Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-0738-2015

zu

macmon, Version 4.0.9

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-0738-2015 (*)

System zur Netzwerkzugriffskontrolle (NAC)

macmon
Version 4.0.9

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

SOGIS
Recognition Agreemen

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 Zerttifizierungsreport Teil A, Kap. 4 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, 9. November 2015

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

Bernd Kowalski
Abteilungspräsident

L.S.

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

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.

Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSIG[1] 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.

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

Gliederung

A. Zertifizierung

1. Grundlagen des Zertifizierungsverfahrens

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

- BSI-Gesetz[2]
- BSI-Zertifizierungs- und - Anerkennungsverordnung[3]
- BSI-Kostenverordnung[4]
- besondere Erlasse des Bundesministeriums des Innern
- 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]
- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation/CC), Version 3.1[5] [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)

2. 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.

2.1. Europäische Anerkennung von ITSEC/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

---

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

3 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

4 Kostenverordnung für Amtshandlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Kostenverordnung-BSI-KostV) vom 3. März 2005, Bundesgesetzblatt I S. 519

5 Bekanntmachung des Bundesministeriums des Innern vom 12. Februar 2007 im Bundesanzeiger, datiert 23. Februar 2007, S. 1941

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 EAL1 bis EAL4 und ITSEC Vertrauenswürdigkeitsstufen E1 bis E3 (niedrig) 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.

Das Abkommen wurde von den nationalen Stellen von Deutschland, Finnland, Frankreich, Großbritannien, Italien, Niederlande, Norwegen, Österreich, Schweden und Spanien unterzeichnet. Eine aktuelle Liste der Unterzeichnerstaaten bzw. der anerkannten Zertifizierungsstellen, Details zur Anerkennung sowie zur Historie des Abkommens können auf der Internetseite http://www.sogisportal.eu eingesehen werden.

Das SOGIS-MRA-Logo auf dem Zertifikat zeigt, dass das Zertifikat unter den Bedingungen des Abkommens von den oben genannten Nationen anerkannt wird.

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

2.2. Internationale Anerkennung von CC - Zertifikaten

Da internationale Abkommen zur gegenseitigen Anerkennung von Zertifikaten basierend auf CC (Common Criteria Recognition Arrangement, CCRA-2014) wurde am 8. September 2014 ratifiiziert. 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).

Das CCRA-2014 ersetzt das frühere CCRA, das im Mai 2000 unterzeichnet worden war (CCRA-2000). CC-Zertifikate, die vor dem 8. September 2014 nach den Regelungen des CCRA-2000 erteilt wurden, fallen weiterhin unter die gegenseitige Anerkennung. Für Zertifizierungsverfahren, die am 8. September 2014 bereits angefangen hatten, sowie für Verfahren zur Aufrechterhaltung alter Zertifikate (Maintenance and Re-Zertifizierungen) wurde eine Übergangsfrist zur Anerkennung nach den Regelungen des CCRA-2000 bis bis 8. September 2017 vereinbart (d.h. für Vertrauenswürdigkeitsstufen bis einschließlich EAL 4 oder die Vertrauenswürdigkeitsfamilie Fehlerbehebung (Flaw Remediation, ALC_FLR).

Im September 2014 wurde das Abkommen CCRA-2014 wurde den nationalen Stellen von Australien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Indien, Israel, Italien, Japan, Kanada, Malaysia, Pakistan, Republik Korea, Neuseeland, Niederlande, Norwegen, Österreich, Schweden, Spanien, Republik Singapur, Tschechische Republik, Türkei, Ungarn und USA unterzeichnet.

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

Das CCRA-Logo auf dem Zertifikat zeigt, dass das Zertifikat unter den Bedingungen des Abkommens von den oben genannten Nationen anerkannt wird.

Da das Zertifizierungsverfahren vor dem 8. September 2014 begonnen hatte, fällt dieses Zertifikat unter die Anerkennungsregeln des CCRA-2000 für alle ausgewählten Vertrauenswürdigkeitskomponenten.

3. 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, Version 4.0.9 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts macmon, Version 4.0.9 wurde von datenschutz cert GmbH durchgeführt. Die Evaluierung wurde am 29. Oktober 2015 abgeschlossen. Das Prüflabor datenschutz cert GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[6].

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.

4. Gültigkeit des Zertifikats

Dieser Zertifizierungsreport bezieht sich nur auf die angegebene Version des Produktes.

Das Produkt ist nur 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 Vertrauenswürdigkeitsstufen werden in den Auszügen aus dem technischen Regelwerk am Ende des Zertifizierungsreports und in den CC selbst erläutert.

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 Re-Zertifizierung). Insbesondere wenn Ergebnisse aus dem Zertifizierungsverfahren in einem nachfolgenden Evaluierung- und Zertifizierungsverfahren oder in einer Systemintegration verwendet werden oder das 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.

---

[6] Information Technology Security Evaluation Facility

Dieses Zertifikat, erteilt am 9. November 2015, ist gültig bis 8. November 2020. 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.

5. Veröffentlichung

Das Produkt macmon, Version 4.0.9 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[7]. Der Zertifizierungsreport kann ebenso in elektronischer Form von der oben angegebenen Internetadresse heruntergeladen werden.

[7] macmon secure GmbH
Charlottenstraße 16
10117 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 ermöglicht die Verwaltung und Überwachung des Netzwerks und der enthaltenen Komponenten. Damit gehört der EVG zu den Network Access Control (NAC) Systemen.

Der Server auf dem der TOE installiert ist, 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 wird 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
Audit	Der EVG bietet unterschiedliche Möglichkeiten, um autorisierten Benutzern Informationen zum Management-Server, dem verwalteten Netzwerk und Endgeräten im Netzwerk anzubieten. Die Report-Funktionen liefern alle Informationen zur Überwachung des Netzwerkes und für Entscheidungen, welche die Sicherheit des Netzwerkes betreffen. Im Menü *Berichte* können Berichte zu unterschiedlichen Themen abgerufen werden. Jeder Bericht kann anhand der enthaltenen Informationen sortiert und durchsucht bzw. gefiltert werden. Die Berichte sind für alle autorisierten Benutzer des EVGs verfügbar. Der Zugriff für Benutzer der Rolle *Helpdesk* ist allerdings auf Berichte zu Endgeräten beschränkt. Alle Berichte und Auditdaten sind in der Datenbank des EVGs gespeichert. Wenn die Kapazität der Datenbank erschöpft ist, werden neue Informationen ignoriert und eine Fehlermeldung an den Benutzer ausgegeben. Der Betrieb des EVG wird daraufhin beendet.
Identifikation und Authentifizierung	Der EVG kontrolliert sämtliche Berechtigungen. Er führt die Identifikation und Authentifikation jedes Benutzers des Management-Servers durch. Der Zugang zu Management- oder Audit-Funktionen wird bis zur erfolgreichen Identifikation und Authentifizierung verweigert.
Management	Der EVG bietet Möglichkeiten zum Management, um den EVG kontrollieren

Sicherheitsfunktionalität des EVG	Thema
	und überwachen zu können. Dabei haben die Benutzer unterschiedliche Berechtigungen auf die Funktionen und Daten zum Management des EVGs. Die Berechtigungen werden mit der Rolle des jeweiligen Benutzers assoziiert. Der Zugang zu Managementfunktionen wird über eine geschützte Verbindung ermöglicht. Die Benutzeroberfläche kann nur über eine HTTPS-Verbindung (TLSv1.0) aufgerufen werden. Der Server kann dabei vom Benutzer durch das SSL-Zertifikat authentifiziert werden. Zur Verwaltung der Rollen und Benutzer wird dem Administrator eine Benutzerverwaltung angeboten. In der Benutzerverwaltung werden die Passwörter von existierenden Accounts nicht angezeigt. Eine Änderung des Passwortes ist nur für den eigenen Account möglich. Ausgenommen sind hierbei Benutzer der Rolle Administrator, welche alle Passwörter verändern können. Zum Schutz vor einem unbemerkten Ausfall der Sicherheitsleistung des EVGs, führt der EVG periodisch Selbsttests durch. Hierbei kontrollieren die verschiedenen Subsysteme des EVGs sich gegenseitig. Bemerkt ein Subsystem den Ausfall eines anderen, wird dies als Log-Eintrag festgehalten und ein Ereignis ausgelöst. Auf das Ereignis kann mithilfe des Regelwerks automatisch reagiert werden, um bspw. den Administrator mit einer E-Mail zu warnen. Außerdem werden Ausfälle der einzelnen Subsysteme auch auf der Startseite der GUI dargestellt.
NAC	Der EVG überwacht durch periodische Abfragen von Daten das verwaltete Netzwerk. Dadurch kann jedes Endgerät, welches sich im verwalteten Netzwerk befindet erkannt werden. Zur Erkennung werden primär die Port-Informationen von den Switches abgerufen. Anhand der Informationen lassen sich der Standort (bzw. der physikalische Port) und die MAC-Adresse des Endgerätes bestimmen. Manuell oder anhand von Regeln können die Endgeräte in eine Referenzliste für autorisierte Geräte eingetragen werden. Dies ermöglicht den Schutz vor neuen und nicht-autorisierten Endgeräten im Netzwerk. Zusätzlich zu den primären Informationen werden interne Informationen (Sicherheitskonfiguration und Fingerprint) zum Endgerät vom macmon Compliance-Agenten abgefragt. Hierbei handelt es sich um einen Dienst, der auf autorisierten Geräten installiert wird. Welche Daten dabei vom Agenten erfasst werden, wird vom Administrator definiert. Zusätzlich kann der Administrator aus diesen Daten Merkmale für einen Fingerprint bestimmen, welcher für jedes Endgerät eindeutig sein sollte. Diese zusätzlichen Daten und der Fingerprint werden für autorisierte Endgeräte ebenfalls erfasst und gespeichert. Durch Analyse dieser Daten zur Laufzeit kann ein verdächtiges Verhalten von Endgeräten erkannt werden. Durch den Fingerprint ist es außerdem möglich, die Endgeräte-Identifikation per MAC-Adresse zu erweitern. Welche Informationen für die Auslösung einer Reaktion notwendig sind, wird vom Administrator oder Operator anhand von Regeln definiert. Ebenfalls kann individuell für die Scan-Methode und das Gerät, das Intervall für die Erfassung der Daten festgelegt werden. Je geringer dieses Intervall, desto schneller werden Events erkannt, aber desto mehr Datenvolumen wird durch den Management-Server erzeugt. Als Reaktion bietet der EVG das Senden eines Alarms per E-Mail an. Dazu kommen restriktive Maßnahmen zum Aussperren eines Endgerätes aus dem Netzwerk. Dies wird durch Deaktivierung des physikalischen Anschlusses oder Umschaltung des VLANs erreicht. Beim Umschalten des VLANs ist es

Sicherheitsfunktionalität des EVG	Thema
	allerdings auch möglich, ein Endgerät nicht auszuschließen, sondern in ein Netzwerk mit geringerer Priorität zu verschieben. Zusätzlich zu den hier genannten Reaktionen, kann der Benutzer eigene Befehle angeben, welche an das Betriebssystem weiter geleitet werden. Alle im NAC-Bereich erkannten Events und ausgelösten Aktionen als Reaktion werden ebenfalls erfasst. Diese Daten werden zusammen mit den Auditdaten in der Datenbank gespeichert. Für diese Daten gelten die gleichen Berechtigungen und Regeln wie für die anderen Auditdaten.

Tabelle 1: Sicherheitsfunktionalität des EVG

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

Die Werte, die durch den TOE 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 den Kapiteln 3.2, 3.3 und 3.4 dar.

Dieses Zertifikat umfasst die in Kapitel 8 beschriebene Konfiguration des EVG.

Die Ergebnisse der Schwachstellenanalyse, wie in diesem Zertifikat bestätigt, erfolgte ohne Einbeziehung der für die Ver- und Entschlüsselung eingesetzten krypthographischen 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 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, Version 4.0.9

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Typ	Identifier	Version	Auslieferungsart
1	SW	Name im Download-Portal: "macmon 4.0.9 USB-Stick-Image" SHA256-Prüfsumme: 5cfa 16b3 4f3a 73b2 07b5 e6b9 bc61 9983 7b6c 4e4c 309a d487 762e 2811 229e ebcb	Version 4.0.9	Download

Nr	Typ	Identifier	Version	Auslieferungsart
2	DOC	Name im Download-Portal: "Sicherheitsvorgaben", Dokumententitel: "macmon - Sicherheitsvorgaben für macmon Version 4.0.9“ [6] SHA256-Prüfsumme: 596a 5921 b9f4 cf39 31f3 3460 61c0 702c adb4 bf2b 3d18 0608 5f12 2f1c 0937 75d9	Version 2.0, 28.10.2015	Download
3	DOC	Name im Download-Portal: "Common-Criteria - Benutzer Handbuch", Dokumententitel: "macmon Dokumentation Benutzer-Handbuch (AGD)" [9] SHA256-Prüfsumme: 78ab 90b3 3892 7f27 07d8 2904 1072 5637 0b03 9640 9b53 f6f3 3ff8 6ae5 2240 490b	Version 1.0.4, 20.05.2015	Download
4	DOC	Name im Download-Portal und Dokumententitel: "macmon-Appliance Inbetriebnahme" [12] SHA256-Prüfsumme: 6025 4400 cfdb 0668 755a a7db 3202 76bc 4494 37fa f923 6027 3d0d 1d0f c4cd 84d3	Version 2014/01	Download
5	DOC	Name im Download-Portal: "macmon-Appliance Handbuch" Dokumententitel: "macmon Appliance Manual" [11] SHA256-Prüfsumme: c017 b57d 0c30 7372 db19 0b84 d829 d5db 02a1 f1f3 3811 a531 dad2 0c15 6884 5a6a	Version 3.0.3, 27.01.2014	Download
6	DOC	Name im Download-Portal und Dokumententitel: "macmon Handbuch" [10] SHA256-Prüfsumme: ee20 b2ef 4384 5660 480e 67f3 598c a75b 2baf 9e7d 783f 4018 d6e2 c163 4bef 18c8	Version 4.0.9, 13.01.2014	Download

Tabelle 2: Auslieferungsumfang des EVG

Der EVG wird als USB-Image per Download zur Verfügung gestellt. Der Download des USB-Image und der benötigten Handbücher wird über das Service-Portal, https://portal.macmon.eu bereitgestellt. Zusätzlich wird auf der gleichen Webseite die in Tabelle 2 genannte SHA256-Prüfsumme zur jeweiligen Datei dargestellt. Die für den TOE benötigte Hardware in Form der macmon Appliance, beschrieben in Abschnitt 1.2.2 in [6], wird an den Anwender per Transportdienstleister übersandt.

Das USB-Stick-Image wird vom Kunden verwendet, um den EVG auf der Appliance zu installieren. Die Installation beinhaltet auch den Compliance-Agenten, der vom installierten macmon-Server als Download bereitgestellt wird. Parallel erhält der Kunde per E-Mail die Lizenz-Datei zugeschickt. Der Inhalt der Lizenz ist auf dem Lieferschein für den Kunden abgebildet.

2.1. Möglichkeit der Identifizierung des EVGs durch den Anwender

Die Integrität und Authentizität der Dateien, die der Kunde auf dem Serviceportal herunterladen kann, kann anhand der SHA-256 Prüfsummen in Tabelle 2 überprüft werden.

Bei der Installation gibt das Installer-boot-Menü die Versionsnummer des EVG (Version 4.0.9) und der Appliance (Version 3.0.3) an. Die Version des EVG wird nach der Installation stets auf der Startseite der Benutzeroberfläche angezeigt. Die angezeigte Versionsnummer lautet: 4.0.9.22651.Ausschlaggebend zur eindeutigen Identifikation des TOE sind die ersten drei Stellen (4.0.9). Die nachfolgenden fünf Stellen stellen die interne Revisionsangabe dar.

Die Versionsnummer des macmon Compliance-Agenten ist über das Kontextmenü des Statussymbols auf dem Client-PC oder aus den Statusinformationen des jeweiligen Endgerätes aufrufbar. Die angezeigte Versionsnummer lautet: 1.2.9.13493. Dabei geben die ersten drei Stellen die Version des Agenten an. Die nachfolgenden fünf Stellen sind eine interne Revisionsangabe.

3. Sicherheitspolitik

Die Sicherheitspolitik wird durch die funktionalen Sicherheitsanforderungen ausgedrückt und durch die Sicherheitsfunktionalität des EVG umgesetzt. Sie behandelt die folgenden Sachverhalte: Der EVG implementiert eine rollenbasierte Zugriffskontrollpolitik, um administrativen Zugriff auf das System zu steuern. Darüber hinaus setzt der EVG Sicherheitsrichtlinien in Bezug auf die Sicherheitsfunktionen Audit, Identifizierung und Authentifizierung, Management und Netzwerkzugriff durch. Konkrete Angaben über die oben genannten Sicherheitsrichtlinien finden Sie in Kapitel 7 der Sicherheitsvorgaben [6].

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:

- Der Management-Server wird vom verantwortlichen Administrator, der ausreichend qualifiziert und geschult ist und frei von böswilligen Absichten, anhand der Installationsanleitung installiert und konfiguriert. Der Server muss in einer physikalisch abgesicherten Umgebung betrieben werden und darf nicht öffentlich im Internet erreichbar sein. Die TSF-, Konfigurations- und Auditdaten des EVGs und die zur Speicherung verwendeten Ressourcen müssen vor direkten Zugriffen über die Betriebsumgebung durch unbefugte Personen geschützt sein.
- Darüber hinaus muss der Management-Server vor Ausfällen geschützt sein. Die vom EVG benötigte Hardwareplattform und die darauf installierte Software müssen dem EVG zur Verfügung stehen. Das Netzwerk unterstützt die benötigten Protokolle und enthält alle geforderten Komponenten, welche ordnungsgemäß funktionieren.
- Ein privilegiertes Endgerät muss vor administrativen Zugriffen und ein unterprivilegiertes Endgerät und dessen physikalischer Netzwerkanschluss vor physikalischen und logischen Zugriffen durch unbefugte Personen geschützt werden. Darüber hinaus muss für jedes unterprivilegiertes Endgerät eine feste Zuordnung des Netzwerkanschlusses zur MAC-Adresse im Management-Server hinterlegt sein.

- Der Compliance-Agent wird auf allen privilegierten Endgeräten, anhand der Installationsanleitung [9] installiert.
- Die Betriebsumgebung muss geeignete Zeitstempel für die korrekte Erzeugung von Auditeinträgen liefern. Von den Auditdaten müssen regelmäßig Sicherheitskopien erzeugt werden.
- Des Weiteren soll die Betriebsumgebung einen Authentifizierungsmechanismus bereitstellen, über den ausschließlich die autorisierten Benutzer Zugriff zur administrativen Schnittstelle des EVGs erhalten.
- Benutzer des EVGs und der autorisierter Endgeräte sollen sicherstellen, dass ihre Zugangsdaten nicht für Dritte zugänglich sind.

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

5. Informationen zur Architektur

Der EVG bietet die Überwachung und Verwaltung des Netzwerkes an. Überwacht werden kann dabei jedes im Netzwerk befindliche Gerät mit einer MAC-Adresse. Der EVG besteht aus dem macmon-Server, mit den drei Subsystemen UI, EMD und Engine, und dem Compliance-Agent (siehe Abbildung 1).

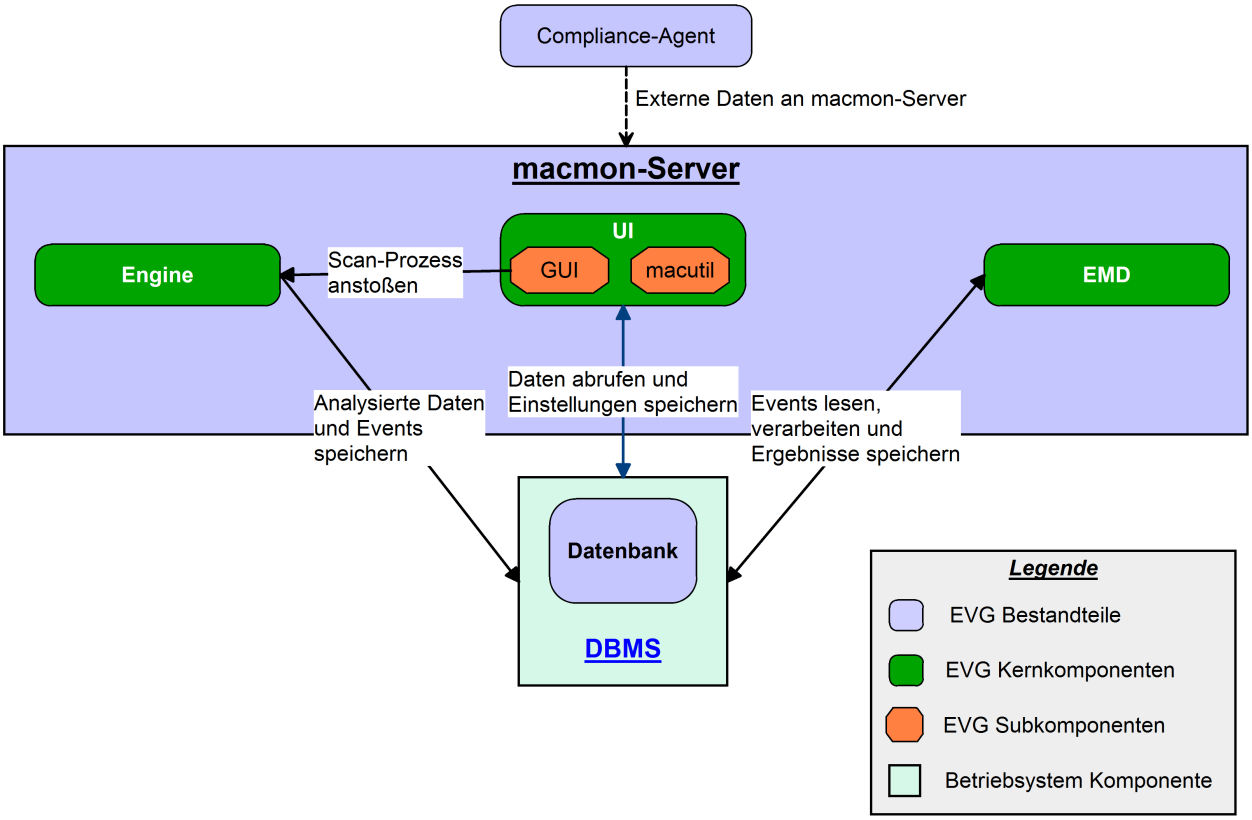

Abbildung 1: macmon Architektur

Der EVG benötigt für den Betrieb eine Datenbank. Die Datenbank wird vom Datenbank-Management-System (DBMS) der Betriebsumgebung verwaltet. Das DBMS regelt die Zugriffe auf die TSF-Daten in der Datenbank. Vom DBMS wird ausschließlich ein lokaler, administrativer Zugang angeboten, welcher ausschließlich vom macmon-Server genutzt wird.

Für die vertrauliche Kommunikation verwendet der EVG die zwei Programme OpenSSL und Net-SNMP. Das Subsystem UI nutzt die Bibliothek OpenSSL zur Absicherung der HTTPS-Verbindungen per TLSv1.0. Die Subsysteme Engine und EMD verwenden den Net-SNMP-Client zur Absicherung aller SNMP-Verbindungen per SNMPv3 mit SHA-1 Authentifikation und AES-Verschlüsselung. Diese beiden Programme sind somit Bestandteile des EVGs.

Der macmon-Server implementiert die NAC-Funktionalitäten (Network Access Control) des EVGs, er stellt den zentralen Management-Server des NAC-Systemes dar und bietet alle Managementfunktionen an. Der macmon-Server wird auch synonym als Management-Server bezeichnet. Die folgenden Kernkomponenten sind im Server enthalten:

- Engine: Die Engine führt die Erfassung von Netzwerkdaten durch. Alle empfangenen Daten werden verarbeitet und in der Datenbank gespeichert. Danach werden die ermittelten Informationen auf spezifische Events hin analysiert. Erkannte Events werden dann mit allen eventspezifischen Informationen in der Datenbank hinterlegt.
- EMD: Die von der Engine hinterlegten Events werden vom Event Management Daemon verarbeitet und analysiert. Dabei werden die Inhalte der Events anhand eines Regelwerks überprüft. Das Regelwerk besteht aus benutzerspezifischen Regeln, welche vom Administrator verwaltet werden. Trifft die Bedingung einer oder mehrerer Regeln zu, werden die konfigurierten Aktionen dieser Regeln ausgeführt.
- UI: Die UI Komponente besteht aus zwei Subkomponenten:
  - Die Bedienung des macmon-Servers geschieht primär über eine webbasierte Benutzeroberfläche (GUI), auf welche über das HTTPS Protokoll zugegriffen werden kann. Alle Konfigurations-, Überwachungs- und Wartungsarbeiten werden von dieser Oberfläche ausgeführt. Des Weiteren bietet die GUI den Zugriff auf die Auditdaten.
  - Alternativ steht die macutil-Schnittstelle zur Verfügung. macutil stellt eine Schnittstelle für externe Applikationen und Dienste dar. Über macutil können rudimentäre Operationen lokal mit Befehlen auf der Kommandozeile des Servers aufgerufen werden. Die macutil-Schnittstelle ist außerdem remote über HTTPS erreichbar.
- Datenbank: Eine relationale Datenbank stellt den primären Speicher dar. In ihr werden alle Einstellungen, Auditdaten und die vom macmon-Server verarbeiteten Netzwerkdaten sowie die erkannten Events gespeichert.

Der Compliance-Agent (Version 1.2.9) dient der Erfassung interner Daten. Zu diesem Zweck wird dieser auf zu prüfenden Endgeräten im Netzwerk benötigt. Der Agent muss vom Administrator des Netzwerkes manuell auf den Endgeräten installiert werden. Der Compliance-Agent prüft verschiedene Eigenschaften des Endgerätes und übermittelt die Ergebnisse über eine verschlüsselte Verbindung an den macmon-Server. Auf dem Server werden die Daten von der Engine analysiert.

Die vom EVG zur Verfügung gestellten Schnittstellen beschreibt Abbildung 2:

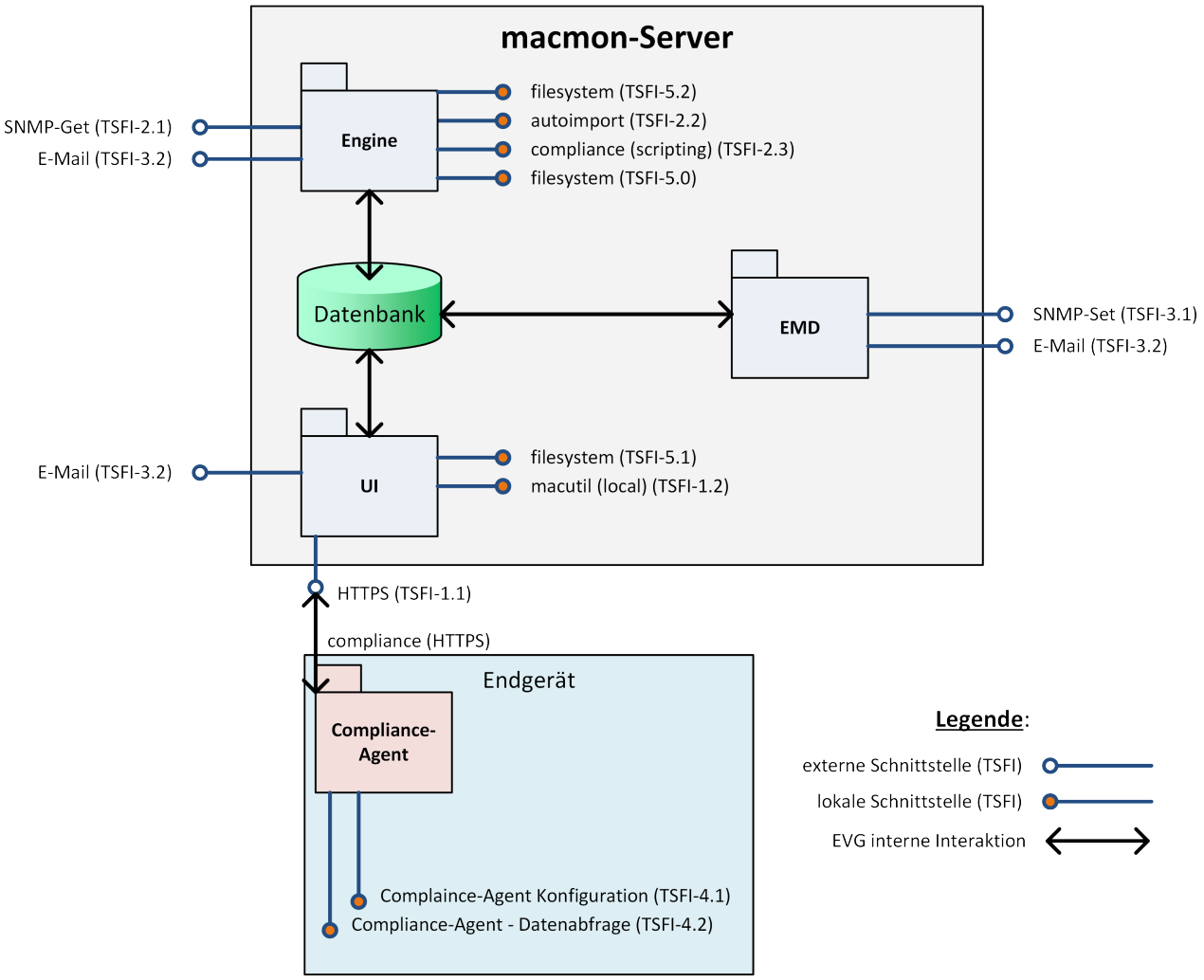

Abbildung 2: TSFI Schnittstellen

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. Herstellertests

Testkonfiguration

Der Hersteller verwendete für die Test den folgenden Testaufbau:

- macmon Appliance: Hardware-basierte macmon Appliance.
- Switch: SNMPv3-fähiger Switch.
- Router: SNMPv3-fähiger Router zur Abfrage von ARP-Daten.

- Testclient A: Autorisierter Windows 7 Client mit installiertem Compliance-Agenten.
- Testclient B: Autorisierter Client ohne Compliance-Agent mit nicht definiertem Betriebssystem (z.B. Windows- / Linux-Client, Drucker, etc.).
- Testclient C: Nicht-Autorisierter Client mit nicht definiertem Betriebssystem.
- Für den Zugriff auf die macmon-UI wurde ein Browser wie in Kapitel 8 spezifiziert verwendet.

Testdurchführung

Der Hersteller hat nur manuelle und keine automatisierten Tests durchgeführt. Die Tests des Herstellers sind nach Subsystemen des EVG gegliedert, so dass die Testabdeckung systematisch sichergestellt worden ist. Es wurde nur an den äußeren Schnittstellen getestet.

Der Hersteller hat die folgenden Testgruppen gebildet:

- T1: Initiate: Initiale Tests
- T2: GUI: Tests der Administrationsoberfläche
- T3: Engine: Tests des Subsystems Engine
- T4: EMD: Tests des Subsystems EMD

Alle Ergebnisse der Herstellertests entsprachen dem erwarteten Ergebnis und wurden protokolliert.

Insgesamt zeigen die Tests, dass sich der EVG wie in den Sicherheitsvorgaben [6], in der Funktionalen Spezifikation und der High-Level Designspezifikation spezifiziert verhält.

7.2. Unabhängige Tests der Prüfstelle

Testkonfiguration

Die Prüfstelle hat den folgenden Aufbau verwendet: Der Testgegenstand ist der in Abschnitt 2.1 in [6] definierte EVG:

- macmon 4.0.9 auf macmon Appliance 3.0.3
- macmon Client-Agent Version 1.2.9

Systeme:

- macmon Appliance (3.0.3)
- Switch (Cisco C2960)
- Authorized Client mit ClientAgent (Windows 7) – PC_A
- Authorized Client ohne ClientAgent (Windows 7)– PC_B / Konfigurations-PC – PC_K,
- Unauthorized Client (Kali-Linux) – PC_C
- DHCP-/Webserver (TPLink)
- Für den Zugriff auf die macmon-UI wurde ein Browser wie in Kapitel 8 spezifiziert verwendet.

Testdurchführung

Unabhängige Tests wurden zum Teil in der Prüfstelle, zum Teil beim Hersteller und zum Teil per remote-Sitzung durchgeführt.

Die unabhängigen Tests durch die Prüfstelle sind in vier Testgruppen unterteilt gewesen. Es wurden ausschließlich manuelle Tests durchgeführt. Es sind alle TSFI entsprechend der Beschreibung getestet worden. Die Prüfstelle hat vier Testgruppen gewählt. Die ersten drei orientieren sich an der Sicherheitsleistung des TOE, entsprechend Kapitel 1.3.2 [6]. Auf diese Weise wurde eine vollständige Abdeckung sichergestellt. Die vierte Testgruppe umfasst Schwachstellentests (siehe Kapitel 7.3).

- T1: Installation, Konfiguration und Inbetriebnahme
- T2: Verwenden des TOE – Wiederholung einzelner Testfälle des Herstellers
- T3: Testen der Auditfunktion

In T1 wird zum einen die Installation und Inbetriebnahme des EVG mit Hilfe der Handbücher überprüft, sowie die Funktionalitäten des EVG zur Identifikation und Authentifikation. Des weiteren wurden die Managementfunktionen zur korrekten Konfiguration überprüft.

In T2 wurde eine Stichprobe der Herstellertests aus allen Hersteller-Testgruppen wiederholt, um diese zu verifizieren und die Funktion der einzelnen Subsysteme und die Sicherheitsfunktion als NAC zu überprüfen

In T3 wurde die dritte Sicherheitsfunktion, das Auditing, überprüft.

Sämtliche Testergebnisse entsprachen den Erwarteten. Insgesamt zeigen die Tests, dass sich der EVG wie in den Sicherheitsvorgaben [6], in der Funktionalen Spezifikation und der High-Level Designspezifikation spezifiziert verhält.

7.3. Schwachstellentests der Prüfstelle

In der Testgruppe T4 wurde überprüft, inwiefern die Sicherheitsfunktionalität des TOE umgangen werden kann. Dazu wurde zuerst nach zusätzlichen Angriffsmöglichkeiten gesucht. Anschließend wurden alle Angriffspunkte, die im ersten Schritt Identifizierten und die in der Funktionalen Spezifikation definierten Schnittstellen auf Schwachstellen hin untersucht. Dabei wurde wie folgt vorgegangen:

- Portscan
- Schwachstellenscan in Abhängigkeit des Ergebnisses vom Portscan
- Exploiting in Abhängigkeit des Ergebnisses vom Schwachstellenscan
- ARP-Spoofing
- SNMP-Angriffe abhängig von den vorhergehenden Tests
- Externe Schnittstellen: Sniffen des Datentransfers während des gesamten Testlaufs
- Interne Schnittstelle:
  - Sniffen des Datentransfers zwischen macmon-Server und Compliance-Agent
  - Man-In-The-Middle-Angriff: Webapplication- Penetrationstest

Es wurde festgestellt, dass für den EVG keine Schwachstellen existieren, die mit einem Angriffspotential der Stärke „Basic“ ausnutzbar sind.

7.4. Zusammenfassung

Der TOE wird wie beschrieben ausgeliefert, lässt sich an Hand der Handbücher erfolgreich in Betrieb nehmen und bedienen. Die Sicherheitsfunktionen Management, Identifikation

und Authentifikation, Audit und NAC sind ausführlich getestet worden. Die erwarteten Ergebnisse konnten ohne Ausnahme bestätigt werden. Die Management Tests haben gezeigt, dass Regeln individuell konfiguriert und vom Benutzer angelegt werden können. Das Berechtigungskonzept konnte nicht umgangen werden. Insbesondere die Schreib- und Lesebefugnisse der verschiedenen Rollen wurden vollständig überprüft. Bei den Schwachstellentests wurden keine Schwächen festgestellt, die bei dem zugrunde gelegten Angriffspotential ausgenutzt werden können.

8. Evaluierte Konfiguration

Dieses Zertifikat bezieht sich auf die folgenden Konfigurationen des EVG: Der EVG besteht aus dem macmon-Server in der Version 4.0.9 und dem Compliance-Agenten in der Version 1.2.9. Der EVG wird installiert auf der macmon-Appliance, die zur EVG-Umgebung gehört.

Der macmon-Server enthält die drei Kernkomponenten UI, Engine und EMD sowie den Compliance-Agent. Die drei Kernkomponenten verwenden zur Erfüllung von einigen Sicherheitsfunktionen die zwei Programme OpenSSL und Net-SNMP. Für mehr Informationen, siehe Kapitel 1.3 in [6]

Zum Betrieb des EVGs wird folgende Nicht-EVG Hardware / Software vorausgesetzt, vergleiche [6], Kap. 1.2:

macmon-Appliance: Als Hardware-Plattform für den macmon-Server wird die macmon-Appliance Version 3.0.3 vorausgesetzt. Die Appliance stellt mit installiertem macmon-Server einen einsatzbereiten Management-Server eines NAC-Systems dar. Die Appliance muss folgenden Mindestanforderungen genügen:

- Hardware:
  - Quad Core CPU mit je 2,4 GHz
  - 4 GB Arbeitsspeicher
  - 250 GB Festplatte
  - 4 mal 1 GBit/s Netzwerkanschlüsse
- Software:
  - Betriebssystem Linux Kernel 2.6.32
  - Datenbank MySQL 5.1 (Datenbank-Management-System)
  - Webserver Apache 2.2.16 (Benötigt für die Authentifizierung von Benutzern des macmon-Servers siehe Kapitel 1.3.2 in [6])
  - PHP 5.3.3
  - Mailserver Postfix 2.7.1
  - SNMP Dienst Net-SNMP 5.4.3
  - Statistik-Framework RRDtool 1.4.3

Web-Browser: Der Zugriff auf den macmon-Server geschieht über eine HTTPS-Verbindung zu einer Web-Oberfläche (GUI). Der Web-Browser eines Gerätes, welches für den Zugriff auf die GUI verwendet werden soll, muss das Transport Layer Security Protokoll (TLS Version 1.0) und Java Script unterstützen.

Es werden die Browser Internet Explorer ab Version 10 und Firefox ab Version 24 unterstützt.

Netzwerkverteiler: Switches im verwalteten Netzwerk müssen die Möglichkeit der entfernten Verwaltung unterstützen. Außerdem müssen die Switches die Konfiguration von VLANs anbieten. Für die genannten Funktionalitäten muss das Protokoll SNMP unterstützt werden. Die Switches müssen diesbezüglich die folgenden Standards implementieren:

- MIB-II (Interface abfragen)
- IF-MIB (Interface managen)
- BRIDGE-MIB (MACs abfragen)
- Q-BRIDGE-MIB (VLANs abfragen und managen)

Router: Router im verwalteten Netzwerk müssen die Abfrage von ARP-Daten per SNMP unterstützen. Hierzu müssen diese den SNMP Standard MIB-II unterstützen.

Server: Sollen zur leichteren Identifizierung DNS-Namen und Hostnamen verwendet werden, müssen der DNS- und DHCP-Server konfiguriert werden. Dies ist nicht Bestandteil der Zertifizierung und rein als Erleichterung beim Identifizieren von Endgeräten für den Benutzer gedacht. Der DNS-Server muss die Abfrage von DNS-Namen durch den macmon-Server entweder via NSLOOKUP oder per Zonentransfer erlauben. Ein DHCP-Server, der mit dem DHCP-Agenten ausgestattet ist, muss im Netzwerk zur Verfügung stehen. Die Abfrage folgender DHCP-Server wird unterstützt:

- Novell NDS (entfernte Abfrage über LDAP(S) möglich)
- Windows Server DHCP
- HaneWIN
- Linux ISC
- DHCP QIP
- Infoblox (entfernte Abfrage HTTPS)

Endgeräte: Für die Erkennung werden alle Endgeräte unterstützt, die über eine MAC-Adresse verfügen. Um erweiterte interne Informationen zum Endgerät abfragen zu können, muss der Compliance-Agent auf den Endgeräten installiert werden.

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

Die kryptografische Algorithmenstärke wurde in diesem Zertifizierungsverfahren nicht bewertet (siehe BSIG §9, Abs. 4, 2). Jedoch können kryptografische Funktionen mit einem Sicherheitsniveau unterhalb von 100 Bit nicht länger als sicher angesehen werden ohne den Anwendungskontext zu beachten. Deswegen muss geprüft werden, ob diese kryptografischen Funktionen für den vorgesehenen Verwendungszweck angemessen sind. Weitere Hinweise und Anleitungen können der 'Technischen Richtline BSI TR-02102' (https://www.bsi.bund.de) entnommen werden.

Jede kryptografische Funktion, die in der Spalte 'Sicherheitsniveau mehr als 100 Bit' ein 'Nein' enthält erreicht ein Sicherheitsniveau unterhalb von 100 Bit (im allgemeinen Anwendungsfall).

Nr.	Zweck	Kryptografische Funktion	Implementierungs-standard	Schlüsselgröße in Bit	Sicherheits niveau mehr als 100 Bit	Bemerk ungen
1	Authent ication	RSA signature verification (RSASSAPKCS1-v1_5) using SHA-1	[PKCS#1 v2.1] (RSA), [FIPS 180-2] (SHA)	Moduluslength = 1024	Nein	-
2	Key Agreem ent	DHE / EDH with Diffie-Hellmanepheme ral-SHA-1	[RFC 2631] (DHE)	Plength= 1024	Nein	-
3	Confide ntiality	AES in CBC mode (TLS)	[FIPS 197] (AES), [SP 800-38A] (CBC)	|k|=128, 256	Ja	-
4		TDES in CBC mode (TLS)	[FIPS 46-3] (DES), [SP 800-38A] (CBC)	|k|=168	Ja	-
5	Integrity	HMAC	FIPS 180-2] (SHA),	|k|=160	Ja	-

Nr.	Zweck	Kryptografische Funktion	Implementierungs-standard	Schlüsselgröße in Bit	Sicherheitsniveau mehr als 100 Bit	Bemerkungen
		with SHA-1 (TLS)	[RFC 2104] (HMAC)			
6	Trusted Channel	TLS v1.0	RFC 2246 (TLS v1.0) [13]	|k| = 128 (AES) = 168 (TDES) = 256 (AES)	Nein	s.u.
	Die verwendeten Ciphersuiten sind: --- TLS_DHE_RSA_WITH_AES_128_CBC_SHA --- TLS_DHE_RSA_WITH_AES_256_CBC_SHA --- TLS_RSA_WITH_AES_128_CBC_SHA --- TLS_RSA_WITH_AES_256_CBC_SHA --- TLS_RSA_WITH_3DES_EDE_CBC_SHA --- TLS_DHE_RSA_WITH_AES_128_CBC_SHA					

Tabelle 3: Kryptografische Funktionen des EVG

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.

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.

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

Zusätzlich sind die folgenden Auflagen und Hinweise zu beachten:

- Der Zugriff auf die Administrationsoberfläche ist nur per TLSv1.0 verschlüsselt. Daher ist der Administrator, wie im Handbuch [9], Kap. 3.1 hervorgehoben, verpflichtet, auf den Einsatz eines aktuellen Browsers zu achten.

- In Kap. 3.3.2 [9] wird der Nutzer bei der Inbetriebnahme mit dem Hinweis „WICHTIG“ darauf hingewiesen, dass Passwörter eine Mindestlänge von acht Zeichen haben müssen und nur dem jeweiligen Benutzer bekannt sein dürfen.
- Es ist zu beachten, dass auf den TOE-Server nicht von externen Netzwerken aus zugegriffen werden können darf.

11. Sicherheitsvorgaben

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

12. Definitionen

12.1. Abkürzungen

AES	Advanced Encryption Standard
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
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAL	Evaluation Assurance Level - Vertrauenswürdigkeitsstufe
EMD	Event Management Daemon
EVG	Evaluierungsgegenstand
ETR	Evaluation Technical Report
IT	Information Technology - Informationstechnologie
ITSEF	Information Technology Security Evaluation Facility - Prüfstelle für IT-Sicherheit
LDAP	Lightweight Directory Access Protocol
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
SNMP	Simple Network Management Protocol
ST	Security Target - Sicherheitsvorgaben
TLSv1	Transport Layer Security Protokoll Version 1.0
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

12.2. 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.

13. 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 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
http://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. 4, September 2012, http://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[8] 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-0738-2015, Version 2.0, 28. Oktober 2015, Sicherheitsvorgaben für macmon Version 4.0.9, macmon secure GmbH

[7] Evaluierungsbericht, Version 1.5, 29.10.2015, Evaluation Technical Report – Zusammenfassung (Summary), datenschutz cert GmbH (vertrauliches Dokument)

[8] Konfigurationsliste für den EVG, Version 1.0.1, Stand 27.01.2015, macmon SVN Output (vertrauliches Dokument)

[9] macmon Dokumentation Benutzer-Handbuch (AGD), Version 1.0.4, 20.05.2015

[10] macmon Handbuch, Version 4.0.9, 13.01.2014

[11] macmon Appliance Manual, Version 3.0.3, 27.01.2014

[12] macmon-Appliance Inbetriebnahme, Version 2014/01

[13] RFC 2246, The TLS Protocol Version 1.0, Januar 1999, https://www.ietf.org/rfc/rfc2246

[14] RFC 3410, Introduction and Applicability Statements for Internet Standard Management Framework, Dezember 2002, https://www.rfc-editor.org/rfc/rfc3410.txt

[8] specifically

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

C. Auszüge aus den Kriterien

Anmerkung: Die folgenden Auszüge aus den technischen Regelwerken wurden aus der englischen Originalfassung der CC Version 3.1 entnommen, da eine vollständige aktuelle Übersetzung nicht vorliegt.

CC Part 1:

Conformance Claim (chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model

Assurance Class	Assurance Components
	ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one

component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Evaluation assurance level 1 (EAL 1) - functionally tested (chapter 8.3)

“Objectives

EAL 1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL 1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL 1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL 1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL 2) - structurally tested (chapter 8.4)

“Objectives

EAL 2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL 2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL 3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering."

Evaluation assurance level 4 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

"Objectives

EAL 4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs."

Evaluation assurance level 5 (EAL 5) - semiformally designed and tested (chapter 8.7)

"Objectives

EAL 5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques."

Evaluation assurance level 6 (EAL 6) - semiformally verified design and tested (chapter 8.8)

"Objectives

EAL 6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL 6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs."

Evaluation assurance level 7 (EAL 7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL 7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

D. Anhänge

Liste der Anhänge zu diesem Zertifizierungsreport

Anhang A: Die Sicherheitsvorgaben werden in einem eigenen Dokument zur Verfügung gestellt.

Dies ist eine eingefügte Leerseite.