Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-1180-2025

zu

macmon NAC, Version 5.36.2

der

macmon secure GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1180-2025 (*)

System zur Netzwerkzugriffskontrolle (NAC)

macmon NAC
Version 5.36.2

von	macmon secure GmbH
PP-Konformität:	Keine
Funktionalität:	Produktspezifische Sicherheitsvorgaben Common Criteria Teil 2 erweitert
Vertrauenswürdigkeit:	Common Criteria Teil 3 konform EAL 2 mit Zusatz von ALC_FLR.1
Gültig bis:	04. Mai 2030

SOGIS
Recognition Agreement

Common Criteria

Das in diesem Zertifikat genannte IT-Produkt wurde von einer anerkannten Prüfstelle nach der Gemeinsamen Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 3.1 ergänzt um Interpretationen des Zertifizierungsschemas unter Nutzung der Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 3.1 (CC) evaluiert. CC und CEM sind ebenso als Norm ISO/IEC 15408 und ISO/IEC 18045 veröffentlicht.

(*) Dieses Zertifikat gilt nur für die angegebene Version des Produktes in der evaluierten Konfiguration und nur in Verbindung mit dem vollständigen Zertifizierungsreport und -bescheid. Details zur Gültigkeit sind dem Zertifizierungsreport Teil A, Kap. 5 zu entnehmen.

Common Criteria
Recognition Arrangement

Die Evaluation wurde in Übereinstimmung mit den Bestimmungen des Zertifizierungsschemas des Bundesamtes für Sicherheit in der Informationstechnik durchgeführt. Die im Evaluationsbericht enthaltenen Schlussfolgerungen der Prüfstelle sind in Einklang mit den erbrachten Nachweisen.

Dieses Zertifikat ist keine generelle Empfehlung des IT-Produktes durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte. Eine Gewährleistung für das IT-Produkt durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte, ist weder enthalten noch zum Ausdruck gebracht.

Bonn, 5. Mai 2025

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Sandro Amendola L.S.
Direktor

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

Dies ist eine eingefügte Leerseite.

Gliederung

A. Zertifizierung....7
1. Vorbemerkung....7
2. Grundlagen des Zertifizierungsverfahrens....7
3. Anerkennungsvereinbarungen....8
4. Durchführung der Evaluierung und Zertifizierung....9
5. Gültigkeit des Zertifizierungsergebnisses....9
6. Veröffentlichung....10
B. Zertifizierungsbericht....11
1. Zusammenfassung....12
2. Identifikation des EVG....15
3. Sicherheitspolitik....17
4. Annahmen und Klärung des Einsatzbereiches....17
5. Informationen zur Architektur....18
6. Dokumentation....19
7. Testverfahren....19
8. Evaluierte Konfiguration....25
9. Ergebnis der Evaluierung....26
10. Auflagen und Hinweise zur Benutzung des EVG....27
11. Sicherheitsvorgaben....27
12. Regulation specific aspects (eIDAS, QES)....28
13. Definitionen....28
14. Literaturangaben....29
C. Auszüge aus den Kriterien....31

A. Zertifizierung

1. Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSIG1 die Aufgabe, für Produkte (Systeme oder Komponenten) der Informationstechnik, Sicherheitszertifikate zu erteilen.

Die Zertifizierung eines Produktes wird auf Veranlassung des Herstellers oder eines Vertreibers - im folgenden Antragsteller genannt - durchgeführt.

Bestandteil des Verfahrens ist die technische Prüfung (Evaluierung) des Produktes gemäß den vom BSI öffentlich bekannt gemachten oder allgemein anerkannten Sicherheitskriterien.

Die Prüfung wird in der Regel von einer vom BSI anerkannten Prüfstelle oder vom BSI selbst durchgeführt.

Das Ergebnis des Zertifizierungsverfahrens ist der vorliegende Zertifizierungsreport. Hierin enthalten sind u. a. das Sicherheitszertifikat (zusammenfassende Bewertung) und der detaillierte Zertifizierungsbericht.

Der Zertifizierungsbericht enthält die sicherheitstechnische Beschreibung des zertifizierten Produktes, die Einzelheiten der Bewertung und Hinweise für den Anwender.

2. Grundlagen des Zertifizierungsverfahrens

Die Zertifizierungsstelle führt das Verfahren nach Maßgabe der folgenden Vorgaben durch:

- BSI-Gesetz[1]
- BSI-Zertifizierungs- und - Anerkennungsverordnung[2]
- Besondere Gebührenverordnung BMI (BMIBGebV)[3]
- besondere Erlasse des Bundesministeriums des Innern und für Heimat
- die Norm DIN EN ISO/IEC 17065
- BSI-Zertifizierung: Verfahrensdokumentation zum Zertifizierungsprozess (CC-Produkte) [3]
- BSI Zertifizierung: Verfahrensdokumentation zu Anforderungen an Prüfstellen, deren Anerkennung und Lizenzierung (CC-Stellen) [3]

1 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. August 2009, Bundesgesetzblatt I S. 2821

2 Verordnung über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungs- und - Anerkennungsverordnung - BSIZertV) vom 17. Dezember 2014, Bundesgesetzblatt Jahrgang 2014 Teil I, Nr. 61, S. 2231

3 Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen indessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) vom 2. September 2019, Bundesgesetzblatt I S. 1365

- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation/CC), Version 3.1[4] [1], auch als Norm ISO/IEC 15408 veröffentlicht
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Methodology for Information Technology Security Evaluation/CEM), Version 3.1 [2] auch als Norm ISO/IEC 18045 veröffentlicht
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS) [4]

3. Anerkennungsvereinbarungen

Um die Mehrfach-Zertifizierung des gleichen Produktes in verschiedenen Staaten zu vermeiden, wurde eine gegenseitige Anerkennung von IT-Sicherheitszertifikaten - sofern sie auf ITSEC oder Common Criteria (CC) beruhen - unter gewissen Bedingungen vereinbart.

3.1. Europäische Anerkennung von CC – Zertifikaten (SOGIS-MRA)

Das SOGIS-Anerkennungsabkommen (SOGIS-MRA) Version 3 ist im April 2010 in Kraft getreten. Es legt die Anerkennung von Zertifikaten für IT-Produkte auf einer Basisanerkennungsstufe und zusätzlich für IT-Produkte aus bestimmten Technischen Bereichen (SOGIS Technical Domain) auf höheren Anerkennungsstufen fest.

Die Basisanerkennungsstufe schließt die Common Criteria (CC) Vertrauenswürdigkeitsstufen EAL 1 bis EAL 4 ein. Für Produkte im technischen Bereich "smartcard and similar devices" ist eine SOGIS Technical Domain festgelegt. Für Produkte im technischen Bereich "HW Devices with Security Boxes" ist ebenfalls eine SOGIS Technical Domain festgelegt. Des Weiteren erfasst das Anerkennungsabkommen auch erteilte Zertifikate für Schutzprofile (Protection Profiles) basierend auf den Common Criteria.

Eine aktuelle Liste der Unterzeichnerstaaten bzw. der anerkannten Zertifizierungsstellen, Details zur Anerkennung sowie zur Historie des Abkommens können auf der Internetseite https://www.sogis.eu eingesehen werden.

Das SOGIS-MRA-Logo auf dem Zertifikat zeigt, dass das Zertifikat unter den Bedingungen des Abkommens von den jeweiligen Stellen der Unterzeichnerstaaten als gleichwertig anerkannt wird. Ein Hinweis unter dem Logo weist auf einen spezifischen Umfang der Anerkennung hin.

Dieses Zertifikat fällt mit allen ausgewählten Vertrauenswürdigkeitskomponenten unter die Anerkennung nach SOGIS-MRA.

3.2. Internationale Anerkennung von CC - Zertifikaten

Das internationale Abkommen zur gegenseitigen Anerkennung von Zertifikaten basierend auf CC (Common Criteria Recognition Arrangement, CCRA-2014) wurde am 8. September 2014 ratifiziert. Es deckt CC-Zertifikate ab, die auf sog. collaborative Protection Profiles (cPP) (exact use) basieren, CC-Zertifikate, die auf Vertrauenswürdigkeitsstufen bis einschließlich EAL 2 oder die Vertrauenswürdigkeitsfamilie Fehlerbehebung (Flaw Remediation, ALC_FLR) basieren und CC Zertifikate für Schutzprofile (Protection Profiles) und für collaborative Protection Profiles (cPP).

[4] Bekanntmachung des Bundesministeriums des Innern und für Heimat vom 12. Februar 2007 im Bundesanzeiger, datiert 23. Februar 2007, S. 1941

Eine aktuelle Liste der Unterzeichnerstaaten bzw. der anerkannten Zertifizierungsstellen kann auf der Internetseite https://www.commoncriteriaportal.org eingesehen werden.

Das CCRA-Logo auf dem Zertifikat zeigt, dass das Zertifikat unter den Bedingungen des Abkommens von den jeweiligen Stellen der Unterzeichnerstaaten als gleichwertig anerkannt wird. Ein Hinweis unter dem Logo weist auf einen spezifischen Umfang der Anerkennung hin.

Dieses Zertifikat fällt unter die Anerkennungsregeln des CCRA-2014 für alle ausgewählten Vertrauenswürdigkeitskomponenten.

4. Durchführung der Evaluierung und Zertifizierung

Die Zertifizierungsstelle führt für jede einzelne Evaluierung eine Prüfbegleitung durch, um einheitliches Vorgehen, einheitliche Interpretation der Kriterienwerke und einheitliche Bewertungen sicherzustellen.

Das Produkt macmon NAC, Version 5.36.2 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts macmon NAC, Version 5.36.2 wurde von TÜV Informationstechnik GmbH durchgeführt. Die Evaluierung wurde am 31. März 2025 abgeschlossen. Das Prüflabor TÜV Informationstechnik GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[5].

Der Sponsor und Antragsteller ist: macmon secure GmbH.

Das Produkt wurde entwickelt von: macmon secure GmbH.

Die Zertifizierung wurde damit beendet, dass das BSI die Übereinstimmung mit den Kriterien überprüft und den vorliegenden Zertifizierungsreport erstellt hat.

5. Gültigkeit des Zertifizierungsergebnisses

Dieser Zertifizierungsreport bezieht sich nur auf die angegebene Version des Produktes. Das Produkt ist unter den folgenden Bedingungen konform zu den bestätigten Vertrauenswürdigkeitskomponenten:

- alle Auflagen hinsichtlich der Generierung, der Konfiguration und dem Einsatz des EVG, die in diesem Report gestellt werden, werden beachtet.
- das Produkt wird in der Umgebung betrieben, die in diesem Report und in den Sicherheitsvorgaben beschrieben ist.

Die Bedeutung der Vertrauenswürdigkeitskomponenten und -stufen kann direkt den CC entnommen werden. Detaillierte Referenzen sind in Teil C dieses Reportes aufgelistet.

Das Zertifikat bestätigt die Vertrauenswürdigkeit des Produktes gemäß den Sicherheitsvorgaben zum Zeitpunkt der Ausstellung. Da sich Angriffsmethoden im Laufe der Zeit fortentwickeln, ist es erforderlich, die Widerstandsfähigkeit des Produktes regelmäßig überprüfen zu lassen. Aus diesem Grunde sollte der Hersteller das zertifizierte Produkt im Rahmen des Assurance Continuity-Programms des BSI überwachen lassen (z.B. durch eine Neubewertung oder eine Re-Zertifizierung). Insbesondere wenn Ergebnisse aus dem Zertifizierungsverfahren in einem nachfolgenden Evaluierung- und Zertifizierungsverfahren oder in einer Systemintegration verwendet werden oder wenn das

[5] Information Technology Security Evaluation Facility

Risikomanagement eines Anwenders eine regelmäßige Aktualisierung verlangt, wird empfohlen, die Neubewertung der Widerstandsfähigkeit regelmäßig, z.B. jährlich vorzunehmen.

Um in Anbetracht der sich weiter entwickelnden Angriffsmethoden eine unbefristete Anwendung des Zertifikates trotz der Erfordernis nach einer Neubewertung nach den Stand der Technik zu verhindern, wurde die maximale Gültigkeit des Zertifikates begrenzt. Dieses Zertifikat, erteilt am 5. Mai 2025, ist gültig bis 04. Mai 2030. Die Gültigkeit kann im Rahmen einer Re-Zertifizierung erneuert werden.

Der Inhaber des Zertifikates ist verpflichtet,

1. bei der Bewerbung des Zertifikates oder der Tatsache der Zertifizierung des Produktes auf den Zertifizierungsreport hinzuweisen sowie jedem Anwender des Produktes den Zertifizierungsreport und die darin referenzierten Sicherheitsvorgaben und Benutzerdokumentation für den Einsatz oder die Verwendung des zertifizierten Produktes zur Verfügung zu stellen,
2. die Zertifizierungsstelle des BSI unverzüglich über Schwachstellen des Produktes zu informieren, die nach dem Zeitpunkt der Zertifizierung durch Sie oder Dritte festgestellt wurden,
3. die Zertifizierungsstelle des BSI unverzüglich zu informieren, wenn sich sicherheitsrelevante Änderungen am geprüften Lebenszyklus, z. B. an Standorten oder Prozessen ergeben oder die Vertraulichkeit von Unterlagen und Informationen zum Evaluierungsgegenstand oder aus dem Evaluierungs- und Zertifizierungsprozess, bei denen die Zertifizierung des Produktes aber von der Aufrechterhaltung der Vertraulichkeit für den Bestand des Zertifikates ausgegangen ist, nicht mehr gegeben ist. Insbesondere ist vor Herausgabe von vertraulichen Unterlagen oder Informationen zum Evaluierungsgegenstand oder aus dem Evaluierungs- und Zertifizierungsprozess, die nicht zum Lieferumfang gemäß Zertifizierungsreport Teil B gehören oder für die keine Weitergaberegelung vereinbart ist, an Dritte, die Zertifizierungsstelle des BSI zu informieren.

Bei Änderungen am Produkt kann die Gültigkeit des Zertifikats auf neue Versionen ausgedehnt werden. Voraussetzung dafür ist, dass der Antragsteller die Aufrechterhaltung der Vertrauenswürdigkeit (d.h. eine Re-Zertifizierung oder ein Maintenance Verfahren) in Übereinstimmung mit den entsprechenden Regeln beantragt und die Evaluierung keine Schwächen aufdeckt.

6. Veröffentlichung

Das Produkt macmon NAC, Version 5.36.2 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: https://www.bsi.bund.de und [5]). Nähere Informationen sind über die BSI-Infoline 0228/9582-111 zu erhalten.

Weitere Exemplare des vorliegenden Zertifizierungsreports können beim Hersteller des Produktes angefordert werden[6]. Der Zertifizierungsreport kann ebenso in elektronischer Form von der oben angegebenen Internetadresse heruntergeladen werden.

[6] macmon secure GmbH
Alte Jakobstraße 79-80
10179 Berlin

B. Zertifizierungsbericht

Der nachfolgende Bericht ist eine Zusammenfassung aus

- den Sicherheitsvorgaben des Antragstellers für den Evaluationsgegenstand,
- den entsprechenden Prüfergebnissen des Prüflabors und
- ergänzenden Hinweisen und Auflagen der Zertifizierungsstelle.

1. Zusammenfassung

Der Evaluierungsgegenstand (EVG) ist ein System zur Kontrolle des Zugriffs von Endgeräten auf ein Netzwerk. Der Einsatz von macmon NAC ermöglicht die Verwaltung und Überwachung des Netzwerks und der enthaltenen Netzwerkgeräte und Endgeräte. Damit gehört das TOE zu den Network Access Control (NAC)-Systemen. Der macmon-Server wird an zentraler Stelle in das bestehende Netzwerk eingebunden. Von diesem Server werden unterschiedliche Daten von verschiedenen Geräten im Netzwerk abgefragt. Auf Grundlage der erfassten Daten wird die Authentifizierung und Autorisierung von Endgeräten vorgenommen. Dadurch werden der Schutz des Netzwerkes und dessen Ressourcen vor unbekannten oder nicht-autorisierten Endgeräten gewährleistet.

Die Sicherheitsvorgaben [6] stellen die Grundlage für die Zertifizierung dar. Sie verwenden kein zertifiziertes Protection Profiles.

Die Vertrauenswürdigkeitskomponenten (Security Assurance Requirements SAR) sind dem Teil 3 der Common Criteria entnommen (siehe Teil C oder [1], Teil 3). Der EVG erfüllt die Anforderungen der Vertrauenswürdigkeitsstufe EAL 2 mit Zusatz von ALC_FLR.1.

Die funktionalen Sicherheitsanforderungen (Security Functional Requirements SFR) an den EVG werden in den Sicherheitsvorgaben [6] Kapitel 6.2 beschrieben. Sie wurden dem Teil 2 der Common Criteria entnommen und durch neu definierte funktionale Sicherheitsanforderungen ergänzt. Der EVG ist daher gekennzeichnet als CC Teil 2 erweitert.

Die funktionalen Sicherheitsanforderungen werden durch die folgende Sicherheitsfunktionalität des EVG umgesetzt:

Sicherheitsfunktionalität des EVG	**Thema**
SF Audit	Der TOE generiert zu sicherheitskritischen Ereignissen und allen Änderungen an den TSF-Daten immer Auditdaten in Form von Datenbankeinträgen oder Logdateien. Die Auditdaten zu Änderungen an den TSF werden hierbei immer dem verantwortlichen Benutzer zugewiesen. Alle vom TOE generierten Auditdaten können vom Administrator, dem Operator, dem Helpdesk und dem Revisor über die webbasierte Benutzeroberfläche des Management-Servers abgefragt werden. Der Zugriff des Helpdesk ist auf Berichte zu Endgeräten beschränkt. Der Zugriff auf die Auditdaten ist ausschließlich für autorisierte Benutzer möglich, welche sich zuvor erfolgreich am TOE angemeldet haben. Die Auditdaten werden über die Benutzeroberfläche für den Benutzer in Form von Logdateien oder Berichten aufbereitet. Die so aufbereiteten Daten können beliebig gefiltert und sortiert werden. In den Berichten werden auch die abgefragten Informationen vom verwalteten Netzwerk dargestellt, wozu insbesondere die endgerätespezifischen Ereignisse gehören, wie wann ein Endgerät mit dem Netzwerk verbunden war. Auch werden das Ergebnis der Authentifizierung eines Endgerätes im Netzwerk und potenzielle Reaktionen auf dessen Autorisierung gespeichert. Alle Auditdaten sind in der Datenbank bzw. dem Dateisystem des TOEs gespeichert. Wenn die Kapazität der Datenbank erschöpft ist, werden neue Informationen ignoriert und eine Fehlermeldung an den Benutzer ausgegeben[7].

Sicherheitsfunktionalität des EVG	Thema
SF I&A	Vor jeglichem Zugriff auf die Benutzeroberfläche des Management-Servers verlangt der TOE, dass der Benutzer sich identifiziert. Alle ausgeführten Aktionen werden so vom TOE diesem Benutzer zugeordnet. Um die Identität des Benutzers festzustellen, muss sich dieser erfolgreich am TOE authentifizieren. Ohne erfolgreiche Authentifizierung hat ein Benutzer ausschließlich Zugriff auf die Anmeldeseite des TOE. Die Anmeldung am TOE erfolgt über die Benutzeroberfläche mit der Eingabe des Benutzernamens und des Passwortes. Die Zugangsdaten werden dabei geschützt vom Browser zum TOE übertragen, wo diese dann mit den gespeicherten Daten abgeglichen werden. Das Passwort wird dabei vom TOE ausschließlich als Hashwert vorgehalten. Schlägt die Authentifizierung fehl, wird der Benutzer erneut zur Eingabe der Zugangsdaten aufgefordert. Das TOE unterstützt mehrfache, simultane Verbindungen zum Management-Server und assoziiert die Sicherheitsattribute individuell zu den Verbindungen. Ändern sich die Sicherheitsattribute eines Benutzers zur Laufzeit, werden die Berechtigungen sofort angepasst und der Benutzer verliert möglicherweise den Zugriff auf Bereiche, die er zuvor noch aufrufen konnte. Ebenfalls ist es möglich, einen Benutzer zur Laufzeit zu deaktivieren, so dass dieser zur nächsten Benutzeraktion keinen Zugriff mehr auf den TOE bekommt.
SF Management	Das TOE bietet Managementmöglichkeiten über die Benutzeroberfläche, um den TOE kontrollieren und überwachen zu können. Dabei haben die Benutzer unterschiedliche Berechtigungen auf die Funktionen und Daten zum Management des TOEs. Die Berechtigungen werden mit der Rolle des jeweiligen Benutzers assoziiert. Sicherheitskritische Funktionen können nur von Benutzern mit den Rollen Administrator und Operator deaktiviert oder angepasst werden, während der Benutzer mit der Rolle Revisor nur den aktuellen Status der Funktionen ermitteln kann. Das gleiche gilt für den Zugang zu allen TSF-Daten, wobei hier zusätzlich die Benutzer mit der Rolle Helpdesk Zugriff auf die Eigenschaften von autorisierten Endgeräten haben. Insgesamt bietet der TOE die folgenden Managementfunktionen zur Verwaltung der folgenden Objekte an: ● Benutzern ● NAC-Regeln ● Systemeinstellungen ● Autorisierte Endgeräte ● Netzwerkkomponenten Über die Managementfunktionen zur Verwaltung von Benutzern hat der Administrator die Möglichkeit, einem Benutzer die vordefinierten Rollen Administrator, Operator, Helpdesk und Revisor zuzuweisen. Eine Änderung des Passwortes ist nur für den eigenen Account möglich. Ausgenommen sind hierbei Benutzer mit der Rolle Administrator, welche alle Passwörter über die Benutzerverwaltung verändern können. Zum Schutz eines unbemerkten Ausfalls der Sicherheitsleistung des TOEs führt das TOE periodisch Selbsttests durch. Hierbei werden die verschiedenen Subsysteme des TOEs vom Management-Server kontrolliert. Bemerkt der Management-Server den Ausfall eines Subsystems, wird dies neugestartet. Außerdem werden Ausfälle

[7] Die Fehlermeldungen werden jedem Benutzer angezeigt, der sich an der Benutzeroberfläche anmeldet.

Sicherheitsfunktionalität des EVG	Thema
	der einzelnen Subsysteme auch auf der Startseite der GUI dargestellt. Diese Schutzfunktion ist nur funktionsfähig, solange der Management-Server nicht komplett ausfällt [8].
SF NAC	Zur Überwachung des verwalteten Netzwerks sammelt der TOE periodisch Daten von Netzwerkkomponenten ein oder erhält Endgeräte-802.1X-Zugangsdaten von Netzwerkverteilern zur Verifizierung. Alle gesammelten Daten enthalten dabei insbesondere die Information, wann (Start- und Endzeitpunkt), von welchem Standort (physikalischer Port) und in welchem Umfang (VLAN-Autorisierung) der Endgeräte-Zugriff auf das Netzwerk bestand. Außerdem enthalten die Daten Informationen darüber, ob dessen Zugriff abgelehnt wurde oder sich dessen Autorisierung verändert hat. Das Endgerät selbst wird dabei anhand seiner MAC-Adresse und den 802.1X-Zugangsdaten identifiziert. Die Autorisierung eines Endgerätes wird auf Grundlage der Analyse der gesammelten Daten vorgenommen. Die Authentifizierung wird mit Hilfe der 802.1X-Zugangsdaten (Benutzername/Passwort oder Zertifikat) und der Liste autorisierter Endgeräte bestimmt. Anhand der Konfiguration am Endgerät und/oder weiterer Regeln wird dann die Autorisierung berechnet. Das Ergebnis der Autorisierung wird vom TOE an den Netzwerkverteiler zurückgeschickt, welcher auf Basis der Daten reagiert. Als Reaktion kann der Netzwerkverteiler den Zugriff auf das Netzwerk freigeben oder verwehren. Darüber hinaus werden vom TOE direkt als Reaktion E-Mails versendet, falls bei der Abfrage der Netzwerkgeräte nicht autorisierte Endgeräte erkannt werden. Alle gesammelten Daten, Analyseergebnisse und ausgeführte Reaktionen werden vom TOE über die grafische Oberfläche für den Administrator, Operator, Helpdesk und Revisor zur Verfügung gestellt. Sonstige Benutzer erhalten vom TOE keinen Zugriff auf diese Daten.

Tabelle 1: Sicherheitsfunktionalität des EVG

Mehr Details sind in den Sicherheitsvorgaben [6] Kapitel 7.1 dargestellt.

Die Werte, die durch den EVG geschützt werden, sind in den Sicherheitsvorgaben [6], Kapitel 3.1.2 definiert. Basierend auf diesen Werten stellen die Sicherheitsvorgaben die Sicherheitsumgebung in Form von Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken in Kapitel 3.2, 3.3 und 3.4 dar.

Dieses Zertifikat umfasst die Konfigurationen des EVG, wie sie in Kapitel 8 beschrieben sind.

Die Ergebnisse der Schwachstellenanalyse, wie in diesem Zertifikat bestätigt, erfolgte ohne Einbeziehung der für die Ver- und Entschlüsselung eingesetzten kryptographischen Algorithmen (vgl. §9 Abs. 4 Nr. 2 BSIG). Für Details siehe Kap. 9 dieses Berichtes.

Dieses Zertifikat gilt nur für die angegebene Version des Produktes in der evaluierten Konfiguration und nur in Verbindung mit dem vollständigen Zertifizierungsreport. Dieses Zertifikat ist keine generelle Empfehlung des IT-Produktes durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte. Eine Gewährleistung für das IT-Produkt durch das

[8] Wenn der Server ausfällt, kann der TOE keine Informationen mehr zu den Subsystemen anzeigen, wobei dann der RADIUS nicht erreichbar und ein Zugang zum Netzwerk nicht mehr möglich ist.

Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte, ist weder enthalten noch zum Ausdruck gebracht.

2. Identifikation des EVG

Der Evaluierungsgegenstand (EVG) heißt:

macmon NAC, Version 5.36.2

Die folgende Tabelle beschreibt den Auslieferungsumfang. Bei den Hashwerten handelt es sich um SHA-256 Hashwerte:

Nr.	Typ	Identifier	Version	Auslieferungsart
1	SW	OVF-Image (ESX 7.0) macmon-appliance-virtual_5.36.2_ovf_ESX7.0.zip 5666 619C AE00 3B14 6377 9B2C 9A89 2519 8DC2 5A34 196E 0D5C 9A90 744A 1A7B 8188	5.36.2	Auslieferung durch Download von der macmon Webseite.
2	DOC	Appliance-Inbetriebnahme [10]: macmon_5.36.2_appliance_ApplianceGettingStarted-de_DE.pdf A9AE 0824 5B04 C6F6 CAB1 5A0F A9ED 36F8 7F45 AD1D 65B6 914D 21CF 95F9 5CF0 FE1B	5.36.2	Auslieferung durch Download von der macmon Webseite.
3	DOC	Appliance Handbuch [11]: macmon_5.36.2_appliance_ApplianceManual-de_DE.pdf D0F7 19CA BBEA A19A CDF6 1E87 9DD1 1850 3B6F 7B94 DE0F 04D3 9F45 3442 788C E409	5.36.2	Auslieferung durch Download von der macmon Webseite.
4	DOC	macmon-Handbuch [9]: macmon_5.36.2_macmon_macmon_manual-de_DE.pdf 38F5 C00E 3577 0F20 4A86 42B1 7C0C 27F0 8361 30DD 6559 F2C8 E255 4A9F A577 E07B	5.36	Auslieferung durch Download von der macmon Webseite.
5	DOC	Common-Criteria Handbuch [12]: common-criteria_AGD_2.10.pdf 4305 4079 27D1 EB4A 1B5F 603F 1089 42E6 3B35 1C35 EC6A 3AA9 2E9E 7A38 2C13 9AAA	2.10	Auslieferung durch Download von der macmon Webseite.
6	DOC	macmon NAC Security Target [6]: common-criteria_ASE_3.8.pdf 21E1 A518 4028 0F17 C9A7 5E88 8A97 7975 47B2 65C0 BC1C 3A24 167D 6F65 C852 AF8F	3.8	Auslieferung durch Download von der macmon Webseite.
7	Hash	Hashwerte (SHA-256) für die EVG Softwareteile und der zugehörigen Dokumentation:		Auslieferung durch Angabe des Hashwerts auf der macmon Webseite (für Nr. 1 – Nr. 6).

Tabelle 2: Auslieferungsumfang des EVG inklusive den jeweiligen SHA-256 Hashwerten

2.1. EVG Auslieferungsprozess

Die virtuelle macmon-Appliance besteht aus einem OVF-Image mit vorinstalliertem macmon NAC. Das Image wird exportiert und inklusive der Prüfsumme für den Kunden im Service Portal bereitgestellt.

Wenn die virtuelle macmon-Appliance erworben wird, werden für das Lieferverfahren folgende Schritte durchgeführt:

1. Der Kunde erhält eine E-Mail mit der Rechnung, der Lizenzdatei und dem Lizenzzertifikat. Die Integrität der Lizenzdatei ist nicht als sicherheitskritisch anzusehen.
2. Parallel dazu wird der Kunde gebeten einen PGP-Schlüssel zur Verschlüsselung von E-Mails zu senden. Anschließend erhält er dann eine personalisierte und verschlüsselte E-Mail mit seinen Zugangsdaten zum Service Portal des Herstellers. Besitzt der Kunde keinen PGP-Schlüssel, werden die Zugangsdaten per Post versendet.
3. Mit den Zugangsdaten kann der Kunde das OVF-Image der macmon-Appliance für die zertifizierte macmon-Version herunterladen (Tabelle 2, #1-#2). Das Service Portal ist mit einer SSL-Verschlüsselung gesichert und stellt neben dem OVF-Image auch alle benötigen Handbücher zum Herunterladen bereit (Tabelle 2, #4-#6).
4. Danach kann der Kunde mit dem OVF-Image das Produkt anhand des mitgelieferten Handbuches (Tabelle 5, #3) in seiner Virtualisierungsumgebung in Betrieb nehmen.

2.2. EVG Identifikation

Die Integrität des macmon-Appliance-Images ist über das gesamte Verfahren gesichert. Die Erstellung und Speicherung des Images auf internen abgesicherten Servern verhindert eine Integritätsverletzung durch nicht-autorisierte Dritte. Das Gleiche gilt für den Bezug des OVF-Images per Herunterladen über eine gesicherte Web-Seite. Die Integrität der Datei ist mit Hilfe des SSL-Protokolls geschützt. Zusätzlich kann der Kunde die Integrität über die auf der Web-Seite aufgeführten Prüfsummen (SHA256) kontrollieren.

Beim Bezug der Handbücher und des OVF-Images zur Installation der macmon-Software auf der macmon-Appliance überzeugt sich der Kunde von der Authentizität der URL und überprüft nach Abschluss der Downloads die Integrität der heruntergeladenen Dateien wie in [12, Kapitel 2.2.2] beschrieben:

Nach Durchführung der Annahme-Prozeduren und der Installation und Inbetriebnahme muss der Kunde sich versichern, dass das Produkt in der zertifizierten Version vorliegt. Hierzu muss die Version auf der Startseite der macmon-Benutzeroberfläche oben rechts mit der in [6, Kapitel 2] definierten Version verglichen werden.

Die Version der Appliance und deren Softwarekomponenten sind an die installierte macmon-Version gebunden. Die Version der macmon-Appliance und der Softwarekomponenten können vom Anwender wie folgt überprüft werden:

- Die Version der macmon-Appliance kann auf der Appliance-Oberfläche in der rechten Seitenleiste kontrolliert werden.
- Die Version des Betriebssystemkernels kann über den Befehl uname -r auf der Kommandozeile der Appliance aufgerufen werden.

- Die Versionen der Softwarekomponenten können über die Kommandozeile und den Befehl aptitude show PACKAGE_NAME abgefragt werden: Die Ausgabe kann mit den Versionen in [12, 2.2.2] verglichen werden.

3. Sicherheitspolitik

Die Sicherheitspolitik wird durch die funktionalen Sicherheitsanforderungen ausgedrückt und durch die Sicherheitsfunktionalität des EVG umgesetzt. Sie behandelt die folgenden Sachverhalte:

Der EVG ist ein System zur Kontrolle des Zugriffs von Endgeräten auf ein Netzwerk. Er ermöglicht die Verwaltung und Überwachung des Netzwerks und der enthaltenen Netzwerkgeräte und Endgeräte Es wird eine rollen basierte Zugriffskontrollpolitik implementiert, um administrativen Zugriff auf das System zu steuern. Der EVG setzt Sicherheitsrichtlinien in Bezug auf die folgenden Sicherheitsfunktionen Audit, Identifizierung und Authentifizierung, Management und Netzwerkzugriff durch. Spezifische Einzelheiten zu den oben genannten Sicherheitsmaßnahmen sind in Kapitel 7.1 des ST [6] zu finden.

4. Annahmen und Klärung des Einsatzbereiches

Die in den Sicherheitsvorgaben definierten Annahmen sowie Teile der Bedrohungen und organisatorischen Sicherheitspolitiken werden nicht durch den EVG selbst abgedeckt. Diese Aspekte führen zu Sicherheitszielen, die durch die EVG-Einsatzumgebung erfüllt werden müssen. Hierbei sind die folgenden Punkte relevant:

- OE.ENV_PROTECT: Schutz des Management-Servers: Die vom Management-Server benötigte Virtualisierungsplattform muss vor physikalischen und logischen Zugriffen durch unberechtigte Personen geschützt sein und der Zugriff darf nur vom internen Netzwerk möglich sein.
- OE.ENV_RESOURCE: Verfügbarkeit von Ressourcen: Die Virtualisierungsumgebung (macmonAppliance, siehe Kapitel 1.3.2 im ST [6]) und die darauf installierte Software müssen dem TOE zur Verfügung stehen, um dessen Funktionsfähigkeit zu gewährleisten.
- OE.ENV_NETWORK: Unterstütztes Netzwerk: Das TOE muss in das bestehende Netzwerk integrierbar sein und benötigte Protokolle müssen von den Netzwerkkomponenten unterstützt werden.
- OE.ENV_DEV: Schutz der autorisierten Endgeräte: Vom Administrator autorisierte Endgeräte mit RADIUS-Zugangsdaten und der installierte Web-Browser für den Zugriff auf den TOE müssen vor administrativen Zugriffen durch unberechtigte Personen gesichert sein.
- OE.TOE_INSTALL: Installation des TOEs: Das TOE muss ordnungsgemäß geliefert, installiert und konfiguriert werden. Der Verantwortliche muss dabei nach der Installationsanleitung des Herstellers handeln.
- OE.TOE_ADMIN: Administrator des TOEs: Der Administrator (Rolle Administrator oder Operator wie in Kapitel 3.1.1 im ST [6] definiert) des TOEs muss qualifiziert und geschult sein, den TOE zu bedienen. Der Administrator darf keine böswilligen Absichten haben.
- OE.TOE_USER: Alle Benutzer: Alle Benutzer des TOEs und die autorisierten Endgeräte müssen sicherstellen, dass ihre Zugangsdaten nicht für Dritte zugänglich sind.

- OE.AUD_TIME: Zeitstempel für Auditdaten: Die Betriebsumgebung muss Zeitstempel für die korrekte Erzeugung von Auditeinträgen liefern.

Details finden sich in den Sicherheitsvorgaben [6], Kapitel 4.2.

5. Informationen zur Architektur

Der EVG besteht aus den folgenden Subsystemen. Die Abbildung 1 gibt einen Überblick über diese:

- Manager: Der Datenmanager ist das Subsystem, welches für das Laden und Verwalter der TSF-Daten in den Speicher zuständig ist. Damit bietet der Manager den Zugriff auf die TSF-Daten für alle anderen Subsysteme an und eine API zur Bedienung von macmon.
- Monitoring: Das Monitoring ist das Subsystem zur Überwachung aller Netzwerkgeräte und sorgt für die periodischen Abfragen per SNMP und die Verarbeitung und Auswertung der empfangenen Daten.
- RADIUS-Handler: Der Handler für RADIUS-Anfragen ist das Subsystem, welches ankommende RADIUS-Anfragen annimmt, parallel verarbeitet und beantwortet.
- Event-Verarbeitung: Dieses Subsystem empfängt im System publizierten Ereignisse und verarbeitet diese. Ereignisse werden dabei anhand eines Regelwerks analysiert und bei Bedarf führt dieses Subsystem eine Reaktion auf das Ereignis aus.
- GUI: Die Bedienung von macmon geschieht primär über dieses Subsystem, welche eine webbasierte Benutzeroberfläche (GUI) darstellt. Alle Konfigurations- und Überwachungsarbeiten werden von dieser Oberfläche ausgeführt.

Die folgende Abbildung gibt einen grafischen Überblick über die Architektur des EVG unter Berücksichtigung der Subsysteme:

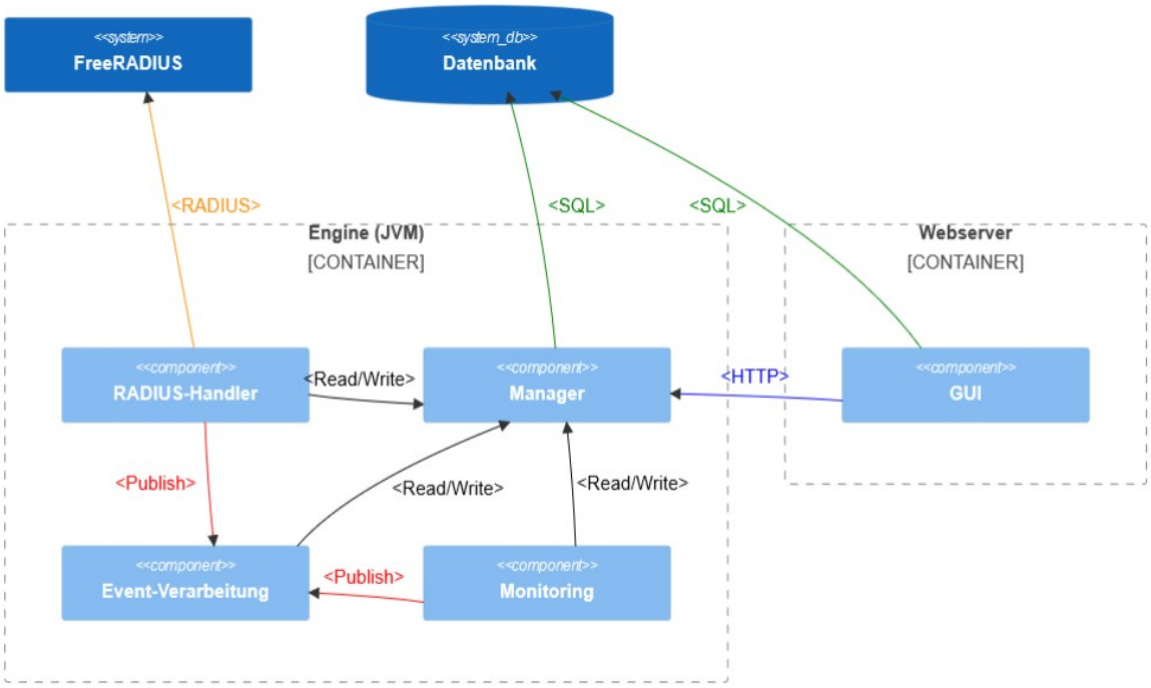

Abbildung 1: Architektur des EVG

6. Dokumentation

Die evaluierte Dokumentation, die in Tabelle 2 aufgeführt ist, wird zusammen mit dem Produkt zur Verfügung gestellt. Hier sind die Informationen enthalten, die zum sicheren Umgang mit dem EVG in Übereinstimmung mit den Sicherheitsvorgaben benötigt werden.

Zusätzliche Hinweise und Auflagen zum sicheren Gebrauch des EVG, die im Kapitel 10 enthalten sind, müssen befolgt werden.

7. Testverfahren

7.1. Genaue Beschreibung der evaluierten EVG-Konfiguration

Der evaluierte EVG ist macmon NAC mit der Version 5.36.2. Das Security Target [6] identifiziert nur eine Konfiguration des EVG. Diese wird durch strikte Einhaltung an die Anleitungen in den Benutzerhandbüchern [12] und [10] erreicht.

Die Einsatzumgebung des EVG in seiner evaluierten Konfiguration kann wie folgt zusammengefasst werden:

Aspekt	Einsatzumgebung
Virtualisierungssoftware	● VMware vSphere ab Version 7 ● VMware ESXi ab Version 7.0
Anforderung an die virtuelle Maschine	● 8 GB Arbeitsspeicher ● 1 CPU mit 4 Kernen ● 250 GB Festplatte

	● 1 GBit/s Netzwerkanschlüsse
Installierte Software	● Betriebssystem Debian Linux Kernel 4.19 ● Datenbank MariaDB 1:10.3.39-0+deb10u1 (DBMS: Datenbank-Management-System) ● Webserver Apache 2.4.38-3+deb10u10 ● PHP 7.3.31-1~deb10u4 ● OpenJDK 11.0.18+10-1~deb10u1 ● OpenSSL 1.1.1n-0+deb10u5 ● FreeRADIUS 3.0.17+dfsg-1.1+deb10u2 ● Mailserver Postfix 3.4.23-0+deb10u1
Web-Browser	● Microsoft Edge (90.0.818.62) ● Mozilla Firefox (88.0.1) ● Google Chrome (90.0.4430.212)
Netzwerkverteiler	● MIB-II (Interfaces abfragen) ● BRIDGE-MIB (MAC-Adressen abfragen) ● Q-BRIDGE-MIB (VLANs abfragen) ● RADIUS mit folgenden Standards: • IEEE 802.1X6 Port-Based NAC • RADIUS Remote Authentication • RADIUS VLANs
Router	Router im verwalteten Netzwerk müssen die Abfrage von ARP-Daten per SNMP unterstützen. Hierzu müssen diese den SNMP-Standard MIB-II unterstützen.
Endgeräte	Für die Erkennung werden alle Endgeräte unterstützt, die 802.1X unterstützen und über eine MAC-Adresse verfügen.
Infrastruktur	Die Unterstützung der genannten Protokolle und die Datenabfrage der genannten Geräte durch den macmon-Server muss von der Infrastruktur des Netzwerkes ermöglicht werden. Vorhandene Firewalls im Netzwerk sind gegebenenfalls anzupassen.

Tabelle 3: Einsatzumgebung des EVG

7.2. Genaue Beschreibung der Testkonfiguration

Der EVG wurde in seiner eindeutigen Konfiguration getestet. Übereinstimmend mit der im ST [6] spezifizierten und in Abschnitt 7.1 dargestellten operativen Einsatzumgebung des EVG, wurden sowohl die Hersteller- als auch die Prüfstellentests mit folgender Konfiguration durchgeführt:

Testaspekt	Sicherheitsziele der Einsatzumgebung oder Softwareanforderungen entsprechend [6, 1.3.2] und [12, 2.2]	Für das Testen genutzte Einsatzumgebung
Einsatzumgebung der macmon-Appliance	Virtualisation software: ● VMware vSphere ab Version 7 ● VMware ESXi > Version 7.0 ● Anforderungen an die VM: ● 8 GB RAM ● 1 CPU mit 4 Kernen ● 250 GB HDD ● 1 GBit/s Netzwerkverbindung Installierte Software: ● OS Debian Linux Kernel 4.19 ● Database MariaDB 1:10.3.39-0+deb10u1 ● Web server Apache 2.4.38-3+deb10u10 ● PHP 7.3.31-1~deb10u4 ● OpenJDK 11.0.18+10-1~deb10u1 ● OpenSSL 1.1.1n-0+deb10u4 ● FreeRADIUS 3.0.17+dfsg-1.1+deb10u2 ● Mailserver Postfix 3.4.23-0+deb10u1	● VMware vSphere >Version 7.0.3 ● VMware ESXi > Version 7.0.3 22348816 ● 8 GB RAM ● 1 CPU mit 4 Kernen ● 250 GB HDD ● 1 GBit/s Netzwerkverbindung ● OS Debian Linux Kernel 4.19 ● Database MariaDB 1:10.3.39-0+deb10u1 ● Web server Apache 2.4.38-3+deb10u10 ● PHP 7.3.31-1~deb10u4 ● OpenJDK 11.0.18+10-1~deb10u1 ● OpenSSL 1.1.1n-0+deb10u5 ● FreeRADIUS 3.0.17+dfsg-1.1+deb10u2 ● Mailserver Postfix 3.4.23-0+deb10u1
Einsatzumgebung	Browsername und Version: ● Microsoft Edge (90.0.818.62) ● Mozilla Firefox (88.0.1) ● Google Chrome (90.0.4430.212)	● Microsoft Edge (90.0.818.62) ● Mozilla Firefox (88.0.1) ● Google Chrome (90.0.4430.212)
	Managebare Switches mit VLAN und RADIUS Support	Managebare Switches mit VLAN und RADIUS Support
	Router mit Support für ARP-Daten Querying	Router mit Support für ARP-Daten Querying

Tabelle 4: Für das Testen genutzte Einsatzumgebung

7.3. Herstellertests

Die folgende Auflistung beschreibt das Testkonzept des Herstellers:

Alle Herstellertests im Rahmen der Evaluation wurden mit einer EVG-Version in zwei verschiedenen Testkonfigurationen durchgeführt, die sich durch die Struktur der im Netz befindlichen Geräte und eine Einstellung des EVG unterscheiden.

Folgende Testkonfiguration wurde für die **manuellen Tests** benutzt:

- macmon Appliance: Der EVG macmon-NAC installiert als virtuelle Maschine,
- Management-Client: Client zum Management des EVG und zur Ausführung der manuellen und automatischen Tests,

- Switch: Netzwerkverteiler Switch (WS-C2960-24TC-L) der alle Komponenten miteinander verbindet und für die Aufteilung des Netzwerks auf VLANs sorgt,
- Mailserver: Microsoft Exchange Mailserver mit einem konfigurierten Mailaccount, welches das Protokoll STARTTLS unterstützt,
- Test-Client: Ein Laptop mit Windows 10 Betriebssystem, welcher als Endgerät im Netzwerk dient,
- Webserver (CRL): Apache-Webserver zum Hosten der Zertifikatsperrliste und zur Abfrage von CRLs als Datei.

Eine Übersicht des Netzwerkes mit den eingesetzten Komponenten bietet die folgende Abbildung:

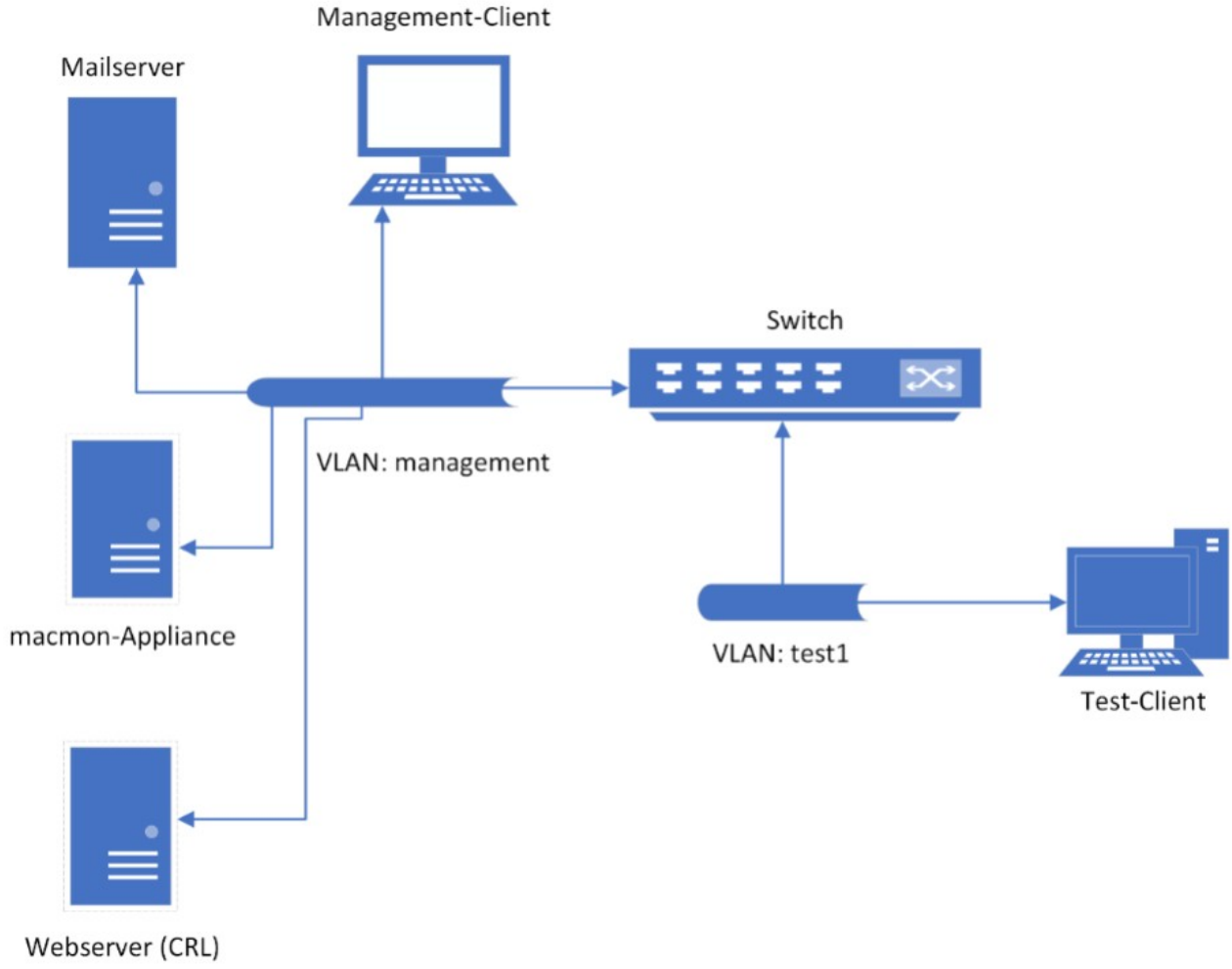

Abbildung 2: Testaufbau für den manuellen Test

Bei den **automatisierten Tests** wurde ein reduzierter Testaufbau benutzt. Dabei wurden folgende Komponenten eingesetzt:

- macmon Appliance: Der EVG macmon-NAC installiert als virtuelle Maschine,
- Management-Client: Client zum Management des EVG und zur Ausführung der manuellen und automatischen Tests,
- Webserver (CRL): Apache-Webserver zum Hosten der Zertifikatsperrliste und zur Abfrage von CRLs als Datei.

Außerdem wurden folgende Einstellungen am EVG vorgenommen:

- Englischsprachige GUI,
- Anpassung der properties um eine interne IF. Schnittstelle für das Netzwerk vom Management-Client erreichbar zu machen,
- Anpassung des Logging für mehr Details.

Sowohl für die manuellen Tests als auch für die automatischen Test des Herstellers wurde der EVG in Version 5.36.2 genutzt.

Testkonzept:

Die Tests decken die definierten TSFI und ihre Verhaltensaspekte ab, indem jedes TSFI mit seinen Aktionen getestet wird.

Die Tests berücksichtigen die verschiedenen Rollen (Administrator, Operator, Revisor und Helpdesk).

Es werden positive und negative Tests durchgeführt.

Umfang der Herstellertests und Testergebnisse:

Der Umfang der Herstellertests des EVG im Rahmen der Evaluation nach Common Criteria war wie folgt:

Es werden alle TSFI (TSFI.GUI, TSFI.API, TSFI.HTTP/remote, TSFI.SNMP, TSFI-RADIUS/remote, TSFI.RADIUS/local, TSFI.SMTP, TSFI.DB, TSFI.FS) abgedeckt, wobei eine Testanzahl von 102 erreicht wird.

Es ist wichtig zu beachten, dass einzelne Testfälle auch mehrere TSFI gleichzeitig testen können. Der Evaluator hat die tatsächlichen Testergebnisse des Herstellertests auf Inkonsistenzen mit den erwarteten Testergebnissen überprüft. Es wurden keine Inkonsistenzen gefunden.

Ergebnis der Herstellertestens:

Der Testaufwand des Herstellers hat sich als ausreichend erwiesen, um nachzuweisen, dass die Sicherheitsfunktionalität / TSFI wie spezifiziert funktionieren, und hat daher die Prüfung durch den Evaluator bestanden.

Alle Testfälle in jedem Testszenario wurden erfolgreich auf dem EVG ausgeführt und alle haben entsprechend dem erwarteten Ergebnis BESTANDEN.

7.4. Unabhängige Tests der Prüfstelle

Alle unabhängigen Tests im Rahmen der Evaluation wurden mit einer EVG-Version in zwei verschiedenen Testkonfigurationen durchgeführt. Die Testkonfigurationen und die Einstellungen am EVG waren übereinstimmend mit denen der Herstellertests. Deren detaillierte Beschreibung befindet sich in Kapitel 7.3.

Sowohl für die manuellen Tests als auch für die automatischen Test der Prüfstelle wurde der EVG in Version 5.36.2 genutzt.

Testkonzept:

Funktionale Tests wurden für alle SFR-enforcing Schnittstellen durchgeführt. Da der Hersteller erschöpfende Tests durchführte, versuchten die Evaluatoren, sich auf Tests zu konzentrieren, die noch nicht definiert waren. Es konnten nur wenige Kombinationen

gefunden werden. Penetrationstests versuchen, Eingaben oder die Ausführung von TSF zu manipulieren.

Für alle unabhängigen Tests wurde der Testcode vom Hersteller zur Verfügung gestellt. Während des Testworkshops wurde jeder Testcode von den Evaluatoren gründlich untersucht, um sicherzustellen, dass dieser das ausführt, was in der Testfallbeschreibung beschrieben ist.

Es werden positive und negative Tests durchgeführt.

Umfang der Prüfstellentests und Testergebnisse:

Der Umfang der unabhängigen Tests der Prüfstelle im Rahmen der Evaluation nach Common Criteria war wie folgt:

Es werden einige TSFI (TSFI.GUI, TSFI.API, TSFI.DB, TSFI-RADIUS/remote) abgedeckt, wobei eine Testanzahl von 12 erreicht wird.

Es ist wichtig zu beachten, dass einzelne Testfälle auch mehrere TSFI gleichzeitig testen können. Der Evaluator hat die tatsächlichen Testergebnisse des unabhängigen Tests auf Inkonsistenzen mit den erwarteten Testergebnissen überprüft. Es wurden keine Inkonsistenzen festgestellt.

Der Hersteller hat 102 relevante Tests erstellt und durchgeführt. Die Prüfstelle hat von diesen 102 Tests 22 Tests aus verschiedenen Bereichen wiederholt und zusätzlich 12 eigene Tests erstellt und diese erfolgreich durchgeführt.

Ergebnis der Prüfstellentestes:

Während der Evaluatortests funktionierte der EVG wie vorgesehen.

Alle Testfälle in jedem Testszenario wurden erfolgreich auf dem EVG ausgeführt und alle haben entsprechend dem erwarteten Ergebnis bestanden.

7.5. Schwachstellentests der Prüfstelle

Überblick:

Die Penetrationstests wurden unter Verwendung der Testumgebung des Herstellers durchgeführt. Dies umfasst den EVG, die Testumgebung, die der Betriebsumgebung entspricht, sowie die Testwerkzeuge und -einstellungen des Herstellers. Diese wurden durch benutzerdefinierte Skripte und Standardwerkzeuge für die Prüstellen-Penetrationstests ergänzt.

Es gibt nur eine Konfiguration des EVG, die evaluiert und von den Tests angesprochen wurde.

Das Gesamtergebnis ist, dass keine Abweichungen zwischen den erwarteten und den tatsächlichen Testergebnissen festgestellt wurden; außerdem war kein Angriffsszenario mit dem Angriffspotenzial Basic tatsächlich erfolgreich.

Ansatz für Penetrationstests:

Auf der Grundlage einer Liste potentieller Schwachstellen, die auf den EVG in seiner Betriebsumgebung zutreffen, entwickelten die Evaluatoren die Angriffsszenarien für Penetrationstests, wenn sie der Meinung waren, dass diese potentiellen Schwachstellen in der Betriebsumgebung des EVG ausgenutzt werden könnten.

Dabei wurden auch die Aspekte der Beschreibung der Sicherheitsarchitektur für Penetrationstests berücksichtigt. Alle anderen Evaluationsbeiträge wurden ebenfalls für

die Erstellung der Tests verwendet. Insbesondere wurde die vom Hersteller zur Verfügung gestellte Testdokumentation verwendet, um herauszufinden, ob es Problembereiche gibt, die durch Tests der Evaluationsstelle abgedeckt werden sollten.

EVG-Testkonfigurationen:

Der EVG wurde in der endgültigen Betriebsumgebung getestet und gemäß den Handbüchern installiert. Die EVG-Parameter für die Prüfung wurden nur innerhalb der in den Handbüchern festgelegten zulässigen Grenzen eingestellt. Es wurden keine invasiven Änderungen am EVG vorgenommen.

Getestete Angriffsszenarien:

Auf der Grundlage des oben erläuterten Testschwerpunkts wurde ein Satz von Angriffsszenarien für Penetrationstests erstellt, um jede potentielle Schwachstelle zu testen. Dieser Testsatz enthält 8 Penetrationstests, die den erklärten Testfokus abdecken.

Penetrationstests für SFRs:

Die verbleibenden SFRs wurden analysiert, aber nicht einem Penetrationstest unterzogen, da die zugehörigen Angriffsszenarien in der Einsatzumgebung des EVG nicht von einem Angreifer mit einem Angriffspotential Basic ausnutzbar sind.

Ergebnis der Teilaktivität:

Das Gesamtergebnis des Tests ist, dass keine Abweichungen zwischen den erwarteten und den tatsächlichen Testergebnissen festgestellt wurden. Kein Angriffsszenario mit dem Angriffspotential Basic war in der Betriebsumgebung des EVG, wie in [6] definiert, tatsächlich erfolgreich, vorausgesetzt, dass alle vom Hersteller geforderten Maßnahmen angewendet werden.

8. Evaluierte Konfiguration

Dieses Zertifikat bezieht sich auf die folgenden Konfigurationen des EVG: Der EVG ist **macmon NAC,** mit der **Version 5.36.2**. Das Security Target [ST] identifiziert nur eine Konfiguration des EVG. Diese wird durch strikte Einhaltung an die Anleitungen in den Benutzerhandbüchern [12] und [10] erreicht.

Die Einsatzumgebung des EVG in seiner evaluierten Konfiguration kann wie folgt zusammengefasst werden:

- Virtualisierungssoftware:
  - VMware ESXi ab Version 7.0
  - VMware vSphere ab Version 7
- Anforderung an die virtuelle Maschine:
  - 8 GB Arbeitsspeicher
  - 1 CPU mit 4 Kernen
  - 250 GB Festplatte
  - 1 GBit/s Netzwerkanschlüsse
- Installierte Software:
  - Betriebssystem Debian Linux Kernel 4.19

  - Datenbank MariaDB 1:10.3.39-0+deb10u1
  - Webserver Apache 2.4.38-3+deb10u10
  - PHP 7.3.31-1~deb10u4
  - OpenJDK 11.0.18+10-1~deb10u1
  - OpenSSL 1.1.1n-0+deb10u4
  - FreeRADIUS 3.0.17+dfsg-1.1+deb10u2
  - Mailserver Postfix 3.4.23-0+deb10u1
- Web-Browser:
  - Microsoft Edge (90.0.818.62)
  - Mozilla Firefox (88.0.1)
  - Google Chrome (90.0.4430.212)
- Netzwerkverteiler:
  - MIB-II (Interfaces abfragen)
  - BRIDGE-MIB (MAC-Adressen abfragen)
  - Q-BRIDGE-MIB (VLANs abfragen)
  - RADIUS mit folgenden Standards:
    - IEEE 802.1X6 Port-Based NAC
    - RADIUS Remote Authentication
    - RADIUS VLANs
- Router:
  - Router im verwalteten Netzwerk müssen die Abfrage von ARP-Daten per SNMP unterstützen. Hierzu müssen diese den SNMP-Standard MIB-II unterstützen.
- Endgeräte:
  - Für die Erkennung werden alle Endgeräte unterstützt, die 802.1X unterstützen und über eine MAC-Adresse verfügen.
- Infrastruktur:
  - Die Unterstützung der genannten Protokolle und die Datenabfrage der genannten Geräte durch den macmon-Server muss von der Infrastruktur des Netzwerkes ermöglicht werden. Vorhandene Firewalls im Netzwerk sind gegebenenfalls anzupassen.

9. Ergebnis der Evaluierung

9.1. CC spezifische Ergebnisse

Der Evaluierungsbericht (Evaluation Technical Report, ETR) [7] wurde von der Prüfstelle gemäß den Gemeinsamen Kriterien [1], der Methodologie [2], den Anforderungen des Schemas [3] und allen Anwendungshinweisen und Interpretationen des Schemas (AIS) [4] erstellt, die für den EVG relevant sind.

Die Evaluierungsmethodologie CEM [2] wurde verwendet.

Das Urteil PASS der Evaluierung wird für die folgenden Vertrauenswürdigkeitskomponenten bestätigt:

- Alle Komponenten der Vertrauenswürdigkeitsstufe EAL 2 der CC (siehe auch Teil C des Zertifizierungsreports)
- Die zusätzlichen Komponenten
  ALC_FLR.1

Die Evaluierung hat gezeigt:

- PP Konformität: Keine
- Funktionalität: Produktspezifische Sicherheitsvorgaben
  Common Criteria Teil 2 erweitert
- Vertrauenswürdigkeit: Common Criteria Teil 3 konform
  EAL 2 mit Zusatz von ALC_FLR.1

Die Ergebnisse der Evaluierung gelten nur für den EVG gemäß Kapitel 2 und für die Konfigurationen, die in Kapitel 8 aufgeführt sind.

9.2. Ergebnis der kryptographischen Bewertung

Der EVG enthält keine kryptographischen Mechanismen. Folglich waren solche Mechanismen nicht Gegenstand der Evaluierung.

10. Auflagen und Hinweise zur Benutzung des EVG

Die in Tabelle 2 genannte Betriebsdokumentation enthält die notwendigen Informationen zur Anwendung des EVG und alle darin enthaltenen Sicherheitshinweise sind zu beachten. Zusätzlich sind alle Aspekte der Annahmen, Bedrohungen und Politiken wie in den Sicherheitsvorgaben dargelegt, die nicht durch den EVG selbst, sondern durch die Einsatzumgebung erbracht werden müssen, zu berücksichtigen.

Der Anwender des Produktes muss die Ergebnisse dieser Zertifizierung in seinem Risikomanagementprozess berücksichtigen. Um die Fortentwicklung der Angriffsmethoden und -techniken zu berücksichtigen, sollte er ein Zeitintervall definieren, in dem eine Neubewertung des EVG erforderlich ist und vom Inhaber dieses Zertifikates verlangt wird.

Die Begrenzung der Gültigkeit der Verwendung der kryptographischen Algorithmen wie in Kapitel 9 dargelegt muss ebenso durch den Anwender und seinen Risikomanagementprozess für das IT-System berücksichtigt werden.

Zertifizierte Aktualisierungen des EVG, die die Vertrauenswürdigkeit betreffen, sollten verwendet werden, sofern sie zur Verfügung stehen. Stehen nicht zertifizierte Aktualisierungen oder Patches zur Verfügung, sollte er den Inhaber dieses Zertifikates auffordern, für diese eine Re-Zertifizierung bereitzustellen. In der Zwischenzeit sollte der Risikomanagementprozess für das IT-System, in dem der EVG eingesetzt wird, prüfen und entscheiden, ob noch nicht zertifizierte Aktualisierungen und Patches zu verwenden sind oder zusätzliche Maßnahmen getroffen werden müssen, um die Systemsicherheit aufrecht zu erhalten.

11. Sicherheitsvorgaben

Die Sicherheitsvorgaben [6] werden zur Veröffentlichung in einem separaten Dokument im Anhang A bereitgestellt.

12. Regulation specific aspects (eIDAS, QES)

Keine.

13. Definitionen

13.1. Abkürzungen

AIS	Anwendungshinweise und Interpretationen zum Schema
ARP	Address Resolution Protocol
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation - Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik
CEM	Common Methodology for Information Technology Security Evaluation - Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik
cPP	Collaborative Protection Profile
DBMS	Datenbank-Management-System
EAL	Evaluation Assurance Level - Vertrauenswürdigkeitsstufe
EVG	Evaluierungsgegenstand
ETR	Evaluation Technical Report
IT	Information Technology - Informationstechnologie
ITSEF	Information Technology Security Evaluation Facility - Prüfstelle für IT-Sicherheit
MAC	Media Access Control
NAC	Network Access Control
PP	Protection Profile - Schutzprofil
SAR	Security Assurance Requirement - Vertrauenswürdigkeitsanforderungen
SF	Security Function - Sicherheitsfunktion
SFP	Security Function Policy - Politik der Sicherheitsfunktion
SFR	Security Functional Requirement - Funktionale Sicherheitsanforderungen
ST	Security Target – Sicherheitsvorgaben
TOE	Target of Evaluation - Evaluierungsgegenstand
TSC	TSF Scope of Control - Anwendungsbereich der TSF-Kontrolle
TSF	TOE Security Functionality – EVG-Sicherheitsfunktionalität
VLAN	Virtual Local Area Network

13.2. Glossar

Erweiterung - Das Hinzufügen von funktionalen Anforderungen, die nicht in Teil 2 enthalten sind, und/oder von Vertrauenswürdigkeitsanforderungen, die nicht in Teil 3 enthalten sind.

Evaluationsgegenstand – Software, Firmware und / oder Hardware und zugehörige Handbücher.

EVG-Sicherheitsfunktionalität - Eine Menge, die die gesamte Hardware, Software, und Firmware des EVG umfasst, auf die Verlass sein muss, um die SFR durchzusetzen.

Formal - Ausgedrückt in einer Sprache mit beschränkter Syntax und festgelegter Semantik, die auf bewährten mathematischen Konzepten basiert.

Informell - Ausgedrückt in natürlicher Sprache.

Objekt - Eine passive Einheit im EVG, die Informationen enthält oder empfängt und mit der Subjekte Operationen ausführen.

Schutzprofil - Eine implementierungsunabhängige Menge von Sicherheitsanforderungen für eine Kategorie von EVG.

Semiformal - Ausgedrückt in einer Sprache mit beschränkter Syntax und festgelegter Semantik.

Sicherheitsfunktion - Ein Teil oder Teile eines EVG, auf die zur Durchsetzung einer hierzu in enger Beziehung stehenden Teilmenge der Regeln der EVG-Sicherheitspolitik Verlass sein muss.

Sicherheitsvorgaben - Eine implementierungsabhängige Menge von Sicherheitsanforderungen für eine Kategorie von EVG.

Subjekt - Eine aktive Einheit innerhalb des EVG, die die Ausführung von Operationen auf Objekten bewirkt.

Zusatz - Das Hinzufügen einer oder mehrerer Anforderungen zu einem Paket.

14. Literaturangaben

[1] Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation/CC), Version 3.1
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, https://www.commoncriteriaportal.org

[3] BSI-Zertifizierung: Verfahrendokumentation zum Zertifizierungsprozess (CC-Produkte) und Verfahrensdokumentation zu Anforderungen an Prüfstellen, die Anerkennung und Lizenzierung (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Anwendungshinweise und Interpretationen zum Schema (AIS), die für den EVG relevant sind[9] https://www.bsi.bund.de/AIS

[5] Deutsche IT-Sicherheitszertifikate (BSI 7148), periodisch aktualisierte Liste, die auch auf der Internet-Seite des BSI veröffentlicht wird, https://www.bsi.bund.de/zertifizierungsreporte

[6] Sicherheitsvorgaben BSI-DSZ-1180, Version 3.8, 2025-03-12, Security Target (ST) macmon NAC, macmon

[7] Evaluierungsbericht, Version 7, 2025-04-16, Evaluatuion Technical Report Summary, TÜV Informationstechnik GmbH (vertrauliches Dokument)

[8] Konfigurationsliste für den EVG: macmon_Git_5.36.2_2024-05-28.txt Version 5.36.2, Stand 2024-05-28, macmon; macmon Common Criteria Dokumente, Version 1.5, Stand 2025-04-16, macmon

[9] macmon NAC NAC Handbuch, Version 5.36, 2023-07-31

[10] macmon-Appliance Inbetriebnahme, Version 5.36.2, 2023-06

[11] macmon-Appliance Handbuch, Version 5.36.2, 2023-05

[12] Handbücher (AGD) macmon NAC, Version 2.10, 2024-05-24

[9]specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

C. Auszüge aus den Kriterien

Die Bedeutung der Vertrauenswürdigkeitskomponenten und -stufen kann direkt den Common Criteria entnommen werden. Folgende Referenzen zu den CC können dazu genutzt werden:

- Definition und Beschreibung zu Conformance Claims: CC Teil 1 Kapitel 10.5
- Zum Konzept der Vertrauenswürdigkeitsklassen, -familien und -kompomenten: CC Teil 3 Kapitel 7.1
- Zum Konzept der vordefinierten Vertrauenswürdigkeitsstufen (evaluation assurance levels - EAL): CC Teil 3 Kapitel 7.2 und 8
- Definition und Beschreibung der Vertrauenswürdigkeitsklasse ASE für Sicherheitsvorgaben / Security Target Evaluierung: CC Teil 3 Kapitel 12
- Zu detaillierten Definitionen der Vertrauenswürdigkeitskomponenten für die Evaluierung eines Evaluierungsgegenstandes: CC Teil 3 Kapitel 13 bis 17
- Die Tabelle in CC Teil 3 Anhang E fasst die Beziehung zwischen den Vertrauenswürdigkeitsstufen (EAL) und den Vertrauenswürdigkeitsklassen, -familien und -komponenten zusammen.

Die Common Criteria sind unter https://www.commoncriteriaportal.org/cc/ veröffentlicht.

Bemerkung: Ende des Reportes