



Bundesamt
für Sicherheit in der
Informationstechnik

Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen

VB-Personen

Version 3.1 vom 18.03.2020



Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-111
E-Mail: service-center@bsi.bund.de
Internet: <https://www.bsi.bund.de>
© Bundesamt für Sicherheit in der Informationstechnik 2009- 2020

Änderungshistorie

Version	Datum	Name	Beschreibung
1.0	02.07.2009	Personenzertifizierungsstelle SZ 12	Erstausgabe
2.0	06.08.2010	Personenzertifizierungsstelle SZ 12	Neuausgabe
2.1	18.03.2011	Personenzertifizierungsstelle SZ 12	Revision
2.2	03.09.2013	Personenzertifizierungsstelle SZ 12	Revision
2.3	15.06.2014	Personenzertifizierungsstelle SZ 12	Revision
2.4	20.06.2017	Personenzertifizierungsstelle SZ 12	Revision: • Änderung im Kapitel 3.1 „Antragsphase“ (Fristen Antragsstellung) • Änderung im Kapitel 3.4 „Erneute Kompetenzfeststellung und Rezertifizierung“ (Fristen Antragsstellung)
2.5	24.08.2017	Personenzertifizierungsstelle SZ 12	Revision: • Ergänzung des Dokuments TR-Prüfer
3.0	20.05.2019	QMB SZ	Neuausgabe aufgrund Dokumentenumstrukturierung und der Umstellung auf ein Antrag-Bescheidverfahren.
3.1	18.03.2020	QMB SZ	Revision: • Änderungen der Fristen in den Kapiteln 4.4 „Rezertifizierung“ und 5.4.4 „Ablehnung eines Antrags“. • BSI-KostV durch BMI-GebV ersetzt, • Ergänzung von Zertifizierungsnummern in Kapitel 6.1, • Konkretisierungen und sprachliche Anpassungen in diversen Kapiteln.

Inhaltsverzeichnis

	Änderungshistorie.....	3
1	Einleitung.....	7
1.1	Zielsetzung und Eingliederung der VB-Personen.....	7
1.2	Nutzen der Zertifizierung für den Antragsteller.....	9
2	Kompetenzfeststellungs- und Zertifizierungsprogramme für Personen.....	10
2.1	Programme für die Zertifizierung von Personen.....	10
2.2	Programme für die Kompetenzfeststellung von Personen für die Anerkennung und Zertifizierung von Stellen.....	10
3	Verfahren zur Kompetenzfeststellung und Zertifizierung.....	12
3.1	Antragsphase.....	12
3.2	Prüfphase - Kompetenzfeststellung.....	12
3.2.1	Fachkundenachweis durch eine Prüfung.....	13
3.2.2	Fachkundenachweis durch eine Fachbegutachtung.....	13
3.3	Zertifizierungsphase.....	13
4	Aufrechterhaltung und Überwachung der Zertifizierung.....	14
4.1	Durchführung der (Prüf-)Tätigkeiten im betreffenden Programm.....	14
4.2	Überwachung der Kompetenz bzw. Zertifizierung.....	14
4.3	Anlassbezogene Begutachtungen.....	14
4.4	Rezertifizierung.....	14
5	Rahmenbedingungen.....	16
5.1	Grundlage für die Zertifizierung.....	16
5.2	Genereller Dokumentenaustausch mit der Personenzertifizierungsstelle.....	16
5.3	Optionale Schulungsmaßnahmen.....	16
5.4	Rahmenbedingungen zum Verfahren.....	16
5.4.1	Obliegenheiten des Antragstellers.....	16
5.4.2	Rücknahme eines Antrags.....	16
5.4.3	Änderungen des Antrags.....	17
5.4.4	Ablehnung eines Antrags.....	17
5.5	Rahmenbedingungen zur Aufrechterhaltung der Zertifizierung.....	17
5.5.1	Bestimmungen zur Aufrechterhaltung.....	17
5.5.2	Regelungen zur Vertraulichkeit.....	18
5.5.3	Regelungen zur Archivierung von Dokumenten und Aufzeichnungen.....	18
5.6	Aufhebung einer Zertifizierung.....	18
5.6.1	Widerruf einer rechtmäßigen Zertifizierung.....	18
5.6.2	Rücknahme einer rechtswidrigen Zertifizierung.....	19
5.6.3	Folgen der Aufhebung.....	19
5.7	Beschwerde- und Verbesserungsmanagement.....	19
5.8	Haftung.....	19
5.9	Kosten.....	19
6	Veröffentlichung der Zertifizierung.....	21
6.1	Zertifizierungsnummer.....	21
7	Referenzen und Glossar.....	22

Abbildungsverzeichnis

Abbildung 1: Zertifizierungs- und Anerkennungsprogramme (Dokumentenübersicht).....8

Tabellenverzeichnis

Tabelle 1: Zertifizierungsnummern der Personengruppen..... 21

1 Einleitung

Das Bundesamt für Sicherheit in der Informationstechnik führt im Bereich der Konformitätsbewertung Zertifizierungen von Personen auf Grundlage des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz, [BSIG]) vom 14. August 2009 durch. Zur Durchführung von Evaluierungen und Prüfungen zum Zwecke der Zertifizierung von Produkten und Managementsystemen sowie zur Unterstützung des BSI im Bereich IT-Sicherheitsdienstleistungen werden qualifizierte Personen benötigt.

Ziel des Verfahrens ist es, kompetente Personen in den verschiedenen Programmen bereitzustellen sowie die Qualität und Vergleichbarkeit der Evaluierungen/Prüfungen, Audits und Dienstleistungen sicherzustellen.

Um diese Aufgaben zu erfüllen, betreibt das BSI ein Kompetenzfeststellungs- und Zertifizierungssystem, das in dieser Verfahrensbeschreibung (VB) beschrieben wird. In dieser VB sind die Regeln (Programme, bedarfsgerechte Begutachtungskriterien, Anforderungen und Nachweise), das Verfahren sowie das Management zur Durchführung der Kompetenzfeststellung und Zertifizierung festgelegt und beschrieben. Die Personenzertifizierung, ist ausschließlich natürlichen Personen vorbehalten.

Aus Gründen der besseren Lesbarkeit wird in diesem Dokument nur die männliche Form für die Bezeichnung der Personengruppe gewählt, dennoch beziehen sich die Angaben auf Angehörige beider Geschlechter.

Diese Verfahrensbeschreibung wird mit der Veröffentlichung für alle Personengruppen (Antragsteller sowie zertifizierte und bei Prüfstellen und IT-Sicherheitsdienstleistern beschäftigten Personen) verbindlich und ersetzt alle vorhergehenden Verfahrensbeschreibungen im Bereich der Zertifizierung von Personen.

1.1 Zielsetzung und Eingliederung der VB-Personen

„Übergeordnetes Ziel der Zertifizierung von Personen ist es, die Kompetenz einer Person, eine Aufgabe oder eine Tätigkeit durchzuführen, anzuerkennen.“

„Das Vertrauen in die jeweiligen Zertifizierungsprogramme wird mittels eines weltweit akzeptierten Prozesses der Begutachtung und periodischer Wiederbegutachtungen der Kompetenz der zertifizierten Personen erreicht.“

aus [17024] A.1.2 und Einleitung

Einen Überblick über das Zertifizierungs- und Anerkennungssystem, die Zertifizierungs- und Anerkennungsprogramme sowie der zugehörigen Dokumente gibt die folgende Abbildung. Diese Dokumente stellen Informationen zielgruppenorientiert zur Verfügung.

Broschüre „Zertifizierte IT-Sicherheit“				
Übersicht der angebotenen Zertifizierungen und Anerkennungen				
Zertifizierungssystem für Produkte, Prozesse und Dienstleistungen ISO/IEC 17065	Zertifizierungssystem für Managementsysteme ISO/IEC 17021 und 27006	Zertifizierungssystem für Personen ISO/IEC 17024	Anerkennungssystem für Stellen (ISO/IEC 17011)	Zertifizierungssystem für IT-Sicherheits- dienstleister
VB-Produkte	VB-Managementsysteme	VB-Personen	VB-Stellen	
Allgemeine Verfahrensbeschreibung für den Antragsteller (Hersteller, Betreiber, Person, Prüfstelle/IT-Sicherheitsdienstleister)				
CC-Produkte		CC-Evaluatoren	CC-Prüfstellen	
TR-Produkte		TR-Prüfer	TR-Prüfstellen	
		IS-Revisor und IS Berater		
		IS-Penetrationstester		
		DigBOS-Prüfer		
		IT-GS-Berater		
	GS-Managementsysteme	VB-Auditor (VB und Programm)		IS-Revision und IS-Beratung
	TR-Managementsysteme			IS-Penetrationstest
				DigBOS
				Lauschabwehr
Programme: Anforderungen und detaillierte Informationen für den Antragsteller (Hersteller, Betreiber, Person, Prüfstelle/IT-Sicherheitsdienstleister)				
Übergreifende Dokumente:		Zeichenordnung	Verzeichnisse	

Abbildung 1: Zertifizierungs- und Anerkennungsprogramme (Dokumentenübersicht)

Die übergeordnete Broschüre „Zertifizierte IT-Sicherheit“ [Broschüre] richtet sich an Personen, die sich über den Auftrag des BSI im Bereich der Konformitätsbewertung im Allgemeinen informieren möchten.

In den „Verfahrensbeschreibungen“ (VB) des Zertifizierungs- und Anerkennungssystems werden der Nutzen für den Antragsteller, das Verfahren und die damit verbundenen Rechte und Pflichten sowie Obliegenheiten dargestellt. Sie sind Entscheidungshilfe, wenn die Absicht besteht einen Antrag zu stellen und richtet sich somit an:

- Hersteller, die ihre Produkte zertifizieren [VB-Produkte],
- Betreiber, die ihre Systeme zertifizieren [VB-Managementsysteme],
- Personen, die sich zertifizieren (vorliegende VB-Personen),
- Prüfstellen, die sich anerkennen [VB-Stellen] und
- IT-Sicherheitsdienstleister, die sich zertifizieren [VB-Stellen]

lassen wollen.

Spezielle Anforderungen für die jeweilige Personengruppe mit detaillierten Hinweisen zu Verfahrensabläufen befinden sich in den jeweiligen Programmen und richten sich an den konkreten Antragsteller.

Die vorliegende VB-Personen wird im Bereich der Personenzertifizierung durch die Dokumente

- [IT-GS-Berater],
- [IS-Revisor und IS-Berater] und
- [IS-Penetrationstester]

und im Bereich der Kompetenzfeststellung durch die Programme

- [CC-Evaluatoren]
- [TR-Prüfer] und
- [DigBOS-Prüfer]

ergänzt. Die Programme sind im folgenden beschrieben.

Das Dokument „Verzeichnisse“ [Verzeichnisse] gibt einen Überblick über alle benötigten Hilfs- und Informationsquellen (Literaturverzeichnis) und enthält ein Stichwort- und Abkürzungsverzeichnis (Glossar).

Das Dokument „Zeichenordnung“ [Zeichenordnung] enthält alle Zeichen der Konformitätsbewertung mit den jeweiligen Rechten und Bedingungen.

1.2 Nutzen der Zertifizierung für den Antragsteller

Eine Personenzertifizierung ist erforderlich, wenn eine Person im Rahmen eines BSI-Zertifizierungsverfahrens tätig sein möchte, bei einem vom BSI zertifizierten IT-Sicherheitsdienstleister beschäftigt ist oder für ein externes Programm (d.h. einer Managementsystem-TR, bei der die Zertifizierung nicht im BSI selbst stattfindet) arbeiten möchte.

Aber auch außerhalb dieser Bereiche haben zertifizierte Personen einen Nutzen von der Zertifizierung. Beispielsweise werden zertifizierte IT-Grundschutzberater regelmäßig bei Projekten im gesetzlich geregelten Bereich sowie in der freien Wirtschaft (z. B. zu Projekten mit Bezug zum Thema Informationssicherheit) herangezogen. Eine Zertifizierung dient dabei oft als Fachkundenachweis und erhöht die Reputation der Person bzw. des Unternehmens, bei dem die Person beschäftigt ist.

2 Kompetenzfeststellungs- und Zertifizierungsprogramme für Personen

Die Personenzertifizierungsstelle des BSI betreibt ein Zertifizierungssystem, in denen die Regeln (Programme, bedarfsgerechte Prüfkriterien, Anforderungen und Nachweise), das Verfahren sowie das Management zur Durchführung der Zertifizierung festgelegt und beschrieben sind.

Die Voraussetzungen für die Zertifizierung bzw. Kompetenzfeststellung sowie die Anforderungen an die verschiedenen Personengruppen sind in den jeweiligen Programmen detailliert beschrieben. Diesen Programmen ist auch zu entnehmen, ob im betreffenden Programm eine Personenzertifizierung erfolgt.

Das Verfahren wird auch zur Kompetenzfeststellung von Mitarbeitern genutzt, die bei anerkannten Prüfstellen beschäftigt sind. Es wird dabei jedoch im Rahmen des Verfahrens zur Anerkennung von Prüfstellen und Zertifizierung von IT-Sicherheitsdienstleistern durchgeführt und stellt keine eigenständige Personenzertifizierung dar.

2.1 Programme für die Zertifizierung von Personen

Folgende Zertifizierungen können beim BSI beantragt werden:

- Zertifizierung als IT-Grundschutz-Berater
für die Unterstützung bei der Einführung eines Informationssicherheitsmanagementsystemen (ISMS);
siehe Anforderungen in „**Personenzertifizierung: Programm IT-Grundschutz-Berater**“ [IT-GS-Berater].
- Zertifizierung als IS-Revisor und IS-Berater
für die Unterstützung von Bundesbehörden bei der Erstellung und Umsetzung von Sicherheitskonzepten sowie die regelmäßige Durchführung von IS-Revisionen gemäß „Leitfaden für die Informationssicherheitsrevision auf der Basis von IT-Grundschutz“;
siehe Anforderungen in „**Personenzertifizierung: Programm IS-Revisor und IS-Berater**“ [IS-Revisor und IS-Berater].
- Zertifizierung als IS-Penetrationstester
für die Unterstützung von Bundesbehörden bei der Durchführung von Penetrationstests;
siehe Anforderungen in „**Personenzertifizierung: Programm IS-Penetrationstester**“ [IS-Penetrationstester].

2.2 Programme für die Kompetenzfeststellung von Personen für die Anerkennung und Zertifizierung von Stellen

Eine Kompetenzfeststellung von Personen wird im Rahmen der Anerkennung von Stellen und Zertifizierung von IT-Sicherheitsdienstleistern [VB-Stellen] für folgende Personengruppen durchgeführt.

- CC-Evaluatoren
für die Durchführung von Evaluierungen für Zertifizierungsverfahren im Produktzertifizierungsprogramm der Common Criteria (CC);
siehe Anforderungen in „**Kompetenzfeststellung: Programm CC-Evaluatoren**“ [CC-Evaluatoren].
- TR-Prüfer
für die Durchführung von Konformitätsprüfungen für Zertifizierungsverfahren im Produktzertifizierungsprogramm Technische Richtlinie des BSI;
siehe Anforderungen in „**Kompetenzfeststellung: Programm TR-Prüfer**“ [TR-Prüfer].
- DigBOS-Prüfer
 - für die Durchführung von Interoperabilitätsprüfungen für Funkgeräte im Digitalfunk BOS,

- für die Durchführung von Interoperabilitätsprüfungen für Leitstellen im Digitalfunk BOS,
- für die Bereitstellung eines Zertifizierungsprüflabors für Interoperabilitätsprüfungen mit Wirknetzrelevanz für den Digitalfunk BOS (ZPL).

Siehe Anforderungen in „**Kompetenzfeststellung: Programm DigBOS-Prüfer**“ [DigBOS-Prüfer].

3 Verfahren zur Kompetenzfeststellung und Zertifizierung

3.1 Antragsphase

Das Zertifizierungsverfahren beginnt in der Antragsphase mit der Antragsstellung und -prüfung für das betreffende Programm.

Die gestellten Anträge zur Zertifizierung von Personen werden in der Reihenfolge des Eingangsdatums beim BSI bearbeitet. Hiervon kann abgewichen werden, wenn das BSI wegen der Zahl und des Umfangs anhängiger Prüfungsverfahren eine Prüfung in angemessener Zeit nicht durchführen kann und an der Erteilung eines Zertifikats ein öffentliches Interesse besteht.

Der Antragsteller muss dem ausgefüllten und unterzeichneten Antrag sämtliche geforderten externen Fachkundenachweise zur Begutachtung der Zulassungsvoraussetzungen gemäß dem entsprechenden Programm beifügen, bevor der Antrag bearbeitet werden kann. Unvollständige Anträge können nicht bearbeitet werden (siehe Ablehnung eines Antrags in Kapitel 5.4.4 „Ablehnung eines Antrags“).

Zur Vorbereitung einer Kompetenzfeststellung im Rahmen der Anerkennung von Prüfstellen und Zertifizierung von IT-Sicherheitsdienstleistern müssen sämtliche geforderten externen Fachkundenachweise zur Begutachtung der Zulassungsvoraussetzungen gemäß dem entsprechenden Programm vorgelegt werden.

Das BSI begutachtet, ob vorgelegte externe Fachkundenachweise den Anforderungen entsprechen. Das BSI behält sich vor, die dort gemachten Angaben zu überprüfen. Bei Fragen oder Zweifeln wird der Antragsteller unterrichtet und aufgefordert, ergänzende oder ggf. weitere Nachweise zu erbringen.

Sollten nicht zutreffende Angaben in diesen Nachweisen offenbar werden, könnten Zweifel an der Vertrauenswürdigkeit des Antragstellers entstehen. Diese könnten einer Zertifizierung entgegenstehen.

Nach positiver Begutachtung der Mindest- bzw. Zulassungsvoraussetzungen, d. h. alle externen Fachkundenachweise sind fristgerecht eingegangen, vollständig und positiv begutachtet, wird der Antragsteller zur Kompetenzfeststellung bzw. zum Zertifizierungsverfahren zugelassen. Der Antragsteller wird entsprechend dem Programm zur Teilnahme an einer Prüfung eingeladen oder es wird ein Termin zur Fachbegutachtung vereinbart.

3.2 Prüfphase - Kompetenzfeststellung

In der Prüfphase erfolgt eine Kompetenzfeststellung. Sie dient bei einer Zertifizierung der Vorbereitung der Zertifizierungsentscheidung.

In der Prüfphase werden alle Anforderungen an die Person in einer Prüfung oder Fachbegutachtung überprüft. Hierbei wird sich auf die Fragen beschränkt, die sich speziell auf die Anforderungen des Programms beziehen.

Die Prüfungsbedingungen werden dem Antragsteller vor Beginn der Prüfung vorgelegt und sind von diesem durch Unterschrift anzuerkennen. Zur Prüfung zieht das BSI gegebenenfalls (externe) Experten hinzu. Die Prüfung bzw. Fachbegutachtung kann nur einmalig wiederholt werden.

Der Antrag auf Zertifizierung wird u. a. abgelehnt, wenn

- der Antragsteller die Anforderungen nicht erfüllt, d. h. die Prüfung oder Fachbegutachtung nicht bestanden wird.

- einem Antragsteller im Rahmen einer Prüfung oder Fachbegutachtung ein Täuschungsversuch nachgewiesen wird. Die Vertrauenswürdigkeit des Antragstellers ist dann nicht mehr gegeben und eine Kompetenzfeststellung bzw. Zertifizierung nicht mehr möglich.

3.2.1 Fachkundenachweis durch eine Prüfung

Der jeweilige Aufbau der Prüfung ist dem Programm zu entnehmen.

Die Prüfungsauswertung erfolgt durch die Personenzertifizierungsstelle des BSI. Das Prüfungsergebnis wird den Prüflingen schriftlich oder elektronisch mitgeteilt.

Sollte der Antragsteller seine Teilnahme an einer Prüfung absagen, so wird er zum nächsten Termin eingeladen. Sollte auch eine dritte Einladung ohne triftigen Grund (z. B. Krankheit) abgesagt werden, so wird das Verfahren beendet.

3.2.2 Fachkundenachweis durch eine Fachbegutachtung

Die jeweiligen Anforderungen an den Antragsteller, die in der Fachbegutachtung durch die Begutachter bewertet werden sowie der Aufbau der Fachbegutachtung, sind den entsprechenden Programmen zu entnehmen.

3.3 Zertifizierungsphase

Nach Abschluss der Prüfphase entscheidet der Leiter der Personenzertifizierungsstelle auf Grundlage des Begutachtungsergebnisses gemäß den Regelungen des § 9 Abs. 4 Nr. 2 BSIG, ob die Zertifizierung für das beantragte Programm erteilt wird.

Nach positiver Zertifizierungsentscheidung erstellt die Personenzertifizierungsstelle des BSI einen Zertifizierungsbescheid und eine Zertifikatsurkunde.

Der Antragsteller erhält den Status einer beim BSI zertifizierten Person für das betreffende Programm befristet, in der Regel für die Dauer von 3 Jahren.

Nach erfolgter Zertifizierungsentscheidung werden die angefallenen Gebühren und Auslagen in Rechnung gestellt.

4 Aufrechterhaltung und Überwachung der Zertifizierung

Während der Laufzeit der Zertifizierung wird mindestens einmal geprüft, ob die Voraussetzungen für die Zertifizierung weiterhin vorliegen. In den jeweiligen Programmen ist die Überprüfung der Kompetenz während der Zertifizierung beschrieben.

Falls notwendig, können anlassbezogene Begutachtungen gemäß Kapitel 5.5.1 „Bestimmungen zur Aufrechterhaltung“ durchgeführt werden.

Zudem muss die zertifizierte Person die Nebenbestimmungen einhalten und bestimmte Tätigkeiten gemäß den Anforderungen (siehe Kapitel 4.1 „Durchführung der (Prüf-)Tätigkeiten im betreffenden Programm“) durchführen.

4.1 Durchführung der (Prüf-)Tätigkeiten im betreffenden Programm

Die Anforderungen an die Durchführung der (Prüf-)Tätigkeiten der Personengruppe sind in den entsprechenden Programmen (jeweils in Kapitel 4.1) beschrieben.

Bei Nichteinhaltung der Anforderungen aus den Programmen und insbesondere der Regelungen aus diesem Abschnitt kann die Zertifizierung aufgehoben werden.

4.2 Überwachung der Kompetenz bzw. Zertifizierung

Die Überwachung der Personen ist in den jeweiligen Programmen beschrieben. Insbesondere wird im Rahmen von Zertifizierungsverfahren die fachliche Kompetenz der Personen im Rahmen der Prüfbegleitung überwacht und eine Vor-Ort-Begutachtung durchgeführt.

4.3 Anlassbezogene Begutachtungen

Anlassbezogene Begutachtungen können stattfinden, insbesondere wenn

1. begründete Zweifel an der Kompetenz der Person bestehen;
2. wiederholt gegen die Verfahrensbeschreibungen oder Programme verstoßen wird;
3. Verfahrensänderungen seitens des BSI u. a. aufgrund von Vorschriften, internationalen Vereinbarungen oder eines Kriterienwechsels notwendig werden;
4. von dritter Stelle Informationen über Unregelmäßigkeiten an die Personenzertifizierungsstelle des BSI herangetragen werden.

4.4 Rezertifizierung

Ein Antrag auf Rezertifizierung kann frühestens 6 Monate vor Ablauf der Zertifizierung gestellt werden, muss aber 6 Wochen vor Ablauf der Zertifizierung beim BSI eingegangen sein., damit die Zertifizierung lückenlos fortgesetzt werden kann.

Der Antragsteller muss dem ausgefüllten und unterzeichneten Antrag sämtliche geforderten externen Fachkundenachweise zur Begutachtung der Zulassungsvoraussetzungen gemäß dem entsprechenden Programm beifügen, bevor der Antrag bearbeitet werden kann. Unvollständige Anträge können nicht

bearbeitet werden. Sollten die externen Fachkundenachweise zum Zeitpunkt des Ablaufs der Gültigkeit der Zertifizierung nicht vollständig vorliegen, wird der Antrag abgelehnt.

Die Personenzertifizierungsstelle des BSI prüft, ob der Antragsteller Tätigkeitsnachweise in ausreichendem Umfang erbracht hat. Tätigkeitsnachweise können nur berücksichtigt werden, wenn sie zeitlich in den laufenden Zertifizierungszeitraum fallen.

Die Person muss nachweisen, dass sie sich ständig fachlich weitergebildet hat und Änderungen der Praxis, einschlägiger Normen und anderer Anforderungen berücksichtigt. Dabei steht die Aufrechterhaltung der Fähigkeiten im Vordergrund, Tätigkeiten im entsprechenden Programm auf Grundlage des aktuellen Standes der Technik und der zugrunde liegenden Richtlinien durchzuführen.

5 Rahmenbedingungen

5.1 Grundlage für die Zertifizierung

Das Verfahren wird nach der „Verordnung über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen durch das Bundesamt für Sicherheit in der Informationstechnik“ [BSI-ZertV], dieser Verfahrensbeschreibung mit den zugehörigen Programmen sowie dem Verwaltungsverfahrensgesetz (VwVfG) durchgeführt.

5.2 Genereller Dokumentenaustausch mit der Personenzertifizierungsstelle

Die elektronische Kommunikation mit der Personenzertifizierungsstelle des BSI erfolgt grundsätzlich über das Postfach auditor@bsi.bund.de und verschlüsselt. Der entsprechende Schlüssel ist auf der Webseite des BSI erhältlich.

5.3 Optionale Schulungsmaßnahmen

Das BSI bietet zu einigen Programmen Schulungsmaßnahmen an. Der jeweilige Inhalt der Schulung ist dem jeweiligen Programm zu entnehmen.

5.4 Rahmenbedingungen zum Verfahren

5.4.1 Obliegenheiten des Antragstellers

Dem Antragsteller obliegt es:

- die notwendigen Nachweise zur Ermittlung des Sachverhalts beizubringen.
Bei fehlenden oder unzureichenden Nachweisen kann ein Verfahren durch die Personenzertifizierungsstelle mit negativem Ergebnis beendet werden.
- im Rahmen seiner Mitwirkungsobliegenheiten die notwendige Mitwirkung etwaiger Dritter sicherzustellen.
- dem Begutachtertteam des BSI oder den vom Bundesamt beauftragten Personen in erforderlichem Umfang kostenfrei Zugang zur Überwachung der Tätigkeiten sowie zu den notwendigen, vom BSI festgelegten Nachweisen zu gewähren.

Ein Zertifizierungsantrag kann negativ beschieden werden, wenn die Nicht-Erfüllung der Obliegenheiten einer sachgerechten Bearbeitung des Verfahrens erheblich entgegenstehen.

5.4.2 Rücknahme eines Antrags

Zu jedem Zeitpunkt im Verfahren kann der Antragsteller den Antrag auf Zertifizierung zurückziehen. In diesem Fall ist das Verfahren erledigt.

Seitens des BSI werden die angefallenen Kosten und Auslagen nach der Besonderen Gebührenverordnung des Bundesministeriums des Innern, für Bau und Heimat für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich [BMIBGebV] erhoben.

5.4.3 Änderungen des Antrags

Ein Antrag kann bis zur Entscheidung über den Zertifizierungsantrag (Entscheidung im Widerspruchs- oder Klageverfahren) abgeändert werden, soweit die Änderung nicht wesentlich ist.

Eine wesentliche Änderung wird behandelt, als wäre der ursprüngliche Antrag zurückgenommen und ein neuer Antrag gestellt worden.

Kostenrechtlich hat sich der ursprüngliche Antrag damit erledigt und wird nach der Besonderen Gebührenverordnung des Bundesministeriums des Innern, für Bau und Heimat für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich [BMIBGebV] behandelt.

5.4.4 Ablehnung eines Antrags

Das BSI kann einen Antrag bei nicht Vorliegen der im BSIG § 9 genannten Voraussetzungen ablehnen sowie wenn

- ein unvollständig eingereichter Antrag nicht innerhalb von 6 Wochen vervollständigt wird oder
- der Antragsteller über einen Zeitraum von mehr als 6 Wochen entgegen der vereinbarten Planung keine Unterlagen liefert, die eine Prüfung durch die Personenzertifizierungsstelle ermöglichen

Der Hinweis auf fehlende Unterlagen wird mit der Anhörung nach § 28 VwVfG verbunden.

5.5 Rahmenbedingungen zur Aufrechterhaltung der Zertifizierung

5.5.1 Bestimmungen zur Aufrechterhaltung

Zur Aufrechterhaltung der Zertifizierung muss die Person die [VB-Personen] sowie mögliche im Bescheid enthaltene Nebenbestimmungen einhalten.

Im Rahmen der Festlegungen der [VB-Personen] kann insbesondere bestimmt werden, dass:

- die Person bei der Nutzung der Zertifizierung, insbesondere bei der Verwendung zu Werbezwecken, Vorlage und Nachweisführung, auf den Zertifizierungsbescheid und das Zertifikat hinweisen und diese Dokumente zur Verfügung stellen muss.
- die Person einmalig für die Dauer der Zertifizierung Überwachungsbegutachtungen zur Aufrechterhaltung der Zertifizierung zulassen muss. Die Gebühren und Auslagen sind von der Person zu tragen.
- die Person regelmäßige oder anlassbezogen Überwachungsbegutachtungen (siehe Kapitel 4.3) zulassen muss. Die Gebühren und Auslagen sind von der Person zu tragen.
- die Person dem BSI unverzüglich schriftlich mitteilen muss, wenn sich seine Arbeitsweise (in Bezug auf die Einhaltung der Anforderungen) ändert.
- die Person an vom BSI angebotenen Arbeitstreffen zum Programm teilnehmen muss:
Das BSI stellt durch diese Treffen und Workshops eine kontinuierliche Zusammenarbeit mit den Personen und ggf. der Managementsystem- bzw. den Produktzertifizierungsstellen sicher.

Sofern Nebenbestimmungen im Bescheid angeordnet sind, muss der Antragsteller diese beachten. Sie sind somit zur Aufrechterhaltung verpflichtend einzuhalten.

5.5.2 Regelungen zur Vertraulichkeit

Der Antragsteller gewährleistet die streng vertrauliche Behandlung der Interna von Verfahren und Projekten. Er wird Beschäftigten und Dritten Informationen nur geben, soweit ihre Kenntnis notwendig ist („Kenntnis-nur-wenn-nötig-Prinzip“).

Die zertifizierte Person wahrt Verschwiegenheit über Betriebsgeheimnisse Dritter sowie über alle Informationen, die ihr im Zusammenhang mit dem Zertifizierungsverfahren und im Rahmen einer späteren Tätigkeit als zertifizierte Person bekannt werden (Informationen, Daten, Gesprächsinhalte und sonstige Sachverhalte, etc.) und der hieraus gewonnenen vertraulichen Erkenntnisse. Eine Weitergabe an Dritte, Aufzeichnung oder sonstige Verwendung darf nur zur Durchführung des Verfahrens im betreffenden Programm oder mit Zustimmung des BSI erfolgen. Gesetzliche Verpflichtungen bleiben unberührt.

Die Nutzung der im Zusammenhang mit der Zertifizierung erworbenen Informationen ist auf den mit der Zertifizierung verfolgten Zweck beschränkt.

5.5.3 Regelungen zur Archivierung von Dokumenten und Aufzeichnungen

Der Antragsteller stellt sicher, dass alle Dokumente und Aufzeichnungen zu den Tätigkeiten im jeweiligen Programm der Zertifizierung 3 Jahre nach Ablauf der Zertifizierung für Rückfragen des BSI vorgehalten werden.

Nach Auslaufen eines Programms wird die weitere Archivierung dieser Dokumente und Aufzeichnungen mit dem BSI vereinbart.

5.6 Aufhebung einer Zertifizierung

Zur Aufhebung einer Zertifizierung werden die Regelungen des Verwaltungsverfahrensgesetzes [VwVfG] berücksichtigt.

5.6.1 Widerruf einer rechtmäßigen Zertifizierung

Ein Widerruf einer rechtmäßigen Zertifizierung kann aufgrund nachträglich eingetretener Tatsachen bzgl. der zugrundeliegenden Sach- und Rechtslage erfolgen (siehe hierzu § 49 [VwVfG]).

Gründe, die zu einem Widerruf einer Zertifizierung führen können, sind beispielsweise, wenn der Antragsteller:

- im Bescheid enthaltene Nebenbestimmungen nicht beachtet (siehe Kapitel 5.5.1 „Bestimmungen zur Aufrechterhaltung“.
- Änderungen dieser Verfahrensbeschreibung oder den jeweils gültigen Anforderungen aus den Programmen widerspricht.
- gegen Anforderungen aus den jeweils gültigen Verfahrensbeschreibungen oder Programmen verstößt: Dies kann beispielsweise der Fall sein, wenn sowohl beim Verfahren zur Zertifizierung als Person als auch bei einem konkreten Zertifizierungsverfahren es in der Zusammenarbeit zwischen dem BSI und der zertifizierten Person aufgrund von Nichteinhaltung von Anforderungen, Vorgaben und Terminen bzw. von mangelhaften Prüftätigkeiten einer zertifizierten Person zu erheblichen Problemen kommt.
- Vertraulichkeits- oder Sicherheitsvorschriften verletzt (siehe Kapitel 5.5.2 „Regelungen zur Vertraulichkeit“.
- Zertifikate oder Zertifizierungszeichen missbräuchlich verwendet.

5.6.2 Rücknahme einer rechtswidrigen Zertifizierung

Eine rechtswidrige Zertifizierung kann ganz oder teilweise zurückgenommen werden (siehe hierzu § 48 [VwVfG]), beispielsweise, wenn:

- bewusst falsche Angaben zu den Zertifizierungsvoraussetzungen gemacht wurden.
- für die Zertifizierungsentscheidung bewusst wesentliche Informationen verschwiegen wurden (vgl. § 48 [VwVfG]).

5.6.3 Folgen der Aufhebung

Wird eine Zertifizierung für ein oder alle Programme unanfechtbar aufgehoben oder ist die Gültigkeit der Zertifizierung aus einem anderen Grund nicht oder nicht mehr gegeben, so kann das Zertifikat, das zum Nachweis der Zertifizierung für das betreffende Programm bestimmt ist, nach § 52 VwVfG zurückgefordert werden.

Der Antragsteller ist zur Herausgabe verpflichtet. Er kann jedoch verlangen, dass ihm die Zertifikate wieder ausgehändigt werden, nachdem sie durch das BSI als ungültig gekennzeichnet wurden.

Die Person wird nicht mehr auf der öffentlichen Liste der zertifizierte Personen für die entsprechenden Programme gelistet und die Kontaktdaten werden entfernt.

5.7 Beschwerde- und Verbesserungsmanagement

Die Personenzertifizierungsstelle verfügt über ein Verfahren, um Beschwerden und Verbesserungsvorschläge entgegenzunehmen, zu evaluieren, sowie Entscheidungen über diese zu treffen. Das Verfahren ist auf der [Webseite des BSI](#) veröffentlicht. Der Erhalt der Beschwerde wird bestätigt. Der Beschwerdeführer wird, sofern möglich, über das Ergebnis und den Abschluss des Verfahrens informiert.

Auch ein Fragebogen zur Kundenzufriedenheit ist an dieser Stelle zu finden.

Es wird in der Konformitätsbewertung ein Beschwerde- und Verbesserungsmanagement gelebt. Dabei fließt jegliche Anregung ein.

Auslöser für den Verbesserungsprozess sind unter anderem:

- Beschwerden und fehlerhafte Arbeitsergebnisse,
- Ergebnisse aus der Ermittlung der Kundenzufriedenheit sowie
- Verbesserungsvorschläge und festgestellte Abweichungen.

5.8 Haftung

Das Bundesamt haftet ausschließlich nach Art. 34 GG i. V. m. § 839 BGB.

5.9 Kosten

Die Kosten des Zertifizierungsverfahrens richten sich nach der Besonderen Gebührenverordnung des Bundesministeriums des Innern, für Bau und Heimat für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich [BMIBGebV]. Ein Informationsgespräch mit dem BSI vor Antragstellung ist kostenfrei.

Die Kosten des Erstzertifizierungsverfahrens setzen sich aus den Gebühren für den tatsächlich angefallenen Zeitaufwand und den entstandenen Auslagen zusammen. Erst nach Eingang des vollständigen Zahlungsbetrages erfolgt eine Veröffentlichung auf den Webseiten des BSI.

Falls eine Vor-Ort-Überwachung erforderlich ist, fallen weitere Gebühren (884 €) sowie zu erstattende Auslagen an.

Die Kosten des Rezertifizierungsverfahrens bestehen aus einer Festgebühr in Höhe von 205 € und den entstandenen Auslagen.

Zusätzliche Unterstützungshandlungen des BSI werden nach Aufwand abgerechnet.

Im Falle eines negativen Ergebnis des Verfahrens oder einer Aufhebung der Zertifizierung sind auch die hierfür entstandenen Kosten zu erstatten.

6 Veröffentlichung der Zertifizierung

Grundsätzlich wird nach Erteilung der Zertifizierung der Name der Person mit Zertifizierungsnummer und Kontaktdaten (Anschrift, Webadresse) sowie die Programme mit dem Gültigkeitszeitraum im Internet und in der Publikation <KES> veröffentlicht.

Der Inhaber eines Zertifikats kann der Veröffentlichung widersprechen.

Das BSI sieht von einer Veröffentlichung ab, soweit durch die Veröffentlichung die öffentliche Sicherheit beeinträchtigt werden könnte. Zudem kann das BSI von der Veröffentlichung ganz oder teilweise absehen, wenn durch die Veröffentlichung öffentliche oder private Interessen beeinträchtigt würden.

6.1 Zertifizierungsnummer

Alle vom BSI zertifizierten Personen erhalten eine Registrierungsnummer. Diese Nummer ist wie folgt aufgebaut:

„BSI-ABCD-XXXX-JJJJ“

Diese Zeichenkette *Zertifizierungsstelle-Vorgangskennung-fortlaufende Vorgangsnummer-Jahr* dient als Bezug für die BSI-internen Vorgänge, den Schriftwechsel und die Kennzeichnung von Dokumenten (im Rahmen des Verfahrens).

Personengruppe	Zertifizierungsnummer
Auditteamleiter	BSI-ZIG-XXXX-JJJJ
Auditor „De-Mail“	BSI-ZADE-XXXX-JJJJ
Auditor „Secure CA Operation“	BSI-ZACA-XXXX-JJJJ
Auditor „Sicherer E-Mail Transport“	BSI-ZAMT-XXXX-JJJJ
Auditor „Smart Meter Gateway Administration“	BSI-ZASM-XXXX-JJJJ
Auditor RESISCAN	BSI-ZARS-XXXX-JJJJ
IT-GS-Berater	BSI-ZGB-XXXX-JJJJ
IS-Revisor	BSI-ZISR-XXXX-JJJJ.
IS-Penetrationstester	BSI-ZPT-XXXX-JJJJ

Tabelle 1: Zertifizierungsnummern der Personengruppen

7 Referenzen und Glossar

Die Aufschlüsselung der referenzierten Dokumente und das Glossar befindet sich im Dokument „Verzeichnisse“ [Verzeichnisse].