Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Anerkennung von Prüfstellen: Programm zur Anerkennung als Prüfstelle im Bereich NESAS

NESAS-Prüfstellen

Version 1.3 vom 01.10.2024

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	01.07.2022	Anerkennungsstelle SZ12	Erstausgabe
1.1	01.10.2023	Anerkennungsstelle SZ12	Revision: • Redaktionelle Änderungen • Gendergerechte Sprache • Fußzeile Seit 2 Korrektur der Telefonnummer • Tabelle 1 Korrektur Dokumentenverweis in VB-Produkte.PD • Abschnitt 1.1: Es richtet sich insbesondere an die Antragsteller, die sich dafür entschieden haben, eine Anerkennung im Bereich NESAS durchführen zu lassen. • Kapitel 4.1.3 Korrektur Tabelle 5 Zeile 2
1.2	01.02.2024	Anerkennungsstelle SZ12	Revision: • Anpassung Kapitel 3.2.2 zur Betrachtung des IMS • 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 • Überarbeitung Kapitel 6 Glossar
1.3	01.10.2024	Anerkennungsstelle S 21	Revision: • Unterbeauftragung von NESAS-Prüfstellen klargestellt • VB-Stellen durch VB-Prüfstellen ersetzt • Redaktionelle und strukturelle Anpassungen

Inhaltsverzeichnis

Tabellenverzeichnis

1 Einleitung

Die Anerkennung einer Prüfstelle[1] wird auf Veranlassung der inhabenden Person 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 NESAS Prüfstellen

Dieses Dokument beinhaltet detaillierte Anforderungen und weitere Informationen als Ergänzung zur übergeordneten „Verfahrensbeschreibung zur Anerkennung von Prüfstellen“ [VB-Prüfstellen]. Es richtet sich insbesondere an die Antragstellenden, die sich dafür entschieden haben, eine Anerkennung im Bereich NESAS durchführen zu lassen.

Es werden die speziellen Anforderungen mit detaillierten Hinweisen zu Verfahrensabläufen benannt, die eine antragstellende Person berücksichtigen muss. An den entsprechenden Stellen im Dokument wird z. B. auf Formulare oder weitere Hilfsmittel hingewiesen, die besonders bei einer Erstzertifizierung hilfreich sind.

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

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

1 Englischer Begriff bzw. Abkürzung "Evaluation Facility" or "IT-Security Evaluation Facility", ITSEF

2 Anerkennungsprogramm

Das „Network Equipment Security Assurance Scheme“ (NESAS) ist ein Rahmenwerk zur Gewährleistung und Verbesserung der Sicherheit in der Mobilfunkbranche. NESAS schafft damit eine Basis zur Bewertung definierter Sicherheitseigenschaften von IT-Komponenten, die der Bereitstellung mobiler Netzinfrastruktur dienen, im folgenden Netzwerkprodukte genannt.

Zum Nachweis müssen entsprechende Netzwerkprodukte in Übereinstimmung mit vorab auditierten Entwicklungs- und Lebenszyklusprozessen durch den Hersteller entwickelt werden. Anschließend wird in einer Evaluierung in einer Prüfstelle die Erfüllung der auditierten Prozesse sowie produktspezifischen Sicherheitsanforderungen nachgewiesen.

NESAS-Evaluierungen dürfen nur durch NESAS-Evaluatoren durchgeführt werden, deren Fachkompetenz im Rahmen einer Kompetenzfeststellung beim BSI festgestellt wurde. Die Anforderungen an die Fachkompetenz von Evaluatoren wird im Dokument „NESAS-Evaluatoren“ [NESAS-Evaluatoren] detailliert beschrieben sind.

2.1 Anforderungen an Prüfstellen im Programm NESAS

Die anerkannte Stelle muss die technischen Fachkompetenzen in den technischen Fachbereichen, in denen NESAS-Evaluierungstätigkeiten angeboten werden, nach dem Stand der Technik vorhalten und nachweisen. Diese Fachkompetenzen beziehen sich sowohl auf die Produkttechnologien als auch die Prüfmethoden.

Für dieses Programmmuss die NESAS-Prüfstelle nachweisen, dass sie alle Anforderungen

- aus der übergeordneten „Verfahrensbeschreibung zur Anerkennung von Prüfstellen“ [VB-Prüfstellen],
- der „Anforderungen an die Sicherheit von Stellen“ [AS-Stellen] sowie
- dem hier vorliegenden Dokument „Anerkennung von Prüfstellen:
  Programm zur Anerkennung als Prüfstelle im Bereich NESAS“ [NESAS-Prüfstellen] erfüllt.

Sie muss außerdem nachweisen, dass

- sie die fachlichen Kenntnisse für Prüfungen im jeweiligen Programm besitzt,
- sie die Prüfungen sowohl fachlich mit der erforderlichen Qualität als auch formal mit der nötigen Unabhängigkeit und Unparteilichkeit sowie Zuverlässigkeit durchführt und
- sie in der Lage ist, Prüfungen nach dem anerkannten Stand der Technik, auf Grundlage des begründeten Einsatzes von Testmitteln (Software und Hardware) durchzuführen.

Zusätzlich sind

- die Regelungen der „Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen“ [VB-Personen] und
- die Anforderungen zur „Kompetenzfeststellung: Programm im Bereich Network Equipment Security Assurance Scheme“ [NESAS-Evaluator] einzuhalten und zu beachten.

3 Verfahren zur Anerkennung von NESAS-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“ [AS-Stellen] 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 mindestens zweierfahrenen NESAS-Evaluatoren sowie Nachweise über die entsprechende Fachkompetenz.

3.2 Spezielle Informationen zur Systembegutachtung

Bei der Systembegutachtung muss zur Erfüllung der DIN EN ISO/IEC 17025 ggf. eine Fachbegutachtung erfolgen, um nachzuweisen, dass ausreichend Fachkompetenz vorhanden ist. Konkretisierte Anforderungen bezüglich der Sicherstellung der Vertraulichkeit, Verfügbarkeit und der Integrität der DIN EN ISO/IEC 17025, werden insbesondere bei der Begutachtung des Informationssicherheitsmanagementsystems des IT-Sicherheitsdienstleisters auf Grundlage des Dokuments „Anforderungen an die Sicherheit von Stellen“ [AS-Stellen] durchgeführt.

3.2.1 Durchführung von Fachbegutachtungen

Fachbegutachtungen werden zur Kompetenzfeststellung der Stelle und der Evaluatoren durchgeführt. Bei der Erstanerkennung einer Prüfstelle im Programm wird die Fachkompetenz der Stelle und der Evaluatoren mittels der in „NESAS-Evaluatoren“ [NESAS-Evaluatoren] festgelegten Fachbegutachtung der Evaluatoren festgestellt. Details zur Kompetenzfeststellung der Personen sind in „NESAS-Evaluatoren“ [NESAS-Evaluatoren] beschrieben.

Eine Fachbegutachtung kann unter anderem wie folgt durchgeführt werden, durch:

- Interviews mit angestellten Personal.
- Begutachtung der technischen Ausstattung.

Im Rahmen der Fachbegutachtung werden insbesondere folgende Aspekte begutachtet:

- Die Fachkenntnisse und Fähigkeiten der eingesetzten Personal.
- Das Vorhandensein und die Nutzung notwendiger technischer Ausstattung zur Durchführung von 3GPP-SCAS-Tests.
- Die Fachkenntnisse und Fähigkeiten zur Durchführung von Konformitätsnachweisbewertungen gemäß NESAS.

Aufgaben der NESAS-Prüfstelle	*Hilfsmittel [Verzeichnisse]*	*Aufgaben der Anerkennungsstelle*
• Fristgerechte Lieferung der für die Begutachtung relevanten Dokumente, Unterlagen und Nachweise (z. B. Verfahrens- und Arbeitsanweisungen für die Durchführung der NESAS-Prüfungen). • Bereitstellung von auskunftsfähigem, fachkundigem Personal während der Begutachtung (z. B. für die NESAS-Prüfungen zuständiges Fachpersonal und für die Abnahme der Prüfergebnisse verantwortliches Personal). • Bei der Fachbegutachtung von Personen müssen alle benannten NESAS-Evaluatoren zur Verfügung stehen. • Ermöglichung des Zugangs zu allen für die Begutachtung relevanten Bereichen und Systemen des Unternehmens. (z. B. Prüflabore, Lagerräume für Prüfgeräte). • Teilnahme an eventuell erforderlichen Prüfungen zur Feststellung der Fachkunde des Prüfpersonals vor Ort oder im BSI (z. B. mündlicher Test, schriftlicher Test oder Versuchsaufbau).	• VB-Produkte.PD • NESAS-Produkte • DIN EN ISO/IEC 17025	• Durchführung der Fachbegutachtung anhand eines Anforderungskatalogs. • Durchführung der Fachbegutachtung in der Prüfstelle mit dem Begutachterteam (bewertet werden die Anforderungen an Verfahren/Prozesse, Räumlichkeiten und Einrichtungen der DIN EN ISO/IEC 17025 [ISO 17025]). • Einbeziehen von Fachexperten des BSI in die Begutachtung • Führen von Aufzeichnungen und Nachweisen zur Durchführung der Fachbegutachtung. • Ziel ist es, die fachliche Kompetenz der Prüfstelle inkl. der Evaluatoren zu bewerten.

Tabelle 1: Aufgaben bei Fachbegutachtung

3.2.2 Durchführung der Betrachtung des Informationsmanagementsystems

Die „Anforderungen an die Sicherheit von Stellen“ [AS-Stellen] konkretisieren Anforderungen der DIN EN ISO/IEC 17025 bezüglich der Sicherstellung von Vertraulichkeit, Verfügbarkeit und Integrität und sind für alle beim BSI anerkannten Prüfstellen im Programm NESAS CCS-GI verbindlich. Im Rahmen der Systembegutachtung wird die Erfüllung der Anforderungen an das Informationssicherheitsmanagement-system überprüft. Dabei ist grundsätzlich die Sicherheitsanforderung „normal“ anzusetzen. Die Anforderungen sind in dem nicht öffentlichen Dokument [AS-Stellen] beschrieben.

Die Prüfstelle kann Prüfeinrichtungen, die nicht unter ihrer ständigen Kontrolle stehen, gemäß den Vorgaben der ISO/IEC EN 17025 und der AS-Stellen einsetzen. Falls darüber hinaus wiederkehrend Prüftätigkeiten durch Personen/Stellen, die nicht unter der dauerhaften Kontrolle des Prüflabors liegen, durchgeführt werden sollen, so sind die Anforderungen in Kapitel 5 zu beachten.

Da die Prüflandschaft im Bereich NESAS derzeit noch im Aufbau ist und die Komplexität nicht abschließend absehbar ist, wird empfohlen, bei möglichen Fallkonstruktionen frühzeitig zur Abklärung von Lösungsmöglichkeiten auf das BSI zuzugehen.

Aufgaben der NESAS-Prüfstelle	*Hilfsmittel [Verzeichnisse]*	*Aufgaben der Anerkennungsstelle*
• Die Prüfstelle muss die Anforderungen an die Sicherheit von Prüfstellen erfüllen und anhand der dokumentierten Regelungen, Festlegungen und Prozesse belegen. Die Nachweise und Dokumentation müssen der Anerkennungsstelle bei der Beantragung vorgelegt werden (s. dazu Kapitel 3.1). Bereitstellung von auskunftsfähigem, fachkundigem Personal für die Begutachtung (z. B. IT-Sicherheitsbeauftragte, Verantwortliche für die Gebäudesicherheit). • Ermöglichung des Zugangs zu allen für die Begutachtung relevanten Bereiche und Systeme des Unternehmens.	• AS-Stellen • Fragenkatalog zu den AS-Stellen • Begutachtungsplan	**Durchführung der Begutachtung gemäß dem Dokument [AS-Stellen]** • Begehung der Räumlichkeiten der Prüfstelle zum Abgleich mit den vorab eingereichten Plänen der Räumlichkeiten und Absicherung. Insbesondere im Hinblick auf Sicherungsmaßnahmen wie EMA, Zutrittspunkte, Wertschutzschränke, Zutrittskontrollmechanismen und potentiellen Schwachstellen in der Absicherung. • Durchführung von Interviews mit fachkundigem Personal (z. B. IT-Sicherheitsbeauftragte, Verantwortliche für die Gebäudesicherheit). • Einsichtnahme in Dokumente (z. B. Schlüssellisten, vertragliche Vereinbarungen mit Sicherheitsdiensten). • Begutachtung der IT-Systeme (z. B. Verschlüsselung, Passwortstärke). • Dokumentation der Feststellungen während der Begutachtung. • Verfassen eines Berichts im Rahmen des Begutachtungsberichts.

Tabelle 2: Aufgaben bei der Begutachtung des Informationssicherheitsmanagementsystems

4 Aufrechterhaltung der Anerkennung

Zur Aufrechterhaltung der Anerkennung und zur sachgerechten Durchführung von Evaluierungen im Programm NESAS muss die Prüfstelle die nachfolgenden Anforderungen an die Abläufe der Evaluierung im Rahmen von NESAS sowie zur Reanerkennung einhalten. Darüber hinaus sind die Anforderungen aus Kap. 5 „Spezielle Rahmenbedingungen“ einzuhalten.

4.1 Anforderungen an den Ablauf der Evaluierung

Im Folgenden wird das Verfahren einer Produktzertifizierung mit den Aufgaben der NESAS-Prüfstelle dargestellt.

4.1.1 Aufgaben in der Vorbereitungsphase einer Evaluierung

Aufgaben der NESAS-Prüfstelle	***Hilfsmittel [Verzeichnisse]***	***Aufgaben des Herstellers/ Antragstellers***	***Aufgaben der Zertifizierungsstelle***
Informationsgespräch: • Hersteller/antragstellende Person über das Verfahren zur Zertifizierung informieren. • Sich über das zu zertifizierende Produkt informieren.	• VB-Produkte.PD NESAS-Produkte • NESAS-Evaluatoren	• Über technische Eigenschaften des Produktes Auskunft geben.	• -
Auftrag des Herstellers zur Konformitätsprüfung prüfen und Vertrag abschließen: • Voraussetzungen zur Auftragsannahme prüfen (z. B. Unparteilichkeit, Personal, Ressourcen, Fähigkeit). • Prüfungsvertrag mit dem Hersteller abschließen.	• DIN EN ISO/IEC 17025	• Prüfvertrag mit der Prüfstelle abschließen.	• -
Prüfplan erstellen: • Prüfungs- und Meilen-steinplan erstellen.	• AIS N2 – Evaluations-methodologie	• -	• -
Optional: • ggf. Unterstützung bei der Änderungsbeschreibung.	• -	**Optional:** • Prüfvertrag prüfen ggf. anpassen.	• -
• -	• -	• -	• Verfahren offiziell eröffnen. • Eine eindeutige Zertifizierungs-ID vergeben und dem Prüfbegleiter der Zertifizierungsstelle des BSI der Prüfstelle und dem Antragsteller mitteilen.

Tabelle 3: Aufgaben in der Vorbereitungsphase einer Evaluierung

4.1.2 Aufgaben in der Evaluierungsphase eines Produktes

Aufgaben der NESAS-Prüfstelle	*Hilfsmittel [Verzeichnisse]*	*Aufgaben des Herstellers / Antragstellers*	*Aufgaben der Zertifizierungsstelle*
Prüfung durchführen und Bericht erstellen: • Prüftätigkeiten zu den geforderten Konformitätsnachweisen aus den Anlagen des Auditreports. • Prüftätigkeiten zu den in NESAS geforderten Prüfaspekten durchführen. • Erstellung des Prüfberichts. • ggf. Kommentare im jeweiligen Review Protokoll beantworten. • ggf. wenn keine Einigung erzielt wird, können Gegenargumente eingebracht werden. • ggf. telefonisch klären oder ein persönliches Gespräch führen.	• AIS N2 – Evaluations-methodologie	**Optional:** • Teilnahme an Prüfungs-besprechungen und Workshops zu strittigen Fragen, Prüfergebnissen etc.	• Die Prüfung durch Begutachtung und mit schriftlichen Kommentaren zum Prüfbericht begleiten.
Finalen Prüfbericht erstellen: • Interne Qualitätssicherung der Prüfberichte durchführen. • Die prüfenden Personen bestätigen mit ihrer Unterschrift die inhaltliche Vollständigkeit und Richtigkeit der technischen Prüfergebnisse und der QMB für die Einhaltung des QM-Systems. • Erstellung einer finalen Version des Prüfberichts nach Kommentierung durch die Zertifizierungsstelle. • Prüfbericht mit ggf. relevanten Zusatzdokumenten an die Zertifizierungsstelle verschicken.	• -	• -	• -
• -	• -	• -	• Den Bericht abnehmen und dies schriftlich bestätigen.

Tabelle 4: Aufgaben in der Evaluierungsphase eines Produktes

4.1.3 Aufgaben in der Zertifizierungsphase eines Produktes

Aufgaben der NESAS-Prüfstelle	*Hilfsmittel [Verzeichnisse]*	*Aufgaben des Herstellers / Antragstellers*	*Aufgaben der Zertifizierungsstelle*
Optional: • Entwurf des Zertifizierungsreports. • ggf. Entwurf des Zertifizierungsreports kommentieren.	• -	• -	• Zertifizierungsbescheid erteilen. • Zertifizierungsurkunde und Zertifizierungs-report erstellen.
• Archivierung der Unterlagen. • Alle prüfungsrelevanten Nachweise archivieren.	• VB-Prüfstellen	• Prüfgegenstand archivieren.	• -

Tabelle 5: Aufgaben in der Zertifizierungsphase eines Produktes

4.2 Reanerkennung

Fünf Monate vor Ablauf der Anerkennung muss ein erneuter Antrag auf Reanerkennung gestellt werden, damit gewährleistet werden kann, dass die Anerkennung lückenlos fortgeführt wird. Das Verfahren zur Reanerkennung verläuft grundsätzlich wie eine Erstanerkennung. In Einzelfällen kann von einer Fachbegutachtung abgesehen werden, wenn die Prüfstelle ihre Fachkompetenz anderweitig nachgewiesen hat und dies durch den entsprechenden Fachexperten des BSI bestätigt wurde.

5 Spezielle Rahmenbedingungen

5.1 Weitere Regelungen zur Zusammenarbeit

1. Die Prüfstelle muss die prozessspezifischen Anforderungen gemäß Kapitel 4.1 „Anforderungen an den Ablauf der Evaluierung“ einhalten und ist gegenüber der Produktzertifizierungsstelle verpflichtet, Auskünfte zum Ablauf und Inhalt laufender Evaluierungsverfahren zu erteilen.

2. Die Prüfstelle teilt der Produktzertifizierungsstelle umgehend mit, wenn es zu Verzögerungen im geplanten Ablauf kommen sollte. Sie passt den Zeitplan an und stimmt diesen ab. Sollte dieser neue Zeitplan der Zertifizierungsstelle nicht unverzüglich zur Verfügung gestellt werden, kann eine zeitnahe Bearbeitung der Prüfergebnisse durch die Zertifizierungsstelle nicht erfolgen. Die Zertifizierungsstelle setzt die antragstellende Person in Kenntnis und kann ein Mahn- und Aussetzungsverfahren einleiten.

3. Die Prüfstelle ist für die technische Korrektheit und für die wahrheitsgemäße Dokumentation ihrer Prüfergebnisse verantwortlich.

4. Die Archivierung des Evaluierungsgegenstandes nach Abschluss der Evaluierung erfolgt grundsätzlich nach Vorgaben der Zertifizierungsstelle des BSI unter Berücksichtigung der Stellungnahme des Herstellers. In der Regel erfolgt die Archivierung des Prüfgegenstands beim Hersteller.

5. Bei der Erstellung und Überarbeitung von Anwendungshinweise und Interpretationen zum Schema (AIS) sind die Prüfstellen verpflichtet, sich am Kommentierungsprozess zu beteiligen.

6. Die Prüfstelle muss für Fachbegutachtungen und für Audits im Rahmen der Anerkennungsabkommen den Begutachtern/Auditoren Einblick in Evaluierungsergebnisse und Prüfberichte ermöglichen. Die NESAS-Evaluatoren und Fachexperten der Prüfstelle müssen für Fachinterviews durch die begutachtenden Personen des BSI bzw. die Auditoren im Abkommen zur Verfügung stehen. Die Evaluierungsverträge mit Herstellern müssen dies ohne spezifische Vertraulichkeitsvereinbarung (NDA) ermöglichen, da die Begutachter des BSI oder der Partnerbehörden in den Anerkennungsabkommen sind.

7. Das Product under Evaluation (PuE) muss grundsätzlich in den Räumlichkeiten der Prüfstelle aufgestellt und evaluiert werden.

8. Unter den folgenden Bedingungen ist eine Produktprüfung auch außerhalb der Räumlichkeiten der anerkannten Prüfstelle möglich:

   - Die andere Einheit wird als weiterer Standort der Prüfstelle anerkannt. Die entsprechende Erweiterung der Anerkennung ist zu einem beliebigen Zeitpunkt möglich. Bei der Erweiterung kann die Akkreditierung der anderen Einheit als Nachweis berücksichtigt werden, sofern diese geeignet ist. Ist sie nicht vollständig geeignet, so ist der erfolgreiche Abschluss der entsprechenden Delta-Prüfungen bei der anderen Einheit (z.B. Kompetenz, AS-Stellen) notwendig.

   - Die andere Einheit kann durch eine reguläre Unterbeauftragung in Evaluierungen eingebunden werden, wenn diese ihrerseits beim BSI anerkannt ist.

   - Für alle Fälle ist zwingend der Nachweis der Unparteilichkeit durch das Prüflabor notwendig.

9. Die Verwendung von Testequipment außerhalb der Räumlichkeiten der Prüfstelle muss 6 Wochen vor der Evaluierung mit der Zertifizierungsstelle und der Hersteller abgeklärt werden. Es müssen angemessene Sicherheitsmaßnahmen zum Schutz des PuE, vertraulicher Informationen und der Expertise des Evaluatoren getroffen werden. Bei Verbleib des PuE oder von vertraulichen Unterlagen in der externen Stelle, z. B. unbeaufsichtigt über Nacht, müssen angemessene Maßnahmen zum Schutz getroffen werden. Wird die Testdurchführung am PuE z. B. aufgrund von Nichtverfügbarkeit von Testequipment, unterbrochen, so müssen Maßnahmen zur Sicherstellung und Neueinrichtung der verwendeten Konfiguration des Testequipments und des PuE getroffen werden. Die Evaluatoren sind für

die Durchführung und für die Ergebnisse solcher extern durchgeführten Tests verantwortlich. Wird extern genutztes Testequipment durch Betriebspersonal (Operator) gesteuert, z. B. bei maßgeschneiderten Geräten, müssen die Evaluatoren bei der Durchführung vor Ort dabei sein und das Betriebspersonal in der Bedienung und Zielsetzung der einzelnen Schritte anweisen. Die Evaluatoren müssen dazu über die notwendigen Kenntnisse zum jeweiligen PuE, zur Art des durchzuführenden Tests, zum eingesetzten Testequipment und dessen Verwendung verfügen.

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

11. Bei der Aktualisierung und Ergänzung des ETR sind die inhaltlichen Änderungen kenntlich zu machen, z. B. in dem mit Änderungsmarkierungen gearbeitet wird. In den gelieferten PDF-Dokumenten müssen die Änderungsmarkierungen sichtbar sein. Dies dient der Beschleunigung der Durchsicht beim Zertifizierer.

12. Prüfberichte enthalten die Namen aller, an der Erstellung des ETR beteiligten, Evaluatoren der Prüfstelle und unterstützenden Fachexperten der Prüfstelle oder ggf. beauftragten Fachexperten.

13. Die Prüfstelle muss bei Übersendung neuer Versionen von Dokumenten, insbesondere des ETR, stets die Änderungen zur Vorgängerversion kenntlich machen.

14. Die abschließende Fassung des ETR (sowohl mit positivem wie negativem Ergebnis) wird

    - von dem für das Evaluierungsprojekt verantwortlichen Projektleitung oder der Prüfstellenleitung mit dem bestimmten Wortlaut (siehe Fußnote) händisch unterzeichnet und
    - von den Qualitätsmanagementbeauftragten (QMB) der Prüfstelle mit dem bestimmten Wortlaut (siehe Fußnote) händisch unterzeichnet und dem BSI zugestellt.[2]
    - Anmerkung: Die Unterzeichnung des Zertifikates kann erst nach Eingang des unterschriebenen ETR bei der Zertifizierungsstelle erfolgen.

15. In vielen Fällen wird die Evaluierung auf mehrere Evaluatoren aufgeteilt und teilweise werden für bestimmte Tätigkeiten Fachexperten hinzugezogen, z. B. für bestimmte Penetrationstests oder Analysen. Die Prozesse innerhalb der Prüfstelle müssen sicherstellen, dass ein hinreichender Informationsaustausch zwischen den beteiligten Personen ermöglicht und tatsächlich praktiziert wird

[2] **Wortlaut zur Unterschrift des Projektleitenden / Prüfstellenleitenden:**
"Alle an dieser Evaluierung beteiligten Personen sind in der wahrgenommenen Rolle angeführt. Die Unabhängigkeit der Evaluatoren war gewährleistet und sie hatten die für die Prüfung notwendigen Mittel / Ressourcen zur Verfügung. Die Prüfberichte geben die tatsächlichen Fakten und Ergebnisse wieder und sind durch keine anderen Sachverhalte als die zwischen Prüf- und Zertifizierungsstelle bestehenden beeinflusst."
bzw.:
"All persons involved in this evaluation are listed with the role they took. The independence of the evaluators had been ensured and they had all means and ressources necessary for the evaluation performed available. The evaluation reports reflect the actual facts and results and are not being influenced by circumstances other than those defined between evaluation body and certification body."
Wortlaut zur Unterschrift QMB:
"Das Verfahren ist gemäß den im Rahmen der Anerkennung durch das BSI abgenommenen Prozessen der Prüfstelle durchgeführt und eventuelle Abweichungen sind individuell dokumentiert und werden von der Prüfstellenleitung verantwortet. Formale und inhaltliche QS wurde wie auf den Dokumenten vermerkt durchgeführt."
bzw.:
"The procedure has been perfomed according to the processes of the evaluation facility as approved by BSI within the ITSEF Approval and Licensing process. Potential deviations have been individually documented and the head of the ITSEF takes responsibility for this. Formal and content quality checks have been perfomed as indicated on the respective documents."

und diese Personen Zugriff auf alle für sie relevanten Herstellernachweise und Prüfergebnisse haben, um ihre jeweilige eigene Aufgaben erfüllen zu können.

16. Sofern eine Prüfstelle Dritte mit der Bereitstellung von ergebnisrelevanter Infrastruktur für Betrieb und Prüfung des PuE beauftragt, behält sich die Zertifizierungsstelle die Durchführung einer Kompetenzfeststellung bei den mit der Bereitstellung befassten Personen vor.

17. Die Prüfstelle muss der Zertifizierungsstelle ermöglichen, bei Bedarf einzelne Evaluationsschritte in den Räumlichkeiten der Prüfstelle bzw. am Ort der Prüfung zu begleiten.

5.2 Unparteilichkeit und Unabhängigkeit der Prüfstelle und der jeweiligen Evaluatoren

Die mit der Evaluierung beauftragte Prüfstelle und die an einer Evaluierung arbeitenden Personen müssen unparteilich handeln und unabhängig sein und der Zertifizierungsstelle darüber eine auf die geplante Evaluierung bezogene Unparteilichkeits-/Unabhängigkeitserklärung als Anlage zum Antrag abgeben.

Wenn ein vorgesehener Evaluator, die Projektleitung oder ein anderer Mitarbeiter der Prüfstelle oder deren Führungskraft in einer Beziehung zum PuE-Hersteller steht, welche einen Interessenskonflikt hervorrufen könnte, kann die Unabhängigkeit gefährdet sein. Eine solche Gefährdung kann z. B. beifolgenden Konstellationen auftreten:

1. Beratung des PuE-Herstellers hinsichtlich des PuE (z. B. zum PuE-Konzept),
2. Mitarbeit an der Entwicklung, Herstellung oder dem Vertrieb des PuEs sowie der für die Zertifizierung benötigten Nachweise des Herstellers,
3. Beteiligung am Audit der Entwicklungsumgebung des Herstellers,
4. andere geschäftliche Verbindungen zwischen der Prüfstelle und dem PuE-Hersteller (z. B. Beratung, Konzeptionierung, Entwicklungsbegleitung, Mutter/Tochter oder Schwester-Beziehung).

PuE im Sinne dieses Abschnittes sind auch vorherige Versionen der letzten zwei Jahre oder Produkte, die sich nur in Details (z. B. zusätzliche Schnittstellen oder Funktionalitäten) vom PuE unterscheiden.

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

Nicht zulässig sind:

1. Ein weisungsbefugte Führungskraft der Person, die Evaluierungstätigkeiten übernimmt, ist oder war an der Entwicklung, der Erstellung von Nachweisen und/oder Beratung zum zu evaluierenden Produkt beteiligt.
2. Ein mitarbeitende Person der Prüfstelle ist oder war an der Entwicklung, der Erstellung von Nachweisen und/oder Beratung zum zu evaluierenden Produkt beteiligt, ist beim Audit der Entwicklungsumgebung involviert oder wird als Projektleitung eingesetzt oder übernimmt Evaluierungstätigkeiten.

5.3 Meldung weiterer NESAS-Evaluatoren

Die Prüfstelle hat jederzeit die Möglichkeit, weitere NESAS-Evaluatoren als erfahrene, eingearbeitete NESAS-Evaluatoren dem BSI nachzumelden. Die Fachkompetenz der NESAS-Evaluatoren ist geeigneter weitere Nachweise (z. B. Lebenslauf, Teilnahmebescheinigungen von Schulungen) nachzuweisen. Die Prüfstelle hat dafür die Nachweise entsprechend „NESAS-Evaluator“ [NESAS-Evaluator] zu erbringen. Diese Nachweise werden seitens des BSI geprüft und bewertet. Bei positiver Bewertung erfolgt zu gegebenen Zeitpunkt eine Fachkundeprüfung durch das BSI (siehe [NESAS-Evaluator]).

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,
- Workshops zum Qualitätsmanagement,
- Informationsaustausch zum Stand der Technik und zu Angriffsmethoden und Analysen,
- Spezifische Treffen.

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

5.5 Verfahren bei Mängeln 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 (PuE)

Fehler sowie nicht nachvollziehbare Aspekte in einem Prüfbericht werden durch den Zertifizierer in einem Review-Protokoll festgehaltenen. Alle Mängel- bzw. Kommentierungspunkte müssen vom NESAS-Evaluatoren nachgebessert bzw. beantwortet werden.

Eine Eskalation bei Mängeln in Prüfberichten wird in folgenden drei Eskalationsstufen ausgeführt:

1. Eskalationsstufe:

Bei einer hohen Zahl von Kommentierungen behält sich die Zertifizierungsstelle vor, das Review für den Prüfbericht vorzeitig abzubrechen. Dies geschieht mit dem Hinweis, alle Prüfaspekte erneut mit der gebotenen Sorgfalt und geltenden Qualität zu wiederholen. Die Leitung der Zertifizierungsstelle wird hierüber informiert.

Ist eine erste Nachbesserung/Kommentierungsrunde nicht zufriedenstellend erfolgt, wird eine zweite Review-Runde durchgeführt.

Ist auch diese Nachbesserung/Kommentierungsrunde nicht zufriedenstellend, erfolgt ggf. noch eine dritte Review-Runde oder das Verfahren geht in die nächste Eskalationsstufe über.

2. Eskalationsstufe:

Ist die Nachbesserung/Kommentierungsrunde nicht zufriedenstellend, wird in dieser Review-Runde die NESAS--Evaluatoren und die Prüfstellenleitung zu einem Klärungsgespräch zur Zertifizierungsstelle unter Beteiligung der Leitung der Zertifizierungsstelle einberufen.

Mängel werden dann noch einmal genauer diskutiert und abgeklärt. Erarbeitete Lösungen sind nach Abstimmung umzusetzen. Die Anerkennungsstelle wird informiert.

3. Eskalationsstufe:

Ist die nachfolgende Nachbesserung nicht zufriedenstellend, ist ein Abbruch des Prüfverfahrens dem Antragsteller vorzuschlagen oder von der Zertifizierungsstelle einzuleiten.

Die Anerkennungsstelle wird im Rahmen ihrer Überwachungstätigkeit aktiv.

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

7 Weitere Hilfsmittel

7.1 Vorlage für Unabhängigkeits-/Unparteilichkeitserklärung der Prüfstelle als Anlage zum Evaluierungsplan

Angaben zur vorgesehenen Evaluierung:

- Name Antragsteller / PuE-Hersteller: _____
- Bezeichnung des zu evaluierenden PuEs: _____

Angaben zur Unparteilichkeit und Unabhängigkeit:

- Ich erkläre, dass mir mit Ausnahme der nachfolgend genannten Verbindungen keine weiteren Verbindungen (gem. Kapitel 5.2 Satz 1 (Beratung) – 2 (Unterstützung bei Entwicklung)) der für die Durchführung der Evaluierung vorgesehenen Mitarbeiter der Prüfstelle (Namen gemäß o.g. Evaluierungsplanes) zum PuE-Hersteller bekannt sind.
- Folgende Verbindungen bestehen von Mitarbeitern der Prüfstelle zum PuE-Hersteller:
  _____
  (bitte Verbindungen, z. B. Art und Umfang der Beratung oder Entwicklungsunterstützung erläutern und ggf. auf separater Anlage die Konstellation darlegen).
- Folgende Verbindungen (gem. Kapitel 5.2 Satz 3. bestehen zwischen der Prüfstelle und dem PuE-Hersteller:_____
  (bitte Verbindungen erläutern und ggf. auf separater Anlage die Konstellation darlegen).
- Für den Fall, dass Personen der Prüfstelle gem. Kapitel 5.2 Satz 1-3 aktiv waren oder sind, gelten folgende Abhängigkeiten zu den benannten Evaluatoren:
  _____
  (z. B. Vorgesetztenverhältnisse, etc. bitte Verbindungen erläutern und ggf. auf separater Anlage die Konstellation darlegen).
- Es bestehen folgende Mutter/Tochter/Schwester- oder ähnliche Beziehungen zwischen Hersteller und Prüfstelle: _____
  (bitte Verbindungen erläutern und ggf. auf separater Anlage die Konstellation darlegen).

Ich sehe die Unabhängigkeit und die Unparteilichkeit der Prüfstelle trotz der o.g. Angaben nicht gefährdet, weil _____
(bitte begründen).

Ich verpflichte mich, Erkenntnisse, welche die hiermit erklärte Unabhängigkeit und Unparteilichkeit in Frage stellen könnten, der Zertifizierungsstelle des BSI unverzüglich mitzuteilen.

_____ _____

Ort, Datum Name und Unterschrift Leiter Prüfstelle