifizierungsentscheidung kann nachträglich, d.h. auch nach Ausstellung der Urkunde, durch die Konformitätsbewertungsstelle zurückgezogen bzw. eingeschränkt werden. Dies erfolgt insbesondere in den folgenden Fällen:

- Die Aufsichtsstelle entzieht dem Kunden den Status eines „qualifizierten Vertrauensdiensteanbieters“ vollständig oder für spezifische Dienste.
- Der Kunde stellt seine Tätigkeiten als „qualifizierter Vertrauensdiensteanbieter“ ein bzw. bietet spezifische Dienste nicht mehr an.

- Es wurde festgestellt, dass bestehende Zertifizierungsanforderungen nicht mehr ausreichend erfüllt werden.

Die Einschränkung, Beendigung bzw. Zurückziehung der Zertifizierung bedarf der Entscheidung der Leitung der Zertifizierungsstelle unter Einbezug des Mitarbeiters der Konformitätsbewertungsstelle, der die Zertifizierungsentscheidung für den Kunden bzw. für die spezifische Dienstleistung des Kunden getroffen hat. In diesem Fall werden der Kunde sowie die zuständige Aufsichtsstelle über die Beendigung, Einschränkung bzw. Zurückziehung der Zertifizierung informiert.

Sofern bestehende Anforderungen geändert bzw. neue Anforderungen definiert werden, ist ein neues Zertifizierungsverfahren einzuleiten.

Die (temporäre) Aussetzung einer Zertifizierung mit einem sich anschließenden wieder in Kraft setzen der Zertifizierung wird nicht unterstützt. Für Dienstleistungen, deren Zertifizierung beendet oder zurückgezogen wurde, ist bei entsprechendem Bedarf immer ein neues Zertifizierungsverfahren vorzunehmen.

4 Beschwerden und Einsprüche

Die SRC Security Research & Consulting GmbH sieht für den Fall von Beschwerden und Einsprüchen gegenüber der Zertifizierungsstelle einen dreistufigen Einspruchsprozess für die beteiligten Parteien vor:

1. In erster Instanz soll versucht werden, das Problem mit dem für das Zertifizierungsverfahren verantwortlichen Ansprechpartner der Zertifizierungsstelle eigenständig zu lösen.
2. Ist dieser Versuch nicht erfolgreich, ist im nächsten Schritt der Leiter der Zertifizierungsstelle hinzuzuziehen.
3. Kann auch nach Einbeziehung des Zertifizierungsstellenleiters keine Einigung erzielt werden, besteht die Möglichkeit, Einspruch gegen die Entscheidung des Leiters der Zertifizierungsstelle einzulegen und den KBS-Beirat der Zertifizierungsstelle als unabhängiges Lenkungsgremium einzuschalten. Solche Einsprüche sind grundsätzlich schriftlich an den KBS-Beirat zu schicken. Die Anschrift des KBS-Beirates lautet wie folgt:

   SRC Security Research & Consulting GmbH

   Zertifizierungsstelle (KBS)
   KBS-Beirat

   Emil-Nolde-Str. 7
   53113 Bonn

   Die Entscheidung des KBS-Beirats erfolgt mit einfacher Mehrheit bzw. bei gleicher Stimmenanzahl durch den Vorsitzenden gemäß der Geschäftsordnung des KBS-Beirates. Die Entscheidung wird schriftlich dokumentiert und enthält die konkreten Gründe, welche zu der Entscheidung geführt haben. Sie wird den am Einspruchsverfahren Beteiligten schriftlich mitgeteilt und ist für alle bindend.

5 Normen

[1] DIN EN ISO/IEC 17065:2013-01 „Konformitätsbewertung – Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren“

[2] ETSI EN 319 401 V2.3.1 (2021-05): Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

[3] ETSI EN 319 403-1 V2.3.1 (2020-06): Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers

ETSI TS 119 403-2 V1.2.4 (2020-11): Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates

ETSI TS 119 403-3 V1.1.1 (2019-03): Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers

[4] ETSI EN 319 411-1 V1.3.1 (2021-05): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements

[5] ETSI EN 319 411-2 V2.3.1 (2021-05): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates[6] ETSI EN 319 412-1 V1.4.4 (2021-05): Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

ETSI EN 319 412-2 V2.2.1 (2020-07): Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

ETSI EN 319 412-3 V1.2.1 (2020-07): Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons

ETSI EN 319 412-4 V1.1.1 (2016-02): Electronic Signatures and Infrastructures (ESI);Certificate Profiles; Part 4: Certificate profile for web site certificates

ETSI EN 319 412-5 V2.3.1 (2020-04): Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

[7] ETSI TS 119 495 V1.5.1 (2021-04): Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking

[8] ETSI EN 319 421 V1.1.1 (2016-03): Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

[9] CEN EN 419 241-1 (2018-09): Trustworthy Systems Supporting Server Signing, Part 1: General System Security Requirements

[10] ETSI TS 119 441 V1.1.1 (2018-08): Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services

[11] ETSI TS 119 511 V1.1.1 (2019-06): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques

[12] ETSI EN 319 521 V1.1.1 (2019-02): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers

[13] ETSI EN 319 531 V1.1.1 (2019-01): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers

[14] ETSI TS 119 461 V1.1.1 (2021-07), Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects

6 Anlagen

Anlage 1 Preisliste

Anlage 2 Abbildung der gesetzlichen Anforderungen der eIDAS-Verordnung, des Vertrauensdienstegesetzes und der Vertrauensdiensteverordnung auf die Produktanforderungen in den Normen und technischen Spezifikationen der Normierungsgremien ETSI und CEN

Anlagen 3 Festlegung von Kriterien und Evaluierungsmethoden

Anlage 3.a, Kriterien gemäß ETSI EN 319 401
Anlage 3.b, Kriterien gemäß ETSI EN 319 411-1
Anlage 3.c, Kriterien gemäß ETSI EN 319 411-2
Anlage 3.d, Kriterien gemäß ETSI EN 319 421
Anlage 3.e, Kriterien gemäß ETSI EN 319 521
Anlage 3.f, Kriterien gemäß ETSI EN 319 531
Anlage 3.g, Kriterien gemäß ETSI TS 119 441
Anlage 3.h, Kriterien gemäß ETSI TS 119 461
Anlage 3.i, Kriterien gemäß ETSI TS 119 495
Anlage 3.j, Kriterien gemäß ETSI TS 119 511
Anlage 3.k, Kriterien gemäß CEN EN 419 241-1
Anlage 3.l, Kriterien der Verfügung gemäß § 11 Absatz 1 VDG

Anlage 3.m, Kriterien der Verfügung gemäß § 11 Absatz 3 VDG

Anlage 4 Zertifizierungsvereinbarung

Anlage 5 Nutzungsbedingungen SRC-Zertifikate und SRC-Prüfsiegel

7 Glossar

Begriff	Erläuterung
eIDAS	VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
Evaluator	Person, welche die Evaluierung durchführt
Evaluierungsteam	Team von Evaluatoren
Evaluierung	Evaluierung umfasst die Tätigkeiten Audit, Prüfung, Inspektion, Begutachtung von Dienstleistungen und Prozessen sowie weitere Tätigkeiten zur Ermittlung von Eigenschaften bei der Konformitätsbewertung von Produkten.
Produkt	Im Kontext der Zertifizierung umfasst der Begriff Produkt die Begriffe Produkt, System, Dienstleistung und Prozess.
Prüfung	Ermittlung eines oder mehrerer Merkmale eines Produktes nach einem festgelegten Zertifizierungsverfahren (siehe auch Evaluierung)
Überwachung	Tätigkeiten (z.B. Überwachungsaudit), um zu prüfen, ob die Konformität des Vertrauensdienstes zu den relevanten eIDAS-Anforderungen weiterhin gegeben ist.
Zertifizierungsentscheider	Person, welche die Zertifizierungsentscheidung trifft.
Zertifizierung	Bestätigung durch eine unabhängige Stelle (Zertifizierungsstelle) bezogen auf Produkte, Prozesse, Systeme oder Personen.
Zertifizierungsprogramm	Zertifizierungssystem, das sich auf bestimmte Produkte bezieht, auf welche dieselben festgelegten Anforderungen, spezifischen Regeln und Verfahren angewendet werden
Zertifizierungssystem	Regeln, Verfahren und Management für die Durchführung von Zertifizierungen