Certification Practice Statement

Zertifizierungsprogramm eIDAS qSCD (akkreditierter Bereich) der Zertifizierungsstelle der Telekom Security (Zertifizierungsprogramm 021)

Vorwort

Telekom Security betreibt eine nach ISO/IEC 17065 und ETSI EN 319 403 von DAkkS[1] akkreditierte Zertifizierungsstelle, DAkkS Registration No. D-ZE-21631-01
(ehemals die Zertifizierungsstelle der T-Systems, DAkkS Registration No. D-ZE-12025-01).

Darüber hinaus ist die Zertifizierungsstelle der Telekom Security eine anerkannte ‚Designated Body' („Benannte Stelle") gemäß EU Verordnung Nr. 910/2014 (eIDAS) und Commission Decision 2000/709/EC (s. FESA) sowie gemäß dem § 17 des Vertrauensdienstegesetzes (VDG, eIDAS-Durchführungsgesetz vom 18.07.2017) für die Konformitätszertifizierung von elektronischen Signaturerstellungseinheiten**.**

Das vorliegende Dokument beschreibt das Zertifizierungsprogramm für die Vergabe der Telekom Security Konformitätszertifikate für qualifizierte elektronische Signatur- und Siegel-Erstellungseinheiten im Sinne des entsprechenden Artikels 30 bzw. 39 der Verordnung (EU) Nr. 910/2014, die in den akkreditierten und anerkannten Bereich als ‚Designated Body' fallen. Es soll Interessenten, die eine Zertifizierung bei Telekom Security durchführen lassen wollen, alle notwendigen Informationen geben.

Das Dokument wird fortlaufend nach den Erfordernissen aktualisiert und auf dem Web unter https://www.t-systems-zert.com/ (Menü „Service-Bereich") zum Download bereit gestellt.

Verteiler: öffentlich

Für weitere Auskünfte ist die Zertifizierungsstelle wie folgt erreichbar:

✉ Zertifizierungsstelle der Telekom Security
c/o Deutsche Telekom Security GmbH, Bonner Talweg 100, 53113 Bonn
☎ +49-(0)228-181-0, FAX -49990
💻 https://www.t-systems-zert.com/

[1] Deutsche Akkreditierungsstelle, www.dakks.de

Inhaltsverzeichnis

Revisionsliste

Revision	Datum	Aktivität
0.9	08.09.2000	Erst-Erstellung (debis Systemshaus)
1.0	28.02.2001	Aktualisierung
1.1	04.07.2001	Aktualisierung
1.2	01.08.2001	Aktualisierung aufgrund neuer Services
1.3	09.01.2002	Umbenennung zu T-Systems
1.4	01.06.2002	Aktualisierung der Services, kleine Korrekturen
1.5	02.01.2003	Namensänderungen, entspr. Anpassungen; Aufnahme von s4b
1.6	07.08.2003	Ergänzungen in Abschnitt 4.3 und 5.6
1.7	27.10.2003	Änderungen: © und Adressangaben
1.8	22.07.2004	Abgleich mit Web
1.9	04.03.2005	Aktualisierung der Prüfgrundlagen und Verfahrensnamen
2.0	04.04.2005	Aufnahme von ETSI 101456
2.1	25.07.2005	Aktualisierung wg. BNetzA
2.2	31.10.2005	Kleinere Reparaturen
2.3	23.02.2006	Update Standards
2.4	18.01.2007	Programm-Anpassungen, verschiedene Aktualisierungen
2.5	06.06.2007	Anpassungen für das Verfahren 08
2.6	19.07.2007	Aktualisierung der AGB
3.0	18.03.2008	Aufteilung in CPS und Zertifizierungsregeln
3.1	01.06.2010	Änderung der Anschrift und editorische Anpassungen; das Programm 06 wurde eingestellt.
4.00-eIDAS-qSCD	11.07.2016	Anpassungen im Kontext der ISO 17065 Akkreditierung durch DAkkS; für jedes Programm wird ein dediziertes CPS herausgegeben. Das Scope des Dokuments erfasst ausschließlich das Programm eIDAS qSCD im anerkannten Bereich.
4.01-eIDAS-qSCD	11.08.2016	Kap. 1.3, ETSI EN 319 411-1: Referenz auf CA/Browser Forum
4.02-eIDAS-qSCD	02.01.2017	Änderung der Anschrift
4.03-eIDAS-qSCD	01.07.2017	Änderung der Rufnummern
4.04-eIDAS-qSCD	01.08.2017	Außerkrafttreten des SigG, Inkrafttreten des VDG
4.05-eIDAS-qSCD	16.07.2018	Editorische Anpassungen, Kap. 2.3
4.06-eIDAS-qSCD	08.02.2019	Editorische Anpassungen, Kap. 2.3
4.07-eIDAS-qSCD	20.02.2019	Editorische Anpassungen: „akkreditierter Bereich“ zusätzlich zu „anerkannter Bereich“
4.08-eIDAS-qSCD	27.06.2019	Referenz auf EN 319 431, EN 319 441, EN 319 521, EN 319 522 sowie auf EN 419 241, EN 419 221
5.00-eIDAS-qSCD	01.07.2020	Umbenennung zu Telekom Security

1 Einführung

1.1 Mission der Zertifizierung

Informations-und Kommunikationstechnik (ICT) spielen in der modernen Gesellschaft eine so herausragende Rolle, dass kein Bereich ohne sie auskommt. Umfragen und Analysen haben gezeigt, dass eine Abhängigkeit von der stetigen Einsatzbereitschaft der Technik und Services besteht: Moderne Unternehmen sehen ihre Existenz bedroht, wenn ihre IT nicht zur Verfügung steht oder nicht wie erwartet funktioniert.

Angesichts solcher Abhängigkeiten und einer Vielzahl von Manipulationsfällen und Sicherheitslücken verwundert es nicht, dass die Sicherheit von Informations- und Telekommunikationstechnik im kommerziellen, behördlichen und privaten Umfeld signifikant an Relevanz gewonnen hat.

Die IT-Sicherheit ist mittlerweile Gegenstand von Gesetzen und Verordnungen, Voraussetzung für die Teilnahme an Ausschreibungen und ein wesentlicher Faktor bei Kaufentscheidungen vieler Kunden und Anwender.

Die Sicherheit der Informationsverarbeitung und der Geschäftsprozesse ist in diesem Sinne ein wesentlicher Eckpfeiler der Unternehmensvorsorge geworden. Hier gilt es Risiken zu erkennen, Schäden zu reduzieren und Schwachstellen auszumerzen.

Sicherheit in diesem Sinne ist durch die klassischen Sicherheitsziele der Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit von Daten bestimmt. Damit verbunden können auch Ziele der Verbindlichkeit, der Revisionssicherheit, des Datenschutzes und der Ordnungsmäßigkeit sein.

Nicht zuletzt im Zusammenhang mit der Globalisierung der Wirtschaft, der Einführung neuer Dienstleistungen im Bereich der Kommunikation und der Diskussion um Persönlichkeitsrechte treten neue Sicherheitsziele wie die Anonymität, der Schutz von Urheberrechten und die Zurechenbarkeit und Unverfälschbarkeit von Daten und Transaktionen (z.B. durch elektronische Signaturen) stärker in den Vordergrund.

Die Risiken bei der Anwendung von Informations- und Kommunikationstechnik werden zukünftig noch ansteigen, wenn nicht durch qualifizierte Sicherheitsvorkehrungen und entsprechende Prüf- und Abnahmeprozesse (Verifizierung und Qualifizierung) gegengesteuert wird.

Die Aufgabe der Zertifizierung besteht in der Einrichtung und dem Betrieb eines Systems, in dem solche Prüfungen und Abnahmen in objektiver und unabhängiger Weise durchgeführt werden können.

Durch solche Verifizierungs- und Qualifizierungsprozesse wird die Reduzierung von Sicherheitsrisiken wesentlich gefördert, da mit den verifizierenden Prüf- und Zertifizierungsberichten sowie qualifizierenden Konformitätszeichen (Zertifikaten, Bestätigungen, Qualitäts- bzw. Prüfsiegeln) eine Transparenz erzeugt wird, die für Risikoträger von ICT - Betreiber, Nutzer, Anbieter und Entwickler - unverzichtbar ist.

1.2 Nutzen der Zertifizierung

Wie in anderen Technikbereichen zielt ein Zertifizierungsprozess im Bereich IT Sicherheit auf die Ausstellung eines Konformitätszeichens, z.B. eines Zertifikates, mit dem bestimmte Sicherheitseigenschaften eines Produktes oder Systems, einer Dienstleistung oder eines Geschäftsprozesses für die Betroffenen transparent gemacht werden.

Das Konformitätszeichen ist eine unabhängige und objektivierte Bestätigung dafür, dass die vom Anbieter behaupteten Sicherheitseigenschaften tatsächlich vorhanden sind und die beabsichtigten Sicherheitsziele erreicht werden.

Die Zertifizierung erfolgt auf der Grundlage von normativen Dokumenten wie Rechtsvorschriften, Normen oder technischen Spezifikationen, welche Anforderungen an Zertifizierungsgegenstände (Produkte / Dienstleistungen / Prozesse) festgelegen. Die Zertifizierung hat für die betroffenen Zielgruppen (Betreiber, Nutzer, Anbieter und Entwickler von ICT) unterschiedliche Bedeutung:

- Betreiber bzw. Nutzer brauchen zuverlässige Bestätigungen über die Sicherheitseigenschaften von IT Produkten und externen Dienstleistungen, um diese adäquat in ihre Systeme und Geschäftsprozesse integrieren zu können.
  System-Zertifizierungen und die Zertifizierung von Geschäftsprozessen können darüber hinaus den Bedarf von Unternehmen und Behörden nach ganzheitlicher Sicherheitsaussage decken.
- Anbieter von Dienstleistungen, insbesondere in den Bereichen der Informationsverarbeitung und der Telekommunikation, und IT Produkten brauchen Bestätigungen über die Sicherheitsleistungen ihrer Services und

Produkte, um im internationalen Markt bestehen, gesetzlichen und kundenspezifischen Anforderungen genügen zu können.

- Entwickler von IT Produkten benötigen im Entwicklungsprozess frühzeitig Informationen über Sicherheitslücken und Beratung über normenkonforme Entwicklungsverfahren. Prüf- und Zertifizierungsverfahren sollten deshalb parallel zur Produktentwicklung laufen.

Diese Prozesse müssen auf der Basis einschlägiger Sicherheitskriterien bzw. -standards durchgeführt werden, wenn sie für die genannten Zielgruppen einen umfassenden Nutzen bringen sollen. Sicherheitskriterien und Sicherheitsstandards haben teilweise schon Eingang in gesetzliche Vorgaben gefunden, die für die genannten Zielgruppen relevant sind, z.B. für den Kontext der elektronischen Signatur, der ID Dokumente, des Gesundheitswesens, der intelligenten Verteilungsnetze (Smartgrid), der digitalen Fahrtenschreiber etc.

Die Anwendung international akzeptierter Kriterien bildet die unerlässliche Voraussetzung für eine internationale Anerkennung der ausgestellten Konformitätszeichen.

1.3 Zertifizierungsstelle der Telekom Security

Die Zertifizierungsstelle der Telekom Security bietet vor dem beschriebenen Hintergrund eine Reihe von Services an, die eine objektive Prüfung und Zertifizierung der Sicherheitseigenschaften

- von IT-Produkten, IT-Systemen und -Netzwerken sowie
- von IT-Dienstleistungen und entsprechenden Geschäftsprozessen

erlauben. Diese Services basieren auf Standards und normativen Dokumenten wie z.B. europäische und nationale Vorgaben zur Vertrauensdiensten (auf der EU Ebene - im Rahmen von eIDAS[2]: elektronische Signaturen, Siegel, Zeitstempel, Dienste für die Zustellung elektronischer Einschreiben, Website-Authentifizierung; national – im Rahmen des deutschen Vertrauensdienstegesetzes (VDG)), europäische und nationale Vorgaben zur Zertifizierung qualifizierter elektronischer Signaturerstellungseinheiten (eIDAS und VDG), ETSI-Standards, eigenen Prüfvorschriften der Zertifizierungsstelle sowie weiteren branchen- bzw. kundenspezifischen Vorgaben.

[2] Verordnung (EU) Nr. 910/2014

Die Zertifizierungsstelle der Telekom Security ist für ihre Services erstmalig im Juni 1998 akkreditiert worden. Die aktuelle Akkreditierungsurkunde – ausgestellt durch DAkkS – findet man unter https://www.t-systems-zert.com/ sowie www.dakks.de (D-ZE-21631-01). Sie enthält im Anhang die akkreditierten Zertifizierungsprogramme der Zertifizierungsstelle.

Die Zertifizierungsstelle wirkt in Prüf- und Zertifizierungsschemata mit, die von folgenden Institutionen betrieben werden:

- EU Verordnung (EU) Nr. 910/2014 (eIDAS)
  (Verfahrenstyp 031):
  Im Zusammenhang mit der EU Verordnung (EU) Nr. 910/2014 ist die Zertifizierungsstelle der Telekom Security eine Konformitätsbewertungsstelle[3] für Vertrauensdiensteanbieter und für Vertrauensdienste, die sie anbieten.
- ETSI EN 319 4xx: Electronic Signatures and Infrastructures (ESI)
  (Verfahrenstyp 032):
  - ETSI EN 319 401: General Policy Requirements for Trust Service Providers
  - ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates;
    Part 1: General requirements
    Anmerkung: Konformität zu diesen Anforderungen wird von CA/Browser Forum anerkannt (s. CA/B Baseline and Extended Validation Requirements, Ballot 171 vom 01.07.2016)
  - ETSI EN 319 411-2: Policy and security requirements for Trust Service Providers issuing certificates;
    Part 2: Requirements for trust service providers issuing EU qualified certificates
  - ETSI EN 319 411-3: Policy and security requirements for Trust Service Providers issuing certificates;
    Part 3: Policy Requirements for Certification Authorities issuing public key certificates
  - ETSI EN 319 411-4: Policy and security requirements for Trust Service Providers issuing certificates;

[3] gemäß Artikel 20 dieser Verordnung (Conformity Assessment Body, CAB)

Part 4: Policy Requirements for Certification Authorities issuing attribute certificates

- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 431: TSP service components operating a remote QSCD / SCDev
- CEN EN 419 241 series: Trustworthy Systems Supporting Server Signing
- CEN EN 419 221 series: Cryptographic Module;

amongst others - EN 419 221-5: Cryptographic Module for Trust Services

- ETSI EN 319 441: Policy and security requirements for TSPs providing signature validation services
- ETSI EN 319 521: Policy and security requirements for Electronic Registered Delivery Service Providers
- ETSI EN 319 522 Serie: Electronic Registered Delivery Service.

Im Zusammenhang mit der o.g. Normenserie ETSI EN 319 4xx / 5xx ist die Zertifizierungsstelle der Telekom Security eine Konformitätsbewertungsstelle für entsprechende Vertrauensdiensteanbieter und für Vertrauensdienste, die sie anbieten.

- Aufgehoben mit Inkrafttreten des Vertrauensdienstegesetzes: *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen*
  (Verfahrenstyp 030):
  - *Die Zertifizierungsstelle der Telekom Security ist als Bestätigungsstelle für die Sicherheitsbestätigung von Produkten nach dem deutschen Signaturgesetz durch die Bundesnetzagentur anerkannt.*
  - *Die Zertifizierungsstelle der Telekom Security ist für die Prüfung und Bestätigung von Zertifizierungsdiensteanbietern (ZDA) als Prüf-und Bestätigungsstelle nach dem deutschen Signaturgesetz durch die Bundesnetzagentur anerkannt.*

- Designated Body gemäß EU Verordnung (EU) Nr. 910/2014 und Commission Decision 2000/709/EC
  (Verfahrenstyp 021):

  Im Zusammenhang mit der EU Verordnung (EU) Nr. 910/2014 ist die Zertifizierungsstelle der Telekom Security ein Designated Body[4]. Dies schließt u.a. die o.g. Normenserien CEN EN 419 241 und CEN EN 419 221 ein.

- Aufgehoben mit Inkrafttreten der eIDAS VO: *Designated Body gemäß EU Richtlinie 1999/93/EG und Commission Decision 2000/709/EC (Verfahrenstyp 020):*

  Im Zusammenhang mit der EU Richtlinie 1999/93/EG ist die Zertifizierungsstelle der Telekom Security ein Designated Body[5].

Bei Prüfungen und Zertifizierungen spielt die Vertraulichkeit der Informationen des Antragstellers (Auftraggebers) stets eine große Rolle. Die Zertifizierungsstelle der Telekom Security verfügt über eine organisatorische und technische Infrastruktur, die auch für den Umgang mit staatlichen Verschlusssachen mindestens bis zum Grad „geheim“ geeignet ist.

Der Akkreditierungsgeber achtet insbesondere darauf, dass die Verfahren der Zertifizierungsstelle allen externen Interessenten zugänglich sind, Unparteilichkeit und Objektivität gewahrt sind und eine Gleichbehandlung aller Antragsteller sichergestellt ist.

[4] gemäß Artikel 30 dieser Verordnung, s. www.europa.eu.int und www.fesa.rtr.at

[5] gemäß Artikel 3 (4) dieser Richtlinie, s. www.europa.eu.int und www.fesa.rtr.at

2 Zertifizierungsprogramm 021: Zertifizierung qualifizierter elektronischer Signaturerstellungseinheiten gemäß Verordnung (EU) Nr. 910/2014

2.1 Zweck des Programms

In diesem Programm für den Bereich der gesamten Europäischen Union werden im Einklang mit der Verordnung (EU) Nr. 910/2014 (Artikel 30 und 39) Prüfungen von elektronischen Signatur- / Siegel-Erstellungseinheiten (qSCD / qSEE[6]; eine technische Komponente) durchgeführt, mit dem Zweck nachzuweisen, dass qSCDs die in dieser Verordnung festgelegten Anforderungen (s. Anhang II der Verordnung) erfüllen. Die Prüfungen umfassen sowohl technische Spezifikationen, User Guidance und Tests des qSCD als auch seine Schwachstellenanalyse, die Notwendig sind, um eine Konformitätsaussage zu den relevanten Anforderungen treffen zu können. Hierzu ist die Evaluierung solcher technischen Komponenten nach den Common Criteria oder nach einem anderen Sicherheitsbewertungsverfahren (Prüfkriterien) gemäß Artikel 30 (3) der Verordnung (EU) Nr. 910/2014 durch für diese Sicherheitsbewertungsverfahren anerkannte Prüfstellen (Designated Bodies) erforderlich. Der entsprechende Konformitätsbewertungsbericht (Zertifizierungsbericht) samt der Konformitätsbestätigung (Zertifikat) wird dem Antragssteller übergeben. Dieses Zertifikat kann vom Antragssteller, wenn notwendig, überall vorgelegt werden.

Bei diesem Programm sind folgende Vorgaben zu beachten:

- Verordnung (EU) Nr. 910/2014
- anwendbare Durchführungsrechtsakte der EC
  aktuell:
  - gemäß Artikel 30 (3): Normen für die Sicherheitsbewertung informationstechnischer Produkte (COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016),
  - gemäß Artikel 27 (5) und 37 (5): Referenzformate für fortgeschrittene elektronische Signaturen und Siegel (COMMISSION IMPLEMENTING

[6] qualified signature creation device / qualifizierte Signaturerstellungseinheit

DECISION (EU) 2015/1506 of 8 September 2015)
der Verordnung (EU) Nr. 910/2014

- aktuelle Veröffentlichungen hinsichtlich zugelassener kryptographischer Algorithmen für die Erstellung von Signaturen
- Festlegungen der Arbeitsgruppe akkreditierter Bewertungsstellen (AGAB).

Anmerkung:

Im Rahmen der Verordnung (EU) Nr. 910/2014 agiert die Zertifizierungsstelle als „designated body“ nach Artikel 30 und Commission Decision 2000/709/EC.

2.2 Angebotsanfrage und Zertifizierungsvereinbarung

Diese Informationen sind der Anlage „Zertifizierungs- und Konformitätsbestätigungsregeln“ zu entnehmen.

Spezifisch für das aktuelle Zertifizierungsprogramm wird eine mögliche Gültigkeitsdauer des Zertifikats mit dem Antragsteller abgestimmt.

2.3 Zertifizierung mit Evaluierung und Überwachung

Allgemeine Informationen sind der Anlage „Zertifizierungs- und Konformitätsbestätigungsregeln“ zu entnehmen.

Spezifisch für das aktuelle Zertifizierungsprogramm ist folgendes:

Nach erfolgter Evaluierung erstellen die Evaluatoren einen Evaluierungsbericht (Evaluation Technical Report - ETR), der die Grundlage für die Zertifizierungsentscheidung darstellt. 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 Zertifizierungsentscheidung wird protokolliert. Der Antragsteller wird über die Zertifizierungsentscheidung informiert.

Bei positiver Zertifizierungsentscheidung wird das Zertifikat ausgestellt, das den Geltungsbereich der Zertifizierung und eine vom Zertifizierungsgegenstand selbst und seinen möglichen Einsatzbedingungen abhängige Gültigkeitsfrist (jedoch max. 7 Jahre) wiedergibt sowie das Konformitätszeichen darstellt. Ein gültiges Zertifikat berechtigt zur öffentlichen Nutzung des Konformitätszeichen im Zusammenhang mit der zertifizierten

qualifizierten elektronischen Signaturerstellungseinheit gemäß der Anlage „Zertifizierungs- und Konformitätsbestätigungsregeln“.

Die Zertifizierungsstelle der Telekom Security bietet SCD-Anbietern und -Nutzern die Bewertung und Zertifizierung von entsprechenden technischen Komponenten an.

Die Bewertung und Zertifizierung muss auf der Grundlage der folgenden Durchführungsrechtsakte erfolgen:

(i) „COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014”,

(ii) COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014.

Die Durchführung der Zertifizierung erfolgt auf Basis entweder der Common Criteria oder eines anderen Sicherheitsbewertungsverfahrens (Prüfkriterien) gemäß Artikel 30 (3) der Verordnung (EU) Nr. 910/2014. Die Evaluierung wird von Evaluatoren / Auditoren durchgeführt, die Mitarbeiter der Zertifizierungsstelle sind oder durch die Zertifizierungsstelle zugelassen sind.

Anforderungen an Prüfstellen:

1) Anerkennung / Lizenzierung für die Durchführung von Common Criteria oder nach „einem anderen Sicherheitsbewertungsverfahren (Prüfkriterien) gemäß Artikel 30 (3) der Verordnung (EU) Nr. 910/2014“ Evaluierungen (üblicherweise nach ISO/IEC 17025).

   Diese Anerkennung / Lizenzierung muss sowohl die technologische Domäne, der der Zertifizierungsgegenstand angehört, als auch die durch Verordnung (EU) Nr. 910/2014 (inkl. relevanter Durchführungsrechtakte) geforderte Prüftiefe einschließen.

   Diese Anerkennung / Lizenzierung soll durch den zuständigen nationalen oder supranationalen Regulator erteilt worden sein;

2) Allgemeine Anforderungen an Prüfstellen, s. Abschn. 4 weiter unten.

Durchführung der Evaluierung:

Der organisatorische und fachliche Ablauf des Evaluierungsprozesses wird gemäß der anzuwendenden Methodologie für das gewählte Sicherheitsbewertungsverfahren gestaltet. Für Common Criteria ist das Common Methodology for Information Technology Security Evaluation (CEM) sowie internationale Interpretationen und Supporting Documents, herausgegeben durch das CCMC[7] (siehe https://www.commoncriteriaportal.org) sowie durch SOGIS[8] (siehe http://www.sogis.eu). Für „eine anderes Sicherheitsbewertungsverfahren (Prüfkriterien) gemäß Artikel 30 (3) der Verordnung (EU) Nr. 910/2014“ wird die für das jeweilige Sicherheitsbewertungsverfahren gültige Bewertungsmethodologie angewendet.

Die Durchführbarkeit einer Evaluierung setzt voraus, dass der Antragsteller alle für die vorgesehene Evaluierungsstufe notwendigen Konstruktionsdetails über sämtliche sicherheitsrelevanten Komponenten des Zertifizierungsgegenstandes offen legt bzw. bereitstellt. Der verantwortliche Zertifizierer und die Evaluatoren stimmen mit dem Antragsteller den zeitlichen Ablauf des Zertifizierungsvorgangs ab.

Diese Beiträge und Beistellungen werden von Evaluatoren gemäß der anzuwendenden Methodologie verifiziert. Diese Verifikation und ihr Ergebnis werden in Einzelprüfberichten dokumentiert. Evaluatoren verständigen den Antragsteller über die von ihnen erkannten Gründe, wegen derer Dokumente durch den Komponentenhersteller überarbeitet werden müssen. Bei Unstimmigkeiten wird die Zertifizierungsstelle zur Klärung hinzugezogen.

Gemäß der anzuwendenden Methodologie führen Evaluatoren des Weiteren alle notwendigen Audits von relevanten Entwicklungs- und Produktionsstätten vor Ort sowie Tests und die Schwachstellenanalyse und –bewertung des Zertifizierungsgegenstandes durch. Die Ergebnisse werden in Einzelprüfberichten dokumentiert.

Soweit vorhanden, können auch Bewertungen anderer unabhängiger Stellen zu einzelnen Teilen des Zertifizierungsgegenstandes herangezogen werden. Zum Beispiel kann die Verifizierung von relevanten Entwicklungs- und Produktionsstätten vor Ort auf wiederverwendbare Ergebnisse einer s.g. Site-Certification zurückgreifen. Die Evaluierung einer zusammengesetzten technischen Komponente kann im Rahmen einer so genannten Composite-Evaluierung durchgeführt werden.

[7] Common Criteria Management Committee

[8] Senior Officials Group Information Systems Security

Der Umfang der Wiederverwendung wird zwischen dem verantwortlichen Zertifizierer und den Evaluatoren abgestimmt. Dabei ist sicherzustellen, dass die wiederverwendeten Ergebnisse für die Zertifizierung des Zertifizierungsgegenstands nach eIDAS anwendbar sind.

Mit Abschluss der Evaluierung erstellen Evaluatoren einen Evaluierungsendbericht (Evaluation Technical Report – ETR) für die Evaluierung des Zertifizierungsgegenstandes mit einer Aussage über die Übereinstimmung der Eigenschaften der elektronischen Signaturerstellungseinheit mit den relevanten eIDAS-Anforderungen und übergeben ihn als Grundlage für die Zertifizierung an die Zertifizierungsstelle und den Antragsteller.

Dieser Bericht bildet die Grundlage für die Entscheidung über die Zertifizierung. Die Entscheidung über die Zertifizierung wird von der Leitung der Zertifizierungsstelle getroffen. Das Zertifikat wird abhängig von den Ergebnissen der Evaluierung mit einer Gültigkeitsdauer ausgestellt, die von dem Zertifizierungsgegenstand selbst und seinen möglichen Einsatzbedingungen abhängt. Diese Gültigkeitsdauer kann maximal 7 Jahre betragen. Nach dem Ablauf dieser Frist ist eine neue Bewertung der Übereinstimmung der Eigenschaften des Zertifizierungsgegenstands mit den relevanten eIDAS-Anforderungen notwendig, um die Zertifikatsgültigkeit zu verlängern.

Überwachung der Verwendung des Konformitätszeichens:

Allgemeine Informationen sind der Anlage „Zertifizierungs- und Konformitätsbestätigungsregeln“ zu entnehmen.

Die Zertifizierungsprogramm-spezifische Überwachung der Verwendung des Konformitätszeichens erfolgt durch

- Die Begrenzung der Gültigkeit des Konformitätszeichens auf maximal 7 Jahre mit der Möglichkeit einer Überprüfung, ob die zu Grunde liegende Konformitätsaussage (Zertifizierungsentscheidung) aufrechterhalten werden kann.
- Ereignisbezogene Überprüfung, ob die zu Grunde liegende Konformitätsaussage (Zertifizierungsentscheidung) aufrechterhalten werden kann. Ein solches Ereignis kann z.B. ein bekannt gewordenes sicherheits-technisches Problem im konkreten Zertifizierungsgegenstand oder in der relevanten Technologie sein.

Sollten innerhalb der Gültigkeitsdauer des Zertifikats Änderungen am Gegenstand der Zertifizierung auftreten, greifen die entsprechenden Regelungen aus Anlage „Zertifizierungs-

und Konformitätsbestätigungsregeln“, darin Kap. „Aufrechterhaltung des Konformitätszeichens nach Änderungen“.

Der qSCD-Anbieter muss die Zertifizierungsstelle unverzüglich über Änderungen, die Auswirkung auf die Zertifizierung haben, informieren und eine Beschreibung der Änderungen zur Verfügung stellen. Die Zertifizierungsstelle entscheidet anhand der Beschreibung, ob eine erneute Evaluierung notwendig ist oder ob die Änderungen im Rahmen des nächsten Überwachungs- bzw. Re-Zertifizierungsverfahrens überprüft werden können.

2.4 Veröffentlichung des Zertifikats und Nutzung des Konformitätszeichens

Allgemeine Informationen sind der Anlage „Zertifizierungs- und Konformitätsbestätigungsregeln“ zu entnehmen, Kap. „Auskünfte und Veröffentlichungen“ und „Überwachung der Verwendung des Konformitätszeichens“.

2.5 Zertifizierungsaufwände

Allgemeine Informationen sind der Anlage „Zertifizierungs- und Konformitätsbestätigungsregeln“ zu entnehmen, Kap. „Verfahrenskosten und Haftung“.

2.6 Beschwerden und Einsprüche

Allgemeine Informationen sind der Anlage „Zertifizierungs- und Konformitätsbestätigungsregeln“ zu entnehmen, Kap. „Beschwerde- und Einspruchsverfahren“.

Zertifizierungsprogramm-spezifisch ist die *Aufsichtsstelle,* die im Rahmen des Beschwerdeverfahrens angerufen werden kann:

> Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Referat Qualifizierte elektronische Signatur, Canisiusstraße 21, 55122 Mainz

3 Ergänzende Services

Die folgenden Dienstleistungen sind sowohl für jeden Verfahrenstyp als auch außerhalb eines oben aufgeführten Zertifizierungsprogramms verfügbar:

- Vorbereitung von Prüf- und Zertifizierungsverfahren in Form von Workshops.
- Training von Entwicklern im Hinblick auf kriterienkonforme Entwicklung und Optimierung der Zertifizierungsverfahren (auch Inhouse).
- Training von IT-Sicherheitsbeauftragten im Hinblick auf mögliche Verifizierung und Zertifizierung von Entwicklungs-, Test- und Produktionsinfrastrukturen (auch Inhouse).

  Wenn Beratungen oder Training für Antragsteller der Zertifizierungsstelle angeboten werden, beschränken sie sich ausschließlich auf Informationsaustausch zwischen der Zertifizierungsstelle und ihren Kunden, wie z. B. Erklärungen zu Feststellungen oder Klärung von Prüf- und Zertifizierungsanforderungen.
- Übersetzung von eigenen Konformitätszeichen und Berichten in andere Sprachen.
- Vervielfältigungs- und Druckarbeiten bei der Herausgabe von eigenen Konformitätszeichen und Berichten.
- Präsentationen über das Zertifizierungsschema und die erzielten Ergebnisse auf Kunden-Veranstaltungen und Kongressen.
- Ankündigung von Verfahren bzw. Bekanntgabe von Ergebnissen (Presse-Erklärungen, Fachzeitschriften, Veröffentlichungen auf der Webseite der Zertifizierungsstelle).

4 Allgemeine Anforderungen an Prüfstellen

Folgende Anforderungen an Prüfstellen gelten unabhängig vom konkret gewählten Zertifizierungsprogramm:

1) Die Prüfstelle muss eine rechtlich verbindliche vertragliche Grundlage (Lizenzvertrag / Lizenzvereinbarung) mit der Zertifizierungsstelle der Telekom Security haben (ISO/IEC 17065, 6.2.2).

2) Für jedes einzelne Zertifizierungsverfahren muss die Prüfstelle eine rechtlich durchsetzbare Vereinbarung mit dem Antragsteller vorweisen können, die es der Prüfstelle ermöglicht, alle im Rahmen des beantragten Zertifizierungsverfahrens notwendigen Prüfungen mindestens auf der im Zertifizierungsantrag angestrebten Prüftiefe durchzuführen. Diese Vereinbarung muss u.a. die Erstellung eines Plans für die Evaluierungstätigkeiten (Evaluierungsplans) durch die Prüfstelle abdecken, um die Anwendung der notwendigen Regelungen des relevanten Zertifizierungsprogramms zu ermöglichen.

3) Die Prüfstelle muss die Ergebnisse aller Evaluierungstätigkeiten dokumentieren. Diese Dokumentation erfolgt in Form von Prüf-, Audit-, Inspektions- oder Beobachtungsberichten. Diese Berichte müssen auf jeden einzelnen im Zertifizierungsprogramm geforderten und auf das konkrete Zertifizierungsverfahren anwendbaren Prüfaspekt eingehen und – für jeden Prüfaspekt – die Prüfergebnisse nachvollziehbar dokumentieren.

5 Glossar

Begriff	Definition
Beratung (im Zusammenhang mit Aktivitäten von Zertifizierungsstellen, des Personals von Zertifizierungsstellen und von Organisationen, die mit Zertifizierungsstellen in Beziehung stehen oder verbunden sind)	ISO/IEC 17065 (3.2): Teilnahme an: a) Entwicklung, Herstellung, Installation, Wartung oder Vertrieb eines zertifizierten oder eines zu zertifizierenden Produktes; oder b) Entwicklung, Einführung, Betrieb oder Aufrechterhaltung eines zertifizierten oder zu zertifizierenden Prozesses; oder c) Entwicklung, Einführung, Bereitstellung oder Aufrechterhaltung einer zertifizierten oder zu zertifizierenden Dienstleistung.
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
Konformitätszeichen (Zertifizierungsurkunde)	ISO/IEC 17030: „Geschütztes Zeichen, das von einer Stelle, die Konformitätsbewertungstätigkeiten einer dritten Seite durchführt, ausgestellt wird und deutlich macht, dass ein Gegenstand der Konformitätsbewertung (Produkt, Prozess, Person, System oder Stelle) mit festgelegten Anforderungen übereinstimmt“. Konformitätsbewertungstätigkeiten können von der Zertifizierungsstelle in Form von Zertifikaten, Bestätigungen und Qualitäts- bzw. Prüfsiegeln ausgestellt werden.
Zertifizierungsprogramm / Verfahrenstyp	In Anlehnung an ISO/IEC 17065: *Zertifizierungssystem* (Konformitätsbewertungssystem), das sich auf bestimmte Klasse / bestimmten Typ von *zu zertifizierenden Objekten* bezieht, auf welche(n)

Begriff	Definition
	dieselben festgelegten Anforderungen, spezifischen Regeln und Verfahren angewendet werden. Die Regeln, Verfahren sowie Leitung und Lenkung der Zertifizierung von Produkten, Prozessen und Dienstleistungen werden durch das Zertifizierungsprogramm festgelegt.
Zertifizierungs- / Konformitätsbestätigungsverfahren	Ein konkretes Qualifizierungsverfahren (Konformitätsbewertungsverfahren), das auf *zu zertifizierendes Objekt* durch die Zertifizierungsstelle im Auftrag des Antragstellers angewendet wird. Ein Zertifizierungs- / Konformitätsbestätigungsverfahren muss im Rahmen eines Zertifizierungsprogramms durchgeführt werden.
Zertifizierungssystem (Konformitätsbewertungssystem)	Regeln, Verfahren und Management für die Durchführung von Zertifizierungen
zu zertifizierendes Objekt (Zertifizierungsgegenstand, Gegenstand der Konformitätsbewertung)	Produkt / Dienstleistung / Prozess, für welche{n,s} die Erlangung eines Konformitätszeichens vom Antragsteller angestrebt wird.
Antragsteller (Auftraggeber)	Juristische Person, die einen Antrag auf die Ausstellung eines Zertifikats gemäß einem Zertifizierungsprogramm, das von der Zertifizierungsstelle angeboten wird, bei der Zertifizierungsstelle gestellt hat.
Besitzer des Konformitätszeichens	Antragsteller, dessen beantragte Zertifizierungsverfahren mit der Ausstellung eines Konformitätszeichens abgeschlossen wurde.
Eigentümer eines Konformitätszeichens	ISO/IEC 17030: “Person oder Organisation, die Rechte an einem Konformitätszeichen einer dritten Seite hat” Im aktuellen Kontext: Die Zertifizierungsstelle der Telekom Security
Herausgeber (Aussteller) eines Konformitätszeichens	ISO/IEC 17030: “Stelle, die das Nutzungsrecht für ein Konformitätszeichen einer dritten Seite vergibt” Im aktuellen Kontext: Die Zertifizierungsstelle der Telekom Security
Evaluation facility (EF) / Prüfstelle	Abgeleitet aus ISO/IEC 17025 (Laboratorium): Stelle, die eine oder mehrere der folgenden Tätigkeiten ausführt:

Begriff	Definition
	- Prüfung (testing); - Audit; - Kalibrierung; - Probenahme in Verbindung mit einer darauf folgenden Prüfung oder Kalibrierung (sampling, associated with subsequent testing or calibration).
Betreiber der EF	Juristische Person, die eine Prüfstelle (EF) betreibet.
Recognition Agreement / Lizenzvereinbarung	Eine rechtlich verbindliche vertragliche Grundlage mit einer EF, die die Erteilung des Status 'recognised EF' beantragt oder bereits als EF mit dem Status 'recognised EF' agiert.
Status 'recognised EF'	Ein Status, der einer EF von der Zertifizierungsstelle der Telekom Security erteilt wird, wenn diese Evaluation Facility die EF-Recognition-Procedure, die im entsprechenden Dokument #040 definiert ist, erfolgreich absolviert hat.

Ende von Certification Practice Statement

Certification Practice Statement

Hrsg.: Deutsche Telekom Security GmbH
Adresse: Bonner Talweg 100, 53113 Bonn
Telefon: +49-(0)228-181-0
Fax: +49-(0)228-181-49990
Web: https://www.t-systems-zert.com/
https://www.telekom.de/security