Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Verfahrensbeschreibung zur Anerkennung von Prüfstellen

VB-Prüfstellen

Version 5.0 vom 01.11.2024

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 (0)800 274 1000
E-Mail: service-center@bsi.bund.de
Internet: https://www.bsi.bund.de

Änderungshistorie

Version	*Datum*	*Name/Org-Einheit*	*Beschreibung*
1.0	09.07.2009	Anerkennung S 25	Erstausgabe
2.0	06.08.2010	Anerkennung S 25	Neuausgabe
3.0	20.07.2015	Anerkennung S 25	Neuausgabe nach Umgestaltung der Dokumentenstruktur
3.1 - 3.9	02.08.2016 bis 30.09.2021	QMB SZ	9 Revisionen
4.0	28.02.2022	QMB SZ	Neuausgabe unter Berücksichtigung des geschlechtergerechten Sprachgebrauchs: • Austausch der Abbildung 1: Dokumentenübersicht (Zertifizierungs- und Anerkennungsprogramm). • Neuer Geltungsbereich „Anerkennung von Prüfstellen: Programm im Network Equipment Security Assurance Scheme (NESAS)“ in den Kapiteln 1.1 „Zielsetzung und Eingliederung der VB-Stellen“ und 2.1.5 „Programm für die Anerkennung: Network Equipment Security Assurance Scheme (NESAS)“ ergänzt. • Präzisierung der Archivierungsregelung in Kapitel 5.4.5 „Regelungen zur Archivierung von Dokumenten, Aufzeichnungen und Testobjekten“. • Neues Kapitel 4.1.1 „Qualitätssicherung bei Prüftätigkeiten in einer Prüfstelle“ eingefügt. • Umbenennung des Programms [VB-Produkte] in [VB-Produkte.PD].
4.1	01.08.2023	QMB SZ	Revision: • Entfernen der Abbildung 1: Dokumentenübersicht (Zertifizierungs- und Anerkennungsprogramm) in Kapitel 1.1 und entsprechende Anpassung im Kapitel. • Ergänzung und Anpassung aufgrund des neuen Zertifizierungssystems PZS-TR in Kapitel 2 „Anerkennungs- und Zertifizierungsprogramme für Stellen“. • Konkretisierungen in Kapitel 3 „Verfahren zur Anerkennung bzw. Zertifizierung“: Für die Ausübung der Tätigkeiten im jeweiligen Programm müssen die benannten Mitarbeitenden fest angestellt sein. Ein Evaluator darf in Zertifizierungsverfahren nur dann eigenverantwortlich eingesetzt werden, wenn das BSI die Kompetenz des Evaluators festgestellt hat. • Konkretisierung in Kapitel 3.2.3 „Anerkennungs- und Zertifizierungsphase“ zum Widerspruch. • Kapitel 5.2 „Genereller Dokumentenaustausch mit der Anerkennungsstelle“ erfolgt mit GPG statt Chiasmus. • Konkretisierung in Kapitel 5.3.4 „Ablehnung eines Antrags“ bzgl. §§ 5 Abs. 2,6 BSI-Zertifizierungs- und Anerkennungsverordnung [BSI-ZertV]. • Umbenennung Kapitel 5.7 „Beschwerde- und Verbesserungsmanagement“ in „Beschwerde-, Verbesserungs- und Qualitätsmanagement“. • Überarbeitung der Literaturangaben und der Zitate der Rechtsnormen. • Redaktionelle und strukturelle Anpassungen.

Version	*Datum*	*Name/Org-Einheit*	*Beschreibung*
5.0	01.11.2024	Anerkennung S 21	Neuausgabe der VB-Prüfstellen 5.0 aus der VB-Stellen • Reduzierung der VB-Stellen auf VB-Prüfstellen (ohne Sicherheitsdienstleister, mit Ausnahme von DigBOS- und Lauschabwehr-Stellen) • Prüfer/Evaluatoren dürfen grundsätzlich nicht zeitgleich für mehrere Stellen tätig sein, um eine klare Arbeitsplatzzuordnung und die Unparteilichkeit sicherzustellen • Bei Erstanträgen ist der original unterschriebene Antrag postalisch ans BSI zu übermitteln. Bei Reanerkennungen reicht eine digitale Unterschrift • Die Anerkennung von ITSEC-Laboren entfällt • Bei den Fristen wird klar zum Ausdruck gebracht, dass nach 2 Begutachtungszyklen/Prüfungen der Antrag abgelehnt wird. • Mentorenkonzept der Evaluatoren/Prüfer wird näher erläutert

Tabelle 1: Änderungshistorie

Inhalt

1 Einleitung 7
1.1 Zielsetzung und Eingliederung der VB-Prüfstellen 7
1.2 Nutzen der Anerkennung für die antragstellende Organisation 8
1.2.1 Nutzen der Anerkennung als Prüfstelle 8
2 Anerkennungsprogramme für Prüfstellen 9
2.1 Programme für die Anerkennung von Prüfstellen 9
2.1.1 Programm für die Anerkennung: Common Criteria (CC) 9
2.1.2 Programm für die Anerkennung: Beschleunigte Sicherheitszertifizierung (BSZ) 9
2.1.3 Programm für die Anerkennung Technische Richtlinien (TR) 9
2.1.4 Programm für die Anerkennung: Network Equipment Security Assurance Scheme (NESAS) 10
3 Verfahren zur Anerkennung 11
3.1 Beteiligte Stellen im BSI 11
Die Anerkennungsstelle im BSI 11
Die Produktzertifizierungsstellen im BSI 11
3.2 Phasen zur Anerkennung 12
3.2.1 Vorbereitungs- und Antragsphase 12
3.2.2 Begutachtungsphase 13
3.2.3 Anerkennungsphase 16
4 Aufrechterhaltung und Überwachung der Anerkennung 17
4.1 Durchführung der (Prüf-)Tätigkeiten im betreffenden Programm 17
4.1.1 Qualitätssicherung bei Prüftätigkeiten in einer Prüfstelle 17
4.2 Überwachung der Anerkennung 18
4.2.1 Begutachtungen zur Systemförderung 18
4.2.2 Fachbegutachtungen 18
4.3 Anlassbezogene Begutachtungen 18
5 Rahmenbedingungen 19
5.1 Grundlage für die Anerkennung 19
5.2 Genereller Dokumentenaustausch mit der Anerkennungsstelle 19
5.3 Rahmenbedingungen zum Verfahren 19
5.3.1 Obliegenheiten der antragstellenden Organisation 19
5.3.2 Rücknahme eines Antrages 19
5.3.3 Änderungen des Antrages 19
5.3.4 Ablehnung eines Antrages 20
5.4 Rahmenbedingungen zur Aufrechterhaltung der Anerkennung 20
5.4.1 Bestimmungen zur Aufrechterhaltung 20
5.4.2 Regelungen zur Unterbeauftragung 21

5.4.3 Regelungen zur Vertraulichkeit 21
5.4.4 Vorkehrungen zum Schutz von Verschlusssachen 22
5.4.5 Regelungen zur Archivierung von Dokumenten, Aufzeichnungen und Testobjekten 22
5.5 Erweiterung der Anerkennung 23
5.6 Nachmeldung weitere Prüfer bzw. Evaluatoren 23
5.6.1 Aufhebung einer Anerkennung 24
5.6.2 Widerruf einer rechtmäßigen Anerkennung 24
5.6.3 Rücknahme einer rechtswidrigen Anerkennung 24
5.6.4 Folgen der Aufhebung 24
5.7 Beschwerde-, Verbesserungs- und Qualitätsmanagement 25
5.8 Haftung 25
5.9 Kosten 25
6 Veröffentlichung der Anerkennung 26
6.1 Anerkennungsnummer 26
6.2 Anerkennungszeichen 26
6.3 Urkundenübergabe und Presseerklärung 26
7 Referenzen und Glossar [Verzeichnisse] 27

1 Einleitung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat nach dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) [BSIG] die Aufgabe, Zertifizierungen informationstechnischer Produkte oder Komponenten sowie informationstechnischer Systeme durchzuführen. Die Prüfungen für diese Zertifizierungen führen vom BSI anerkannte Prüfstellen durch.

Um diese Aufgaben zu erfüllen, betreibt das BSI ein Anerkennungssystem, 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 Anerkennung von Stellen festgelegt und beschrieben.

Eine Anerkennung als Prüfstelle wird auf Antrag einer Betreiberin bzw. Betreibers einer Organisation durchgeführt. Grundvoraussetzung für eine Anerkennung als Prüfstelle ist die Erfüllung der Anforderungen der Norm DIN EN ISO/IEC 17025 [17025] in seiner jeweils gültigen Fassung sowie dieser Verfahrensbeschreibung mit den zugehörigen Programmen.

In bestimmten Geltungsbereichen (z.B. DigBOS und Lauschabwehr) zertifiziert das BSI auch IT-Sicherheitsdienstleister für Prüftätigkeiten, die sehr ähnlich der Anerkennung einer Prüfstelle sind. Diese Zertifizierungsverfahren werden in Anlehnung an diese Verfahrensbeschreibung [VB-Prüfstellen] durchgeführt, wobei der Begriff „Anerkennung“ dann als „Zertifizierung“ zu verstehen ist.

1.1 Zielsetzung und Eingliederung der VB-Prüfstellen

In dieser Verfahrensbeschreibung [VB-Prüfstellen] werden der Nutzen für die antragstellende Organisation, das Verfahren zur Anerkennung von Prüfstellen und die damit verbundenen Rechte und Pflichten sowie Obliegenheiten dargestellt. Sie ist Entscheidungshilfe, wenn die Absicht besteht, einen Antrag zu stellen und richtet sich an Organisationen, die sich formal als Prüfstelle anerkennen lassen möchten.

Spezielle Anforderungen für die jeweilige Anerkennung mit detaillierten Hinweisen zu Verfahrensabläufen befinden sich in den jeweiligen Programmen.

Die vorliegende VB-Prüfstellen beschreibt das Anerkennungssystem für die folgenden Programme:

- Anerkennung von Prüfstellen: Programm im Bereich Common Criteria, [**CC-Prüfstellen**],
- Anerkennung von Prüfstellen: Programm im Bereich Beschleunigte Sicherheitszertifizierung (BSZ) [**BSZ-Prüfstellen**],
- Anerkennung von Prüfstellen: Programm im Bereich Technischer Richtlinien, [**TR-Prüfstellen**],
- Anerkennung von Prüfstellen: Programm im Network Equipment Security Assurance Scheme (NESAS) [**NESAS-Prüfstellen**],
- Zertifizierung von IT-Sicherheitsdienstleistern: Programm im Bereich Lauschabwehr [**Lauschabwehr**] und Programm im Bereich Digitalfunk BOS [**DigBOS**].

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

Einen Überblick über alle benötigten Anforderungen, Quellen und Hilfsmittel gibt das Dokument „Verzeichnisse als Nachschlagewerk für Interessenten und Beteiligte an Zertifizierungs- und Anerkennungsverfahren“ [**Verzeichnisse**]. Es enthält zudem ein Glossar- und Abkürzungsverzeichnis.

1.2 Nutzen der Anerkennung für die antragstellende Organisation

1.2.1 Nutzen der Anerkennung als Prüfstelle

Zur Durchführung einer Produktzertifizierung benötigen Herstellerorganisationen eine Prüfstelle, die die Evaluierung des zu zertifizierenden Produktes durchführt. Die Prüfstelle wird von der Herstellerorganisation ausgewählt und (in der Regel kostenpflichtig) beauftragt. Eine Prüfstelle kann grundsätzlich nur dann als sachverständige Stelle für die Produktzertifizierungsstellen des BSI Evaluierungen durchführen, wenn sie durch das BSI als sachverständige Stelle für das jeweilige Programm formal anerkannt wurde.

Anerkannte Prüfstellen haben die Möglichkeit, aktiv an der Stärkung der Sicherheit von nationalen und internationalen IT-Produkten mitzuwirken und sind berechtigt, Evaluierungen im Rahmen von Produktzertifizierungen des BSI durchzuführen.

2 Anerkennungsprogramme für Prüfstellen

Die Anerkennungsstelle des BSI betreibt ein Anerkennungssystem und die folgenden Anerkennungsprogramme, in denen die speziellen Anforderungen für die jeweilige Anerkennung mit detaillierten Hinweisen zu Verfahrensabläufen festgelegt sind.

Die Anerkennung einer Prüfstelle für ein bestimmtes Programm setzt ein Verständnis der entsprechenden Produktzertifizierung und somit die Kenntnis des Dokuments „Verfahrensbeschreibung zur Zertifizierung von Produkten“ [VB-Produkte.PD] mit einem entsprechenden Programmen [CC-Produkte], [BSZ-Produkte] oder [NESAS-Produkte] voraus. Das Zertifizierungssystem für Technische Richtlinien ist im Dokument [PZS-TR] und den dazugehörigen Programmen beschrieben. In diesen Dokumenten ist der Ablauf der Zertifizierung beim BSI im Ganzen dargestellt. Aus diesem Grund wird das Zertifizierungsverfahren für Produkte im vorliegenden Dokument VB-Prüfstellen nicht noch einmal beschrieben.

2.1 Programme für die Anerkennung von Prüfstellen

Im Folgenden sind alle Programme für die Anerkennung von Prüfstellen mit den zugehörigen Dokumenten aufgeführt. Die Zertifizierung von IT-Sicherheitsdienstleistern im Bereich Lauschabwehr [**Lauschabwehr**] und im Bereich Digitalfunk BOS [**DigBOS**] erfolgt analog der Verfahren zur Anerkennung als Prüfstelle.

2.1.1 Programm für die Anerkennung: Common Criteria (CC)

- Anerkennung als Prüfstelle im Bereich Common Criteria (CC);
  siehe Anforderungen in „Anerkennung von Prüfstellen: Programm im Bereich Common Criteria“ [CC-Prüfstellen].

  1. Anerkennung als Prüfstelle im Bereich „Smartcards and Similar Devices”;
     siehe Anforderungen in „Anerkennung von Prüfstellen: Programm im Bereich Common Criteria“ [CC-Prüfstellen].
  2. Anerkennung als Prüfstelle im Bereich „Hardware Devices with Security Boxes“;
     siehe Anforderungen in „Anerkennung von Prüfstellen: Programm im Bereich Common Criteria“ [CC-Prüfstellen].

Hinweis: Anerkennungen im Bereich Common Criteria gelten nur für die nationale CC-Zertifizierung, die am 31.01.2026 ausläuft und können daher nur noch bis zum 31.01.2026 erteilt werden. Für die Arbeit im Rahmen der europäischen CC-Zertifizierung ist eine Befugniserteilung gem. [VB-Befugnis] notwendig.

2.1.2 Programm für die Anerkennung: Beschleunigte Sicherheitszertifizierung (BSZ)

- Anerkennung als Prüfstelle im Bereich der Beschleunigten Sicherheitszertifizierung (BSZ);
  siehe Anforderungen in „Anerkennung von Prüfstellen: Programm im Bereich Beschleunigte Sicherheitszertifizierung (BSZ)“ [BSZ-Prüfstellen].

2.1.3 Programm für die Anerkennung Technische Richtlinien (TR)

- Anerkennung als Prüfstelle im Bereich Technischer Richtlinien (TR); siehe Anforderungen in „Anerkennung von Prüfstellen: Programm im Bereich Technischer Richtlinien“ [TR-Prüfstellen].

2.1.4 Programm für die Anerkennung: Network Equipment Security Assurance Scheme (NESAS)

- Anerkennung als Prüfstelle im Bereich der Network Equipment Security Assurance Scheme (NESAS); siehe Anforderungen in „Anerkennung von Prüfstellen: Programm im Bereich Network Equipment Security Assurance Scheme (NESAS)“ [NESAS-Prüfstellen].

3 Verfahren zur Anerkennung

Eine Anerkennung als Prüfstelle erfolgt, wenn festgestellt wird, dass die jeweiligen Anforderungen des Programms erfüllt sind und dass überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung nicht entgegenstehen.

Für die Ausübung der Tätigkeiten im jeweiligen Programm müssen i. d. R. mindestens zwei fachlich kompetente Mitarbeitende seitens der antragstellenden Organisation benannt und fest angestellt sein. Die benannten Personen dürfen grundsätzlich nicht zeitgleich für mehrere Stellen tätig sein, um eine klare Arbeitsplatzzuordnung und die Unparteilichkeit sicherzustellen. Details hierzu sind im jeweiligen Programm festgelegt.

Ein Evaluator darf in Zertifizierungsverfahren nur dann eigenverantwortlich eingesetzt werden, wenn das BSI die Kompetenz des Evaluators festgestellt hat. Das zur Kompetenzfeststellung notwendige Verfahren ist in der „Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen“ [VB-Personen] beschrieben.

3.1 Beteiligte Stellen im BSI

Die Anerkennungsstelle im BSI

Die Aufgabe der Anerkennungsstelle ist es festzustellen, dass die antragstellende Organisation die entsprechenden Anforderungen des Programms erfüllt.

Die Fachkompetenz der antragstellenden Organisation wird im Rahmen der Fachbegutachtungen bewertet.

Die Produktzertifizierungsstellen im BSI

Es ist Aufgabe der jeweiligen Produktzertifizierungsstelle während der Gültigkeit einer Anerkennung die Gleichwertigkeit aller Evaluierungsergebnisse und den vollständigen und korrekten Ablauf aller Produktzertifizierungsverfahren sicherzustellen. Um dies zu erreichen, führen die Produktzertifizierungsstellen in jedem Verfahren eine Prüfbegleitung im Hinblick auf eine einheitliche Vorgehensweise und Methodik durch.

Zur Überprüfung der formalen und fachlichen Voraussetzungen tauschen die Anerkennungsstelle und die Produktzertifizierungsstelle des BSI untereinander Informationen aus.

Werden bei einer Produktprüfung Mängel bei einer Prüfstelle bekannt, erfolgt eine Information an die Anerkennungsstelle zur möglichen Einleitung von Maßnahmen (siehe Kapitel 5.3 „Rahmenbedingungen zum Verfahren“).

3.2 Phasen zur Anerkennung

Die Anerkennung einer Prüfstelle erfolgt in drei Phasen.

3.2.1 Vorbereitungs- und Antragsphase

Vor einer Antragstellung ist ein kostenloses Informationsgespräch mit dem BSI obligatorisch. Das Informationsgespräch dient dazu, die antragstellende Organisation umfassend über den Anerkennungsprozess zu informieren, einschließlich der einzelnen Schritte, Anforderungen und zeitliche Abläufe (u. a. zur Koordinierung des Austausches der asymmetrischen Verschlüsselung mit OpenPGP zum Datenaustausch). Die antragstellende Organisation hat die Möglichkeit, grundlegende Fragen zu klären. Falls im Gespräch deutlich wird, dass die antragstellende Organisation noch nicht ausreichend vorbereitet ist, wird auf die Notwendigkeit weiterer Vorbereitungen vor Antragstellung hingewiesen. Insgesamt sorgt das Gespräch dafür, dass die antragstellende Organisation ein klares Verständnis des Verfahrens erhält und gut vorbereitet ist.

Die antragstellende Organisation stellt einen formalen Antrag auf Anerkennung für ein oder mehrere Programme bei der Anerkennungsstelle des BSI. Bei Erstanträgen ist der original unterschriebene schriftliche Antrag postalisch ans BSI zu übermitteln. Bei Anträgen zur Reanerkennung ist eine elektronische Übermittlung mit digitaler Unterschrift ausreichend.

Eine Vorlage für den Antrag wird auf der Webseite des BSI zur Verfügung gestellt. Die gestellten Anträge 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 einer Anerkennung ein öffentliches Interesse besteht.

Die antragstellende Organisation muss insbesondere folgende Unterlagen dem Antrag als Nachweise beifügen:

- ausgefüllte Anlage 1 zum Antragsformular (siehe BSI-Webseite),
- ausgefüllte Anlage 2 „Matrix Evaluatorenkompetenz“ (nur notwendig für den Geltungsbereich CC)
- Firmendarstellung bei Erstanerkennung,
- einen aktuellen Auszug aus dem Handels-, Genossenschafts-, Vereins- bzw. Partnerschaftsregister (nicht älter als 6 Monate). Neben den Eigentums- sind auch die Beteiligungsverhältnisse offenzulegen,
- Eigenversicherung, dass das Unternehmen sich nicht in Insolvenz oder in Liquidation befindet, gegen das Unternehmen kein Insolvenzverfahren eingeleitet ist oder das Unternehmen sich nicht in einer entsprechenden Lage befindet oder eine solche Lage einzutreten droht,
- Benennung der fest angestellten Mitarbeitenden der antragstellenden Organisation (i.d.R. mindestens zwei pro Programm) mit für das Programm relevanter Projekt- und Arbeitshistorie sowie Kompetenzprofilen.
- Systemdokumentation Qualitätsmanagement:
  - Dokumentation eines Qualitätsmanagementsystems nach DIN EN ISO/IEC 17025 [17025] bezogen auf das beantragte Programm,
  - Detaillierte Beschreibung der Arbeitsabläufe sowie alle Vorlagen, die zur Dokumentation und Unterstützung des Qualitätsmanagements verwendet werden (umfassende Beschreibung aller Regelungen, Verfahren und Prozeduren zur Erfüllung der Normanforderungen).
- dokumentierte Verfahren zur Durchführung von Prüfungen einschließlich der Regelungen zur Handhabung von Prüfgegenständen und Einrichtungen sowie zur Sicherung der Qualität von Prüfergebnissen DIN EN ISO/IEC 17025 [17025]. Aufzeichnungen:

  - Aufzeichnungen zum letzten internen Systemaudit nach DIN EN ISO/IEC 17025 [17025]
  - Aufzeichnungen zur letzten Managementbewertung
  - Aufzeichnungen zum Personal über Verantwortungen und Befugnisse.
- Stellungnahme:
  - Eine schriftliche Stellungnahme zu allen Einzelaspekten der DIN EN ISO/IEC 17025 [17025] im elektronischen Dokument „Referenzkatalog“ mit den Informationen darüber, durch welche Maßnahmen die antragstellende Organisation die Einzelaspekte der Norm erfüllt und an welchen Stellen in der QM-Dokumentation die Maßnahmen dokumentiert sind. Der Referenzkatalog wird vom BSI zur Verfügung gestellt und ist der Anerkennungsstelle zur weiteren Bearbeitung in elektronischer, editierbarer Form zu übersenden. Der Referenzkatalog ist keine Alternative für ein QM-System, sondern dient dem BSI dazu, das bestehende System des Antragstellers besser zu verstehen.
- Informationssicherheitsmanagementsystem:
  - Ein ISMS gemäß den Anforderungen der AS-Stellen [AS-Stellen], einschließlich der Bereitstellung aller erforderlichen Nachweise
  - Vollständig ausgefüllter Fragenkatalog zu den AS-Stellen [AS-Stellen]

Nach Antragstellung erfolgt eine Sichtung der eingereichten Dokumente durch das BSI um festzustellen, ob die eingereichten Nachweise und Unterlagen ausreichend für die Durchführung der Begutachtung sind. In dieser Dokumentensichtung erfolgt somit ein Abgleich mit den Anforderungen des beantragten Programms. Die Anerkennungsstelle weist die antragstellende Organisation auf fehlende oder unzureichende Unterlagen im Rahmen ihrer gesetzlichen Hinweispflicht (vgl. § 24 Verwaltungsverfahrensgesetz [VwVfG]) hin. Sind die eingereichten Unterlagen unvollständig oder entsprechen nicht den Anforderungen, hat die antragstellende Organisation die Gelegenheit, die Unterlagen zu überarbeiten und erneut einzureichen. Sind die eingereichten Unterlagen auch nach wiederholter Einreichung unvollständig oder entsprechen nicht den Anforderungen, wird seitens des BSI per Anhörung angekündigt, das Anerkennungsverfahren mit einem negativen Ergebnis zu beenden. Ist das Ergebnis der Antragsprüfung nach der Überarbeitungsrunde negativ, so wird der Anerkennungsantrag durch das BSI abgelehnt.

Entsprechen die Unterlagen den Anforderungen, vereinbart die Anerkennungsstelle mit der antragstellenden Organisation Termine für die Systembegutachtung. Bei Reanerkennungen vereinbart das Begutachterteam erst nach Eingang der Antragsunterlagen (inklusive aller dazugehörigen Nachweise) einen Termin zur Systembegutachtung. Daher ist es wichtig, dass die Antragstellende Organisation eigenständig und fristgerecht die vollständigen Antragsunterlagen zur Reanerkennung einreicht.

Die antragstellende Organisation kann Einwände gegen die Bestellung der Begutachterinnen und Begutachter erheben.

Allen Beteiligten am Verfahren obliegt es, Abweichungen von der vereinbarten Zeitplanung den anderen Beteiligten mitzuteilen und erneut abzustimmen.

Nach einer Antragsprüfung mit negativem Ergebnis wird der Antrag durch das BSI abgelehnt.

Auf Wunsch der antragstellenden Organisation kann eine kostenpflichtige Vorabbegehung durch das BSI durchgeführt werden, um Mängel im System der antragstellenden Organisation aufzudecken.

3.2.2 Begutachtungsphase

In der Begutachtungsphase wird durch das Begutachtungsteam des BSI eine Systembegutachtung durchgeführt, die sich aus den folgenden Teilen zusammensetzt:

- Begutachtung des Qualitätsmanagementsystems gemäß DIN EN ISO/IEC 17025 [17025],

- Begutachtung des Informationssicherheitsmanagementsystems nach dem nicht öffentlichen Dokument „Anforderung an die Sicherheit von Stellen“ [AS-Stellen] und
- ggf. einer Fachbegutachtung je Programm.

Bei einem Erstantrag erfolgt die Begutachtung vor Ort beim Antragsteller. Bei Reanerkennungen oder Erweiterungen der Anerkennung kann die Begutachtung auch als Fernbegutachtung durchgeführt werden. Die Entscheidung darüber trifft das BSI.

Die Systembegutachtung wird durchgeführt, um zu überprüfen, ob mit den getroffenen Maßnahmen die Anforderungen des Programms erfüllen, umgesetzt und wirksam sind. Hierbei werden stichprobenartig auch Projekte und weitere Tätigkeiten der antragstellenden Organisation mit Bezug zum jeweiligen Programm herangezogen. Eine Systembegutachtung für ein Programm beläuft sich auf zwei Arbeitstage. Für jedes weitere Programm kann grundsätzlich bis zu einem weiteren Arbeitstag angesetzt werden. Im Rahmen dessen wird grundsätzlich auch das Informationssicherheitsmanagementsystem begutachtet.

Fachbegutachtungen werden zur Kompetenzfeststellung der Prüfstelle entsprechend des Programms durchgeführt. Die Anforderungen und der Ablauf der Fachbegutachtung sind im jeweiligen Programm beschrieben.

Nach der Erhebung von Begutachtungsnachweisen mittels Interviews, Einsichtnahme in Aufzeichnungen und Dokumente der antragstellenden Organisation sowie weiterer Maßnahmen (z. B. Einsichtnahme in technische Systeme) werden die Begutachtungsfeststellungen (Abweichungen und Verbesserungspotenzial) getroffen. Diese und das daraus resultierende Begutachtungsergebnisse werden der antragstellenden Organisation in einem Abschlussgespräch mitgeteilt.

Falls Abweichungen festgestellt werden, muss im Abschlussgespräch ein gemeinsames Verständnis darüber entwickelt werden. Die Abstimmung und Terminierung von Korrekturmaßnahmen erfolgt im Abschluss-gespräch oder ggf. nach durchgeführter Ursachenanalyse.

3.2.2.1 Umgang mit Abweichungen

Es gibt zwei Arten von Abweichungen:

Kritische Abweichungen:

- Abweichung von einer festgelegten Anforderung, die ein falsches Ergebnis der Arbeiten der antragstellenden Organisation verursacht bzw. verursachen kann.
- Abweichung, die die grundlegende Wirksamkeit des QM-Systems in Frage stellt.
- Wiederholtes Auftreten einer nicht kritischen Abweichung zur gleichen Anforderung.

Bei kritischen Abweichungen ist die Durchführung einer Ursachenanalyse sowie die Umsetzung von geeigneten und wirksamen Korrekturmaßnahmen die Voraussetzung für die Erteilung einer Anerkennung.

Nicht kritische Abweichungen:

- Abweichung von einer festgelegten Anforderung.
- Es ist keine unmittelbare Auswirkung auf das Ergebnis der Arbeiten der antragstellenden Organisation zu erwarten.
- Die grundlegende Wirksamkeit des QM-Systems wird nicht in Frage gestellt.

Für festgestellte nicht kritische Abweichungen muss eine Ursachenanalyse durchgeführt werden auf deren Basis geeignete und wirksame Korrekturmaßnahmen entwickelt werden. Zur Behebung von nicht kritischen Abweichungen wird in der Regel eine Frist von max. 3 Monaten gewährt. Das Vorliegen einer nicht kritischen Abweichung steht einer Erteilung der Anerkennung grundsätzlich nicht im Weg.

3.2.2.2 Begutachtungsergebnis und Begutachtungsbericht

Das Begutachtungsergebnis wird mit einer Begutachtungsempfehlung zur Entscheidung in einem Begutachtungsbericht zusammengefasst.

3.2.3 Anerkennungsphase

Auf Grundlage des Begutachtungsberichts sowie ggf. dem Ergebnis aus den Fachbegutachtungen entscheidet das BSI gemäß den Regelungen § 9 Abs. 6 BSI-Gesetz [BSIG] über die Anerkennung einer Stelle.

Vor Erteilung einer Anerkennung wird der antragstellenden Organisation der Begutachtungsbericht sowie ein Anhörungsschreiben inklusive möglicher Nebenbestimmungen zugesandt. Die antragstellende Organisation hat die Gelegenheit, sich zu dem Erlass des Bescheids und dessen Nebenbestimmungen im Rahmen einer Anhörung zu äußern. Teilt die antragstellende Organisation vor Ablauf der Anhörungsfrist mit, dass sie von der Möglichkeit einer Stellungnahme keinen Gebrauch zu machen beabsichtigt, so kann die Anerkennung unmittelbar nach dieser Mitteilung erteilt werden.

Bei positiver Anerkennungsentscheidung erstellt die Anerkennungsstelle die Urkunde und den Anerkennungsbescheid.

Die Anerkennung kann Nebenbestimmungen (siehe Kapitel 5.4.1 „Bestimmungen zur Aufrechterhaltung“) enthalten und ist zu befristen. Die Geltungsdauer für das jeweilige Programm wird im Bescheid festgesetzt. Dieser Zeitraum wird ggf. mit bereits bestehenden Anerkennungen synchronisiert und beträgt in der Regel maximal drei Jahre.

Eine negative Anerkennungsentscheidung erfolgt, wenn die in dieser Verfahrensbeschreibung und in dem Programm zur beantragten Anerkennung beschriebenen Anforderungen nicht erfüllt werden oder das Bundesministerium des Innern und für Heimat festgestellt hat, dass überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung entgegenstehen. In diesem Fall werden vor Ablehnung des Antrages die Gründe der voraussichtlichen Ablehnung im Rahmen der Anhörung mitgeteilt. Die antragstellende Organisation hat innerhalb einer Frist Gelegenheit zur Äußerung und zur Nachbesserung.

Gegen den Bescheid kann Widerspruch innerhalb eines Monats ab Bekanntgabe beim Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 87, 53175 Bonn, erhoben werden.

Die Veröffentlichung der Anerkennung erfolgt erst nach Ablauf der Widerspruchsfrist, sofern nicht auf den Widerspruch verzichtet wurde. Die Verzichtserklärung ist durch formloses Schreiben möglich.

Mit dem Anerkennungsbescheid entscheidet die Anerkennungsstelle auch über die Verfahrenskosten. Über die Höhe der Kosten wird durch gesonderten Kostenbescheid entschieden.

4 Aufrechterhaltung und Überwachung der Anerkennung

Während der Laufzeit der Anerkennung kann regelmäßig und anlassbezogen überprüft werden, ob die Voraussetzungen für die Anerkennung weiterhin vorliegen. Dazu werden im Anerkennungszeitraum nach 18 Monaten eintägige Begutachtungen zur Systemförderung (siehe Kapitel 4.2 „Überwachung der Anerkennung“) durchgeführt. Zudem können entsprechend den Anforderungen des Programms Fachbegutachtungen (siehe Kapitel 4.2.2 „Fachbegutachtungen“) vorgenommen werden.

Falls notwendig, können „Anlassbezogene Begutachtungen“ gemäß Kapitel 4.3 durchgeführt werden.

Des Weiteren muss die anerkannte Stelle im Bescheid enthaltene Nebenbestimmungen einhalten und ihre (Prüf-)Tätigkeiten gemäß Kapitel 4.1 „Durchführung der (Prüf-)Tätigkeiten im betreffenden Programm“ durchführen.

Werden während der Laufzeit oder im Rahmen von Überprüfungen Mängel bekannt, kann der Anerkennungsbescheid aufgehoben werden (siehe Kapitel 5.6.2 „Widerruf einer rechtmäßigen Anerkennung“).

Fünf Monate vor Ablauf der Anerkennung sollte ein erneuter Antrag auf Anerkennung gestellt werden, damit gewährleistet werden kann, dass die Anerkennung lückenlos aufrechterhalten wird.

4.1 Durchführung der (Prüf-)Tätigkeiten im betreffenden Programm

Die Anforderungen an die Durchführung der (Prüf-)Tätigkeiten der Stellen sind im Programm zur Anerkennung jeweils beschrieben.

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

4.1.1 Qualitätssicherung bei Prüftätigkeiten in einer Prüfstelle

Bei jeder Prüftätigkeit muss eine abschließende interne Qualitätssicherung (QS) des Prüfberichts bzw. des Evaluierungsberichts (ETR) durch eine zweite kompetente und unparteiisch handelnde Person (TR-Prüferin bzw. TR-Prüfer oder Evaluatorin bzw. Evaluator) der Prüfstelle durchgeführt werden.

In den Programmen CC und BSZ muss zusätzlich zur QS auch die für das Qualitätsmanagement (QM) zuständige Person (z.B. QM-Beauftragte) in der abschließenden Fassung des Evaluierungsberichts (ETR) die Einhaltung der Prozesse bestätigen. Ist die für das QM zuständige Person in einem Projekt gleichzeitig die verantwortliche Projektleiterin bzw. Projektleiter, muss diese Bestätigung durch deren bzw. dessen Stellvertreter im Bereich QM (z. B. stellvertretende QM-Beauftragt) erfolgen.

4.2 Überwachung der Anerkennung

4.2.1 Begutachtungen zur Systemförderung

Ziel der Begutachtung zur Systemförderung ist es zu überprüfen, ob die Anforderungen aus den Programmen dauerhaft eingehalten werden. Während des Anerkennungszeitraums von in der Regel 3 Jahren wird einmal nach ca. 18 Monaten eine Begutachtung zur Systemförderung durchgeführt. Ziel der Begutachtung zur Systemförderung ist es zu überprüfen, ob die Anforderungen aus den Programmen dauerhaft eingehalten werden. Es muss der Nachweis erbracht werden, dass das Managementsystem wirksam aufrechterhalten und weiterentwickelt wird. Zur Begutachtung der antragstellenden Organisation können Projekte und Arbeiten mit Bezug zu den jeweiligen Programmen herangezogen werden.

Die Stelle kann Begutachtungsthemen für diese Begutachtung vorschlagen.

Die Ergebnisse werden in einem Abschlussgespräch mitgeteilt und in einem Begutachtungsbericht zusammengefasst.

Sollten in einer Begutachtung zur Systemförderung kritische Abweichungen festgestellt werden, so ist für diese eine Ursachenanalyse durchzuführen. Geeignete und wirksame Sofortmaßnahmen müssen innerhalb von 4 Wochen ergriffen und nachgewiesen werden.

Kann eine kritische Abweichung innerhalb dieser Frist nicht behoben werden, wird ein Aufhebungsverfahren gemäß Kapitel 5.6.1 „Aufhebung einer Anerkennung“ für die betroffenen Programme eingeleitet.

4.2.2 Fachbegutachtungen

Fachbegutachtungen werden zur Kompetenzfeststellung der Prüfstelle und der Personen durchgeführt und sind insbesondere dann erforderlich, wenn im jeweiligen Programm keine Personenzertifizierung vorgesehen ist.

Die Anforderungen und der jeweilige Ablauf der Fachbegutachtung sind in den jeweiligen Programmen beschrieben.

4.3 Anlassbezogene Begutachtungen

Anlassbezogene Begutachtungen können stattfinden, insbesondere wenn

- sich in der antragstellenden Organisation Änderungen (z. B. örtliche Verlagerung der antragstellenden Organisation oder Änderung der Unternehmenszugehörigkeit) ergeben, die Auswirkungen auf die Erfüllung der DIN EN ISO/IEC 17025 [17025] haben;
- begründete Zweifel an der Einhaltung der DIN EN ISO/IEC 17025 [17025] oder an der Kompetenz der antragstellenden Organisation besteht;
- wiederholt gegen die Verfahrensbeschreibungen oder Programme verstoßen wird;
- Verfahrensänderungen seitens des BSI u. a. aufgrund von Vorschriften, internationalen Vereinbarungen oder eines Kriterien- bzw. Programmwechsels notwendig werden;
- von dritter antragstellenden Organisation Informationen über Unregelmäßigkeiten an die Anerkennungsstelle des BSI herangetragen werden.

5 Rahmenbedingungen

5.1 Grundlage für die Anerkennung

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

5.2 Genereller Dokumentenaustausch mit der Anerkennungsstelle

Die elektronische Kommunikation mit dem BSI erfolgt grundsätzlich über das Postfach postfach-anerkennung@bsi.bund.de und mit GPG verschlüsselt. Der entsprechende Schlüssel ist bei der Anerkennungsstelle erhältlich.

5.3 Rahmenbedingungen zum Verfahren

5.3.1 Obliegenheiten der antragstellenden Organisation

Der antragstellenden Organisation obliegt es:

- die notwendigen Nachweise zur Ermittlung des Sachverhalts beizubringen. Bei fehlenden oder unzureichenden Nachweisen kann ein Verfahren durch die Anerkennungsstelle mit negativem Ergebnis beendet werden.
- im Rahmen ihrer Mitwirkungsobliegenheiten die notwendige Mitwirkung etwaiger Dritter sicherzustellen.
- dem Begutachterteam des BSI oder den vom Bundesamt beauftragten Personen in erforderlichem Umfang kostenfrei Zugang zu den Standorten, zu den zur Prüfung vorgesehenen Systemen sowie zu den notwendigen, vom BSI festgelegten Nachweisen zu gewähren.
- das BSI oder die vom BSI beauftragten Personen kostenfrei durch fachkompetente Mitarbeitende der antragstellenden Organisation zu unterstützen.
- aktiv an der Termingestaltung mitzuwirken und die Einhaltung der vereinbarten Termine sicherzustellen. Bei sich abzeichnenden Veränderungen muss die Anerkennungsstelle umgehend informiert werden, um eine aktualisierte Verfahrensplanung abzustimmen.

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

5.3.2 Rücknahme eines Antrages

Zu jedem Zeitpunkt im Verfahren kann die antragstellende Organisation den Antrag auf Anerkennung zurückziehen. In diesem Fall ist wird Verfahren unverzüglich beendet.

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

5.3.3 Änderungen des Antrages

Ein Antrag kann bis zur Entscheidung über den Anerkennungsantrag (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 BMI [BMIBGebV] behandelt.

5.3.4 Ablehnung eines Antrages

Das BSI kann einen Antrag bei nicht Vorliegen der in § 9 BSI-Gesetz [BSIG] genannten Voraussetzungen ablehnen.

Dabei obliegt es dem Antragsteller, die notwendigen Beweismittel zur Ermittlung des Sachverhaltes beizubringen. Das BSI ist nach § 6 BSI-Zertifizierungs- und Anerkennungsverordnung [BSIZertV] nicht verpflichtet, eigene Ermittlungen im Sinne des § 26 Abs. 1 Verwaltungsverfahrensgesetz [VwVfG] anzustellen, kann aber auf ihm bereits vorliegende Erkenntnisse zurückgreifen. Aus diesem Grund wird ein Antrag auch dann abgelehnt, wenn

- ein unvollständig eingereichter Antrag nicht innerhalb von 3 Monaten vervollständigt wird oder
- die antragstellende Organisation über einen Zeitraum von mehr als 3 Monaten entgegen der vereinbarten Planung keine Unterlagen liefert, die eine Prüfung durch die Anerkennungsstelle ermöglichen.

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

5.4 Rahmenbedingungen zur Aufrechterhaltung der Anerkennung

5.4.1 Bestimmungen zur Aufrechterhaltung

Zur Aufrechterhaltung der Anerkennung muss die anerkannte Stelle die Festlegungen dieser Verfahrensbeschreibung [VB-Prüfstellen] sowie mögliche im Bescheid enthaltene Nebenbestimmungen einhalten.

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

- die Stelle bei der Nutzung der Anerkennung, insbesondere bei der Verwendung zu Werbezwecken, Vorlage und Nachweisführung, auf den Anerkennungsbescheid und die Anerkennungsurkunde hinweisen und diese Dokumente zur Verfügung stellen muss.
- die Stelle regelmäßig oder anlassbezogen Überprüfungen zur Aufrechterhaltung der Anerkennung zulassen muss. Die Kosten sind von der Stelle zu tragen.
- die Stelle dem BSI unverzüglich schriftlich mitteilen muss, wenn sich ihre Arbeitsweise in Bezug auf die Einhaltung der Anforderungen des Programms, ihre Unternehmensform, ihre Eigentums- und Beteiligungsverhältnisse oder ihr Unternehmenssitz ändert.
- die Stelle dem BSI unverzüglich schriftlich mitteilen muss, wenn Umzüge oder bauliche Änderungen an den Räumlichkeiten der Stelle geplant sind. Sobald eine anerkannte Stelle plant, in neue Räumlichkeiten umzuziehen, muss das BSI über diese Absicht informiert werden. Vor Umzug der Stelle muss eine Eignungsprüfung der neuen Räumlichkeiten durch das BSI erfolgen. Zur Eignungsprüfung muss dem BSI die aktualisierte Dokumentation des Informationssicherheitsmanagementsystems (inkl. Netztopologie) sowie die aktualisierte Dokumentation der materiellen Sicherheit (inkl. Lageplan der Räumlichkeiten) zur Verfügung gestellt werden. Falls notwendig wird eine anlassbezogene Begutachtung der neuen Räumlichkeiten durch das BSI durchgeführt. Erst nach Freigabe durch das BSI darf die Stelle ihre Prüftätigkeiten an einem neuen Standort fortsetzen.
  Zieht eine Stelle ohne Freigabe der neuen Räumlichkeiten um, besteht keine Anerkennung der Stelle in

den neuen Räumlichkeiten. Es dürfen dann keine Arbeiten im Rahmen der Anerkennung als Prüfstelle in den neuen Räumlichkeiten durchgeführt werden. Unterlagen, Datenträger sowie Prüfgegenstände, die im Zusammenhang mit der Arbeit als Stelle beim BSI stehen, dürfen vor Freigabe ebenfalls nicht in den neuen Räumlichkeiten aufbewahrt werden.

- die Stelle eine bestimmte Zahl von Personen für das jeweilige Programm beschäftigen muss. Neues Personal, das in der Prüftätigkeit eingesetzt werden soll, ist der Anerkennungsstelle vor der Aufnahme von Tätigkeiten im entsprechenden Programm zu melden. Die benannten Personen dürfen grundsätzlich nicht zeitgleich für mehrere anerkannte Prüfstellen tätig sein, um eine klare Arbeitsplatzzuordnung und die Unparteilichkeit sicherzustellen.
- die Stelle an vom BSI angebotenen Arbeitstreffen zum Programm teilnehmen muss. Das BSI stellt durch diese Treffen und Workshops eine kontinuierliche Zusammenarbeit mit den Stellen und ggf. den Produktzertifizierungsstellen sicher.

Sofern Nebenbestimmungen im Bescheid angeordnet sind, muss die antragstellende Organisation diese beachten. Sie sind somit zur Aufrechterhaltung verpflichtend einzuhalten.

5.4.2 Regelungen zur Unterbeauftragung

Grundsätzlich muss eine Tätigkeit im Programm vollständig und ausschließlich durch die Stelle erfolgen. Eine Unterbeauftragung kann kein in der unterbeauftragenden Prüfstelle nicht vorhandenes Programm oder nicht vorhandenen Kompetenzbereich ausgleichen.

Bei anerkannten Prüfstellen ist in begründeten Ausnahmen und bei Vorliegen der folgenden Voraussetzungen eine Unterbeauftragung möglich:

- Die Verantwortung für alle Prüfergebnisse verbleibt bei der unterbeauftragenden Stelle. Diese muss somit das Prüfkonzept sowie die Testspezifikationen erstellen und die Ergebnisse der Tests auswerten.
- Dem BSI muss eine Beschreibung vorliegen, welche Teile einer Prüfung oder Evaluierung unterbeauftragt werden sollen. Die Fachkompetenz der beteiligten Evaluatorinnen und Evaluatoren zu diesen Teilen muss dem BSI gegenüber nachgewiesen und deren Namen müssen dem BSI benannt werden.
- Die unterbeauftragte Stelle muss eine vom BSI anerkannte Prüfstelle sein und für das betreffende Programm ihre Fachkompetenz nachgewiesen haben. Zur Durchführung der Evaluierungen und Prüfungen sind nur die fest angestellten, benannten bzw. nachgewiesen kompetenten Personen der unterbeauftragten Stelle einzusetzen.
- Die Herstellerorganisation bzw. die antragstellende Organisation muss einer Unterbeauftragung zustimmen.
- Die Zustimmung des BSI muss in jedem Einzelfall vorliegen.

Des Weiteren gelten die speziellen Anforderungen des jeweiligen Programms.

5.4.3 Regelungen zur Vertraulichkeit

Die antragstellende Organisation muss die streng vertrauliche Behandlung der Interna von Verfahren und Projekten in den Programmen gewährleisten. Er wird Beschäftigten und Dritten Informationen nur geben, soweit ihre Kenntnis notwendig ist („Kenntnis-nur-wenn-nötig-Prinzip“).

Die Stelle wahrt Verschwiegenheit über Betriebsgeheimnisse Dritter sowie über alle Informationen, die ihr im Zusammenhang mit dem Anerkennungsverfahren und im Rahmen einer späteren Tätigkeit als anerkannte Stelle 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 Bearbeitung, Kenntnisnahme und Aufbewahrung jeglicher Unterlagen zur Bearbeitung, Zertifizierung, Prüfung und Evaluierung bei Fernarbeitsplätzen und ähnlichen Formaten ist nur unter Einhaltung der seitens des BSI veröffentlichten Anforderungen [AS-Stellen] gestattet. Ansonsten ist die Arbeit ausschließlich in den Räumlichkeiten der anerkannten Organisation oder bei der jeweiligen Herstellerorganisation bzw. der jeweiligen Behörde gestattet. Ausnahmen bedürfen der ausdrücklichen Zustimmung des BSI.

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

5.4.4 Vorkehrungen zum Schutz von Verschlusssachen

Wenn einer Stelle im Rahmen ihrer Tätigkeiten im Programm Verschlusssachen (VS) des Geheimhaltungsgrades „VS-NUR FÜR DEN DIENSTGEBRAUCH“ (VS-NfD) zur Kenntnis gelangen sollen, verpflichtet sich die Stelle zuvor die Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA) [VSA] bzw. das Geheimschutzhandbuch [GHB] (siehe dortige Anlage 3), in der jeweils aktuellen Fassung, insbesondere das Merkblatt für die Behandlung von Verschlusssachen des Geheimhaltungsgrades „VS-NUR FÜR DEN DIENSTGEBRAUCH“ (VS-NfD), einzuhalten.

Eine Verpflichtung der Personen, denen Zugang zu Verschlusssachen des Geheimhaltungsgrades VS-NfD gewährt werden muss, wird durch die zuständige Behörde bzw. auf deren Veranlassung vorgenommen.

Als zentrale Ansprechpartnerin bzw. Ansprechpartner für Angelegenheiten des Geheimschutzes muss die Stelle eine für den Schutz von VS-NfD verantwortliche Person (bei geheimschutzbetreuten Unternehmen ist dies die Sicherheitsbevollmächtigte bzw. der Sicherheitsbevollmächtigte) benennen. Im Besonderen ist dieser für die Sicherstellung des Schutzes von Verschlusssachen und die Umsetzung und Einhaltung der in der Verschlusssachenanweisung [VSA] und im Geheimschutzhandbuch [GHB] enthaltenen Vorschriften verantwortlich.

Wenn Verschlusssachen mit dem Geheimhaltungsgrad „VS-VERTRAULICH“ (VS-V) und höher ausgetauscht werden sollen, sind die entsprechenden Regelungen des Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitsüberprüfungsgesetz - SÜG) [SÜG], der Verschlusssachenanweisung [VSA] und des Geheimschutzhandbuches [GHB] umzusetzen und einzuhalten.

Neben den organisatorischen und materiellen Schutzmaßnahmen werden ab dem Geheimhaltungsgrad VS-V und höher auch Maßnahmen des personellen Geheimschutzes erforderlich.

Ggf. stellt die zuständige Behörde beim Bundesministerium für Wirtschaft und Klimaschutz (BMWK) einen Antrag auf Aufnahme der Stelle in die Geheimschutzbetreuung.

Sofern die Stelle für die Bearbeitung von Verschlusssachen IT einsetzt, hat sie ebenfalls die Vorschriften der Verschlusssachenanweisung [VSA] bzw. des Geheimschutzhandbuchs [GHB] zu beachten.

Dem BSI ist auf Verlangen darzulegen, wie die Schutzmaßnahmen umgesetzt wurden. Dem BSI oder dessen Bevollmächtigten ist eine Überprüfung zu ermöglichen.

5.4.5 Regelungen zur Archivierung von Dokumenten, Aufzeichnungen und Testobjekten

Die vom BSI anerkannte Stelle stellt sicher, dass Aufzeichnungen und Testobjekte, die aus Evaluierungsverfahren im Zusammenhang mit einer Zertifizierung durch das BSI resultieren, für die Dauer der Gültigkeit des Zertifikates plus 3 Jahre, mindestens aber 10 Jahre aufbewahrt werden. Vorschriften oder Pflichten, die eine längere Aufbewahrungsfrist vorsehen, bleiben hiervon unberührt. Bei Wiederverwendung von Aufzeichnungen und Testobjekten in nachfolgenden Prüfungen oder Evaluierungen müssen diese Teile aus dem Altverfahrens ins neue Verfahren transferiert werden und nach

den Regeln/Fristen des neuen Verfahrens archiviert werden. Dem BSI ist in dem Zeitraum der Archivierung auf Anfrage Zugang zu diesen Aufzeichnungen und Testobjekten zu gewähren.

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

5.5 Erweiterung der Anerkennung

Zur Erweiterung des Programms bei einer bestehenden Anerkennung durch eine zusätzliche Anerkennung kann ein Antrag auf Erweiterung bei der Anerkennungsstelle gestellt werden.

Es wird grundsätzlich eine entsprechende Fachbegutachtung durchgeführt, um alle erforderlichen Anforderungen für das beantragte Programm zu überprüfen.

Endet die Fachbegutachtung erfolgreich und wird die Anerkennung für das neu beantragte Programm ausgesprochen, so wird auch die gültige Urkunde erweitert.

Die Laufzeit der (ersten) Anerkennung bleibt unverändert. Die Laufzeiten der verschiedenen Anerkennungen werden synchronisiert, ggf. auch mit Zertifizierungen zum IT-Sicherheitsdienstleister. D.h. sie enden zum gleichen Zeitpunkt wie die bestehende Anerkennung oder Zertifizierung.

5.6 Nachmeldung weitere Prüfer bzw. Evaluatoren

Die Prüfstellen müssen gewährleisten, dass sie über genügend Personalressourcen verfügen, um ihre Evaluierungsarbeiten sachgerecht durchführen zu können. Während der Anerkennungsperiode können weitere erfahrene Prüfer/Evaluatoren benannt werden. Dafür müssen die im jeweiligen Programm genannten Angaben und Nachweise für die nachzumeldenden Prüfer/Evaluatoren elektronisch oder per Post eingereicht werden.

In der Regel beschäftigen die Prüfstellen sowohl erfahrene Prüfer und Evaluatoren als auch solche, die weniger oder gar keine Erfahrung haben. Um diese Situation zu berücksichtigen und gleichzeitig ein hohes Qualitätsniveau der Verfahren aufrechtzuerhalten, gibt es eine zusätzliche Kategorie: „Prüfer/Evaluator in Einarbeitung“.

Folgende Anforderungen sind dabei zu beachten:

- Meldung des „Prüfers/Evaluators in Einarbeitung“ beim BSI
- Die Prüfstelle muss ein Mitarbeiterentwicklungskonzept (Mentorenkonzept) in Hinblick auf die genannten Fachanforderungen etablieren und umsetzen. Das Konzept muss folgende Mindestinhalte einschließen:
  - Einarbeitung in die Einrichtungen und Prozesse durch einen Mentor
  - Einsatz des Prüfers/Evaluators in Einarbeitung in die aktuellen Evaluierungsverfahren
  - Bewertung des Fortschritts der Ausbildung.

Sobald die Einarbeitung aus Sicht der Prüfstelle abgeschlossen ist, kann die Prüfstelle den Prüfer/Evaluator unter Mitsendung der erforderlichen Nachweise (Einarbeitungsnachweise sowie Nachweise zu den Kompetenzen zur Feststellung der Kompetenz durch das BSI) an die BSI-Anerkennungsstelle melden. Diese überprüft die Vollständigkeit und formale Korrektheit der Nachweise, fordert gegebenenfalls fehlende Nachweise bei der Prüfstelle nach bzw. beauftragt bei Vollständig- und Korrektheit der Nachweise die zuständige Produktzertifizierungsstelle des BSI mit der fachlichen Prüfung und Bewertung.

In einigen Bereichen erfolgt die fachliche Prüfung und Bewertung der Nachweise durch die (im BSI) fachlich zuständigen Organisationseinheiten.

Diese fordert gegebenenfalls weitere Nachweise an, führt ggf. ein Fachinterview mit den zukünftigen Prüfern/Evaluatoren durch und gibt ein Votum ab, ob nach ihrer fachlichen Expertise der Prüfer/Evaluator

in Einarbeitung als erfahrener Prüfer/Evaluator anerkannt werden kann oder nicht. Dieses Votum wird der BSI-Anerkennungsstelle mitgeteilt. Der Leiter der BSI-Anerkennungsstelle trifft dann aufgrund der ihm vorliegenden Informationen die Entscheidung über die Kompetenzfeststellung als erfahrener Prüfer/Evaluator.

5.6.1 Aufhebung einer Anerkennung

Zur Aufhebung einer Anerkennung werden die Regelungen des Verwaltungsverfahrensgesetzes [VwVfG] angewendet.

5.6.2 Widerruf einer rechtmäßigen Anerkennung

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

Gründe, die zu einem Widerruf einer Anerkennung führen können sind beispielsweise, wenn die antragstellende Organisation:

- im Bescheid enthaltene Nebenbestimmungen nicht beachtet (siehe Kapitel 5.4.1 „Bestimmungen zur Aufrechterhaltung“.
- Änderungen dieser Verfahrensbeschreibung oder den jeweils gültigen Programmen und dessen Anforderungen widerspricht.
- gegen Anforderungen aus den jeweils gültigen Verfahrensbeschreibungen oder Programmen verstößt. Dies kann beispielsweise der Fall sein, wenn es sowohl beim Verfahren zur Anerkennung von Prüfstellen als auch bei einem konkreten Produktzertifizierungsverfahren in der Zusammenarbeit zwischen dem BSI und der Stelle aufgrund von Nichteinhaltung von Anforderungen, Vorgaben und Terminen bzw. von mangelhaften Prüftätigkeiten einer Stelle zu erheblichen Problemen kommt.
- Vertraulichkeits- oder Sicherheitsvorschriften verletzt (siehe Kapitel 5.4.3„Regelungen zur Vertraulichkeit“ und 5.4.4 „Vorkehrungen zum Schutz von Verschlusssachen“).
- Anerkennungsurkunden oder Anerkennungszeichen missbräuchlich verwendet.

5.6.3 Rücknahme einer rechtswidrigen Anerkennung

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

- bewusst falsche Angaben zu den Anerkennungsvoraussetzungen gemacht wurden, oder
- für die Anerkennungsentscheidung bewusst wesentliche Informationen verschwiegen wurden (vgl. § 48 Verwaltungsverfahrensgesetz [VwVfG]).

5.6.4 Folgen der Aufhebung

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

Die antragstellende Organisation ist zur Herausgabe verpflichtet. Sie kann jedoch verlangen, dass ihr die Urkunden wieder ausgehändigt werden, nachdem sie durch das BSI als ungültig gekennzeichnet wurden.

Die Stelle wird nicht mehr auf der öffentlichen Liste der anerkannten Stellen für die entsprechenden Programme gelistet und die Kontaktdaten der Stelle werden entfernt.

5.7 Beschwerde-, Verbesserungs- und Qualitätsmanagement

Die Anerkennungsstelle 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 (https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Beschwerde-und-Verbesserungsmanagement/verbesserungsmanagement_node.html;jsessionid=ED8D6B099D0C7926DA2E665CE2C3398B.internet461).

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 Grundgesetz für die Bundesrepublik Deutschland (GG) i. V. m. § 839 Bürgerliches Gesetzbuch (BGB).

5.9 Kosten

Die Kosten des Anerkennungsverfahrens richten sich nach der Besonderen Gebührenverordnung BMI [BMIBGebV].

Die Kosten sind auch bei negativem Ergebnis des Verfahrens zu zahlen.

Ein Informationsgespräch mit dem BSI vor Antragstellung ist kostenfrei.

Zusätzliche Unterstützungshandlungen des BSI, wie z. B. die Vorabbegehung, werden nach Aufwand abgerechnet.

Im Falle einer Aufhebung der Anerkennung sind auch die hierfür entstandenen Kosten zu erstatten.

6 Veröffentlichung der Anerkennung

Grundsätzlich wird nach Erteilung der Anerkennung der Name der Stelle mit einer Kontaktperson und Kontaktdaten (Telefon, E-Mail) sowie die Programme mit dem Gültigkeitszeitraum veröffentlicht. Dieser Veröffentlichung kann widersprochen werden.

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. Dies geschieht z. B. während eines laufenden Aufhebungsverfahrens für den entsprechenden Zeitraum.

6.1 Anerkennungsnummer

Alle vom BSI anerkannten Stellen erhalten eine Anerkennungsnummer in der Form „BSI-APS 9XXX“ (BSI-Vorgangskennung-fortlaufende Vorgangsnummer).

Sie dient als Bezug für die BSI-internen Vorgänge, den Schriftwechsel und die Kennzeichnung von Dokumenten (im Rahmen des Verfahrens).

6.2 Anerkennungszeichen

Die antragstellende Organisation hat die Möglichkeit, bei positivem Abschluss des Verfahrens ein Anerkennungszeichen (als elektronische Druckvorlage) zu erhalten, das z. B. im Rahmen des Marketings verwendet werden kann.

Die Zeichenordnung des BSI enthält die Nutzungsbedingungen der Anerkennungszeichen.

6.3 Urkundenübergabe und Presseerklärung

Soll nach Abschluss des Verfahrens eine Presseerklärung veröffentlicht werden, so bittet das BSI den Wortlaut zuvor mit der Anerkennungsstelle des BSI abzustimmen.

Das BSI bietet die Möglichkeit, auf bestimmten öffentlichen Veranstaltungen wie z. B. Kongressen und Messen, auf denen das BSI vertreten ist, die Urkunde an eine Vertreterin bzw. einen Vertreter des Unternehmens auszuhändigen.

Nach Absprache kann ebenso eine Übergabe in den Räumen des BSI organisiert werden.

7 Referenzen und Glossar [Verzeichnisse]

Das Dokument Verzeichnisse als Nachschlagewerk für Interessenten und Beteiligte an Anerkennungsverfahren [Verzeichnisse] gibt einen Überblick über alle benötigten Anforderungen, Quellen und Hilfsmittel mit einem Glossar- und Abkürzungsverzeichnis.

Die Listen im Bereich der Anforderungen, Quellen und Hilfsmittel sind als Stammliste zu verstehen und decken für sämtliche Anforderungen und Dokumente die Information über aktuelle Quellenhinweise ab.