Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Anerkennung von Prüfstellen: Programm im Bereich Beschleunigte Sicherheitszertifizierung (BSZ)

BSZ-Prüfstellen

Version 2.2 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
© Bundesamt für Sicherheit in der Informationstechnik 2021-2024

Änderungshistorie

Version	*Datum*	*Name/ Org.-Einheit*	*Beschreibung*
1.0	30.09.2021	Anerkennungsstelle SZ 12	Erstausgabe
1.1	01.02.2022	Anerkennungsstelle SZ 12	Revision: • Austausch der Abbildung 1 „Zertifizierungs- und Anerkennungsprogramme (Dokumentenübersicht)“ • Ausgliederung der Informationen zum Ablauf der Evaluierung im Zertifizierungsverfahren, Regeln und Randbedingungen in ein separates Schemadokument BSZ-Evaluierungsprozess [BSZ-EP] • Anpassung der Unparteilichkeit und Unabhängigkeit der Prüfstelle und der jeweiligen Evaluatorinnen bzw. Evaluatoren • Anpassung der Anforderungen für Antragsteller • Einführung des Geltungsbereichs „Allgemeine Netzwerkkomponenten und eingebettete IP-vernetzte Geräte“ • Anpassungen des Verfahrens zur Anerkennung • Anpassungen der Nachmeldung von Evaluatorinnen bzw. Evaluatoren
1.2	01.05.2023	Anerkennungsstelle SZ 12	Revision: • Redaktionelle Änderungen • Neustrukturierung Kapitel 4 • Gendergerechtes Wording
2.0	01.10.2023	Anerkennungsstelle SZ 12	Revision: • EN 17640 [FiT CEM] als grundlegende Evaluierungsmethodologie eingeführt • Geltungsbereich Highspeed Konnektor (HSK) für die Telematikinfrastruktur hinzugefügt • Entfernen der Abbildung 1: Dokumentenübersicht (Zertifizierungs- und Anerkennungsprogramm) in Kapitel 1.1 und entsprechende Anpassung im Kapitel. • Überarbeitung der Literaturangaben und der Zitate der Rechtsnormen. • Redaktionelle und strukturelle Anpassungen
2.1	01.07.2024	Anerkennungsstelle SZ 12	Revision: • Kompetenzbereich im Geltungsbereich BSZ Komponenten im HAN des SMGW hinzugefügt • Anpassung der Nomenklatur bezüglich Geltungsbereich in Kompetenzbereich im Geltungsbereich BSZ
2.2	01.11.2024	Anerkennungsstelle S 21	Revision: • Änderung der Referenzen der VB-Stellen zu VB-Prüfstellen

Tabelle 1: Änderungshistorie

Inhalt

1 Einleitung

Die Anerkennung einer Prüfstelle wird auf Veranlassung der Inhaberin oder des Inhabers oder der Geschäftsleitung einer Stelle durchgeführt.

Anerkannt werden Stellen, die von natürlichen oder juristischen Personen des Privatrechts betrieben werden. Hinsichtlich staatlicher Prüfstellen gelten ggf. abweichende Regelungen.

1.1 Zielsetzung und Eingliederung der BSZ-Prüfstellen

Dieses Dokument beinhaltet verpflichtende Anforderungen und weitere wichtige Informationen und Regelungen als Ergänzung zu dem übergeordneten Dokument „Verfahrensbeschreibung zur Anerkennung von Prüfstellen“ [VB-Prüfstellen] und richtet sich an Antragsteller, die im Bereich der Beschleunigten Sicherheitszertifizierung anerkannt werden möchten.

Es werden die speziellen Anforderungen mit detaillierten Hinweisen zu Verfahrensabläufen benannt, die ein Antragsteller berücksichtigen muss. An den entsprechenden Stellen im Dokument wird auf weitere Dokumente, Formulare oder weitere Hilfsmittel hingewiesen. Zum Beispiel sind die detaillierten Anforderungen und Hinweise zum Ablauf eines Evaluationsprozesses im untergeordneten Dokument „Programm [BSZ-Prüfstellen]: BSZ-Evaluierungsprozess“ [BSZ EP] geregelt.

Die Beschreibung der verschiedenen Dokumentenkategorien befindet sich in der übergeordneten „Verfahrensbeschreibung zur Anerkennung von Prüfstellen“ [VB-Prüfstellen].

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

2 Anerkennungsprogramm

Das hier beschriebene Anerkennungsprogramm bietet die Möglichkeit der Anerkennung als Prüfstelle für die Beschleunigte Sicherheitszertifizierung (kurz BSZ-Prüfstelle).

Die Beschleunigte Sicherheitszertifizierung im BSI stellt einen schlanken Ansatz zur Zertifizierung von IT-Produkten dar. Ziel der BSZ ist, die Dauer der einzelnen Produktzertifizierungsverfahren relativ gering und insbesondere planbar zu gestalten. Dies wird zum einen durch Vermeidung von Formalismen und Kommunikationsschleifen und zum anderen durch den Einsatz von hochqualifizierten Expertinnen und Experten für die Durchführung von Prüfschritten erreicht.

Die BSZ setzt dazu die europäische Norm EN 17640 „Zeitlich festgelegte Cybersicherheitsevaluations-methodologie für IKT-Produkte“ [FiT CEM] mit der Vertrauenswürdigkeitsstufe „hoch“ um. Kern des BSZ-Verfahrens ist die Evaluierung mit vier Prüftätigkeiten: Prüfung der Installationsdokumentation, Prüfung der Konformität, Prüfung durch Penetrationstests und die Bewertung der Implementierung verwendeter kryptographischer Algorithmen. Der verfügbare Gesamtaufwand für diese Prüftätigkeiten und die dadurch entstehende Gesamtprüfdauer ist begrenzt und hängt von der Komplexität des IT Produktes ab. Die Gesamtprüfdauer wird im Rahmen der Auftaktbesprechung abschließend ermittelt und liegt grundsätzlich im Bereich von 15 bis 60 Personentagen bei einem Erstverfahren. Bei Wiederholungen, wie z. B. einer Rezertifizierung, kann der Zeitaufwand deutlich geringer sein. Die konkrete Verteilung des verfügbaren Gesamtaufwands auf die einzelnen Prüftätigkeiten obliegt der Prüfstelle.

Das Programm der BSZ ist in Kompetenzbereiche unterteilt, für die jeweils eigene Anforderungen an Prüfstellen und Durchführung der Evaluierung gelten können.

Unabhängig von den Kompetenzbereichen muss eine BSZ-Prüfstelle nachweisen, dass sie alle Anforderungen

- aus der „Verfahrensbeschreibung zur Anerkennung von Prüfstellen“ [VB-Prüfstellen],
- der DIN EN ISO/IEC 17025 in seiner jeweils gültigen Fassung,
- dem hier vorliegenden Dokument „Anerkennung von Prüfstellen: Programm im Bereich Beschleunigte Sicherheitszertifizierung (BSZ)“ [BSZ-Prüfstellen] inklusive der untergeordneten Dokumente wie „Programm [BSZ-Prüfstellen]: BSZ-Evaluierungsprozess“ [BSZ-EP] erfüllt.

Sie muss außerdem nachweisen, dass

- sie die fachlichen Kenntnisse für Prüfungen im jeweiligen Kompetenzbereich besitzt,
- sie die Prüfungen sowohl fachlich mit der erforderlichen Qualität als auch formal mit der nötigen Unabhängigkeit und Unparteilichkeit sowie Zuverlässigkeit durchführt,
- sie ein Informationssicherheitsmanagementsystem (ISMS) entsprechend dem Dokument „Anforderungen an die Sicherheit von Stellen“ [AS-Stellen] betreibt. Dabei ist grundsätzlich die Sicherheitsanforderung „normal“ anzusetzen. Bei Evaluierungen von Produkten mit Kryptoaspekten sind die Sicherheitsanforderungen als „hoch“ anzusetzen. Sofern die Unterlagen nur auf IT bearbeitet werden, können die Anforderung „hoch“ auch auf die IT selbst beschränkt werden.

Evaluierungen dürfen grundsätzlich nur von Evaluatorinnen bzw. Evaluatoren durchgeführt werden, deren Fachkompetenz im Rahmen einer Kompetenzfeststellung für die BSZ durch das BSI festgestellt wurde. Die Prüfstelle muss nachweisen, dass sie mindestens

- drei kompetente Evaluatorinnen bzw. Evaluatoren beschäftigt.

Davon müssen

- mindestens zwei Personen die Fachkompetenz im Kompetenzbereich BSZ-Evaluator sowie

- mindestens eine Person die Fachkompetenz im Kompetenzbereich BSZ-Evaluator für Kryptographie nachgewiesen haben.

Hierfür sind die Regelungen der „Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen“ [VB-Personen] und die Anforderungen zur „Kompetenzfeststellung: Programm im Bereich Beschleunigte Sicherheitszertifizierung (BSZ)“ [BSZ-Evaluatoren] zu beachten.

Falls für die Evaluierung die Unterstützungsleistung von Fachexperten und Fachexpertinnen, die keine BSZ-Evaluatoren bzw. Evaluatorinnen sind, notwendig ist, muss die Zertifizierungsstelle vorab über dieses Vorgehen informiert werden und dem Einsatz zustimmen.

2.1 Kompetenzbereich im Geltungsbereich BSZ – Allgemeine Netzwerkkomponenten und eingebettete IP-vernetzte Geräte

Der Kompetenzbereich „Allgemeine Netzwerkkomponenten und eingebettete IP-vernetzte Geräte“ umfasst eine große Bandbreite von Produkten. Gemeinsam haben diese Produkte, dass sie über Netzwerkschnittstellen mit der Außenwelt kommunizieren. Beispiele für typische Produkte hier sind IP basierte Netzwerk-Router, eingebettete und vernetzte industrielle Steuerungsgeräte oder mobile Handhelds für Spezialaufgaben. Für die BSZ steht in diesem Bereich die Prüfung Sicherheitsleistung der IT-Produkte über die Netzwerkschnittstellen im Fokus.

Für die Anerkennung in diesem Kompetenzbereich muss die Prüfstelle nachweisen, dass sie die Kompetenz und die Ausstattung nach dem Stand der Technik hat, um alle für die Evaluierung nötigen IT-Sicherheitsuntersuchungen durchzuführen. Zu den Prüfaufgaben gehören

- Untersuchung von IT-Dokumentationen, Konzepten, Richtlinien und Plänen,
- Funktionstests von Netzwerkschnittstellen und -diensten,
- Penetrationstests von IT-Produkten, insbesondere über Netzwerkschnittstellen,
- Penetrationstests von typischen über die Netzwerkschnittstellen bereitgestellten Diensten und Funktionen (z.B. administrative Weboberflächen, Firewalls)
- Funktions- und Robustheitstests typischer kryptographischer Funktionen von IP-vernetzten Geräten,
- Abschätzung von Schadenspotenzialen und Risiken im Rahmen einer nachvollziehbaren,
- Einstufung der Kritikalität identifizierter Mängel.

2.2 Kompetenzbereich im Geltungsbereich BSZ – Highspeed Konnektor (HSK) für die Telematikinfrastruktur

Ein HSK ist eine performante und skalierbare Lösung für die Anbindung an die Telematikinfrastruktur des deutschen Gesundheitswesens (TI) und die Nutzung ihrer Anwendungen. Zertifikate in diesem Kompetenzbereich sind ausschließlich für den Zulassungsprozess für Highspeed Konnektoren bei der gematik GmbH gedacht.

Für die Anerkennung in diesem Kompetenzbereich muss die Prüfstelle nachweisen, dass sie die Kompetenz und die Ausstattung nach dem Stand der Technik erfüllt, um alle für die Evaluierung nötigen IT-Sicherheitsuntersuchungen durchzuführen. Die Anforderungen entsprechen denen aus Abschnitt 2.1 Kompetenzbereich im Geltungsbereich BSZ – Allgemeine Netzwerkkomponenten und eingebettete IP-vernetzte Geräte und eine entsprechende Anerkennung kann übertragen werden.

2.3 Kompetenzbereich im Geltungsbereich BSZ – Komponenten im HAN des SMGW

Dieser Kompetenzbereich umfasst die Komponenten im Home-Area-Netzwerk (HAN) des Smart-Meter-Gateway (SMGW), die nach der TR-03109-5 Kommunikationsadapter ihre IT-Sicherheit durch ein BSZ-Zertifikat nachweisen müssen.

Für die Anerkennung in diesem Kompetenzbereich muss die Prüfstelle nachweisen, dass sie die Kompetenz und die Ausstattung nach dem Stand der Technik erfüllt, um alle für die Evaluierung nötigen IT-Sicherheitsuntersuchungen durchzuführen. Die Anforderungen entsprechen denen aus Abschnitt 2.1 Kompetenzbereich im Geltungsbereich BSZ – Allgemeine Netzwerkkomponenten und eingebettete IP-vernetzte Geräte und eine entsprechende Anerkennung kann übertragen werden.

3 Verfahren zur Anerkennung von BSZ-Prüfstellen

3.1 Zusätzlich notwendige Unterlagen zur Beantragung

Notwendige Unterlagen zur Beantragung der Anerkennung sind in der Verfahrensbeschreibung [VB-Prüfstellen] beschrieben.

Folgende zusätzliche Unterlagen müssen dem Antrag auf Anerkennung beigefügt werden:

- Systemdokumentation Informationssicherheitsmanagement: Dokumentation des Informationssicherheitsmanagementsystems (inkl. Netztopologie) und materieller Sicherheit (inkl. Lageplan der Räumlichkeiten),
- Stellungnahme zum Informationssicherheitsmanagement: Eine schriftliche Stellungnahme zu allen Einzelaspekten der „Anforderungen an die Sicherheit von Prüfstellen“ mit den Informationen darüber, durch welche Maßnahmen der Antragsteller die Einzelaspekte der Anforderungen erfüllt und an welchen Stellen in der ISMS-Dokumentation die Maßnahmen dokumentiert sind,
- Benennung von drei kompetenten Evaluatoren bzw. Evaluatorinnen, von denen mindestens ein Evaluator oder Evaluatorin die Anforderungen des BSZ-Evaluators für Kryptographie erfüllt, sowie Nachweise über die entsprechende Fachkompetenz.

Die Anerkennung als BSZ-Prüfstelle kann nur in Verbindung mit einem von dieser Prüfstelle durchgeführten BSZ-Produktzertifizierungsverfahren erfolgen. Im Rahmen dieses Erstverfahrens wird die Fachkunde der Prüfstelle sowie die Kompetenz der in diesem Verfahren aktiv eingesetzten Evaluatoren bzw. Evaluatorinnen im jeweiligen Kompetenzbereich abschließend durch das BSI beurteilt. Die Verfahren zur Anerkennung und zur Produktzertifizierung laufen grundsätzlich parallel. Daher ist eine zeitliche Nähe beider Anträge, d.h. regelmäßig nicht mehr als 4 Wochen Abstand erforderlich, wobei keine zwingende Reihenfolge vorgeschrieben ist. Das Verfahren für den jeweils ersten Antrag kann beginnen, bevor der zweite Antrag gestellt wurde. Folgt der zweite Antrag dem ersten nicht innerhalb des genannten Zeitraums, wird das BSI das aus dem Erstantrag resultierende Verfahren regelmäßig einstellen.

Ob eine Prüfstelle als BSZ-Prüfstelle fachlich geeignet ist, wird über eine Fachbegutachtung überprüft. Diese besteht aus einer intensiven Prüfbegleitung der Stelle und der Personen in einem BSZ-Produktzertifizierungsverfahren und einer Fachkompetenzfeststellung der Evaluatoren bzw. Evaluatorinnen.

Die Kompetenzfeststellung eines BSZ-Evaluators wird auf Veranlassung einer Prüfstelle (Erstanerkennung) durchgeführt bzw. kann bei einer Nachmeldung von Evaluatoren bzw. Evaluatorinnen einer anerkannten Prüfstelle für ihre Mitarbeiter durchgeführt werden (vgl. Kap. 5.3).

3.1.1 Spezielle Informationen zur Systembegutachtung

Bei einer Systembegutachtung wird überprüft, ob

- die Stelle die Anforderungen der DIN EN ISO/IEC 17025 in seiner jeweils gültigen Fassung erfüllt,
- die Anforderungen an ein Informationsmanagementsystem aus dem Dokument „Anforderungen an die Sicherheit von Stellen“ [AS-Stellen] umgesetzt sind,
- ausreichend Fachkenntnis im Kompetenzbereich vorhanden ist (Fachbegutachtung).

3.1.2 Durchführung der Fachbegutachtungen

Fachbegutachtungen werden zur Kompetenzfeststellung der Stelle und der Evaluatoren bzw. Evaluatorinnen getätigt.

Im Rahmen der Fachbegutachtung wird überprüft,

- ob die Stelle über ausreichende Kenntnisse im und die technische Ausstattung für den Kompetenzbereich verfügt,
- ob die genannten Evaluatoren bzw. Evaluatorinnen über ausreichend Kenntnisse im Kompetenzbereich verfügen.

Die regelmäßigen Fachbegutachtungen der Prüfstelle geben die Möglichkeit, die getroffenen Feststellungen zu bestätigen oder zu widerrufen.

Bei der Erstanerkennung einer Prüfstelle wird die Fachkompetenz der Stelle und der Evaluatoren bzw. Evaluatorinnen mittels einer intensiven Prüfbegleitung festgestellt. Ein reales Verfahren wird dabei durch kompetente Mitarbeiter oder Mitarbeiterinnen des BSI begleitet. Dieses entscheidet, ob die Fachkompetenz der Stelle und der Personen gegeben ist. Die dafür entstehenden Aufwände des BSIs werden der Prüfstelle in Rechnung gestellt und sind durch diese zu tragen. Details zur Kompetenzfeststellung der Personen sind im Dokument [BSZ-Evaluatoren] beschrieben.

Gegebenenfalls kann die Fachbegutachtung auch anhand eines sogenannten Schattenverfahrens festgestellt werden. Dabei führt eine andere als die beauftragte Prüfstelle oder das BSI selbst eine Evaluierung des real zu prüfenden Produkts durch.

3.1.3 Durchführung der Begutachtung des Informationssicherheitsmanagementsystems

Im Rahmen der Systembegutachtung wird die Erfüllung der Anforderungen an das Informationssicherheitsmanagementsystem überprüft. Die Anforderungen sind in dem nicht öffentlichen Dokument [AS-Stellen] beschrieben.

4 Aufrechterhaltung der Anerkennung

4.1 Durchführung der (Prüf-)Tätigkeiten im betreffenden Programm

Zur Aufrechterhaltung der Anerkennung und zur sachgerechten Durchführung von Evaluierungen im Programm BSZ muss die Prüfstelle die Anforderungen an die Abläufe der Evaluierung im Rahmen der Beschleunigten Sicherheitszertifizierung (siehe [BSZ-EP]) sowie zur Reanerkennung einhalten. Darüber hinaus sind die Anforderungen aus Kap. 5 „Spezielle Rahmenbedingungen“ einzuhalten.

4.2 Reanerkennung

Spätestens fünf Monate vor Ablauf der Anerkennung muss ein erneuter Antrag auf Anerkennung gestellt werden, damit die Anerkennung lückenlos fortgeführt werden kann.

Auf eine Fachbegutachtung im Rahmen der Systembegutachtung kann ggf. verzichtet werden, wenn die Prüfstelle im vorhergehenden Anerkennungszeitraum mindestens zwei Verfahren im Programm durchgeführt und die Ergebnisse im Abschlussgespräch verteidigt hat.

5 Spezielle Rahmenbedingungen

5.1 Weitere Regelungen der Zusammenarbeit

Bei der Erstellung und Überarbeitung von AIS sind die Prüfstellen verpflichtet, sich am Kommentierungsprozess zu beteiligen.

Die Prüfstelle muss für Fachbegutachtungen oder für Audits im Rahmen der Anerkennungsabkommen den Begutachterinnen und Begutachtern sowie Auditorinnen und Auditoren Einblick in Evaluierungsergebnisse und Prüfberichte ermöglichen. Die BSZ-Evaluatorinnen und Evaluatoren sowie Fachexpertinnen und Fachexperten der Prüfstelle müssen für Fachinterviews durch die Begutachterinnen und Begutachter des BSI sowie die Auditorinnen und Auditoren im Abkommen zur Verfügung stehen. Die Evaluierungsverträge mit Herstellern müssen dies ohne spezifische Vertraulichkeitsvereinbarung (NDA) ermöglichen, da die Begutachter Mitarbeiterinnen und Mitarbeiter des BSI oder der Partnerbehörden in den Anerkennungsabkommen sind. Die Vergabe von Unteraufträgen ist nicht zulässig.

Da die Prüfstelle durch den Anerkennungsbescheid mit dem BSI zur Einhaltung der Vorgaben des Zertifizierungsschemas verpflichtet ist, darf der Evaluierungsvertrag keine Regelungen enthalten die eine sachgerechte Evaluierung und Prüfbegleitung behindern, insbesondere keine Regelungen, die eine Informationsweitergabe zu Erkenntnissen aus der Evaluierung an die Zertifizierungsstelle behindern könnte. Der Vertrag muss berücksichtigen, dass sich in der Auftaktbesprechung oder im laufenden Verfahren neue oder zusätzliche Sachverhalte (z. B. zusätzliche Penetrationstests, Korrekturen und Ergänzungen zum Prüfbericht wie von der Zertifizierungsstelle als erforderlich betrachtet, Workshops) ergeben können, welche die Evaluierungsaufwände beeinflussen.

Weitere Regelungen zur Zusammenarbeit sind in dem Dokument BSZ-EP beschrieben.

5.2 Unparteilichkeit und Unabhängigkeit der Prüfstelle und der jeweiligen Evaluatorinnen bzw. Evaluatoren

Die mit der Evaluierung beauftrage Prüfstelle und die an einer Evaluierung arbeitenden Personen müssen gegenüber der Zertifizierungsstelle ihre Unabhängigkeit von Antragsteller und Hersteller darlegen und ihre Unparteilichkeit versichern. Eine entsprechende Erklärung muss durch den Antragsteller bei Antragstellung eingereicht werden. Hilfestellungen und Prüfungen vor der Antragstellung durch die Prüfstelle müssen in der Erklärung angegeben werden.

Es ist darauf zu achten, dass keine Evaluatorin bzw. kein Evaluator bei der Erstellung involviert werden kann.

Wenn eine vorgesehene Evaluatorin bzw. ein vorgesehener Evaluator, die Projektleiterin bzw. der Projektleiter oder eine andere Mitarbeiterin oder ein Mitarbeiter der Prüfstelle oder deren Vorgesetzten in einer Beziehung zum Hersteller des zu evaluierenden Produkts steht, welche einen Interessenskonflikt hervorrufen könnte, kann die Unabhängigkeit gefährdet sein. Eine solche Gefährdung kann z. B. bei folgenden Konstellationen auftreten:

- Beratung des Herstellers oder Antragstellers hinsichtlich des Produkts (z. B. zur zertifizierenden Konfiguration des Produkts),
- Mitarbeit an der Entwicklung, Herstellung oder dem Vertrieb des Produkts sowie der für die Zertifizierung benötigten Dokumente,
- andere geschäftliche Verbindungen zwischen der Prüfstelle und dem Antragsteller oder Hersteller (z. B. Beratung, Konzeptionierung, Entwicklungsbegleitung, Mutter/Tochter oder Schwester-Beziehung).

Dieser Abschnitt schließt auch vorherige Versionen der letzten zwei Jahre oder Produkte, die sich nur in Details (z. B. zusätzliche Schnittstellen oder Funktionalitäten) vom zu evaluierenden Produkt unterscheiden, mit ein.

Die Feststellung der Unparteilichkeit und Unabhängigkeit durch das BSI ist Voraussetzung für die Annahme eines Zertifizierungsantrags.

Nicht zulässig ist insbesondere:

- ein weisungsbefugter Vorgesetzter, bzw. Vorgesetzte der Evaluatorin oder des Evaluators, der/die an der Entwicklung, der Erstellung von Nachweisen und/oder Beratung zum zu evaluierenden Produkt beteiligt ist oder war.
- eine Mitarbeiterin oder Mitarbeiter der Prüfstelle, die/der an der Entwicklung, der Erstellung von Dokumenten und/oder Beratung zum zu evaluierenden Produkt beteiligt ist oder war und als Projektleiterin bzw. Projektleiter oder Evaluatorin bzw. Evaluator für die Evaluierung eingesetzt wird.

Bei der Erstellung der für die Zertifizierung erforderlichen Dokumente, kann der Antragsteller Beratungsleistungen z. B. bei anerkannten BSZ-Prüfstellen unabhängig von der Evaluierung beauftragen. Diese darf jedoch nicht in die Evaluierung eingebunden sein, um die Unabhängigkeit und Objektivität der Evaluierung nicht zu gefährden.

Die für die Evaluierung innerhalb des BSZ-Verfahrens vorgesehene Prüfstelle kann und soll die Dokumente inklusive der Sicherheitsvorgaben bereits vor Antragsstellung prüfen (siehe Dokument [AIS B4]). Hierbei ist zu beachten, dass als Rückmeldung an den Antragssteller nur eine reine Mängelliste ohne Hinweise zur Behebung der Mängel übergeben werden darf. Die Unabhängigkeit und Objektivität der Evaluierung muss gewährleistet bleiben.

Eine Ausnahme bildet hier die in Dokument [AIS B1] beschriebene Auflistung der kryptographischen Mechanismen (Algorithmen und Kommunikationsprotokolle). Hier kann die Prüfstelle basierend auf Informationen von Antragsteller oder Hersteller bei der Erstellung unterstützen. Zu beachten ist, dass die Unterstützung auf die Zusammenstellung der Liste begrenzt ist und die Unabhängigkeit und Objektivität der Evaluierung gewährleistet bleiben muss. Die Unterstützung bei Erstellung der Auflistung der kryptographischen Mechanismen ist gegenüber der Zertifizierungsstelle anzugeben.

Die für die Evaluierung innerhalb des BSZ-Verfahrens vorgesehene Prüfstelle kann den TOE bereits vor Antragsstellung einer technischen Prüfung mit geringer Prüftiefe und ohne tiefgehende Tests der Sicherheitsfunktionen unterziehen. Hierbei ist das Ziel festzustellen, ob der TOE überhaupt die technische Mindestreife hat, um ein BSZ-Verfahren mit Erfolgsaussichten zu beginnen. Diese Prüfung ist kein Teil der Beschleunigten Sicherheitszertifizierung, insbesondere nicht der Evaluierungsphase. Es ist zu beachten, dass als Rückmeldung nur eine reine Mängelliste ohne Hinweise zur Behebung der Mängel an den Antragsteller übergeben werden darf. Eine solche technische Vorprüfung ist bei Antragstellung gegenüber der Zertifizierungsstelle anzugeben. Die Zertifizierungsstelle kann bei Bedarf Auskunft über Art und Umfang der Vorprüfung und der Rückmeldung verlangen. Die Unabhängigkeit und Objektivität der Evaluierung muss gewährleistet bleiben.

5.3 Meldung weiterer BSZ-Evaluatorinnen bzw. Evaluatoren

Die Prüfstelle hat jederzeit die Möglichkeit, weitere BSZ-Evaluatorinnen bzw. Evaluatoen dem BSI nachzumelden. Dazu ist zu benennen, in welchem Kompetenzbereich die Evaluatorin bzw. der Evaluator tätig sein soll. Bei positiver Bewertung erfolgt zu gegebenen Zeitpunkt eine Fachkundeprüfung durch das BSI (siehe [BSZ-Evaluator]).

Auch bei einer Nachmeldung ist eine abschließende Kompetenzfeststellung im Rahmen eines BSZ-Produktzertifizierungsverfahrens, an dem die betreffende Mitarbeiterin oder Mitarbeiter maßgeblich mitwirken, erforderlich. Eine Nachmeldung ist daher grundsätzlich nur in Verbindung mit einem

entsprechenden Antrag auf BSZ Produktzertifizierung möglich, in dem die zu meldenden Personen namentlich benannt sind. Es dürfen grundsätzlich nur so viele Personen für ein BSZ-Produktzertifizierungsverfahren angemeldet werden, wie typischerweise für die Durchführung des Verfahrens erforderlich sind.

5.4 Arbeitstreffen mit den Prüfstellen

Auf Vorschlag des BSI oder einer Prüfstelle werden Arbeitssitzungen zu spezifischen Fragestellungen durchgeführt.

Hierunter fallen z. B.

- Prüfstellentreffen: Diskussionen Prüfvorgehensweisen und zu Interpretationen, Änderungen des Zertifizierungsverfahrens, Schulung hinsichtlich spezieller Methoden und Werkzeuge, Entwicklungen in internationalen Gremien und Abkommen,
- Workshops zum Qualitätsmanagement,
- Informationsaustausch zum Stand der Technik und zu Angriffsmethoden und Analysen,
- Spezifische Treffen z. B. zu Kryptothemen.

Die Anzahl solcher Arbeitssitzungen wird nach Dringlichkeit und fachlichen Erfordernissen festgelegt. Grundsätzlich sind maximal vier reguläre Prüfstellentreffen im Jahr vorgesehen. In der Regel müssen die Prüfstellen mit zumindest einem für das jeweilige Thema geeigneten Mitarbeiter vertreten sein.

5.5 Verfahren bei Mängel in der Evaluierung

Mängel können in folgende Mangelarten eingeteilt werden:

- Terminplanung und -treue
- QS-Mangel
- Mangel an Kenntnissen
- Mangel im Ablauf des Verfahrens
- mangelnde Kenntnisse über den Evaluierungsgegenstand (TOE)/das Produkt

Mängel und/oder nicht nachvollziehbare Aspekte in einem Prüfbericht werden durch die Zertifiziererin oder Zertifizierer in einem Review-Protokoll oder im Protokoll eines Workshops festgehalten. Alle Mängel- bzw. Kommentierungspunkte müssen von der Evaluatorin bzw. dem Evaluator nachgebessert bzw. beantwortet werden.

Eine Eskalation bei erheblichem Mängel in der Prüfdokumentation erfolgt gemäß den rechtlichen Vorgaben.

6 Referenzen und Glossar [Verzeichnisse]

Das Dokument Verzeichnisse als Nachschlagewerk für Interessenten und Beteiligte an Zertifizierungs- und 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.