Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Produktzertifizierung: Programm Network Equipment Security Assurance Scheme (NESAS)

NESAS-Produkte

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	Referat SZ 33	Erstausgabe
1.1	14.12.2022	Referat SZ 33	Revision: • Ergänzung von Bedingungen für die Aufnahme des Verfahrens bzgl. der Audits und Bedingungen für die Durchführung der Evaluierung • Anpassungen die sich aus der Verwendung der NESAS-Zert und weiterer referenzierter Dokumente ergeben • • Redaktionelle Änderungen sowie Präzisierung von Verfahrensschritten
1.2	01.10.2023	Referat SZ 33	Revision: • Überarbeitung Kapitel 3.2 • Präzisierung Aufbewahrungsfristen • Kontaktdaten BSI • Prozessabläufe Überarbeitung • Redaktionelle Überarbeitung
1.3	01.10.2024	Referat S 26	Revision: • Aktualisierung Kapitel 4.1 - Geringfügige Aktualisierungen • Aktualisierung Kapitel 4.2 - Einbeziehung unterschiedlicher Ausführungsumgebungen in das Zertifikat • Überarbeitung der notwendigen Dokumente im Zertifizierungsprozess (Kapitel 3.3.2.2, 3.3.3.2, 3.3.4.2) • Ergänzungen zum Datenaustausch in Kapitel 3.3.3.2 • Redaktionelle Überarbeitung

Tabelle 1 Änderungshistorie

Inhalt

1 Einleitung

Eine Zertifizierung eines Produktes wird auf Veranlassung des Herstellers, Sponsors oder Vertreibers von IT-Produkten durchgeführt. Dieses Dokument richtet sich daher in erster Linie an alle Antragsteller für ein NESAS CCS-GI Sicherheitszertifikat.

1.1 Zielsetzung und Eingliederung des Programms

Dieses Programm beinhaltet detaillierte Anforderungen und Informationen als Ergänzung zum Dokument „Verfahrensbeschreibung zur Zertifizierung von Produkten“ [VB-Produkte.PD] für den Fall, dass sich der Antragsteller entschieden hat, eine Zertifizierung nach NESAS durchführen zu lassen. Der Antragsteller findet hier Informationen zur Durchführung des Verfahrens.

Eine Prüfstelle kann einen Hersteller auf Grundlage dieser Unterlagen zur Vorbereitung über den Ablauf eines Verfahrens informieren.

Es werden konkret die Aufgaben benannt, die ein Antragsteller berücksichtigen muss, um den Regelungen und Anforderungen zum Verfahren gerecht zu werden. An den entsprechenden Stellen im Dokument wird z. B. auf Formulare oder andere Hilfsmittel hingewiesen.

Die Beschreibung der verschiedenen Dokumentenkategorien befindet sich in der übergeordneten „Verfahrensbeschreibung zur Zertifizierung von Produkten, Prozessen und Dienstleistungen“ [VB-Produkte.PD].

2 Zertifizierungsprogramm

Das Programm zur IT-Sicherheitszertifizierung beschreibt die folgenden Zertifizierungsmöglichkeiten:

- Zertifizierung eines IT-Produktes nach „Network Equipment Security Assurance Scheme Cybersecurity Certification Scheme – German Implementation" (NESAS CCS-GI).

Die für das Zertifizierungsprogramm notwendigen und aktuell gültigen Dokumente sind im Dokument „Verzeichnisse" [Verzeichnis] aufgelistet.

Für eine bessere Lesbarkeit wird im nachfolgenden Dokument die Abkürzung NESAS anstelle von NESAS CCS-GI verwendet. Andere NESAS-Varianten werden, sofern referenziert, explizit als solche qualifiziert.

2.1 Zertifizierung der IT-Sicherheit von IT-Produkten nach NESAS

2.1.1 Generelle Aspekte der Zertifizierung nach NESAS

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-Produkten, die der Bereitstellung mobiler Netzinfrastruktur dienen, im folgenden Netzwerkprodukte genannt. Damit ist NESAS CCS-GI ein Zertifizierungsschema für Produkte, die komplett oder in Teilen zum Betrieb von Mobilfunknetzen entwickelt wurden.

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.

Das im BSI angewendete Zertifizierungsverfahren basiert auf dem GSMA-NESAS Bewertungsschema, welches durch die Groupe Speciale Mobile Association (GSMA) entwickelt wurde.

Für bestimmte Verfahrensschritte, Auditangelegenheiten oder Prüftätigkeiten kann es zusätzliche Anforderungen geben. Diese werden in den Anwendungshinweisen und Interpretationen zum Schema (AIS) als separate Dokumente von der Zertifizierungsstelle des BSI veröffentlicht. Themen der AIS-Dokumente sind z. B. verfahrensbezogene Regelungen zum Audit- oder Evaluierungsablauf. Zur Abgrenzung der AIS der Zertifizierung nach Common Criteria (siehe [CC-Produkte]) sind die AIS für die Zertifizierung nach NESAS im Nummernkreis „N#" organisiert, wobei # die laufende Nummer der AIS ist.

Die genannten Dokumente sowie weitere Informationen können von der Webseite des BSI im Themenbereich „Zertifizierung und Anerkennung", Rubrik „Zertifizierung von Produkten" abgerufen werden. Die Dokumente sind in den jeweiligen Auditierungs-, Evaluierungs- und Zertifizierungsverfahren entsprechend ihrer Einstufung (z. B. als Leitfaden oder verbindlich) anzuwenden.

Neben den Regularien muss eine Zertifizierung durch das BSI die Randbedingungen des „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)" [BSIG] einhalten. Daraus resultiert ein Zertifizierungsvorbehalt nach BSIG § 9, Abs. 4 (2) etwa, wenn überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung entgegenstehen. Die Prüfung eines Zertifizierungsvorbehaltes erfolgt grundsätzlich vor Annahme eines Zertifizierungsantrages und abschließend vor der Erteilung eines Zertifikates.

3 Verfahren zur Zertifizierung

3.1 Beteiligte Stellen an einer Zertifizierung

Am Gesamtprozess der Zertifizierung sind vier Stellen beteiligt:

1. **Der Antragsteller**:
   Ein Hersteller, Sponsor oder Vertreiber oder eine Behörde, die ein Zertifikat für ein Netzwerkprodukt erlangen möchten können als Antragsteller agieren.
2. **Das Audit-Team**:
   Das von BSI ausgewählte Audit-Team zur Auditierung der Entwicklungs- und Lebenszyklusprozessen beim Hersteller. Die Auditoren sind vertraglich an das BSI gebunden und für die Durchführung von NESAS-Audits geeignet. Die Regelungen und Prozesse der Auditoren stellen sicher, dass Vertraulichkeit gewahrt ist. Eine spezielle verfahrensbezogene Vertraulichkeitsvereinbarung (NDA) zwischen Antragsteller und Auditor ist auf Grund der Vertragsgestaltung mit dem BSI nicht erforderlich.
3. **Die Prüfstelle**:
   Die vom Antragsteller ausgewählte und für das jeweilige Programm anerkannte Prüfstelle. Anhand der vom BSI veröffentlichten Liste der anerkannten Prüfstellen beauftragt der Antragsteller eine für das Programm geeignete Prüfstelle mit der Durchführung der Evaluierung seines Produktes. Das BSI hat vertragliche Vereinbarungen bzw. verwaltungsrechtliche Nebenbestimmungen mit den anerkannten Prüfstellen zur Durchführung von Evaluierungen im Hinblick auf eine Zertifizierung. Die Regelungen und Prozesse der Prüfstelle stellen sicher, dass die Vertraulichkeit gewahrt ist. Die Befugnis für Mitarbeiter der Prüfstelle bezieht sich auf bestimmte Techniken, Produktgruppen und Prüfaspekte.
4. **Die Zertifizierungsstelle des BSI**:
   Die Mitarbeiter der Zertifizierungsstelle begleiten den Auditprozess sowie die von der Prüfstelle durchgeführte Evaluierung. Die Mitarbeiter der Zertifizierungsstelle nehmen den Auditbericht des Audit-Teams sowie die von der Prüfstelle durchgeführte Evaluierungsbericht ab und fordern, falls notwendig, Nachprüfungen ein. Auf dieser Grundlage wird die Zertifizierungsentscheidung gefällt und ein entsprechender Bescheid ergeht dem Antragsteller.

3.2 Gegenstand der Konformitätsbewertung

Der Gegenstand der Konformitätsbewertung in einem NESAS-Zertifizierungsverfahren besteht aus zwei Objekten, für die festgelegte Anforderungen gelten:

- die zu einem oder einer Klasse von Netzwerkprodukten gehörenden Entwicklungs- und Lebenszyklusprozesse und
- die technischen Eigenschaften von einzelnen oder allen zu einem Netzwerkprodukt gehörenden Funktionseinheiten.

Die Ermittlung zur Einhaltung von festgelegten Anforderungen an die Entwicklungs- und Lebenszyklusprozesse erfolgt durch eine Auditierung und an die technischen Eigenschaften des Netzwerkproduktes durch eine Evaluierung.

Im Programm NESAS der Produktzertifizierung werden grundsätzlich die Ergebnisse aus einer Kombination beider Objekte und den zugehörigen Anforderungen für eine Konformitätsbewertung betrachtet.

3.2.1 Auditierung der Entwicklungs- und Lebenszyklusprozesse

Im Fokus der Auditierung stehen die Entwicklungs- und Lebenszyklusprozesse eines Netzwerkprodukts oder einer Klasse von Netzwerkprodukten mit identischen Prozessen. Hersteller, die Produkte entwickeln und in den Verkehr bringen, müssen geeignete Maßnahmen definieren und umsetzen, um diese Prozesse nach vorgegebenen Sicherheitsanforderungen zu gestalten.

Der Lebenszyklusprozess eines Produktes besteht aus der Produktentwicklung, einer Markteinführung mit dem ersten Release für die kommerzielle Nutzung, geringfügige und umfassende Produktaktualisierungen zur Behebung von Schwachstellen und Anpassungen des Funktionsumfanges sowie dem Lebensende des Produktes. Der initiale Entwicklungsprozess zu Beginn des Lebenszyklus besteht aus den Phasen Planung, Konzeption, Implementierung, Test, Freigabe und Auslieferung (vgl. „Network Equipment Security Assurance Scheme – Overview“ [FS.13]).

Im Audit analysiert ein Audit-Team diese Prozesse eines Herstellers und bewertet, ob die vom Hersteller definierten Maßnahmen zur Umsetzung der Sicherheitsanforderungen angemessen und wirksam sind. Anschließend wird in einem Vor-Ort-Audit überprüft, ob die vom Hersteller definierten Maßnahmen zu den Prozessen auch in der Praxis angewendet werden. Im Audit werden weiterhin Prüfkriterien und Nachweise definiert, welche der Hersteller für die nachgelagerte Evaluierung erbringen muss, um nachweisen, dass die Prozesse für das zu evaluierende Produkt genutzt und umgesetzt wurden.

Das Audit der Entwicklungs- und Lebenszyklusprozesse bildet die Grundlage für eine nachgelagerte Evaluierung des Netzwerkproduktes in einer Prüfstelle. Innerhalb der zeitlichen Befristung des Audits (vgl. Abschnitt 5.4.2.1) können sich mehrere Produkte auf dasselbe Audit als Basis für eine Evaluierung stützen.

3.2.2 Evaluierung des Netzwerkproduktes

Die Evaluierung befasst sich mit der technischen Prüfung des Netzwerkproduktes sowie der Bewertung, ob die Produktentwicklungs- und Lebenszyklusprozesse für das zu evaluierende Produkt eingehalten wurden.

Ein Produkt wird einer Evaluierung durch eine Prüfstelle mit standardisierten Sicherheitstests unterzogen. Die Details der Evaluierung sowie die erforderliche Methodologie werden im Dokument [AIS N2] geregelt. Während der Evaluierung bewertet die Prüfstelle weiterhin, ob die vom Hersteller vorgelegten Nachweise die im Auditbericht definierten Prüfkriterien erfüllen und somit eine Konformität zur Einhaltung von Sicherheitsanforderungen an die Produktenwicklungs- und Lebenszyklusprozesse für das spezifische Netzwerkprodukt gegeben ist.

Der Antragsteller muss eine durch das BSI für das Programm NESAS CCS-GI anerkannte Prüfstelle auswählen und einen Vertrag zur Evaluierung des Netzwerkproduktes mit dieser abschließen. Hinweise zum Evaluierungsvertrag finden sich in Abschnitt 5.3.2.

Die Sicherheitsanforderungen und Testfälle ergeben sich aus standardisierten Netzwerkfunktionalitäten im Mobilfunkbereich und richten sich nach den, durch die 3rd Generation Partnership Project (3GPP) (SA3) definierten, SeCurity Assurance Specifications (SCAS). Das zu prüfende Netzwerkprodukt muss dafür einer durch die 3GPP definierten Produktklasse zugeordnet werden können, für die SCAS-Tests definiert und spezifiziert sind. Weiterhin sind die im Dokument [AIS N2] aufgeführten Voraussetzungen für die Evaluierung gemäß SCAS zu beachten. Kann das Netzwerkprodukt keiner im Dokument [AIS N2] aufgeführten Produktklasse zugeordnet werden, kann keine Evaluierung nach NESAS erfolgen.

Eine wesentliche Bedingung ist, dass die am Ende des Verfahrens im Zertifikat zu bestätigenden Sicherheitseigenschaften im Zusammenhang mit der Wahrung von Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität von zu schützenden Werten (Assets) stehen.

Ein Netzwerkprodukt kann eine Kombination aus Hardware- und Softwarekomponenten oder eine reine Softwarekomponente für eine bestimmte Betriebsumgebung mit definierten Schnittstellen sein. Die Produktzertifizierung nach NESAS adressiert marktfähige Produkte. Es findet keine entwicklungsbegleitende Evaluierung statt.

Voraussetzung für die Evaluierung eines Netzwerkproduktes ist ein gültiges Audit (vgl. Abschnitt 5.4.2.1), welches alle Entwicklungs- und Lebenszyklusprozesse, nach denen das Netzwerkprodukt entwickelt wurde, mit einschließt. Ein Netzwerkprodukt muss den auditierten Entwicklungs- und Lebenszyklusprozessen eindeutig zugeordnet werden können.

3.3 Zertifizierungsprozess

3.3.1 Überblick Zertifizierungsprozess

Die Zertifizierung von Netzwerkprodukten ist in vier Phasen aufgeteilt: die Vorbereitungsphase, die Auditierungsphase, die Evaluierungsphase und die Zertifizierungsphase.

Es müssen grundsätzlich alle vier Phasen durchlaufen werden. Je nach Phase müssen unterschiedliche Nachweise und Informationen gegenüber dem Audit-Team, der Prüfstelle oder der Zertifizierungsstelle durch den Antragsteller/Hersteller erbracht werden. Nach erfolgreichen Abschluss des Zertifizierungsprozesses erfolgt die Vergabe des Zertifikates.

3.3.2 Vorbereitungsphase

3.3.2.1 Allgemeines

In der Vorbereitungsphase erfolgen alle Schritte von der initialen Vorbereitung des Antrages, über die Antragstellung bis hin zur offiziellen Eröffnung des Zertifizierungsverfahrens.

Für die Erstellung der Antragsunterlagen, insbesondere der Anlagen zum Zertifizierungsantrag, kann Hilfestellung aus dem Bereich der Prüfstellen hinzugezogen werden.

Typischer Ablauf im Einzelnen:

Aufgaben Hersteller	*Hilfsmittel*	*Aufgaben Prüfstelle*	*Aufgaben Zertifizierungsstelle*
• Informationen mit beteiligten Stellen austauschen und Informationen über technische Eigenschaften des Produktes bereitstellen	• NESAS-Produkte • AIS N2	• Hersteller über Verfahren informieren • Sich über Produkt und Hersteller informieren	• Prozess und Randbedingungen zur Zertifizierung darlegen
• Auf Verfügbarkeit, grundsätzliche Eignung und Vollständigkeit der erforderlichen Nachweise prüfen	• -	Auftrag Hersteller prüfen: • Voraussetzungen zur Auftragsannahme prüfen (z. B. Unparteilichkeit, Personal, Ressourcen, techn. Umsetzbarkeit der notwendigen gewünschten SCAS-Tests)	• -
• Evaluierungsvertrag mit Prüfstelle abschließen • Der Evaluierungsvertrag regelt die Beauftragung der Prüfstelle zur Durchführung der Evaluierung • Bei der Erstellung des Zeitplanes mitwirken	• DIN EN ISO/IEC17025	• Evaluierungsvertrag mit Antragsteller abschließen	• -

Aufgaben Hersteller	*Hilfsmittel*	*Aufgaben Prüfstelle*	*Aufgaben Zertifizierungs-stelle*
• Bei der Erstellung des Prüfplans mitwirken	• AIS N2	Prüfplan erstellen: • Evaluierungstätigkeiten mit dem Antragsteller vorbereiten/abstimmen	• -
• Antrag inklusive notwendiger Anlagen erstellen	• AIS N1 • AIS N2	• Ggf. unterstützen	• -
• Zertifizierungsantrag stellen • Zertifizierungsantrag gemäß Hinweisen im Antrag ausfüllen, mit Firmenstempel versehen und persönlich unterschreiben und mit den erforderlichen Anlagen an die Zertifizierungsstelle senden (Antrag in Papierform oder elektronisch als Scan an das BSI, Anlagen vorzugsweise elektronisch) • Anm.: Der Antragsteller sollte auch einen PGP-Schlüssel bereitstellen	• Antragsformular • öffentlicher PGP-Schlüssel der Zertifizierungs-stelle des BSI (auf der Webseite verfügbar)	• Mit Antragsteller abgestimmten Entwurf des Evaluierungsplans bereitstellen	• Antragseingang bestätigen • Antrag und Anlagen formal und inhaltlich prüfen • Aussage zur grundsätzlichen Zertifizierbarkeit aus technischer Sicht treffen, vorbehaltlich rechtlicher Rahmenbedingungen
• Terminplanung durchführen und Vorschlag eines Zeitplans erstellen	• AIS N2	• Terminplanung durchführen • Evaluierungsplan erstellen[1] und an Zertifizierungsstelle weiterleiten	• Vorläufige Zeitplanung mit Antragsteller und Prüfstelle abstimmen
• Auf Start des Evaluierungs-verfahrens warten	• -	• Evaluierungsaktivitäten vorbereiten • Ggf. Vertrag anpassen	• Schreiben über den Start des Verfahrens versenden

Tabelle 2 Aufgaben in der Vorbereitungsphase

3.3.2.2 Notwendige Unterlagen für die Vorbereitungsphase

Folgende Nachweise, Informationen und Gegenstände werden vom Antragsteller/Hersteller während des Zertifizierungsprozesses benötigt:

- Zertifizierungsantrag (deutsch oder englisch) mit Anlagen.

Der Zertifizierungsantrag enthält Erklärungen und Hinweise, die für das Ausfüllen behilflich sind.

[1] Der Evaluierungsplan enthält Angaben zur inhaltlichen Durchführung der Evaluierung, der anzuwendenden und vom Antragsteller gewünschten SCAS-Tests sowie zur zeitlichen Planung, den Evaluatoren, ebenso eine Unabhängigkeits- und Unparteilichkeitserklärung und eine Bestätigung, dass die technische Ausstattung der Prüfstelle zur Durchführung der SCAS-Tests ausreichend ist.

3.3.2.3 Antragsformulare

Die Antragsformulare erfragen Angaben, die für den Start des Verfahrens und seine Abwicklung benötigt werden. Das Formular steht auf der Internetseite des BSI in der Rubrik „Zertifizierung und Anerkennung / Zertifizierung von Produkten / Zertifizierung nach NESAS CCS-GI / Dokumente zum Download“ (www.bsi.bund.de/dok/NESAS-Dokumente) zur Verfügung. Das Formular enthält Erklärungen/Hinweise, die zum Ausfüllen behilflich sind.

Dieses Formular bezieht sich ausschließlich auf die NESAS-Zertifizierung eines Netzwerkproduktes.

Wird ein Antrag auf Produktzertifizierung nicht durch den Hersteller, sondern durch einen Sponsor oder Vertreiber des Produktes gestellt, muss dem Antrag eine schriftliche Erklärung des Herstellers beigefügt werden, dass die Mitwirkung im Verfahren und die Bereitstellung der erforderlichen Produktnachweise sichergestellt ist.

Werden prüfungsrelevante Produktteile oder Nachweise durch Dritte entwickelt, bereitgestellt oder verfügt der Antragsteller nicht über die Rechte an allen prüfungsrelevanten Nachweisen oder Teilen, so muss die Mitwirkung der beteiligten Dritten sichergestellt werden. Dazu muss eine Erklärung der dritten Parteien vorgelegt werden, die die Mitwirkung im Verfahren bestätigt. Das Erklärungsschreiben muss darlegen: den Namen der Organisation, die ihre Mitwirkung erklärt, die konkret vereinbarten Mitwirkungs- und Beistellungspflichten sowie eine vollständige Darstellung, auf welche Bestandteile des Evaluierungsgegenstandes der Zertifizierung sich diese Mitwirkung bezieht.

Der Zertifizierungsantrag muss handschriftlich unterzeichnet werden und einen Firmenstempel enthalten. Er kann als Scan per E-Mail an nesas@bsi.bund.de eingereicht werden. Zur Vereinfachung der Handhabung kann der Antrag auch akzeptiert werden, wenn er unterschrieben und eingescannt per E-Mail zur Verfügung gestellt wird. In diesem Fall wird keine Papierversion eingefordert. Die Unterschrift muss händisch sein oder das Formular muss qualifiziert elektronisch signiert (eIDAS) sein.

Die Anlagen sollten in elektronischer Form zugesendet werden. Auf der Internetseite des BSI ist dazu zu den Antragsformularen auch ein öffentlicher PGP-Schlüssel für das o. g. NESAS-Postfach verfügbar. Alternativ zur elektronischen Übermittlung kann der Antrag auch in schriftlicher Form an nachfolgende Adresse gesendet werden:

Bundesamt für Sicherheit in der Informationstechnik
Referat S 26 – Zertifizierungsstelle
Postfach 20 03 63
53133 Bonn

Die Auditoren und die Prüfstelle stellen die Dokumente auf separatem Wege der Zertifizierungsstelle in elektronischer Form zur Verfügung.

3.3.3 Die Auditierungsphase

3.3.3.1 Allgemeines

In der Auditierungsphase erfolgt die Überprüfung der Entwicklungs- und Lebenszyklusprozesse. Ein Audit wird von mindestens zwei Auditoren, dem Audit-Team, durchgeführt. Ein Auditor ist der Teamleiter, dieser ist der Hauptansprechpartner für den Hersteller und die Zertifizierungsstelle.

Sofern das Netzwerkprodukt nach Entwicklungs- und Lebenszyklusprozessen erstellt wurde, für die bereits ein noch gültiges Audit vorliegt, ist in der Auditierungsphase lediglich der Nachweis dieses Audits zu erbringen.

Das Audit der Entwicklungs- und Lebenszyklusprozesse und der daraus resultierende Auditbericht bilden die Grundlage für alle weiteren Evaluierungstätigkeiten in der Prüfstelle und eine daraus folgende Zertifizierung. Aus diesem Grund muss das Audit mit entsprechender Sorgfalt durch den Hersteller

vorbereitet und das Audit-Team während des gesamten Auditprozesses unterstützt werden. Grundlage der Auditierung bilden die im Dokument [AIS N1] referenzierten GSMA-Dokumente und Ergänzungen sowie die ISO/IEC 27007. Der Auditprozess besteht aus einer Prüfung der Prozessdokumentation und einer anschließenden Vor-Ort-Auditierung an einem durch den Antragsteller explizit benannten Standort, an dem die entsprechenden Entwicklungs- und Lebenszyklusprozesse implementiert sind. Bei der Auswahl des Auditstandorts sind die in der [AIS N1] festgelegten Bedingungen für die Durchführung des Vor-Ort-Audits zu beachten. In begründeten Ausnahmefällen kann bei Wiederholungs-Audits nach Rücksprache und Genehmigung durch die Zertifizierungsstelle ersatzweise ein Fernaudit durchgeführt werden, sofern hierbei im konkreten Fall ein hinreichendes Auditierungsniveau sichergestellt ist. Die Zertifizierungsstelle kann hierbei fallbezogen die notwendigen, gesonderten Anforderungen festlegen.

Ist das Vor-Ort-Audit aufgrund von im Dokument [AIS N1] genannten Rahmenbedingungen zum Zeitpunkt der Antragstellung nicht durchführbar und die oben benannten Bedingungen für die Durchführung eines Fernaudits sind nicht gegeben, wird die Bearbeitung des Verfahrens zurückgestellt. Der Antragsteller/Hersteller hat die Möglichkeit den Antrag zurückzuziehen und in korrigierter Form oder zu einem späteren Zeitpunkt erneut einzureichen.

3.3.3.2 Notwendige Unterlagen für den Auditprozess

Folgende Nachweise, Informationen und Gegenstände werden vom Antragsteller/Hersteller während des Zertifizierungsprozesses benötigt:

- Eine Liste mit Produktentwicklungsstandorten. Hierbei muss angegeben werden (sofern zutreffend), welcher Standort exemplarisch auditiert werden soll.
- Eine Dokumentation von Prozessen und Maßnahmen beim Hersteller, die dazu beitragen sollen, dass die Sicherheitsanforderungen aus dem Dokument „NESAS Development and Lifecycle Security Requirements“ [FS.16] eingehalten werden.

Die Dokumentation der Prozesse und Maßnahmen wird spätestens zu Beginn der Auditierungsphase direkt durch den Hersteller an den Audit-Teamleiter übergeben. Der Dokumentenaustausch erfolgt über die von der Zertifizierungsstelle benannte Datenaustauschplattform (momentan bscw.bund.de). Daten, die über die Datenaustauschplattform bereitgestellt werden, müssen mittels OpenPGP für jeden Empfänger persönlich verschlüsselt werden. Die Zertifizierungsstelle muss bei jedem Datenaustausch als Empfänger durch Nutzung des gültigen Verfahrensschlüssels einbezogen werden. Auf diesem Weg werden auch Nachforderungen an Dokumenten, um Rückfragen zu beantworten, an die Auditoren übermittelt.

3.3.3.3 Vergabe eines Audits an ein Audit-Team

Die Auswahl und Zuweisung der Auditoren, die das Audit bei Hersteller durchführen, erfolgt durch die Zertifizierungsstelle entsprechend dem Ablauf der im Dokument [AIS N1] beschrieben ist. Der Hersteller hat die Möglichkeit, in begründeten Fällen innerhalb von 5 Arbeitstagen nach Bekanntgabe ein Votum gegen einen zugewiesenen Auditor einzulegen. Die Zertifizierungsstelle wird das Votum prüfen, das weitere Vorgehen abstimmen und die Entscheidung im Anschluss dem Hersteller und Auditor bekanntgeben. Sollte dem Votum stattgegeben werden, wird ein neuer Auditor gewählt.

Typischer Ablauf des Verfahrens:

Aufgaben Hersteller	*Hilfsmittel*	*Aufgaben Audit-Team*	*Aufgaben Zertifizierungsstelle*
• -	• -	• -	• Auswahl Audit Team
• Ggf. Votum gegen Auditor einlegen	• -	• Audit bestätigen • Ggf. Audit ablehnen	• Ggf. Votum prüfen und neuen Auditor auswählen
• -	• -	• -	• Audit Team an Hersteller und Auditoren mitteilen

Tabelle 3 Aufgaben bei der Vergabe eines Audits

3.3.3.4 Auditprozess

Das Evaluierungs- und Zertifizierungskonzept basiert auf einer engen Kooperation zwischen den beteiligten Parteien Antragsteller, den zugewiesenen Auditoren und dem Zertifizierer in der Zertifizierungsstelle. Die Kommunikation erfolgt i. d. R. in Textform (z. B. Dokumente, E-Mail, Formschreiben) oder im laufenden Verfahren telefonisch oder per webbasierten Konferenzsystemen (z. B. Status-Telefonkonferenzen, Klärung von kleineren Fachfragen, die nicht vertraulichkeitskritisch sind) oder in gemeinsamen Besprechungen. Mails, die zwischen Hersteller, Audit-Team und Zertifizierungsstelle ausgetauscht werden, sind grundsätzlich mittels OpenPGP zu verschlüsseln. Die notwendigen öffentlichen Verfahrensschlüssel müssen dazu im Vorfeld des Verfahrens ausgetauscht werden.

Zu Beginn der Auditierungsphase findet ein Kick-Off-Meeting statt, in welchem ein gegenseitiges Kennenlernen von Audit-Team und Hersteller sowie eine initiale Abstimmung des weiteren Vorgehens erfolgt. Für die Planung und Durchführung dieses Treffens ist das Audit-Team zuständig. Das Audit-Team informiert zudem die Zertifizierungsstelle mindestens sieben Tage im Voraus über den Termin des Kick-Off-Meetings, so dass diese bei Bedarf ebenfalls an dem Treffen teilnehmen kann.

Alle Parteien sind angehalten, den zu Beginn des Verfahrens vereinbarten Zeitplan einzuhalten. Der Leiter des Audit-Teams ist für die Einhaltung der fristgerechten Durchführung des Audits (innerhalb von drei Monaten ab dem Tag des Kick-Off-Meetings des Audits) zuständig. Bei sich abzeichnenden oder bereits eingetretenen Verzögerungen sind die anderen Beteiligten zu informieren, um eine aktualisierte Verfahrensplanung neu abzustimmen. Die aktualisierte Verfahrensplanung muss durch die Zertifizierungsstelle abgenommen werden.

Die Nachweise und Dokumentationen des Herstellers werden direkt mit dem Audit-Team, i. d. R. über den Auditoren-Teamleiter, ausgetauscht. Um sicherzustellen, dass das Audit im gewünschten Zeitrahmen durchgeführt werden kann, sollte sich der Antragsteller/Hersteller bewusst sein, dass eine ausreichende Vorbereitung der Prozessdokumentation erforderlich ist. Der Teamleiter leitet die Kopien der Dokumente (digitale Form) an die Zertifizierungsstelle weiter.

Im Rahmen der Dokumentenprüfung festgestellter Ergänzungsbedarf, Fehler oder Inkonsistenzen in den Herstellernachweisen müssen geklärt und durch den Hersteller behoben werden. Hierfür muss der Hersteller Ressourcen und Ansprechpartner mit entsprechender Auskunfts- und Entscheidungsbefugnis bereitstellen. Der Hersteller muss sicherstellen, dass alle erforderlichen Dokumente, Informationen und Nachweise bereitgestellt und Vor-Ort-Termine ermöglicht werden.

Der Zertifizierer kann die Herstellerdokumente stichprobenhaft einem internen Review unterziehen sowie an Besprechungen zwischen dem Antragsteller/Hersteller und dem Auditor teilnehmen, um die Prüfaussage des Auditors besser zu verstehen und ggf. auf notwendigen Klärungsbedarf hinzuweisen. Der Umfang der Stichproben liegt im Ermessen der Zertifizierungsstelle. Weiterhin hat der Zertifizierer die Möglichkeit, an Vor-Ort-Audits zusammen mit dem Audit-Team teilzunehmen und sich einen Eindruck über die Umsetzung der beschriebenen Prozesse zu verschaffen.

Die Rahmenbedingungen zum Verfahren gemäß Kapitel 5.3 „Verfahrensbeschreibung zur Zertifizierung von Produkten“ [VB-Produkte.PD], speziell zur Ablehnung eines Antrages oder einer negativen Bescheidung, finden Anwendung. Dies kann sich z. B. auf eine Verletzung der Unparteilichkeit oder Nichterfüllung der Obliegenheiten des Antragstellers beziehen, z. B. bei fehlenden Nachweisen oder wesentlichen Änderungen am Antrag oder am Zertifizierungsgegenstand.

Ein Audit der Entwicklungs- und Lebenszyklusprozesse bei einem Hersteller kann nur mit einem positiven Ergebnis abgeschlossen werden, wenn die Maßnahmen und Prozesse zur Einhaltung der Sicherheitsmaßnahmen aus dem Dokument „NESAS Development and Lifecycle Security Requirements“ [FS.16] durch den Auditor und die Zertifizierungsstelle als vollständig, korrekt und fachlich geeignet angesehen werden.

Wird festgestellt, dass Sicherheitsanforderungen auch nach möglichen Nachbesserungen nicht erfüllt sind, ergibt das Audit der Prozesse ein negatives Ergebnis. Aufgrund dessen würde der Zertifizierungsprozess ohne ein Zertifikat mit einem negativen Bescheid beendet werden.

Wenn ein Audit durchgeführt wurde und wenn während des Audits festgestellt wurde, dass der Hersteller durch seine Maßnahmen und Prozesse nicht alle im Dokument „NESAS Development and Lifecycle Security Requirements“ [FS.16] definierten Anforderungen erfüllt, können sich der Hersteller und der Auditor in Absprache mit der Zertifizierungsstelle auf die Durchführung eines erneuten Audits einigen, nachdem der Hersteller die erforderlichen Verbesserungen eingeführt hat. Dies ist nur möglich, wenn das vollständige Audit und das zusätzliche Audit die maximale Gesamtdauer von drei Monaten nicht überschreiten.

Nachdem der Hersteller das Audit durchlaufen hat, erfolgt in dieser Phase die Erstellung des Auditberichtes mit allen Anhängen sowie die Erstellung der Audit-Zusammenfassung für eine spätere Veröffentlichung bei erfolgreicher Zertifizierung.

Typischer Ablauf des Verfahrens:

Aufgaben Hersteller	*Hilfsmittel*	*Aufgaben Audit-Team*	*Aufgaben Zertifizierungsstelle*
• -	• -	• Kontaktaufnahme zum Hersteller durch Lead-Auditor	• -
• Teilnahme an Kick-Off Meeting für Audit	• -	• Planung, Einladung und Durchführung Kick-Off Meeting für Audit	• Kenntnisnahme • Optional: Teilnahme an Kick-Off Meeting
• Abstimmung Audit-Prozess mit Audit-Team/Lead-Auditor	• AIS N1	• Planung/Abstimmung Audit-Prozess mit Hersteller	• -
• -	• -	• Mitteilung Ablauf Audit an Zertifizierungsstelle: • Geplanter Zeitraum Audit • Geplantes Datum Fertigstellung erstes Dokumentenaudit • Geplantes Datum Fertigstellung Dokumentenaudit • Geplanter Zeitraum Vor-Ort-Audit • Geplanter Ort des Audits • Geplanter Übergabetermin des Auditreport	• Kenntnisnahme
• Bereitstellung notwendiger Dokumente an das Audit-Team sowie die Zertifizierungsstelle	• AIS N1, von der Zertifizierungsstelle gestellte Datenaustauschplattform	• Entgegennahme der bereitgestellten, relevanten Dokumente	• Bereitstellung eines Ordners mit passenden Berechtigungen und Entgegennahme der relevanten Dokumente.
• -	• AIS N1	• Dokumentenaudit 1. Runde	• -

Aufgaben Hersteller	*Hilfsmittel*	*Aufgaben Audit-Team*	*Aufgaben Zertifizierungsstelle*
• Qualitätssicherung und Kommentierung des Ergebnisses der 1. Runde des Dokumentenaudits	• -	• Übermittlung der Ergebnisse des erstes Dokumentenaudits an den Hersteller zur Qualitätssicherung und Kommentierung	• -
• Übermittlung der kommentierten Ergebnisse an den Auditor zur Entscheidung über die Kommentare und deren Einarbeitung. Die Zertifizierungsstelle erhält die Kommentare zur Kenntnis.	• -	• Entscheidung über Annahme der Kommentare und deren eventuelle Einarbeitung	• Kenntnisnahme der Kommentare und notwendiger Nachlieferungen des Herstellers
• Besprechung der Ergebnisse aus der 1. Runde des Dokumentenaudits	• -	• Ergebnisbesprechung der 1. Runde des Dokumentenaudits	• -
• Erfüllung der Nachforderungen aus der Ergebnisbesprechung	• von der Zertifizierungs-stelle gestellte Datenaustausch plattform	• -	• -
• -	• AIS N1	• Dokumentenaudit 2. Runde	• -
• Qualitätssicherung und Kommentierung des Ergebnisses der 2. Runde des Dokumentenaudits	• -	• Übermittlung der Ergebnisse des zweiten Dokumentenaudits an den Hersteller zur Qualitätssicherung und Kommentierung	• -
• Übermittlung der kommentierten Ergebnisse an den Auditor zur Entscheidung über die Kommentare und deren Einarbeitung. Die Zertifizierungsstelle erhält die Kommentare zur Kenntnis.	• -	• Entscheidung über Annahme der Kommentare und deren eventuelle Einarbeitung sowie Schwerpunktsetzung für das Vor-Ort-Audit	• Kenntnisnahme der Kommentare
• Abstimmung Audit-Prozess mit Audit-Team/Lead-Auditor	• -	• Aktualisierung Terminvereinbarung Vor-Ort-Audit • Mitteilung weiterer Hinweise für Folgeschritte	• -
• -	• -	• Mitteilung exakter Termin Vor-Ort-Audit an Zertifizierungsstelle	• Kenntnisnahme
• Bereitstellung notwendiger Ressourcen und Daten für Audit (z. B. Personal, Zeit,	• AIS N1	• Vor-Ort-Audit	• Optional: • Ggf. Teilnahme an Vor-Ort-Audit

Aufgaben Hersteller	*Hilfsmittel*	*Aufgaben Audit-Team*	*Aufgaben Zertifizierungsstelle*
Arbeitsraum für Auditoren)			
• -	• AIS N1	• Erstellung Auditbericht und aller notwendigen Anlagen	• -
• Qualitätssicherung und Kommentierung des Auditberichts	• -	• Übermittlung des Auditberichts an den Hersteller zur Qualitätssicherung und Kommentierung	• -
• -	• -	• Übermittlung des kommentierten Auditberichts an die Zertifizierungsstelle zur Kenntnis	• Kenntnisnahme der Kommentare
• -	• -	• Einarbeitung der Kommentare nach eigenem Ermessen unter Berücksichtigung der referenzierten Dokumente	• -
• -	• -	• Bereitstellung des Auditberichts an die Zertifizierungsstelle • ggf. Einarbeitung der Kommentare der Zertifizierungsstelle	• Kommentierung des Auditberichtes • Abnahme des Auditberichts und Mitteilung an Audit-Team
• -	• AIS N1	• Finalisierung Auditbericht • Erstellung Audit-Zusammenfassung	• -
• Kenntnisnahme und Eingangsbestätigung	• -	• Übermittlung Auditbericht, Anlagen und Audit-Zusammenfassung an Hersteller und Zertifizierungsstelle	• Kenntnisnahme und Eingangsbestätigung
• -	• -	• Kostenstellung Auditor gegenüber Zertifizierungsstelle	• Prüfung Plausibilität Kostenabrechnung

Tabelle 4 Aufgaben im Auditprozess

3.3.4 Die Evaluierungsphase

3.3.4.1 Allgemeines

In der Evaluierungsphase erfolgt eine Überprüfung, ob die auditierten Entwicklungsprozesse bei der Entwicklung des Netzwerkproduktes eingehalten wurden. Basis dafür bildet der Auditbericht und die darin im Audit festgelegten und für die Evaluierung geforderten geeigneten Nachweise, die durch den Hersteller gegenüber der Prüfstelle zu erbringen sind. Weiterhin werden an dem realen Netzwerkprodukt standardisierte Sicherheitstests (SeCurity Assurance Specifications (SCAS-Tests)) durchgeführt. Die für die Evaluierung auszuwählenden SCAS-Tests hängen von der Funktionalität ab, die das Netzwerkprodukt bietet, und müssen durch den Antragsteller im Antrag festgelegt werden. Eine Zuordnung erfolgt mit Hilfe des Dokuments [AIS N2]. Die, aus den SCAS-Tests, hervorgehenden Prüfergebnisse werden durch die Prüfstelle in einem Evaluierungsbericht (ETR) festgehalten und zusammengefasst.

Die Evaluierungsphase kann nur mit einem gültigen Audit (vgl. 5.4.2.1) und dem zugehörigen Auditbericht gestartet werden. Für die Evaluierung notwendige Unterlagen sind in Kapitel 3.3.4.2 aufgeführt.

3.3.4.2 Notwendige Unterlagen für die Evaluierungsphase

Folgende Nachweise, Informationen und Gegenstände werden vom Antragsteller/Hersteller während des Zertifizierungsprozesses benötigt:

- Ein bereits vorhandener Auditbericht mit allen zugehörigen Anlagen.
- Im Auditbericht geforderte Konformitätsnachweise des Herstellers zum Nachweis, dass das zu evaluierende Produkt nach den auditierten Entwicklungs- und Lebenszyklusprozessen entwickelt wurde. Der Hersteller kann auf diese Weise gegenüber der Prüfstelle bestätigen, dass bei der Entwicklung des Netzwerkproduktes die auditierten Entwicklungs- und Lebenszyklusprozessen eingehalten wurden.
- Netzwerkprodukt, Handbücher und Produktspezifikationen sowie notwendige Peripherie/ Testequipment und zugehörige Beschreibung müssen der Prüfstelle bereitgestellt werden, um der Prüfstelle/den Evaluatoren eine Prüfung in der prüfstelleneigenen Testumgebung zu ermöglichen.
- Falls notwendig: Eine Anleitung, wie das Netzwerkprodukt in einen betriebsbereiten Zustand gebracht werden kann.
- Alle weiteren in der [AIS N2], Kapitel 2.4.1 genannten Nachweise und Informationen.

Der Auditbericht sowie die im Auditbericht geforderten Konformitätsnachweise sind der Zertifizierungsstelle (soweit nicht durch ein vorgelagertes Audit vorhanden) vom Hersteller bereitzustellen. Die Zertifizierungsstelle leitet die Dokumente anschließend an die Prüfstelle weiter.

3.3.4.3 Evaluierungsprozess

Das Evaluierungs- und Zertifizierungskonzept basiert auf einer engen Kooperation zwischen dem beteiligten Antragsteller, den zugewiesenen Evaluatoren, dem Leiter des Evaluierungsprojektes in der Prüfstelle und dem zugewiesenen Zertifizierer in der Zertifizierungsstelle. Die Kommunikation erfolgt i. d. R. in Textform (z. B. Dokumente, E-Mail, Formschreiben) oder im laufenden Verfahren telefonisch oder per webbasierten Konferenzsystemen (z. B. Status-Telefonkonferenzen, Klärung von kleineren Fachfragen, die nicht vertraulichkeitskritisch sind) oder in gemeinsamen Besprechungen.

Alle Beteiligten sind angehalten, den zu Beginn des Verfahrens vereinbarten Zeitplan einzuhalten. Die Prüfstelle ist für die Einhaltung einer fristgerechten Durchführung der Evaluierung zuständig. Bei sich abzeichnenden Verzögerungen sind die anderen Beteiligten zu informieren, um eine aktualisierte Verfahrensplanung neu abzustimmen.

Zu Beginn der Evaluierung erfolgt ein Kick-Off-Meeting, das nach Möglichkeit in physischer Präsenz in den Räumen der Prüfstelle stattfindet. Nach Maßgabe der Zertifizierungsstelle ist alternativ eine Durchführung als Videokonferenz möglich. Während des Treffens wird das Netzwerkprodukt, die verwendeten SCAS-Dokumente sowie das beabsichtigte Scoping durch die Prüfstelle vorgestellt. Dies ermöglicht Fragen und Anmerkungen durch Zertifizierungsstelle oder Antragsteller/Hersteller.

Für den Fall, dass vereinzelte Prüfungen/Testfälle nicht mit zumutbaren Aufwand in einer Prüfstelle durchgeführt werden können, besteht die Möglichkeit einzelne Tests beim Hersteller durchzuführen. Entsprechende Aktivitäten müssen mindestens 4 Wochen vor Durchführung durch die Prüfstelle mit der Zertifizierungsstelle abgestimmt werden. Dabei ist darzulegen, wie die Unabhängigkeit der Prüfung gewährleistet wird. Die Durchführung von Tests beim Hersteller muss durch einen Evaluator der Prüfstelle erfolgen. Eine Durchführung von Evaluierungstätigkeiten aus der Ferne (remote) ist nicht zulässig.

Im Rahmen der Evaluierung festgestellte Ergänzungsbedarfe, Fehler oder Inkonsistenzen an den Herstellernachweisen müssen geklärt und durch den Antragsteller behoben werden. Hierfür muss der Antragsteller

Ressourcen und Prozesse bereitstellen. Dies führt in der Regel zur Wiederholung von Evaluierungsschritten. Dadurch entstehende Verzögerungen sind dem BSI zeitnahe mitzuteilen.

Erfolgen Nachbesserungen und Nachtests, so ist in dem ETR klar darzulegen, welche Tests mit welcher Version des zu evaluierenden Netzwerkproduktes fehlgeschlagen sind und welche Tests mit welche(n) Versionen (erneut) durchgeführt wurden.

Für den Zertifizierungsprozess ist von besonderer Bedeutung, dass der Evaluierungsbericht folgende Informationen enthält:

- die Evidenzbewertung der im Auditbericht festgelegten Herstellernachweise und
- die Testergebnisse, die aus den SCAS-Tests hervorgehen.

Nur durch die Verbindung der genannten Resultate (Evidenzbewertung und Testergebnisse der SCAS-Tests) ist es der Zertifizierungsstelle möglich zu einem aussagekräftigen Zertifizierungsergebnis zu gelangen.

Der Zertifizierer kann die Herstellerdokumente stichprobenhaft einem internen Review unterziehen sowie an Besprechungen zwischen dem Antragsteller/Hersteller und der Prüfstelle teilnehmen, um die Prüfaussage der Evaluierung besser zu verstehen und ggf. auf notwendigen Klärungsbedarf hinzuweisen. Der Umfang der Stichproben liegt im Ermessen der Zertifizierungsstelle. Weiterhin hat der Zertifizierer die Möglichkeit, an Evaluierungen oder Teilen davon teilzunehmen, um sich einen Eindruck über die Umsetzung der Evaluierungstätigkeiten zu verschaffen, eine einheitliche Vorgehensweise, Methodik und vergleichbare Bewertungen sicherzustellen und um frühzeitig auf eine mögliche Nichterfüllung der Zertifizierungsanforderungen hinzuweisen. Die Prüfstelle hat die Möglichkeit Evaluierungsfragen mit der Zertifizierungsstelle zu klären.

Aktualisierungen der Prüfanforderungen (z. B. neue SCAS-Tests), die während des laufenden Verfahrens veröffentlicht werden, müssen nicht umgesetzt werden. Auf expliziten Wunsch des Antragstellers und unter Zustimmung aller beteiligten Parteien können die aktuelleren Prüfanforderungen umgesetzt werden. Im Evaluierungsbericht müssen die tatsächlich verwendeten Prüfanforderungen referenziert werden.

Bei fehlenden oder unzureichenden Nachweisen des Antragstellers oder der Prüfstelle oder bei Verletzung der Unparteilichkeit kann ein Zertifizierungsverfahren durch die Zertifizierungsstelle nach Anhörung der Parteien abgebrochen oder mit negativem Ergebnis beendet werden.

Die Rahmenbedingungen zum Verfahren gemäß Kapitel 5.3 „Verfahrensbeschreibung zur Zertifizierung von Produkten“ [VB-Produkte.PD], speziell zur Ablehnung eines Antrages oder einer negativen Bescheidung, finden Anwendung. Dies kann sich z. B. auf eine Verletzung der Unparteilichkeit, Nichterfüllung der Obliegenheiten des Antragstellers z. B. bei fehlenden Produktnachweisen oder wesentlichen Änderungen am Antrag oder am Zertifizierungsgegenstand, beziehen.

Typischer Ablauf des Verfahrens:

Aufgaben Hersteller	*Hilfsmittel*	*Aufgaben Prüfstelle*	*Aufgaben Zertifizierungsstelle*
Bereitstellung/Übergabe von: • Netzwerkprodukt inkl. Zubehör • Betriebsanleitungen • ggf. notwendige Peripherie/ Testequipment soweit möglich, an Prüfstelle	• AIS N2	Entgegennahme • Netzwerkprodukt inkl. Zubehör • Betriebsanleitungen • ggf. notwendige Peripherie/ Testequipment • weitere Bestandteile	• -
Bereitstellung/Übergabe von: • Auditbericht • Nachweise zu den Sicherheitsanforderungen	• AIS N2	• Entgegennahme der Dokumente vom Hersteller	• Entgegennahme der Dokumente vom Hersteller zur Kenntnis

Aufgaben Hersteller	*Hilfsmittel*	*Aufgaben Prüfstelle*	*Aufgaben Zertifizierungsstelle*
• ggf. Begründung für fehlende Sicherheits-anforderungen an Prüfstelle und Zertifizierungsstelle			
• Ggf. bei der Erstellung des Prüfplans mitwirken	• AIS N2	Prüfplan erstellen/anpassen: • Evaluierungstätigkeiten mit dem Antragsteller vorbereiten/abstimmen	• -
• Teilnahme an Kick Off-Meeting zur Klärung von Fragen zur Evaluierung	• -	• Teilnahme an Kick Off-Meeting zur Klärung von Fragen zur Evaluierung	• Teilnahme an Kick Off-Meeting zur Klärung von Fragen zur Evaluierung
• -	• -	• Warten auf Freigabe Zertifizierungsstelle	• Freigabe der Evaluierung
• Kostenfreie Bereitstellung von Kapazitäten und Ressourcen für Evaluierungs-tätigkeiten durch die Prüfstelle • Kostenfreien Zugang zu prüfrelevanten Standorten und Herstellerumgebungen für Evaluator und Zertifizierer ermöglichen	• AIS N2	• Evaluierung durchführen • Prüftätigkeiten zu den geforderten Konformitäts-nachweisen aus den Anlagen des Auditberichts • Prüftätigkeiten zu den in den SCAS-Tests geforderten Prüfaspekten durchführen • Prüfdokumentation erstellen • Prüfergebnisse und Evaluierungsbericht der Zertifizierungsstelle vollständig zur Verfügung stellen • Kommentare und Nachforderungen bearbeiten • ggf. offene Fragen Antrag-steller/Hersteller klären	• Evaluierung begleiten (Prüfbegleitung) • Optional: Teilnahme an Evaluierungen • Evaluierungsbericht bewerten und kommentieren
• Warten auf ETR-Abnahme durch Zertifizierungsstelle: Damit sind bei positivem Ergebnis der Evaluierung die fachlichen Voraussetzungen für die Erteilung des Zertifikates gegeben	• -	• Abschließenden ETR mit allen Prüfergebnissen erstellen	• Prüfung, ggf. Kommentierung ETR • Fachliche Abnahme der Evaluierung im Hinblick auf die Zertifizierungs-entscheidung durchführen • Antragsteller und Prüfstelle über Abnahme informieren

Tabelle 5 Aufgaben in der Evaluierungsphase

3.3.5 Zertifizierungsphase

Aufgaben Hersteller	*Hilfsmittel*	*Aufgaben Prüfstelle*	*Aufgaben Zertifizierungsstelle*
• Ggf. Mitwirkung bei der Erstellung des Zertifizierungsreports und Reaktion auf die Anhörung: • Ggf. den Entwurf des Zertifizierungsreports kommentieren • Ggf. Reaktion auf formale Anhörung	• -	• Ggf. Entwurf des Zertifizierungs-reports kom-mentieren	• Zertifizierungsentscheidung treffen und Verfahren abschließen • Bei positiver Zertifizierungsentscheidung: • Zertifikatsurkunde, Zertifizierungsreport, Zertifizierungsbescheid erstellen • Formale Anhörung des Antragstellers zu Nebenbestimmungen (Insbesondere Bedingungen und Auflagen) im Bescheid (Frist 14 Tage) • Erteilung Zertifikat • Bei negativer Zertifizierungsentscheidung: • Negativbescheid nach formaler Anhörung • Postalische Zustellung von • Bescheid, Zertifikat und Zertifizierungsreport an den Antragsteller (Widerspruchsfrist 1 Monat oder Widerspruch-verzichtserklärung) • Wenn gewünscht: • Zertifizierungszeichen (Button) bereitstellen
• Versand Empfangsbestätigung und ggf. Widerspruchsverzicht: • Empfangsbestätigung an BSI senden • Widerspruchsverzicht ausstellen und an BSI senden, sonst 1 Monat Zeit, schriftlich Widerspruch gegen die Zertifizierungsentscheidung bei der Zertifizierungsstelle einzulegen • (Bei Verzicht auf Widerspruch verkürzt sich die Frist zur Veröffentlichung)	• -	• -	• Ggf. Bearbeitung des Widerspruchs • Nach Ablauf der Widerspruchsfrist ist der Bescheid bestandskräftig Veröffentlichung des Ergebnisses der Zertifizierung sowie dem Zertifizierungsreport einschließlich der Audit-Zusammenfassung

Aufgaben Hersteller	*Hilfsmittel*	*Aufgaben Prüfstelle*	*Aufgaben Zertifizierungsstelle*
• Kostenerstattung: Aufwände des Verfahrens (Gebühren und Auslagen) dem BSI erstatten (siehe Kap. 5.5)	• BMIBGebV	• -	• Kostenbescheid an Antragsteller schicken
• Archivierung durchführen: Alle evaluierungsrelevanten Nachweise und das evaluierte Produkt für den Zeitraum der Gültigkeit des Zertifikates plus 3 Jahre archivieren	• VB-Stellen	• Alle evaluierungs-relevanten Nachweise archivieren	• Alle zertifizierungsrelevanten Nachweise archivieren
• Einhaltung der Nebenbestimmungen im Bescheid und der Regelungen der Zeichenordnung	• Zeichen-ordnung	• -	• Wenn relevant: Bearbeitung von Nachlieferungen aus Nebenbestimmungen

Tabelle 6 Aufgaben in der Zertifizierungsphase

3.3.6 Abschlussdokumente

Der bei positivem Abschluss der Evaluierung von der Zertifizierungsstelle erstellte Zertifizierungsreport enthält neben einer sicherheitstechnischen Beschreibung des Produktes u. a. ausgewählte Angaben zum Ergebnis des Audits und der Evaluierung sowie Hinweise und Auflagen zur Benutzung des zertifizierten Netzwerkproduktes.

Weiterhin wird bestätigt, dass das Audit und die Evaluierung nach den anerkannten Verfahren und Kriterien durchgeführt worden sind und dass die in den SCAS-Tests definierten Sicherheitsanforderungen hinsichtlich Funktionalität und Prüfumfang erfüllt werden. Der Report enthält Hinweise und Auflagen an den Anwender, die für den Einsatz des Netzwerkproduktes einzuhalten sind.

Der Zertifizierungsbescheid stellt das im rechtlichen Sinne offizielle Votum der Zertifizierungsstelle dar und enthält als Nebenbestimmungen insbesondere Bedingungen und Auflagen, die durch den Antragsteller einzuhalten sind.

Das Zertifikat und der Zertifizierungsreport können in deutscher oder englischer Sprache erstellt werden. Maßgeblich ist i. d. R. die gewählte Sprache im Antrag.

4 Aufrechterhaltung einer Zertifizierung

4.1 Geringfügige Aktualisierung

Ein Zertifikat wird für eine eindeutig bestimmte und evaluierte Produktversion erteilt. Geringfügige Aktualisierungen an einem Produkt bilden dabei die Ausnahme und können unter die Zertifizierung fallen. Eine geringfügige Aktualisierung eines Produktes muss eindeutig in der Produktversion erkennbar sein. Auf den Internetseiten des BSI werden stets alle Versionen des Produktes aufgeführt, auf welche sich das Zertifikat bezieht.

Sofern der Antragsteller während der Zertifikatslaufzeit Veränderungen des zertifizierten Netzwerkproduktes veröffentlicht, welche nur geringfügige Aktualisierungen darstellen, können diese ebenfalls von dem bestehenden Sicherheitszertifikat erfasst sein (d. h. das Produkt einschließlich der geringfügigen Aktualisierung ist weiterhin zertifiziert). Die geringfügige Aktualisierung ändert nicht die Zertifikatslaufzeit.

Für das Zertifizierungsprogramm NESAS gilt insoweit folgende Begriffsbestimmung: Geringfügige Aktualisierungen sind Anpassungen von Sicherheitsfunktionen oder der Beschaffenheit des Produktes, die der Aufrechterhaltung oder Wiederherstellung der zertifizierten Sicherheitsleistung (als Summe der Sicherheitsaussagen der Produktevaluation) dienen oder die für die Sicherheitsleistung irrelevant sind.

Diese Anpassungen sind entweder funktional-erhaltender Natur (um den geplanten, funktionalen Ablauf des Netzwerkproduktes zu erreichen; funktionale Fehlerbeseitigung) oder Sicherheitskorrekturen (um ungeplante, i. d. R. missbräuchliche Verwendungen des Produktes zu vermeiden; Beseitigung von Sicherheitsmängeln). Eine funktional-erhaltende Anpassung oder Sicherheitskorrektur, welche eine neue Funktionalität benötigt (z. B. eine neue Filterschicht, eine zusätzliche Firewall, zusätzliche Virtualisierung) stellt keine nur geringfügige Aktualisierung dar, da damit keine eindeutige Sicherheitsaussage mehr für das Sicherheitszertifikat möglich ist.

Eine geringfügige Aktualisierung muss bei der Zertifizierungsstelle beantragt werden. Das Audit der Entwicklungs- und Lebenszyklusprozesse muss zum Zeitpunkt der Bekanntmachung gegenüber der Zertifizierungsstelle gültig sein.

Folgende Nachweise und Informationen werden vom Antragsteller/Hersteller benötigt:

- Zertifizierungsantrag/Antragsformular mit Anlagen,
- Impact Analysis Report (IAR),
- Im Auditbericht geforderte Konformitätsnachweise des Herstellers als Nachweis über die Einhaltung der auditierten Entwicklungs- und Lebenszyklusprozessen während der Erstellung der geringfügigen Aktualisierung und eine
- Beurteilung der Änderung mit einem eindeutigen Votum der sachverständigen Stelle (Prüfstelle, die das Netzwerkprodukt evaluiert hat).

Der Antragsteller/Hersteller muss sich von der sachverständigen Stelle (Prüfstelle, die das Netzwerkprodukt evaluiert hat) auf Basis des IAR eine schriftliche Beurteilung mit einem eindeutigen Votum für die Zertifizierungsstelle erstellen lassen, dass die im IAR beschriebenen Änderungen unter die Definition der geringfügigen Aktualisierungen fallen und die auditierten Prozesse genutzt wurden. Der Antragsteller/ Hersteller muss, sofern von der sachverständigen Stelle benötigt oder angefordert, zusätzlich Informationen und Nachweise bereitstellen.

Die geringfügige Aktualisierung ist ab dem Zeitpunkt von der Zertifizierung vorläufig erfasst, an dem der Antragsteller die aufgeführten Nachweise und Informationen darüber der Zertifizierungsstelle übersandt hat.

Die Zertifizierungsstelle behält sich vor innerhalb von 30 Kalendertagen ab Antragseingang dem Votum der sachverständigen Stelle zu widersprechen.

Kommt die Zertifizierungsstelle auf Basis des IAR und des Votums der sachverständigen Stelle zu dem Ergebnis, dass die Aktualisierung geringfügig ist, wird der Zertifizierungsreport mit der im IAR angegebenen Produktversion durch einen Anhang ergänzt. Eine geringfügige Aktualisierung ändert nicht die Zertifikatslaufzeit.

Kommt die Zertifizierungsstelle auf Basis des IAR und des Votums der sachverständigen Stelle zu dem Ergebnis, dass die Aktualisierung nicht geringfügig ist, gibt sie dem Antragsteller die Gelegenheit, innerhalb von 5 Arbeitstagen die Bedenken der Zertifizierungsstelle auszuräumen. Gelingt dies nicht, ist das Sicherheitszertifikat auf das Produkt im letzten zertifizierten Zustand nebst etwaiger gültiger geringfügiger Aktualisierungen beschränkt. Diese Frist kann bei Vorliegen sachlicher Gründe einmalig verlängert werden.

Der Antragsteller/Hersteller wird durch einen Bescheid über die endgültige Entscheidung der Zertifizierungsstelle informiert. Der Zertifizierungsbescheid stellt das im rechtlichen Sinne offizielle Votum der Zertifizierungsstelle dar und enthält als Nebenbestimmungen insbesondere Bedingungen und Auflagen, die durch den Antragsteller einzuhalten sind. Der Antragsteller ist verpflichtet, den Umfang der Gültigkeit des Zertifikates einschließlich eventueller Beschränkungen bei allen Angaben zum Sicherheitszertifikat zu erwähnen. Dies wird auch auf der Liste der zertifizierten Produkte vermerkt.

Für den Fall, dass der Antragsteller im Zertifizierungsprogramm NESAS geringfügige Aktualisierungen zur Bewertung unter dem zugrundeliegenden Sicherheitszertifikat bei der Zertifizierungsstelle einreicht, können weitere Verfahrenskosten für die zusätzliche Bewertung anfallen. Über die Höhe der Kosten entscheidet das BSI durch einen gesonderten Kostenbescheid.

4.2 Einbeziehung unterschiedlicher Ausführungsumgebungen in das Zertifikat

Für das Zertifizierungsprogramm NESAS gilt folgende Begriffsbestimmung: "Ausführungsumgebungen" sind Computersysteme und deren Konfiguration und Parametrierung, die der Ausführung des Netzwerkproduktes dienen und die für den Betrieb des Netzwerkproduktes notwendigen Umgebungsbedingungen bereitstellen.

Sofern der Antragsteller während der Zertifikatslaufzeit weitere Ausführungsumgebungen in seine Liste der möglichen Ausführungsumgebungen für das Netzwerkprodukt hinzufügt, können diese ebenfalls vom bestehenden Sicherheitszertifikat erfasst sein (d. h. das Produkt wird in diesen Ausführungsumgebungen nach den Bestimmungen des Zertifikats betrieben).

Eine Aufnahme einer weiteren Ausführungsumgebung muss bei der Zertifizierungsstelle beantragt werden. Das Audit der Entwicklungs- und Lebenszyklusprozesse muss zum Zeitpunkt der Beantragung gültig sein.

Folgende Nachweise und Informationen werden vom Antragsteller/Hersteller benötigt:

- Zertifizierungsantrag/Antragsformular mit Anlagen,
- Impact Analysis Report (IAR) und eine
- Beurteilung der Änderung mit einem eindeutigen Votum der sachverständigen Stelle (Prüfstelle, die das Netzwerkprodukt evaluiert hat).

Der Antragsteller/Hersteller muss sich von der sachverständigen Stelle (Prüfstelle, die das Netzwerkprodukt evaluiert hat) auf Basis des IAR eine schriftliche Beurteilung mit einem eindeutigen Votum für die Zertifizierungsstelle erstellen lassen, dass die Sicherheitsaussagen des Zertifikats für das Produkt auch in der ergänzten Ausführungsumgebung Bestand haben. Der Antragsteller/Hersteller muss, sofern von der sachverständigen Stelle benötigt oder angefordert, zusätzlich Informationen und Nachweise bereitstellen.

Kommt die Zertifizierungsstelle auf Basis des IAR und des Votums der sachverständigen Stelle zu dem Schluss, dass die Sicherheitsaussagen des Zertifikats für das Produkt auch in der ergänzten Ausführungsumgebung Bestand haben, wird der Zertifizierungsreport mit der im IAR angegebenen Ausführungsumgebung durch einen Anhang ergänzt. Die Änderung der Ausführungsumgebung ändert nicht die Zertifikatslaufzeit.

Kommt die Zertifizierungsstelle auf Basis des IAR und des Votums der sachverständigen Stelle zu dem Schluss, dass die Sicherheitsaussagen des Zertifikats für das Produkt in der ergänzten Ausführungsumgebung keinen Bestand haben, gibt sie dem Antragsteller die Gelegenheit, innerhalb von 5 Arbeitstagen die Bedenken der Zertifizierungsstelle auszuräumen. Gelingt dies nicht, ist das Sicherheitszertifikat auf das Produkt im Betrieb in einer der im Zertifikat benannten Ausführungsumgebungen beschränkt. Diese Frist kann bei Vorliegen sachlicher Gründe einmalig verlängert werden.

Der Antragsteller/Hersteller wird durch einen Bescheid über die endgültige Entscheidung der Zertifizierungsstelle informiert. Der Zertifizierungsbescheid stellt das im rechtlichen Sinne offizielle Votum der Zertifizierungsstelle dar und enthält als Nebenbestimmungen insbesondere Bedingungen und Auflagen, die durch den Antragsteller einzuhalten sind.

Der Antragsteller ist verpflichtet, den Umfang der Gültigkeit des Zertifikates einschließlich eventueller Beschränkung bei allen Angaben zum Sicherheitszertifikat zu erwähnen. Dies wird auch auf der Liste der zertifizierten Produkte vermerkt.

Für den Fall, dass der Antragsteller im Zertifizierungsprogramm NESAS Ausführungsumgebungen zur Bewertung unter dem zugrundeliegenden Sicherheitszertifikat bei der Zertifizierungsstelle einreicht, können weitere Verfahrenskosten für die zusätzliche Bewertung anfallen. Über die Höhe der Kosten entscheidet das BSI durch einen gesonderten Kostenbescheid.

4.3 Rezertifizierung

Damit eine geänderte Produktversion, die nicht unter die Regelung einer geringfügigen Aktualisierung fällt, wieder als zertifiziert deklarieren werden kann, ist eine Erneuerung des Zertifikates unter Berücksichtigung der Änderungen erforderlich.

Der grundsätzliche Ablauf einer Rezertifizierung entspricht einem Erstverfahren. Das Audit der Entwicklungs- und Lebenszyklusprozesse muss, falls es nicht mehr gültig ist, erneut durchgeführt werden.

Nach positivem Abschluss werden die technischen Ergebnisse durch die Zertifizierungsstelle in einem aktualisierten Zertifizierungsreport dokumentiert und ein neues Zertifikat erteilt.

Die formale Gültigkeit eines Zertifikats sowie die sicherheitstechnische Bewertung des Produktes werden im Rahmen einer Rezertifizierung erneuert. Der Antragsteller hat durch eine Rezertifizierung die Möglichkeit die ursprüngliche vergebene Zertifikatsnummer durch Ergänzung von zusätzlichen alphanumerischen Elementen beizubehalten.

5 Spezielle Rahmenbedingungen

5.1 Grundlage für die Zertifizierung

Die Dienstleistung der Sicherheitszertifizierung von IT-Produkten nach NESAS durch das BSI wird als Antragsverfahren angeboten. Eine Zertifizierung kann erfolgen, wenn festgestellt wird, dass die jeweiligen Prüfvorschriften erfüllt sind und dass überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung nicht entgegenstehen (BSIG § 9, Abs.4 (2)). Die Prüfung nach BSIG § 9, Abs.4 (2) erfolgt bei Antragsannahme, jedoch vorbehaltlich einer abschließenden Entscheidung zum Zeitpunkt der Unterzeichnung eines Zertifizierungsbescheides und des Zertifikates.

Zertifizierungsverfahren für IT-Produkte beim BSI müssen unter Verwendung von Prüfvorschriften, die vom BSI als geeignet anerkannt wurden, durchgeführt werden. Prüfvorschriften für NESAS ergeben sich aus dem Dokument „NESAS Development and Lifecycle Security Requirements“ [FS.16] sowie den, von der 3GPP bereitgestellten, SCAS-Tests. Ist für einen Produkttyp kein vom BSI als geeignet anerkannter SCAS-Test verfügbar (vgl. [AIS N2]), entscheidet das BSI vor Aufnahme des Verfahrens im Einzelfall über die grundsätzliche Zertifizierbarkeit.

Die Auswahl der möglichen SCAS-Tests erfolgt durch das BSI auf Basis eines Risikomanagements für die Einsatzumgebung und Anwendung eines Produktes eine Sicherheitsaussage benötigen, oder sie resultieren aus Anforderungen aus nationalen IT-Sicherheitsprojekten, nationalen oder EU-Gesetzen oder Vorschriften.

Die Verfahrensabwicklung kann innerhalb der Zertifizierungsstelle priorisiert werden, wenn ein besonderes öffentliches Interesse festgestellt wurde oder bei Produkten, die in nationalen IT-Infrastrukturen zum Einsatz kommen.

5.2 Vertraulichkeit und Dokumentenaustausch

Die Firmenpolitik des Antragstellers und die Praxis hinsichtlich der vertraulichen Handhabung oder Weitergabe der Unterlagen zum evaluierten Produkt an Dritte, die nicht der Überwachung durch die Zertifizierungsstelle unterliegen, hat Einfluss auf die Bewertung der Ausnutzbarkeit von potenziellen Schwachstellen im Rahmen der Evaluierung, da z. B. vom Hersteller veröffentlichte Informationen zum Produkt als verfügbar für einen Angreifer gelten und somit ggf. die Angreifbarkeit vereinfachen.

Quellcode von Produkten oder anderweitig hochsensible Informationen, die nach einer dokumentierten Sicherheitspolitik des Herstellers klassifiziert sind und die Entwicklungsumgebung nicht verlassen dürfen, können in bestimmten Fällen anstatt bei der Prüfstelle auch beim Antragsteller vor Ort, z. B. in der Entwicklungsumgebung, vom Auditor, Evaluator und vom Zertifizierer begutachtet und analysiert werden. Dazu muss der Antragsteller gegenüber der Zertifizierungsstelle jeweils glaubhaft machen, dass einer Weitergabe der Unterlagen wesentliche Interessen des Antragstellers entgegenstehen. Bei dieser Vorgehensweise entstehen i. d. R. erhöhte Zeitaufwände und erhöhte Kostenaufwände für alle Parteien, die der Antragsteller zu tragen hat.

Der Dokumentenaustausch zwischen Antragsteller, Prüfstelle und Zertifizierungsstelle erfolgt i. d. R. auf elektronischem Wege per verschlüsselter E-Mail. Dazu wird OpenPGP entsprechend der Empfehlungen aus TR-02102-1 eingesetzt. Der Schlüsselaustausch für die Kommunikation über OpenPGP erfolgt spätestens während der Kick-Off-Meetings für Evaluierung und Auditierung. Für die Übermittlung des Antrags sind Antragsteller angehalten, den auf der Website verfügbaren öffentlichen Schlüssel für die Mail-Adresse nesas@bsi.bund.de zu nutzen, der sich unter der Rubrik „Zertifizierung und Anerkennung / Zertifizierung von Produkten / Zertifizierung nach NESAS CCS-GI“ (www.bsi.bund.de/nesas) findet.

Die Lieferung von elektronischen Dokumenten zu einem Zertifizierungsverfahren muss an die E-Mail-Adresse: nesas@bsi.bund.de erfolgen. Die Lieferung an persönliche BSI-E-Mail-Adressen von Zertifizierern erfolgt in der Regel zusätzlich in Kopie zur Kenntnis.

Für Dokumente, die in Papierform an das BSI geschickt werden oder die per Kurierversand direkt an der Pforte des BSI abgegeben werden sowie für bereitgestellte DVD/CDs gelten die Regelungen im übergeordneten Dokument „Verfahrensbeschreibung zur Zertifizierung von Produkten“ [VB-Produkte.PD].

Wird für die Unterlagen, die für die Auditierung der Entwicklungs- und Lebenszyklusprozesse benötigt werden, die elektronische Übertragung gewählt, so müssen die Unterlagen in verschlüsselten zip-Archiven auf dem von der Zertifizierungsstelle benannten Server bereitgestellt werden. Das Passwort der zip-Archive wird separat per Mail an nesas@bsi.bund.de übermittelt.

5.3 Rahmenbedingungen zum Verfahren

5.3.1 Evaluierungsplanung

Der Evaluierungsplan enthält Angaben zur organisatorischen und inhaltlichen Durchführung der Evaluierung, der anzuwendenden Kriterien und Interpretationen sowie zur zeitlichen Planung, ebenso eine Unabhängigkeits- und Unparteilichkeitserklärung. Die Prüfstelle muss gegenüber der Zertifizierungsstelle zusätzlich bestätigen, dass die technische Ausstattung für die Durchführung der für das jeweilige Netzwerkprodukt notwendigen SCAS-Tests ausreichend ist.

Die Zertifizierungsstelle kann einen Evaluierungsplan u. a. ablehnen, wenn er unvollständig ist, kein Einvernehmen über die Planung erzielt werden kann oder wenn die Fachkompetenz der Prüfstelle oder der eingesetzten Evaluatoren nicht hinreichend nachgewiesen ist.

Die Beteiligten verpflichten sich, Abweichungen von der vereinbarten Zeitplanung den anderen Beteiligten mitzuteilen und den Zeitplan erneut abzustimmen. Regelmäßige Telefonkonferenzen zum Abgleich des Verfahrensstatus werden empfohlen.

5.3.2 Evaluierungsvertrag

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

5.3.3 Gültigkeit von Standards und Interpretationen

Mit der offiziellen Annahme eines Zertifizierungsantrages werden die relevanten Versionen der Prüfkriterien und Interpretationen (AIS) festgelegt. Ein Übergang auf neuere, von der Zertifizierungsstelle anerkannte und in Dokument „Verzeichnisse“ [Verzeichnisse] aufgeführte Versionen, ist auf expliziten Wunsch des Antragstellers und unter Zustimmung aller beteiligten Parteien während des laufenden Verfahrens möglich.

Die Schemadokumente für NESAS sind in der vom BSI als verbindlich veröffentlichten Version zu verwenden. Bei Verfügbarkeit einer neuen Version der Kriterien wird, sobald sie vom BSI dafür freigegeben sind, für neue Verfahren eine Übergangszeit in Abhängigkeit vom Umfang der Änderungen gewährt.

Dokumente der GSMA, SCAS-Tests oder sonstige mit NESAS in Verbindung stehende Dokumente, die nicht von der Zertifizierungsstelle verantwortet werden, finden in der zum Antragszeitpunkt bestehenden Fassung Anwendung. Änderungen der Fassungen im laufenden Verfahren sind auf expliziten Wunsch des Antragstellers und unter Zustimmung aller beteiligten Parteienwährend des laufenden Verfahrens möglich.

5.3.4 Wiederverwendung von Prüfergebnissen

Die Wiederverwendung von Prüfergebnissen der Evaluierung eines Netzwerkproduktes für ein anderes Zertifizierungsverfahren eines Netzwerkproduktes von demselben Antragsteller ist nicht möglich.

5.3.5 Zertifizierungsnummer

Die Zertifizierungsnummer ist die Vorgangskennung beim BSI; sie wird bei jedem Schriftwechsel zur Kennzeichnung von Dokumenten und des Zertifizierungsreports verwendet.

Produktzertifikat: **BSI-DSZ-NESAS-nnnn-jjjj**

(DSZ= Deutsches IT-Sicherheitszertifikat, NESAS= Angabe des Kriterienwerkes, nnnn = laufende Antragsnummer, jjjj = Jahr der Erteilung des Zertifikats (wird erst bei Erteilung des Zertifikats angefügt)).

Rezertifizierung: **BSI-DSZ-NESAS-nnnn-Vx-jjjj**

Ergänzung der jeweiligen Zertifizierungsnummer um eine Versionsnummer: (nnnn=bisherige laufende Antragsnummer, Vx=Versionskennung der Rezertifizierung, jjjj=Jahr der Rezertifizierung).

5.4 Rahmenbedingungen zur Aufrechterhaltung eines NESAS-Zertifikates

5.4.1 Gültigkeit und ihre Randbedingungen

Ein Produktzertifikat bezieht sich auf die angegebene Version des Produktes sowie geringfügige Aktualisierungen am Produkt, wenn alle Auflagen hinsichtlich der Generierung, der Konfiguration und dem Einsatz des Produktes beachtet werden, die im Zertifizierungsreport beschrieben sind.

Ein Zertifikat bestätigt die Vertrauenswürdigkeit des Produktes gemäß den zugrunde gelegten Auditierungs- und Evaluierungsvorgaben zum Zeitpunkt der Ausstellung.

Auflagen für den Anwender ergeben sich aus dem Zertifizierungsreport. Auflagen und andere Nebenbestimmungen für den Zertifikatsinhaber ergeben sich aus dem Zertifizierungsbescheid. Der Anwender eines zertifizierten Produktes muss die mit dem Zertifikat zum Ausdruck gebrachten Ergebnisse, Randbedingungen und Auflagen in seinem Risikomanagementprozess berücksichtigen.

5.4.2 Zeitliche Befristung

Die Zertifizierungsstelle muss gemäß den rechtlichen Grundlagen die formale Gültigkeit eines Zertifikates für das jeweilige Zertifizierungsprogramm zeitlich befristen. Dennoch bezieht sich die inhaltlich-technische Zertifikatsaussage zur Vertrauenswürdigkeit auf den Zeitpunkt der Ausstellung, da eine Vorhersage der Angriffsresistenz in die Zukunft schwierig ist und individuell sehr unterschiedlich sein kann. Durch eine geringfügige Aktualisierung erfolgt keine Verlängerung der Zertifikatslaufzeit. Die zeitliche Befristung eines Zertifikates bleibt durch eine geringfügige Aktualisierung unberührt.

5.4.2.1 Gültigkeit eines NESAS-Audits

Ein NESAS-Audit besitzt eine Gültigkeit von zwei Jahren ab dem Datum des finalisierten Auditberichtes für die darin angegebene Version der Sicherheitsanforderungen aus dem Dokument „NESAS Development and Lifecycle Security Requirements“ [FS.16]. Ein Audit darf zu Beginn einer Evaluierung nicht älter als zwei Jahre sein. Wurden

- durch den Hersteller wesentliche Änderungen der beim Audit betrachteten Prozesse vorgenommen oder
- eine Sicherheitsverletzung beim Hersteller festgestellt, die Auswirkungen auf auditierte Prozesse haben, muss eine erneute Auditierung für darauf basierende Evaluierungen erfolgen.

5.4.2.2 Gültigkeit eines NESAS-Zertifikates

Die inhaltlich-technische Zertifikatsaussage zur Vertrauenswürdigkeit ist auf den Zeitpunkt der Ausstellung des Zertifikates bezogen. Die formale Gültigkeit eines IT-Sicherheitszertifikates ist aufgrund des Fortschritts der Technik grundsätzlich auf zwei Jahre zeitlich befristet. Abweichende Fälle können aufgrund besonderer rechtlicher Rahmenbedingungen für bestimmte Produktklassen festgelegt werden.

5.5 Kosten

Das BSI stellt dem Antragsteller Gebühren und Auslagen auf Basis der Gebührenverordnung des BMI [BMIBGebV] in Rechnung. Dabei wird nach Aufwand abgerechnet. Die Vorgespräche mit dem BSI vor Antragstellung sind kostenfrei.

Zu den Auslagen gehören auch die Kosten für das Audit. Die Vergütung der Auditoren erfolgt nach Aufwand, Reisekosten werden gemäß Bundesreisekostengesetz abgerechnet.

Die Abrechnung der bei der Prüfstelle anfallenden Evaluierungskosten wird zwischen Antragsteller und Prüfstelle vertraglich vereinbart. Der Aufwand für die Evaluierung hängt von der Komplexität des Produktes und dem Produkttyp ab und kann nicht pauschal beziffert werden. Die Prüfstellen können auf Anfrage Schätzwerte angeben oder erstellen entsprechende Angebote.

Für die Abrechnung ergeht ein Kostenbescheid des BSI. Die für die Buchhaltung notwendigen Daten zur Rechnungsstellung durch das BSI lassen sich bei folgender Mail-Adresse erfragen: forderungsmanagement-z21@bsi.bund.de

Bei Antragstellung durch eine Behörde gelten besondere Regelungen, die im Einzelfall besprochen werden.

5.6 Kontakt zur Zertifizierungsstelle

Erster Ansprechpartner bei laufenden Zertifizierungsverfahren ist der zugewiesene Zertifizierer. Die Kontaktdaten sind dem jeweiligen Schreiben zur Aufnahme des Verfahrens (ID-Vergabe) zu entnehmen.

Übergeordnete Fragen zur Zertifizierung oder zu den Prüfkriterien können adressiert werden an:

- E-Mail: nesas@bsi.bund.de
- Telefon: +49 (0) 800 274 1000 oder an die
- Organisationseinheit: referat-s26@bsi.bund.de.

Telefonisch kann bei Nichterreichen des Zertifizierers die zentrale Rufnummer des BSI (Telefon: +49 (0) 800 274 1000) mit Nennung des Zertifizierungsreferates S 26 oder das Geschäftszimmer Abteilung S kontaktiert werden.

Dokumente zur Zertifizierung müssen an die zentrale E-Mail-Adresse: nesas@bsi.bund.de gesendet werden. Ein PGP-Schlüssel steht auf der Internetseite des BSI in der Rubrik „Zertifizierung und Anerkennung / Zertifizierung von Produkten / Zertifizierung nach NESAS CCS-GI“ zur Verfügung.

6 Veröffentlichung der Zertifizierung

6.1 Veröffentlichung durch das BSI

Informationen zu zertifizierten Netzwerkprodukten werden vom BSI in folgenden regelmäßig aktualisierten Publikationen veröffentlicht:

- BSI-Forum (Organ des BSI in der Zeitschrift KES): In dieser Publikation wird der Inhalt eines seit der letzten Ausgabe der Zeitschrift neu erteilten Zertifikates zusammenfassend dargestellt.
- Rubrik „Zertifizierung und Anerkennung“ auf den Internetseiten des BSI: Hier werden in Form von Übersichtslisten Zertifikate aufgelistet und der Zertifizierungsreport und etwaige Ergänzungen zum Download angeboten.

Widerruft der Antragsteller schriftlich gegenüber dem BSI die im Antrag gemachte Zustimmung zur Veröffentlichung des Zertifizierungsergebnisses oder wurde diese im Antrag nicht erteilt, erfolgt keine Nennung in den genannten Publikationen.

7 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.