Zertifizierungs- und Konformitätsbestätigungsregeln

Zertifizierungs- und Konformitätsbestätigungsstelle
der Telekom Security

Vorwort

Telekom Security betreibt eine gemäß 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 Registrierungsnummer: D-ZE-12025-01).

Ziel dieses Dokumentes ist es, Interessenten über

- die Regeln der Zertifizierung / Konformitätsbestätigung,
- den Ablauf von Zertifizierungs- / Konformitätsbestätigungs-Verfahren und
- die zu beachtenden Rahmenbedingungen

zu informieren.

Dieses Dokument wird laufend nach den Erfordernissen aktualisiert und auf dem Web unter www.telekom-zert.com („Service-Bereich“) zum Download bereit gestellt.

Für Durchführung eines Verfahrens ist stets die zum Zeitpunkt des Vertragsabschlusses gültige Fassung anzuwenden.

Eine Beschreibung der Zertifizierungsprogramme der Telekom Security findet man im „Certification Practice Statement“ (CPS), das an gleicher Stelle publiziert wird.

© Deutsche Telekom Security GmbH, 2000-2024

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
💻 www.telekom-zert.com

[1] Deutsche Akkreditierungsstelle, www.dakks.de

Inhaltsverzeichnis

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	Umbenennungen zu 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 101.456
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 Richtlinien
3.1	01.06.2010	Änderung der Anschrift und editorische Anpassungen; das Programm 06 wurde eingestellt.
4.0	02.06.2016	Anpassungen im Kontext der ISO 17065 und ETSI EN 319 403 Akkreditierung durch DAkkS
4.01	22.06.2016	Editorische Anpassungen
4.02	24.06.2016	Lenkungsgremium, Kap. 3.5
4.03	11.08.2016	Editorische Anpassungen
4.04	02.01.2017	Änderung der Anschrift
4.05	01.07.2017	Änderung der Rufnummern
4.06	05.06.2018	Editorische Anpassungen, Kap. 1.1, 1.2
4.07	17.07.2018	Glossar ergänzt
4.08	17.04.2019	Anpassung an die aktuelle Corporate-ID
5.00	01.07.2020	Umbenennungen zu Telekom Security
5.01	04.01.2022	Umbenennung „Besitzer des Konformitätszeichens“ zum „Inhaber des Konformitätszeichens“
5.02	23.08.2023	Editorische Anpassungen
5.03	11.03.2024	Editorische Anpassungen
5.04	08.04.2024	Berücksichtigung R-17065 (darin Kap. 7.4.5) in Kap. 1.4

1 Verfahrensablauf

In den folgenden Abschnitten wird der typische Ablauf eines Zertifizierungsverfahrens beschrieben.

1.1 Vorgespräche und Antrag auf Zertifizierung / Konformitätsbestätigung

Bei diesem Verfahrensabschnitt wird der Interessent mit allen notwendigen Informationen versorgt, bevor eine Entscheidung zur Durchführung einer Zertifizierung getroffen wird. Vorgespräche werden formal als Antrag auf Zertifizierung / Konformitätsbestätigung betrachtet.

Themen sind:

- Gegenstand der Zertifizierung,
- anzuwendendes Zertifizierungsprogramm (Verfahrenstyp) und relevante Prüfkriterien sowie die Anwendbarkeit des Zertifizierungsprogramms auf den Gegenstand der Zertifizierung,
- Rollen der Beteiligten im Rahmen des anzuwendenden Zertifizierungsprogramms,
- Rechte und Pflichten (Verantwortlichkeiten) der Beteiligten,
- vorhandene / zu erstellende Dokumente,
- technisches, organisatorisches und rechtliches Umfeld des Auftraggebers inkl. einzubeziehender Standorte und ausgegliederter Prozesse (Outsourcing),
- Verfahrensablauf und anschließende Überwachung zur Aufrechterhaltung des Konformitätszeichens,
- Vertraulichkeit der Informationen,
- Meilensteinplan, Zeit und Kosten.

Falls die Zertifizierungsstelle aufgrund der durchgeführten Bewertung der erhaltenen Informationen zur Auffassung gelangt, dass das angestrebte Zertifizierungsverfahren bereits a priori nicht durchführbar ist, unterbreitet sie dem Interessenten kein Angebot, sondert erklärt ihm die Gründe ihrer Entscheidung.

1.2 Zertifizierungsvereinbarung

Die Zertifizierungsstelle erstellt auf Anfrage und unter Berücksichtigung der Vorgespräche ein Angebot über die gewünschte Zertifizierung / Konformitätsbestätigung.

Das Angebot benennt

- den Zertifizierungsgegenstand;
- das anzuwendende Zertifizierungsprogramm (öffentlich zugängliches Dokument ‚Certification Practice Statement' gibt Normen und/oder andere normative Dokumente, nach denen der Auftraggeber eine Zertifizierung wünscht, an);
- die allgemeinen Merkmale des Auftraggebers, einschließlich dessen Name sowie die Anschrift(en) seines/seiner physischen Standorts(e), bedeutsamer Aspekte seiner Prozesse und seines Betriebs (falls vom betreffenden Zertifizierungsprogramm gefordert);
- allgemeine Informationen bezüglich des Auftraggebers, die für den beantragten Zertifizierungsbereich relevant sind, wie z. B. seine Tätigkeiten, personelle und technische Ressourcen einschließlich Labor- und/oder Zertifizierungseinrichtungen, Funktionen und ggf. Beziehungen in einer größeren Körperschaft;
- Informationen bezüglich aller ausgegliederten Prozesse, die vom Auftraggeber genutzt werden und die die Konformität mit den Anforderungen beeinflussen. Wenn der Kunde eine juristische Person(en) zur Herstellung des Zertifizierungsgegenstands identifiziert hat, die jemand anders als der Auftraggeber ist, dann kann die Zertifizierungsstelle entsprechende vertragliche Kontrollen über die juristische(n) Person(en) festlegen, wenn dies für eine wirksame Überwachung erforderlich ist. Wenn solche vertraglichen Kontrollen nötig sind, können sie vor der Bereitstellung der formellen Zertifizierungsdokumentation festgelegt werden;
- alle anderen Informationen, die entsprechend den betreffenden Zertifizierungsanforderungen benötigt werden, wie beispielsweise Informationen über Erstevaluierung und Überwachungstätigkeiten (z. B. die Standorte, an denen der Zertifizierungsgegenstand hergestellt wird, Kontaktpersonen an diesen Standorten);
- Verantwortlichkeiten der Zertifizierungsstelle und des Auftraggebers (Antragstellers) sowie alle maßgeblichen rechtlichen Verpflichtungen;
- beinhaltet eine grobe Terminplanung sowie die weiteren kommerziellen Bedingungen.

Der ‚Auftraggeber' (‚Antragsteller') stellt bei jedem Verfahrenstyp eine dedizierte Rolle dar und ist u.a. dafür verantwortlich, die Durchführung des beantragten Verfahrens durch die Zertifizierungsstelle (und ggf. durch die von ihm beauftragte Prüfstelle) zu ermöglichen. Wird das beantragte Verfahren mit der Ausstellung eines Konformitätszeichens abgeschlossen, so wird der Antragsteller zum Inhaber des Konformitätszeichens. Die Zertifizierungsstelle ist

und bleibt der Eigentümer[2] und der Aussteller[2] aller von ihr ausgestellten Konformitätszeichen (Zertifikate, Bestätigungen, Prüfsiegel).

Das Angebot wird von einem zur Unterschrift Bevollmächtigten des Betreibers der Zertifizierungsstelle unterzeichnet.

Der Antrag auf Erteilung eines Konformitätszeichens kommt durch die rechtlich verbindliche Annahme des Angebots zustande. Das Auftragsschreiben muss von einem zur Unterschrift Bevollmächtigten des Auftraggebers unterzeichnet sein und insbesondere den Unternehmensnamen, seine Rechtsform sowie die Anschrift enthalten.

Das vorliegende Dokument „Zertifizierungs- und Bestätigungsregeln“ ist stets Angebots- und Vertragsbestandteil.

1.3 Start des Verfahrens

Ein Verfahren wird nach Annahme des Zertifizierungsantrags gestartet, d.h. nachdem die Zertifizierungsvereinbarung in Kraft getreten ist.

Die Zertifizierungsstelle teilt dem Verfahren anschließend eine eindeutige Verfahrenskennung zu, die vom Antragsteller (Auftraggeber) zu Referenzzwecken verwendet werden kann. Sofern der Antragsteller einverstanden ist, kann das Zertifizierungsverfahren unter www.telekom-zert.com angekündigt werden.

Es findet bei Bedarf ein gemeinsames Kick-Off Meeting aller Beteiligten statt. Der Terminplan für das Verfahren wird einvernehmlich festgelegt.

Arbeitsort für die Durchführung des Verfahrens sind die Geschäftsräume der Zertifizierungsstelle in Bonn - mit Ausnahme ggf. verfahrensbedingt durchzuführender Audits und Inspektionen in den Geschäftsräumen des Auftraggebers und der vom Auftraggeber beauftragten Dienstleister.

Die Übergabe des Zertifikats erfolgt grundsätzlich in den Räumlichkeiten der Zertifizierungsstelle. Auf Wunsch kann das Zertifikat auch an anderen Orten übergeben werden.

Die am Projekt beteiligten Parteien entscheiden gemeinsam über ggf. notwendige Änderungen am Zertifizierungsauftrag, z. B. den Zertifizierungsgegenstand und die Abwicklung der Prüfung betreffend.

[2] Im Sinne von ISO/IEC 17030

1.4 Prüfaktivitäten

Je nach Typ des Verfahrens (auch Zertifizierungsprogramm genannt) werden Prüfschritte von der durch den Antragsteller beauftragten externen Prüfstelle (unter Begleitung durch die Zertifizierungsstelle) oder von der Zertifizierungsstelle selbst durchgeführt.

Über den Ablauf und das Ergebnis der Prüfungen werden Prüf-, Audit-, Inspektions- oder Beobachtungsberichte erstellt, die dem Antragsteller jeweils zur inhaltlichen Prüfung vorgelegt werden.

Die Prüf-, Audit-, Inspektions- oder Beobachtungsberichte gehen auf jeden einzelnen im gewählten Zertifizierungsprogramm geforderten und auf das konkrete Verfahren anwendbaren Prüfaspekt ein und nachvollziehbar dokumentieren – für jeden Prüfaspekt – die Prüfergebnisse. So wird der Antragsteller u.a. über alle festgestellten Nichtkonformitäten informiert.

Wenn eine oder mehrere Nichtkonformitäten festgestellt wurden, und der Antragsteller Interesse an der Fortsetzung des Zertifizierungsprozesses äußert, dann stellt die Zertifizierungsstelle Informationen über zusätzliche Evaluierungsaufgaben bereit, die erforderlich sind, um zu verifizieren, dass die Nichtkonformitäten korrigiert wurden. Wenn der Antragsteller einem Abschluss der zusätzlichen Evaluierungsaufgaben zustimmt, so wird die Evaluierung in einem Umfang wiederholt, um die zusätzlichen Evaluierungsaufgaben abzuschließen.

Hat der Antragsteller keine Einwände, gilt der Bericht als formell abgenommen. Bestehen Einwände seitens des Antragstellers, wird die Zertifizierungsstelle darüber nach pflichtgemäßem Ermessen entscheiden und die Entscheidung dem Antragsteller mitteilen.

Die Zertifizierungsstelle kann Ergebnisse von Konformitätsbewertungstätigkeiten (Prüf-, Inspektions- oder Auditergebnisse u.a.), die vor der Antragsstellung auf Zertifizierung abgeschlossen wurden, übernehmen, und zwar nur unter folgenden Voraussetzungen:

1) Das Zertifizierungsprogramm sieht eine solche Einbeziehung vorab bestehender Ergebnisse anderweitiger Konformitätsbewertung vor;
2) Die Zertifizierungsstelle kann anhand geeigneter Aufzeichnungen nachweisen, dass alle relevanten Anforderungen der jeweils zutreffenden ISO-Normen der 17000er-Serie eingehalten wurden;

3) Es kann anhand von Aufzeichnungen die Kompatibilität der Auswahlfunktion, die dem Ergebnis zugrunde lag, mit der zu ersetzenden Evaluierungstätigkeit hergestellt werden;
4) Es muss technische Äquivalenz im engeren Sinne bestehen, was erfordert, dass sich z.B. die Messunsicherheit des zu übernehmenden Ergebnisses im Rahmen der zulässigen Bandbreite in der übernehmenden Stelle bewegt oder andere Programmanforderungen vergleichbar sind.

1.5 Abschluss des Verfahrens

Nach dem Abschluss der Prüfaktivitäten wird eine Zertifizierungsentscheidung durch die Zertifizierungsstelle getroffen.

Nach erfolgreichem Abschluss aller Prüfaktivitäten kann positive Zertifizierungsentscheidung getroffen werden, d.h. die vom Antragsteller angestrebte Konformität bestätigt und ein Konformitätszeichen ausgestellt werden. Bei bestimmten Verfahrenstypen wird zusätzlich ein Zertifizierungs- bzw. Bestätigungsreport oder ein Anhang / Nachtrag zum bereits ausgestellten Konformitätszeichen erstellt. Diese Unterlagen werden dem Antragsteller in elektronischer und gedruckter Form übergeben.

Unter www.telekom-zert.com können in Abstimmung mit dem Antragsteller diese Dokumente und Urkunden veröffentlicht werden.

Verfahrenstypbedingt kann es erforderlich sein, diese Unterlagen an Aufsichtsstellen (Bundesamt für Sicherheit in der Informationstechnik, Bundesnetzagentur, Akkreditierer) weiterzuleiten oder diesen Stellen Einblick in die Unterlagen zu geben.

Hinsichtlich der Veröffentlichung der Ergebnisse des Verfahrens durch solche Stellen ist die Zertifizierungs- und Bestätigungsstelle der Telekom Security an deren Fristen gebunden und kann keine Termine für die Veröffentlichung garantieren.

Ist das Verfahren insgesamt nicht erfolgreich abgeschlossen worden, enthält der abschließende Bericht die maßgeblichen Gründe. Der Antragsteller kann nach Behebung der Mängel eine erneute Prüfung veranlassen, s. Abschn. 1.4 weiter oben.

Alle Unterlagen aus dem Verfahren werden bei der Zertifizierungsstelle archiviert. Falls eine Hinterlegung des Prüfobjektes bei der Zertifizierungsstelle vereinbart ist (z. B. bei Produkten), wird eine entsprechende Verwahrung eingeleitet. Näheres wird zwischen den Beteiligten abgestimmt.

1.6 Aufrechterhaltung des Konformitätszeichens nach Änderungen

Nach Änderungen am Gegenstand der Zertifizierung / Bestätigung, Änderungen an den Prüfgrundlagen oder bei neuen technischen Erkenntnissen, die für den Zertifizierungsgegenstand relevant sein können, ist über die Aufrechterhaltung, die Änderung, Erweiterung/Einschränkung, Suspendierung/Wiederinkraftsetzung oder Rücknahme des Konformitätszeichens zu entscheiden.

Im Einzelnen:

- Wird der Gegenstand der Zertifizierung / der Bestätigung verändert oder erweitert, ist je nach Art der Änderung eine Erweiterung des Konformitätszeichens auf die geänderte Fassung (ggf. unter Auflagen) oder die Beschränkung des Konformitätszeichens auf die alte Fassung möglich.
  Eine Erweiterung des Konformitätszeichens durch einen Anhang / Nachtrag zum bereits bestehenden Konformitätszeichen kann nur vom Antragsteller des zu erweiternden Konformitätszeichens (vom Konformitätszeicheninhaber) beantragt werden.
- Bei Änderungen an den Prüfgrundlagen (am relevanten Zertifizierungsprogramm) wird die Zertifizierungsstelle den Antragsteller frühzeitig informieren. Die Zertifizierungsstelle wird dem Antragsteller die Auswirkungen der Änderung auf den Zertifizierungsgegenstand und seine Zertifizierung / Bestätigung erläutern. Möglicherweise kann das Konformitätszeichen auf der Basis der veränderten Prüfgrundlagen nicht ohne Weiteres aufrechterhalten werden und bedarf einer erneuten Prüfung.
- Führen neue technische Erkenntnisse, die für den Zertifizierungsgegenstand relevant sein können, dazu, dass ein Konformitätszeichen aus technischen Gründen nicht mehr zu rechtfertigen ist, besteht für den Antragsteller die Gelegenheit, erkannte Schwachstellen in angemessener Frist zu beseitigen: Diese Vorgänge sind verfahrensgerecht zu dokumentieren, die Zertifizierungsstelle ist entsprechend zu informieren. Die Zertifizierungsstelle entscheidet aufgrund dieser Mitteilung, ob die Zertifizierung / Bestätigung (ggf. unter Auflagen) entweder aufrechterhalten werden kann oder eingeschränkt oder - vorbehaltlich der Abstellmaßnahmen durch den Antragsteller - suspendiert oder zurückgezogen werden muss.

Abhängig vom Umfang und der Art der Änderungen, die - für jedes einzelne Zertifizierungsverfahren zur Aufrechterhaltung des Konformitätszeichens - in einer vom Antragsteller anzufertigenden Auswirkungsanalyse zu beschreiben sind, kann für die Entscheidungsfindung bzgl. der Aufrechterhaltung, der Änderung, Erweiterung/Einschränkung, Suspendierung/Wiederinkraftsetzung oder Rücknahme des Konformitätszeichens eine Re-Zertifizierung[3] oder eine Re-Evaluierung[4] des Zertifizierungsgegenstands erforderlich sein. Die endgültige Entscheidung darüber wird der Zertifizierungsstelle vorbehalten.

Jede Änderung, Erweiterung, Suspendierung oder Rücknahme des Konformitätszeichens wird entsprechend den Maßgaben in Kap. 3.2 beauskunftet und veröffentlicht.

[3] wird ausschließlich durch die Zertifizierungsstelle, ohne Beteiligung einer Prüfstelle, durchgeführt

[4] wird durch eine Prüfstelle durchgeführt, mit anschließender Re-Zertifizierung

2 Zertifizierungsregeln

2.1 Pflichten der Zertifizierungsstelle

Die Zertifizierungsstelle ist gemäß den einschlägigen Normen

- DIN EN ISO/IEC 17065: Konformitätsbewertung – Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren, aktuelle Fassung
- ETSI EN 319 403: Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment-Requirements for conformity assessment bodies assessing Trust Service Providers.

bei DAkkS unter der DAkkS-Registriernummer D-ZE-21631-01 akkreditiert.

Die Erfüllung dieser Normen und die Aufrechterhaltung der entsprechenden Akkreditierung sind für die Zertifizierungsstelle unverzichtbar. Folgende Grundsätze und Verpflichtungen sind daraus für die Dienste der Zertifizierungsstelle ableitbar:

- Die Zertifizierungsprogramme der Zertifizierungsstelle sind allen externen[5] Interessenten zugänglich[6].
- Unparteilichkeit und Objektivität sind gewahrt und eine Gleichbehandlung aller Auftraggeber ist sichergestellt.
- Soweit technische Prüfungen durch unabhängige (externe) Prüfstellen durchgeführt werden, ist eine Gleichbehandlung aller Prüfstellen garantiert.
- Interessen und Vorbehalte Dritter haben keinerlei Einfluss auf die Verfahren und Ergebnisse der Zertifizierungsstelle.

Die Zertifizierungsstelle ist gehalten, diese Grundsätze dauerhaft umzusetzen, und wird diesbezüglich durch den Akkreditierungsgeber und Aufsichtsstellen überwacht. Der Akkreditierungsgeber achtet insbesondere darauf, dass die Verfahren der

[5] D.h. nicht aus dem Konzern Deutsche Telekom AG

[6] Die Zertifizierungsstelle kann es ablehnen, einen Antrag auf einen Vertrag zur Zertifizierung eines Antragstellers anzunehmen oder aufrechtzuerhalten, wenn es grundlegende oder nachgewiesene Gründe gibt, wie z. B. dass der Kunde an illegalen Aktivitäten beteiligt ist, wiederholt gegen die Zertifizierungs- bzw. Produktanforderungen verstoßen hat oder ähnliche auf den Kunden bezogene Probleme.

Zertifizierungsstelle allen externen Interessenten zugänglich sind, Unparteilichkeit und Objektivität gewahrt sind und eine Gleichbehandlung aller Antragsteller sichergestellt ist.

Die Zertifizierungsstelle verwendet und verwaltet ihre Konformitätszeichen im Sinne von ISO/IEC 17030.
Die Zertifizierungsstelle überwacht grundsätzlich die Verwendung ihrer Konformitätszeichen. Bei irreführender oder missbräuchlicher Verwendung behält sich die Zertifizierungsstelle korrigierende, bekanntmachende oder im Extremfall rechtliche Schritte vor.

Entfallen die Grundlagen, auf der ein Konformitätszeichen ausgestellt wurde, entscheidet die Zertifizierungsstelle, ob das Konformitätszeichen (ggf. unter einschränkenden Auflagen) aufrechterhalten werden kann oder zurückgezogen (widerrufen) werden muss. Auch der Antragsteller als Konformitätszeicheninhaber kann Änderungen oder den Widerruf des Konformitätszeichens beantragen.

Die Zertifizierungsstelle beschränkt ihre Anforderungen, Evaluierung, Bewertung, Entscheidung und Überwachung (falls erforderlich) auf solche Aspekte, die sich speziell und ausschließlich auf den Geltungsbereich der Zertifizierung beziehen.

2.2 Pflichten des Antragstellers

Der Antragsteller (Auftraggeber) verpflichtet sich mit Auftragserteilung zur dauerhaften Einhaltung der nachfolgenden Grundsätze (aus der ISO/IEC 17065 und den jeweiligen Prüfkriterien).

Bei wesentlicher Nichtbeachtung dieser Auflagen seitens des Antragstellers behält sich die Zertifizierungsstelle vor, Ankündigungen unter www.telekom-zert.com zu löschen, Konformitätszeichen nicht zu erteilen, erteilte Konformitätszeichen zurückzuziehen (zu widerrufen).

2.2.1 Alle Zertifizierungsprogramme

1. Der Antragsteller erfüllt stets die Zertifizierungsanforderungen, einschließlich der Umsetzung entsprechender Änderungen, wenn diese durch die Zertifizierungsstelle mitgeteilt werden.
2. Der Antragsteller stellt sicher, dass, wenn die Zertifizierung für eine laufende Produktion gilt, das zertifizierte Produkt weiterhin die Produktanforderungen erfüllt.

3. Der Antragsteller trifft alle notwendigen Vorkehrungen für

   1) die Durchführung der Evaluierung und Überwachung (falls erforderlich), einschließlich der Berücksichtigung der Prüfung der Dokumentation und Aufzeichnungen, des Zugangs zu der entsprechenden Ausstattung, dem/den Standort(en), dem/den Bereich(en) und dem Personal, und den Unterauftraggebern des Antragstellers;

   2) die Untersuchung von Beschwerden;

   3) die Teilnahme von Beobachtern, falls zutreffend.

4. Der Antragsteller kann seine Ansprüche hinsichtlich der Zertifizierung nur im Einklang mit dem Geltungsbereich der Zertifizierung erheben.

5. Der Antragsteller darf nicht die Produktzertifizierung in einer Weise verwenden, die die Zertifizierungsstelle in Misskredit bringen könnte, sowie Äußerungen über ihre Produktzertifizierung treffen, die die Zertifizierungsstelle als irreführend oder unberechtigt betrachten könnte.

6. Bei der Verteilung von Konformitätszeichen ist immer die aktuell gültige Version zu verwenden.

7. Das Konformitätszeichen (die Zertifizierungsurkunde) darf nur unverändert, d.h. genau wie von der Zertifizierungsstelle ausgestellt, verwendet werden.

8. Wenn die Zertifizierungsdokumente inkl. des Konformitätszeichens (der Zertifizierungsurkunde) anderen zur Verfügung gestellt werden, so müssen die Dokumente in ihrer Gesamtheit bzw. so, wie im Zertifizierungsprogramm festgelegt, vervielfältigt werden.

9. Bei Aussetzung, Entzug oder Beendigung der Zertifizierung / Bestätigung ist die Verwendung aller Werbematerialien, die jeglichen Bezug auf die Zertifizierung / Bestätigung enthalten, einzustellen und die vom Zertifizierungsprogramm geforderten Maßnahmen zu ergreifen (z. B. die Rückgabe von Zertifizierungsdokumenten) sowie alle anderen erforderlichen Maßnahmen zu ergreifen.

10. Bei Bezugnahme auf das zertifizierte Objekt in Kommunikationsmedien, wie z. B. Dokumenten, Broschüren oder Werbematerialien, sind die Anforderungen der Zertifizierungsstelle, oder wie im Zertifizierungsprogramm festgelegt, zu erfüllen.

    Eine Bezugnahme auf das zertifizierte Objekt in öffentlich zugänglichen Medien und Materialien muss in eindeutiger Form erfolgen und darf nicht irreführend sein; insbesondere darf die Zertifizierung nur benutzt werden, um auf die Konformität des

zertifizierten Objektes zu dem angewendeten Standard hinzuweisen.

Neue Versionen von früher zertifizierten Objekten dürfen erst dann als „zertifiziert“ bzw. „bestätigt“ bezeichnet werden, wenn eine Re-Zertifizierung / Nachtragsbestätigung erfolgreich abgeschlossen und beurkundet wurde.

11. Die Zertifizierungsstelle ist unverzüglich über Veränderungen zu informieren, die die Fähigkeit des Antragstellers, die Zertifizierungsanforderungen zu erfüllen, beeinträchtigen könnten[7].

12. Produkte und Systeme sowie verfahrensrelevante Dokumentation sind vom Antragsteller so zu kennzeichnen, dass geänderte Versionen eindeutig an neuen Versionsnummern, Release-Ständen, etc. erkennbar sind.

13. Führen neue Sicherheitserkenntnisse dazu, dass ein Konformitätszeichen aus technischen Gründen nicht mehr zu rechtfertigen ist, besteht für den Antragssteller die Gelegenheit, erkannte Schwachstellen in angemessener Zeit zu beseitigen, dies zu dokumentieren und die Zertifizierungsstelle entsprechend zu informieren.

14. Aufzeichnungen aller Beschwerden und neuer Erkenntnisse über Eigenschaften eines zertifizierten Objektes sind aufzubewahren, die dem Kunden des Antragsstellers in Bezug auf die Einhaltung der Zertifizierungsanforderungen bekannt gemacht wurden, und diese Aufzeichnungen der Zertifizierungsstelle auf Anfrage zur Verfügung zu stellen; und

    1) geeignete Maßnahmen sind vom Antragssteller zu ergreifen in Bezug auf solche Beschwerden sowie jegliche Mängel, die an den Produkten entdeckt wurden und die die Einhaltung der Anforderungen an die Zertifizierung beeinflussen;

    2) die ergriffenen Maßnahmen sind zu dokumentieren.

15. Alle Anforderungen sind zu erfüllen, die im Zertifizierungsprogramm beschrieben sein können und die sich auf die Verwendung von Konformitätszeichen sowie auf Informationen in Bezug auf das Produkt beziehen.

    Die Zertifizierungsstelle verwendet und verwaltet ihre Konformitätszeichen im Sinne

[7] *Beispiele für Veränderungen können mit einschließen:*

- den rechtlichen, wirtschaftlichen oder organisatorischen Status bzw. die Eigentümerschaft;

- Organisation und Management (z. B. Schlüsselpositionen, Entscheidungsprozesse oder technisches Personal);

- Änderungen am Produkt oder der Herstellungsmethode;

- Kontaktadressen und Produktionsstätten;

- wesentliche Änderungen am Qualitätsmanagementsystem.

von ISO/IEC 17030.

Die Zertifizierungsstelle überwacht grundsätzlich die Verwendung ihrer Konformitätszeichen. Bei irreführender oder missbräuchlicher Verwendung behält sich die Zertifizierungsstelle korrigierende, bekanntmachende oder im Extremfall rechtliche Schritte vor.

16. Falls erforderlich, hat der Antragsteller spätestens 8 Wochen nach Start des entsprechenden Verfahrens eine für das gewählte Zertifizierungsprogramm geeignete externe Prüfstelle mit der Durchführung der technischen Evaluierung zu beauftragen.
17. Die Zertifizierungsstelle erhält das Recht zur Einsicht in alle prüfungsrelevanten Unterlagen des Antragstellers sowie in die Prüfberichte der beauftragten Prüfstelle, soweit dies für die Prüfung und Zertifizierung nach den zugrunde liegenden Kriterien erforderlich ist.
18. Die Zertifizierungsstelle hat das Recht, nach Ankündigung und zum Zwecke einer Prüfung die Entwicklungs-, Test-, Produktionsumgebung und andere Liegenschaften des Antragstellers, der von ihm beauftragten Dritten, seiner Zulieferer und anderer Stellen, die für die Prüfung relevant sind, zu betreten und zu inspizieren, soweit dies für die Prüfung erforderlich ist.

Einzelne Zertifizierungsprogramme sind im jeweiligen öffentlich zugänglichen Dokument „Certification Practice Statement“ der Zertifizierungsstelle dargelegt. Für jedes Zertifizierungsprogramm oder eine Gruppe von verwandten Zertifizierungsprogrammen gibt ein dediziertes „Certification Practice Statement“.

3 Sonstiges

3.1 Vertraulichkeit

Die Wahrung der Vertraulichkeit von Informationen, die im Rahmen von Verfahren anfallen, ist ein zentraler Grundsatz der Zertifizierungsstelle. Dies bezieht sich sowohl auf die Aufbewahrung als auch auf Übertragung aller verfahrensbezogenen Informationen. Hierfür ist ein System von drei Vertraulichkeitsstufen eingerichtet, deren Auswahl durch das Angebot und die Beauftragung vorgenommen wird:

Standard: Zugang zu bei der Zertifizierungsstelle gespeicherten verfahrensbezogenen Informationen haben alle Zertifizierer und Auditoren der Zertifizierungsstelle, die IT-Administration der Telekom Security sowie die ggf. beteiligte Prüfstelle. Bei der elektronischen Übertragung von Daten wird individuell entschieden, ob Daten zu verschlüsseln sind.

Need-To-Know: Zugang zu bei der Zertifizierungsstelle gespeicherten bzw. zu übertragenden verfahrensbezogenen Informationen haben nur die am Verfahren beteiligten Zertifizierer und Auditoren der Zertifizierungsstelle und die ggf. beteiligte Prüfstelle. Bei der elektronischen Übermittlung werden Daten nach einem zwischen den Beteiligten abgestimmten Verfahren verschlüsselt.

Hoch: Es werden die Verfahren aus dem staatlichen Verschlusssachenbereich angewendet. Die Zertifizierungsstelle verfügt über eine organisatorische und technische Infrastruktur, die für den Umgang mit staatlichen Verschlusssachen mindestens bis zum Grad „geheim“ geeignet ist.

3.2 Auskünfte und Veröffentlichungen

Sowohl Auskünfte über den Stand laufender Verfahren als auch Informationen über den Antragsteller selbst werden von der Zertifizierungsstelle nicht an Dritte weitergegeben, es sei denn, der Antragsteller stimmt explizit zu.

Eine Veröffentlichung von Verfahrensergebnissen durch die Zertifizierungsstelle erfolgt nur mit Zustimmung des Antragstellers. Wurden Zertifizierungsergebnisse eines Zertifizierungsverfahrens durch die Zertifizierungsstelle veröffentlicht, wird jede Änderung, Erweiterung, Suspendierung oder Rücknahme des Konformitätszeichens durch die Zertifizierungsstelle auch entsprechend beauskunftet und veröffentlicht. Das Verzeichnis der

durch die Zertifizierungsstelle zertifizierten Objekten wird standardmäßig, d.h. für alle Zertifizierungsprogramme, auf ihrer Webseite unter www.telekom-zert.com veröffentlicht.

Unabhängig davon muss die Zertifizierungsstelle - verfahrenstypabhängig - Dritten (z.B. aufsichtsführenden Behörden, Akkreditierer) eine Einsicht in Prüfergebnisse gewähren. Der Antragsteller wird darüber stets, sofern nicht gesetzlich verboten, unterrichtet.

Alle von der Zertifizierungsstelle ausgestellten Konformitätszeichen und Dokumente sind Eigentum der Zertifizierungsstelle. Sie enthalten auch Copyright-Vermerke, die Auskunft über die Möglichkeit der Vervielfältigung durch Dritte geben: Der Betreiber der Zertifizierungsstelle behält das Copyright für alle von der Zertifizierungsstelle ausgestellten Konformitätszeichen und Dokumente (Reviews, Berichte, Gutachten, etc.). Sofern vertraglich nicht anders vereinbart, ist der Antragsteller berechtigt, ausschließlich Konformitätszeichen zu vervielfältigen und zu verteilen – vorausgesetzt, dass Inhalt, Form und Herkunft (die Zertifizierungsstelle als Eigentümer und Aussteller) von Konformitätszeichen unverändert bleiben.

3.3 Überwachung der Verwendung des Konformitätszeichens

Die Zertifizierungsstelle überwacht grundsätzlich die Verwendung ihrer Konformitätszeichen. Bei irreführender oder missbräuchlicher Verwendung behält sich die Zertifizierungsstelle korrigierende, bekanntmachende oder im Extremfall rechtliche Schritte vor.

Eine sach- und ordnungsgemäße Verwendung des Konformitätszeichens wird dem Antragsteller vertraglich auferlegt, s. Kap. 2.2 weiter oben.

Die Regelungen bzgl. der Überwachung (durch die Zertifizierungsstelle) der Verwendung des Konformitätszeichens werden im jeweiligen Zertifizierungsprogramm festgelegt. Einzelne Zertifizierungsprogramme sind im öffentlich zugänglichen Dokument „Certification Practice Statement“ der Zertifizierungsstelle dargelegt.

3.4 Verfahrenskosten und Haftung

Für die Durchführung eines Verfahrens werden Kosten erhoben. Diese Kosten richten sich hauptsächlich nach dem beantragten Verfahrenstyp, dem konkreten zu zertifizierenden Objekt, dem angestrebten oder geforderten Zertifizierungsumfang und nach der angestrebten oder geforderten Prüftiefe. Die Verfahrenskosten werden jedoch unabhängig von Attributen des Auftragsgebers (von seiner Firmierung, von der Firmengröße, Firmensitz, Sparte etc.) erhoben. Näheres wird im Angebot festgelegt.

Zertifizierungskosten werden stets im vereinbarten Umfang erhoben - unabhängig davon, ob ein Konformitätszeichen erteilt worden ist oder wegen technischer oder anderer Mängel nicht erteilt werden konnte, das Verfahren durch den Antragsteller abgebrochen oder wegen Nicht-Bereitstellung der notwendigen Informationen durch die Zertifizierungsstelle eingestellt worden ist.

Werden vom Auftraggeber Änderungen an von ihm bereits abgenommenen Berichten, Gutachten, Konformitätszeichen gewünscht, wird der Mehraufwand dem Auftraggeber zusätzlich in Rechnung gestellt. Dies gilt auch für die Durchführung von Wiederholungsprüfungen, wenn solche aus Gründen, die beim Auftraggeber liegen, erforderlich werden. Auftraggeber und Zertifizierungsstelle stimmen sich hierüber vorher ab.

Die jedem Angebot beigefügten Allgemeinen Geschäftsbedingungen (AGB) beschreiben die Art und den Umfang der Haftung durch die Telekom Security.

3.5 Beschwerde– und Einspruchsverfahren

Gegen Entscheidungen der Zertifizierungsstelle kann von den Beteiligten (Antragsteller, Prüfstelle) Beschwerde bzw. Einspruch eingelegt werden. Das Beschwerde- und Einspruchsverfahren sieht folgendes vor:

(i) Die Zertifizierungsstelle bestätigt den Erhalt einer formalen Beschwerde / eines formalen Einspruchs.

(ii) Die Zertifizierungsstelle setzt sich mit der Beschwerde / dem Einspruch inhaltlich auseinander, um festzustellen, ob sich die Beschwerde / der Einspruch auf Zertifizierungstätigkeiten bezieht, für die die Zertifizierungsstelle verantwortlich ist.
Falls die Zertifizierungsstelle die Beschwerde / den Einspruch nicht annimmt, wird dies gegenüber dem Beschwerdeführer schriftlich begründet.
Nimmt die Zertifizierungsstelle die Beschwerde / den Einspruch an, befasst sie sich damit. Hierbei wird die Zertifizierungsstelle alle erforderlichen Informationen (soweit möglich) erfassen und verifizieren, um eine Entscheidung über die Beschwerde / den Einspruch herbeizuführen.

(iii) Zunächst wird es versucht, eine Einigung über den strittigen Sachverhalt mit dem für das betreffende Verfahren zuständigen Zertifizierer / Konformitätsbestätiger zu erzielen.

(iv) Wenn dies nicht möglich ist, wird es versucht, eine Einigung mit dem Leiter der Zertifizierungsstelle herbeizuführen.

(v) Wenn dies nicht möglich ist, kann sich der Beschwerdeführer an das „Lenkungsgremium zur Sicherung der Unparteilichkeit der Zertifizierungsstelle der Telekom Security“. Die Anschrift des Lenkungsgremiums lautet: Lenkungsgremium der Zertifizierungsstelle der Telekom Security, Telekom Security International GmbH, Bonner Talweg 100, 53113 Bonn, Deutschland.

(vi) Wenn dies nicht möglich ist, können sich der Beschwerdeführer und die Zertifizierungsstelle gemeinsam an die relevante Aufsichtsstelle wenden; welche Aufsichtsstelle relevant ist, hängt vom Zertifizierungsprogramm ab, im Rahmen dessen das in Frage kommende Zertifizierungsverfahren durchgeführt wurde / wird, s. Dokument „Certification Practice Statement“ für das jeweilige Zertifizierungsprogramm.

(vii) Die Zertifizierungsstelle ergreift alle erforderlichen Folgemaßnahmen, um die Beschwerde / den Einspruch beizulegen.

(viii) Wo immer möglich, informiert die Zertifizierungsstelle den Beschwerde- / den Einspruchsführer formell über das Ergebnis und die Beendigung des Beschwerde- bzw. des Einspruchsverfahrens.

Dieses Schlichtungsverfahren präjudiziert weder den Rechtsweg, noch schließt es ihn aus.

4 Glossar

Begriff	Definition
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 bestätigt werden.
Zertifizierungsprogramm (EN: certification scheme) / Verfahrenstyp	In Anlehnung an ISO/IEC 17065 (3.9): *Zertifizierungssystem* (Konformitätsbewertungssystem), das sich auf bestimmte Klasse / bestimmten Typ von *zu zertifizierenden Objekten* bezieht, auf welche(n) 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,	Produkt / Dienstleistung / Prozess, für welche{n,s} die Erlangung eines Konformitätszeichens vom Antragsteller

Begriff	Definition
Gegenstand der Konformitätsbewertung)	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.
Inhaber 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: - Prüfung (testing); - Audit; - Kalibrierung; - Probenahme in Verbindung mit einer darauffolgenden 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.

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.

Ende von Zertifizierungs- und Bestätigungsregeln

Zertifizierungs- und Bestätigungsregeln

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