Certification Practice Statement

Zertifizierungsprogramm ETSI EN 319 4xx / 5xx (akkreditierter Bereich) der Zertifizierungsstelle der Telekom Security (Zertifizierungsprogramm 032)

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' gemäß EU Verordnung Nr. 910/2014 (eIDAS) und Commission Decision 2000/709/EC (s. FESA) für die Konformitätszertifizierung von elektronischen Signaturerstellungseinheiten**.**

Das vorliegende Dokument beschreibt das Zertifizierungsprogramm für die Vergabe der Telekom Security Zertifikate für Vertrauensdiensteanbieter und der von ihnen erbrachten Vertrauensdienste im Sinne der Normenserie ETSI EN 319 4xx / 5xx, die in den akkreditierten Bereich 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 bereitgestellt.

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

1 EINFÜHRUNG 5

1.1 MISSION DER ZERTIFIZIERUNG 5

1.2 NUTZEN DER ZERTIFIZIERUNG 6

1.3 ZERTIFIZIERUNGSSTELLE DER TELEKOM SECURITY 7

2 ZERTIFIZIERUNGSPROGRAMM 032: ZERTIFIZIERUNG FÜR VERTRAUENSDIENSTEANBIETER GEMÄß ETSI EN 319 4XX / 5XX 11

2.1 ZWECK DES PROGRAMMS 11

2.2 ANGEBOTSANFRAGE UND ZERTIFIZIERUNGSVEREINBARUNG 13

2.3 ZERTIFIZIERUNG MIT EVALUIERUNG UND ÜBERWACHUNG 13

2.4 VERÖFFENTLICHUNG DES ZERTIFIKATS UND NUTZUNG DES KONFORMITÄTSZEICHENS 17

2.5 ZERTIFIZIERUNGSAUFWÄNDE 17

2.6 BESCHWERDEN UND EINSPRÜCHE 18

3 ERGÄNZENDE SERVICES 19

4 ALLGEMEINE ANFORDERUNGEN AN PRÜFSTELLEN 20

5 GLOSSAR 21

Revisionsliste

Revision	Datum	Aktivität
0.9	08.09.2000	Erst-Erstellung (debis Systemhaus)
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 (Telekom Security)
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-ETSI-TSP	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 ETSI TSP im akkreditierten und nicht akkreditierten Bereich.
4.01-ETSI-TSP	11.08.2016	Kap. 1.3 und 2.1, ETSI EN 319 411-1: Referenz auf CA/Browser Forum
4.02-ETSI-TSP	02.01.2017	Änderung der Anschrift
4.03-ETSI-TSP	01.07.2017	Änderung der Rufnummern
4.04-ETSI-TSP	01.08.2017	Außerkrafttreten des SigG, Inkrafttreten des VDG
4.05-ETSI-TSP	17.07.2018	Glossar ergänzt; Kap. 2.3 (Anforderungen an Prüfstellen) angepasst
4.06-ETSI-TSP	29.03.2019	a) ETSI TS 119 431-1: remote signature service components, Kap. 1.1, Kap. 2.3 b) ETSI TS 119 441-1: signature validation service, Kap. 1.1, Kap. 2.3 c) ETSI EN 319 522 Serie: eRDS, Kap. 1.1, Kap. 2.3 d) optional: PSD2: optionale Konformitätsbestätigung bzgl. der Profile von qualifizieren Zertifikaten für elektronische Siegel und Website-Authentifizierung gemäß ETSI TS 119 495; Kap. 2.3
4.07-ETSI-TSP	27.06.2019	a) ETSI EN 319 521: eRDS (zusätzlich zu ETSI EN 319 522), Kap. 1.1, Kap. 2.3
5.00-ETSI-TSP	01.07.2020	Umbenennung zu Telekom Security
5.01-ETSI-TSP	12.08.2020	Kap. 2.6: BSI als Aufsichtsstelle für VDA, die qualifizierte Zertifikate für die Website-Authentifizierung ausstellen

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 Betreiber, Nutzer, Anbieter und Entwickler von ICT 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 TS 119 431: 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 TS 119 441: Policy requirements for TSP 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 032: Zertifizierung für Vertrauensdiensteanbieter gemäß ETSI EN 319 4xx / 5xx

2.1 Zweck des Programms

Für den Bereich der gesamten Europäischen Union, aber auch für die Schweiz, hat die Normenserie ETSI 319 4xx „Electronic Signatures and Infrastructures (ESI)“ eine wichtige Bedeutung für Vertrauensdiensteanbieter (VDA / TSP) erlangt. Diese Normenserie kann u.a. auch für die Konformitätsbewertungen gemäß dem Zertifizierungsprogramm 031 (eIDAS) angewendet werden.

Darüber hinaus werden die entsprechenden Konformitätsbewertungsergebnisse von CA/Browser Forum[6] anerkannt.

Mit dem aktuellen Zertifizierungsprogramm bietet die Zertifizierungsstelle der Telekom Security die Prüfung, Auditierung und Zertifizierung von Vertrauensdiensteanbietern nach der Normenserie ETSI 319 4xx „Electronic Signatures and Infrastructures (ESI)“ an. Diese Normenserie adressiert auch Vertrauensdiensteanbieter, deren Vertrauensdienste nicht zwangsläufig qualifiziert im Sinne der Verordnung (EU) Nr. 910/2014 sind.

Bei diesem Programm sind - abhängig von den zu zertifizierenden Vertrauensdiensten - folgende Vorgaben zu beachten:

a) Alle Bereiche

- aktuelle Veröffentlichungen hinsichtlich zugelassener kryptographischer Algorithmen für die relevanten technischen Komponenten
- Festlegungen der Arbeitsgruppe anerkannter Bestätigungsstellen (AGAB).

b) DAkkS-akkreditierter Bereich

- 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

[6] https://cabforum.org/

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 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI TS 119 431: TSP service components operating a remote QSCD / SCDev
- ETSI TS 119 441: Policy requirements for TSP providing signature validation services
- ETSI EN 319 521 und ETSI EN 319 522 Serie: Electronic Registered Delivery Service.

c) Nicht akkreditierter Bereich

- 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;
  Part 4: Policy Requirements for Certification Authorities issuing attribute certificates
- Optional für PSD2: ETSI TS 119 495: Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366.
  Zusätzlich kann die Bewertung und Zertifizierung bzgl. der Konformität der Profile der qualifizieren Zertifikate für elektronische Siegel und Website-Authentifizierung den Anforderungen des Artikels 34 der DELEGATED REGULATION (EU) 2018-389 im Rahmen der Payment Services DIRECTIVE (EU) 2015-2366 (PSD2) durchgeführt werden.

Anmerkung:

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.

2.2 Angebotsanfrage und Zertifizierungsvereinbarung

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

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 (Konformitätsbewertungsbericht), 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 Gültigkeit von maximal 24 Monate wiedergibt sowie das Konformitätszeichen darstellt. Ein gültiges Zertifikat berechtigt zur öffentlichen Nutzung des Konformitätszeichen im Zusammenhang mit dem zertifizierten qualifizierten Vertrauensdienst gemäß der Anlage „Zertifizierungs- und Konformitätsbestätigungsregeln“.

Einzelne Vertrauensdienste:

Die Zertifizierungsstelle der Telekom Security bietet Vertrauensdiensteanbietern[7] die Bewertung und Zertifizierung von Vertrauensdiensten an, durch die ETSI EN 319 4xx Serie standardisiert sind. ETSI TS 119 612 V2.1.1 (2016-04), Abschnitt 5.5.1 kann als weitere Orientierung dienen.

[7] Im Folgenden zusammenfassend kurz TSP (Trust Service Provider) oder VDA (Vertrauensdiensteanbieter) genannt

Die Bewertung und Zertifizierung muss auf der Grundlage der o.g. Normen der ETSI erfolgen, wobei ETSI EN 319 401 allgemeine Anforderungen an TSPs stellt, die einen oder mehrere Vertrauensdienste anbieten.

Die Durchführung der Zertifizierung erfolgt auf Basis der ETSI EN 319 403. Die Evaluierung wird von Evaluatoren / Auditoren durchgeführt, die Mitarbeiter der Zertifizierungsstelle sind oder durch die Zertifizierungsstelle zugelassen sind.

Anforderungen an Prüfstellen:

1) Entweder Akkreditierung als Konformitätsbewertungsstelle im Sinne des Artikels 3 (18) der Verordnung (EU) Nr. 910/2014 durch die zuständige nationale Akkreditierungsstelle im Sinne der Verordnung (EU) Nr. 765/2008,
2) Oder Akkreditierung für die Durchführung von Prüfungen gemäß der Normenserie ETSI EN 319 4xx „Electronic Signatures and Infrastructures (ESI)“ durch die zuständige nationale Akkreditierungsstelle im Sinne der Verordnung (EU) Nr. 765/2008,
3) Oder Anerkennung / Lizenzierung für die Durchführung jeder anderer Bewertungskriterien, die Sicherheitsaudit von Prozessen/Services/Produkten abdecken (üblicherweise nach ISO/IEC 17025 oder/und ISO/IEC 17021).
   Diese Anerkennung / Lizenzierung muss sowohl die technologische Domäne, der der Zertifizierungsgegenstand angehört, als auch die durch die Normenserie ETSI EN 319 4xx „Electronic Signatures and Infrastructures (ESI)“ geforderte Prüftiefe einschließen.
   Diese Anerkennung / Lizenzierung soll durch den zuständigen nationalen oder supranationalen Regulator erteilt worden sein;
4) Allgemeine Anforderungen an Prüfstellen, s. Abschn. 4 weiter unten.

Durchführung des Audits:

Die Auditoren untersuchen den TSP bzgl. der Konformität zu den für den Vertrauensdienst relevanten ETSI-Anforderungen. Im Rahmen des Audits wird festgestellt, ob die organisatorischen und technischen Maßnahmen des TSP den Anforderungen genügen.

Das Audit des Vertrauensdienstes unterteilt sich in zwei Phasen:

- die Dokumentationsprüfung und das daran anschließende
- Audit vor Ort.

Der verantwortliche Zertifizierer und die Auditoren stimmen mit dem Kunden den zeitlichen Ablauf des Zertifizierungsvorgangs ab.

In der ersten Phase des Audits des TSP wird die in den Normen geforderte Dokumentation durch die Auditoren analysiert und auf Konformität überprüft. Falls die Prüfung zeigt, dass der Vertrauensdienst die Anforderungen nicht erfüllt, wird kein Audit vor Ort durchgeführt. Der Antragsteller hat Gelegenheit, die Dokumentation des TSP an die Anforderungen anzupassen und erneut durch die Auditoren prüfen zu lassen.

Kommen die Auditoren nach der Bewertung der TSP-Dokumentation zu dem Schluss, dass die Dokumentation die Anforderungen der anzuwendenden Normen erfüllt, so folgt die zweite Phase der Evaluierung, das Audit vor Ort. Ziel dieses Audits ist es festzustellen, dass der Vertrauensdienst so wie in den Dokumentationen beschrieben implementiert ist und seine Umsetzung den Anforderungen entspricht. Das Audit vor Ort wird an einem vorher mit dem Antragsteller abgestimmten Termin beim TSP durchgeführt.

Das Audit 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 Auditoren stichprobenhaft Nachweise durch Befragungen, Prüfungen von Unterlagen, Beobachtungen von Tätigkeiten und Bedingungen und 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 Auditoren eigene Evaluationen von technischen Komponenten durchführen. Sie können für ihre Beurteilung Prüfberichte und Zertifikate anderer unabhängiger Stellen heranziehen. Ist die Konformität des im Rahmen der Zertifizierung betrachteten TSPs im Sinne von Artikel 20 (1) der eIDAS VO bereits positiv bewertet, so können Evaluierungsergebnisse aus der Konformitätsbewertung nach eIDAS VO für die Zertifizierung des (auch qualifizierten) Vertrauensdiensteanbieters und der von ihm erbrachten (auch qualifizierten) Vertrauensdienste wiederverwendet werden, um unnötige Redundanz in den Prüfungen und damit Kosten für den TSP zu vermeiden. Die Wiederverwendung ist aufgrund der gesetzliche Anforderungen gemäß Artikel 24 eIDAS VO, nach denen das Sicherheitskonzept des TSP umfassend auf seine Eignung und praktische Umsetzung durch eine nach Artikel 20 eIDAS VO anerkannte Konformitätsbewertungsgsstelle geprüft worden sein muss, grundsätzlich möglich.

Der Umfang der Wiederverwendung wird zwischen dem verantwortlichen Zertifizierer und den Auditoren abgestimmt. Dabei ist sicherzustellen, dass die wiederverwendeten Ergebnisse für die Zertifizierung des Vertrauensdiensteanbieters und der von ihm erbrachten Vertrauensdienste anwendbar sind.

Nach erfolgtem Audit vor Ort erstellen die Auditoren auf Grundlage der Dokumentenprüfung und dem Audit einen Konformitätsbewertungsbericht mit einer Aussage über die Übereinstimmung des Vertrauensdienstes zu den relevanten ETSI-Normen. 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 des Audits mit einer Gültigkeitsdauer von maximal zwei Jahren ausgestellt. Nach spätestens 2 Jahren ist ein vollständiges Audit 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, in der Regel, auf maximal 24 Monate mit der Möglichkeit einer vollständigen Überprüfung, ob die zu Grunde liegende Konformitätsaussage (Zertifizierungsentscheidung) aufrechterhalten werden kann, vgl. ETSI EN 319 403, Kap. 7.6.4 „Audit Frequency“.
- Durchführung von regelmäßigen Kontroll-Audits, in der Regel, nicht seltener als jährlich, vgl. ETSI EN 319 403, Kap. 7.9 „Surveillance“.
- 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 TSP 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 ein erneutes Audit notwendig ist oder ob die Änderungen im Rahmen des nächsten Überwachungs- bzw. Re-Zertifizierungsaudits 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 sind folgende *Aufsichtsstellen,* die im Rahmen des Beschwerdeverfahrens angerufen werden können:

a) für VDA / TSP, die qualifizierte Zertifikate für die Website-Authentifizierung ausstellen:
   Bundesamt für Sicherheit in der Informationstechnik, Referat SZ 25, Postfach 20 03 63, 53133 Bonn
b) für VDA / TSP, die alle anderen qualifizierten Vertrauensdienste aus diesem Zertifizierungsprogramm anbieten:
   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):

Begriff	Definition
	Stelle, die eine oder mehrere der folgenden Tätigkeiten ausführt: - 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