Sicherheitsvorgaben

für

SegoAssurance Module Version 1.2

(SegoSoft ab Version 7.0.7.0*)*

Version 1.4/2014/07/11

von

Comcotec® Messtechnik GmbH

Version Nr.: **1.4**

Autor: **Comcotec[1] Messtechnik GmbH**

Gutenbergstr. 3

85716 Unterschleißheim

Evaluierungsgrundlage:

Common Criteria, Version 3.1

Gemeinsame Kriterien für die Prüfung und Bewertung

der Sicherheit von Informationstechnik

Vertrauenswürdigkeitsstufe: EAL1

[1] SegoSoft, SEGO, Comcotec sind eingetragene Warenzeichen von Comcotec Messtechnik GmbH

Inhaltsverzeichnis

1 ST-Einführung

1.1 EVG Referenz

EVG-Name: SegoAssurance Module
EVG-Version: 1.2

Der Evaluierungsgegenstand SegoAssurance ist Teil des Produkts SegoSoft. SegoSoft ist eine Software zur Prozessdokumentation, welche Prozesse von Geräten zur Aufbereitung von Produkten im Hygienekreislauf aufzeichnet und die Freigabeentscheidung des Benutzers für die aufbereiteten Produkte dokumentiert.

Produkt-Name: SegoSoft
Produkt-Version: ab Version 7.0.7.0

Der Evaluierungsgegenstand SegoAssurance besteht aus mehreren Softwarekomponenten, die in Kapitel 2 aufgeführt sind.

1.2 ST Übersicht

Dieses Dokument stellt die Sicherheitsvorgaben (Security Target) für das Produkt Sego Assurance Module Version 1.2 der Comcotec Messtechnik GmbH, Unterschließheim dar. Das Dokument ist als low assurance Security Target formuliert.

Identifikationsdaten:
BSI-Zertifizierungs-ID: BSI-DSZ-CC-0930

ST-Titel: Sicherheitsvorgaben für SegoAssurance Module 1.2
ST-Dateiname: SegoAssurance Sicherheitsvorgaben 1-4.pdf
ST-Version Nummer/Datum: Version 1.4/11.07.14

Verfasser: Comcotec Messtechnik GmbH, Gutenbergstr.6, 85716 Unterschleißheim

Vertrauenswürdigkeitsstufe: EAL1

Die vorliegenden Sicherheitsvorgaben basieren auf den „Common Criteria (CC)“ [CC] in Version 3.1, die aus den folgenden drei Teilen bestehen:

- [CC_P1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, September 2012
- [CC_P2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, Version 3.1, September 2012
- [CC_P3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance Components, Version 3.1, September 2012

Ziel der Sicherheitsvorgaben ist es, ein gewisses Maß an Vertrauen in die Funktionalität des Systems zu erreichen. Dabei liegt das Hauptargument auf der Nachvollziehbarkeit der Freigabeentscheidung über den Aufbereitungsprozess und die aufbereiteten Produkte.

1.3 Postulat der Übereinstimmung

1.3.1 CC-Konformität

Diese Sicherheitsvorgaben wurden gemäß Common Criteria Version 3.1 Revision 4 erstellt.

Es wurde eine funktionale Sicherheitsanforderung (FDP_DAU.2EX, siehe Abschnitt 4.1.1) definiert, die nicht in CC Teil 2 [2] enthalten ist. Die Anforderungen an die Vertrauenswürdigkeit wurden ausschließlich aus CC Teil 3 [3] entnommen.

Daher sind diese Sicherheitsvorgaben:

- CC Teil 2 [2] erweitert (extended) und
- CC Teil 3 [3] konform (conformant).

1.3.2 PP-Konformität

Diese Sicherheitsvorgaben behaupten keine Konformität zu einem Schutzprofil.

1.3.3 Paket-Konformität

Diese Sicherheitsvorgaben erfordern die Vertrauenswürdigkeitsstufe EAL1.

1.3.4 Erklärung der Übereinstimmung

Die Sicherheitsvorgaben verwenden funktionale Sicherheitsanforderungen aus CC Teil 2 [2] sowie eine funktionale Sicherheitsanforderung, die nicht in CC Teil 2 [2] enthalten ist, daher sind die Sicherheitsvorgaben CC Teil 2 erweitert (extended).

Die Sicherheitsvorgaben verwenden nur Anforderungen an die Vertrauenswürdigkeit aus CC Teil 3 [3], daher sind die Sicherheitsvorgaben CC Teil 3 konform (conformant).

Da diese Sicherheitsvorgaben keine Konformität zu einem Schutzprofil behaupten, können auch keine Widersprüche zwischen Typ des EVG, der Definition des Sicherheitsproblems, der Sicherheitsziele und der Sicherheitsanforderungen auftreten.

2 EVG Beschreibung (TOE Description)

Der Evaluierungsgegenstand (EVG) ist Teil der Prozessdokumentationssoftware SegoSoft und umfasst die Erstellung einer signierten Freigabeentscheidung.

2.1 EVG Übersicht (TOE Overview)

Der Evaluationsgegenstand (EVG) ist das „SegoAssurance Module“ (nachfolgend kurz als SegoAssurance bezeichnet), bei der es sich um einen Teil der SegoSoft-Prozessdokumentation handelt.

In der SegoSoft-Prozessdokumentation werden Prozessdaten von externen Geräten wie Sterilisatoren, Thermodesinfektoren, Inkubatoren und Siegelgeräte dargestellt. Der Benutzer bewertet anhand von physikalischen, chemischen und/oder biochemischen Indikatoren und/oder der Prozessdaten auf Grundlage seines Fachkönnens den Geräteprozess. Anschließend gibt er den Geräteprozess sowie nach Sichtprüfung das durch den Geräteprozess aufbereitete Produkt frei.

Mittels des SegoAssurance Moduls (EVG) der SegoSoft- Prozessdokumentation wird die Freigabeentscheidung dieses Benutzers dokumentiert, indem über die Freigabe des Benutzers ein PDF/A-Dokument erzeugt und mit einer digitalen Signatur abgespeichert wird. Hierzu wird das dem Benutzer eindeutig zugeordnete Zertifikat verwendet.

Die Freigabeentscheidung des Benutzers kann mittels AdobeReader überprüft werden, indem die Daten des Zertifikats mit den vom SegoAssurance erzeugten Zertifikatsdaten verglichen werden.

Die wichtigsten Sicherheitsmerkmale des EVG sind somit die

- Erstellung eines eindeutigen Benutzerzertifikats auf Basis des ITU-T-Standards X.509 Version 3. Zur Erstellung des Benutzerzertifikats werden kryptographische Funktionen des Betriebssystems verwendet, die außerhalb des EVG liegen.

- Dokumentation der Freigabeentscheidung mit einer digitalen Signatur[2]. Die Erzeugung der Signatur findet in der Einsatzumgebung statt, die hierfür notwendigen kryptographischen Funktionen sind nicht Teil des EVG.
  Eine Überprüfung der Signatur des Dokuments (und damit der Freigabeentscheidung) ist nach Import des Comcotec Messtechnik GmbH Wurzel-Zertifikats möglich.

Das Wurzel-Zertifikat wird mit der Software ausgeliefert und kann zur Überprüfung der Signatur des Dokuments über die Freigabeentscheidung verwendet werden.

2.1.1 Produkt-Typ

Die Aufgaben einer Prozessdokumentation bestehen in der Erhebung und Verwaltung von Daten, die von externen Geräten (sogenannten Endgeräten) an das System übermittelt werden.

[2] Als digitale Signatur wird eine fortgeschrittene elektronische Signatur verwendet. Die Evaluierung des EVG umfasst nicht die Zertifizierung der fortgeschrittenen elektronischen Signatur.

Der Fokus der SegoSoft liegt in der Erfassung und Darstellung von Prozessdaten der Aufbereitungsgeräte (Sterilisatoren, Thermodesinfektoren, Inkubatoren, Siegelgeräte). SegoSoft unterstützt die Bewertung des Aufbereitungsprozesses und der aufbereiteten Produkte. Diese Bewertung in Form einer Freigabe wird dokumentiert und stellt die Nachvollziehbarkeit der Freigabeentscheidung sicher.

Abbildung 1: Aufgaben der Prozessdokumentation SegoSoft (EVG gelb hervorgehoben)

Wird das Gerät, dessen Prozess dokumentiert werden soll (Sterilisatoren, Thermodesinfektoren, Inkubatoren, Siegelgeräte) gestartet, zeichnet SegoSoft alle relevanten Daten des Prozesses automatisch auf.

Die Daten werden für das Fachpersonal am Bildschirm angezeigt. Die Aufgabe des Fachpersonals besteht darin, den Prozess zu beurteilen (Prozessbeurteilung „nicht in Ordnung“/„in Ordnung“), die Produkte freizugeben (Produktfreigabe „Ja“/„Nein“) und den Freigabedialog über eine Passworteingabe abzuschließen.

Als Prozessbeurteilung wird dabei die Beurteilung des dokumentierten Prozesses des Gerätes verstanden. Diese Beurteilung wird anhand von physikalischen, chemischen und/oder biochemischen Indukatoren und/oder der Prozessdaten vorgenommen und ist abhängig vom Gerät, Gerätetyp und dessen Verwendung. SegoSoft überprüft nicht, ob der Prozess vom Fachpersonal korrekt bewertet wird.

Als Produktfreigabe wird die Benutzerbeurteilung verstanden, ob das durch den Geräteprozess aufbereitete Produkt (z.B. sterilisierte oder desinfizierte Produkt), für die spätere Verwendung geeignet/freigegeben ist. Die Kriterien hierfür werden nicht von SegoSoft festgelegt oder überprüft. Wie bei der Prozessbeurteilung erfolgt in der SegoSoft lediglich die Dokumentation des Ergebnisses der Produktfreigabe.

SegoSoft speichert die Freigabeentscheidung zusammen mit einer digitalen Signatur als PDF/A-Datei ab.

Die Überprüfung der Signatur des Freigabedokuments erfolgt mittels des AdobeReaders und ist nicht Bestandteil der Prozessdokumentation SegoSoft und des EVG.

Für die Überprüfung der Signatur des Dokuments ist der AdobeReader zu verwenden, in dem vorab das Wurzel-Zertifikat Root-CA als vertrauenswürdiges Zertifikat eingelesen wurde.

Damit wird festgestellt, ob das zur Signatur des Freigabedokuments verwendete Zertifikat auf dem vertrauenswürdigen Wurzel-Zertifikat der Comcotec GmbH beruht. Ebenso wird überprüft, ob das Zertifikat des Freigabedokuments mit den Daten des beim Anlegen des Benutzers ausgedruckten Zertifikatdokuments übereinstimmt.

2.1.2 EVG-Typ

Der Evaluierungsgegenstand (EVG) ist ein Softwaremodul des Produkts SegoSoft. Er gewährleistet mit seinen Sicherheitsfunktionen die Korrektheit der dokumentierten Freigabeentscheidung. Hierfür beinhaltet der EVG die Benutzerverwaltung mit Speicherung eindeutiger Benutzerzertifikate und die Dokumentation der Freigabeentscheidung mit einer digitalen Signatur.

2.1.3 Systemvoraussetzungen

Die Software des Dokumentationssystems SegoSoft ist auf handelsüblichen Personal Computern lauffähig.

2.1.3.1 Hardware

• CPU-Taktfrequenz mind. 1,6 GHz, empfohlen ab 2,0 GHz

• Hauptspeicher mind. 1 GB, empfohlen 4 GB

• Grafiksystem SVGA mit 1024 x 768 Bildpunkten, 17 Zoll Monitor oder besser

• Festplatte mit mind. 1 GB freiem Speicherplatz, empfohlen ab 10 GB

• CD-ROM-Laufwerk zur Installation

• USB-Schnittstelle zum Anschluss eines Konverterkabels von RS232 auf USB-Schnittstelle, alternativ serielle Schnittstelle nach RS232 (Nur relevant bei Anbindung von seriellen Endgeräten)

• Ethernet (nur in Verbindung mit ethernetfähigen Geräten)

2.1.3.2 Software

Die Prozessdokumenatation SegoSoft ist auf folgenden Betriebssystemen lauffähig:

• Betriebssystem MS Windows 7 Professional

• Betriebssystem MS Windows 8.1 Pro

Für den sicheren Betrieb des EVG ist es notwendig, dass das jeweilige Betriebssystem die aktuellen Sicherheitsaktualisierungen enthält.

Weiter wird folgendes Softwarepaket benötigt.

• Adobe Acrobat Reader ab Version XI

2.2 EVG-Beschreibung

2.2.1 Abgrenzung des EVG

Zum EVG gehören die Komponenten Benutzerverwaltung und Dokumentation der Freigabeentscheidung. Alle anderen Komponenten (siehe auch folgende Abbildung) sind nicht Bestandteil des EVGs und gehören zu dessen Umgebung.

Die Prozessdokumentation SegoSoft enthält zusätzlich zu den Komponenten des EVG (SegoAssurance, blau gekennzeichnet) folgende funktionale Einheiten, die nicht Bestandteil des Evaluierungsgegenstandes sind:

- Prozessdatenerfassung, -parser
- Speicherung der Prozessdaten
- Analyse der Prozessdaten
- Audit-Trail

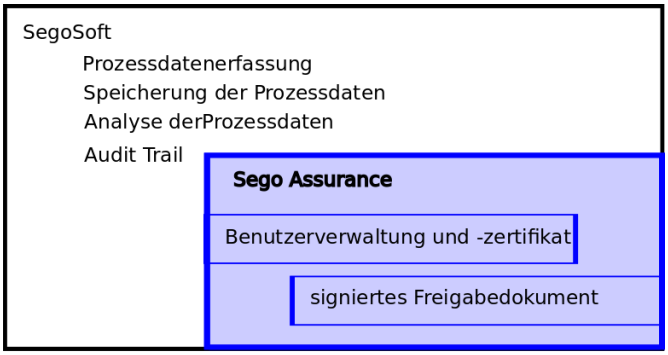


Abbildung 2: Komponenten der SegoSoft und des Evaluierungsgegenstandes

Die folgende Grafik zeigt die Komponenten des Evaluierungsgegenstandes in der Einsatzumgebung.

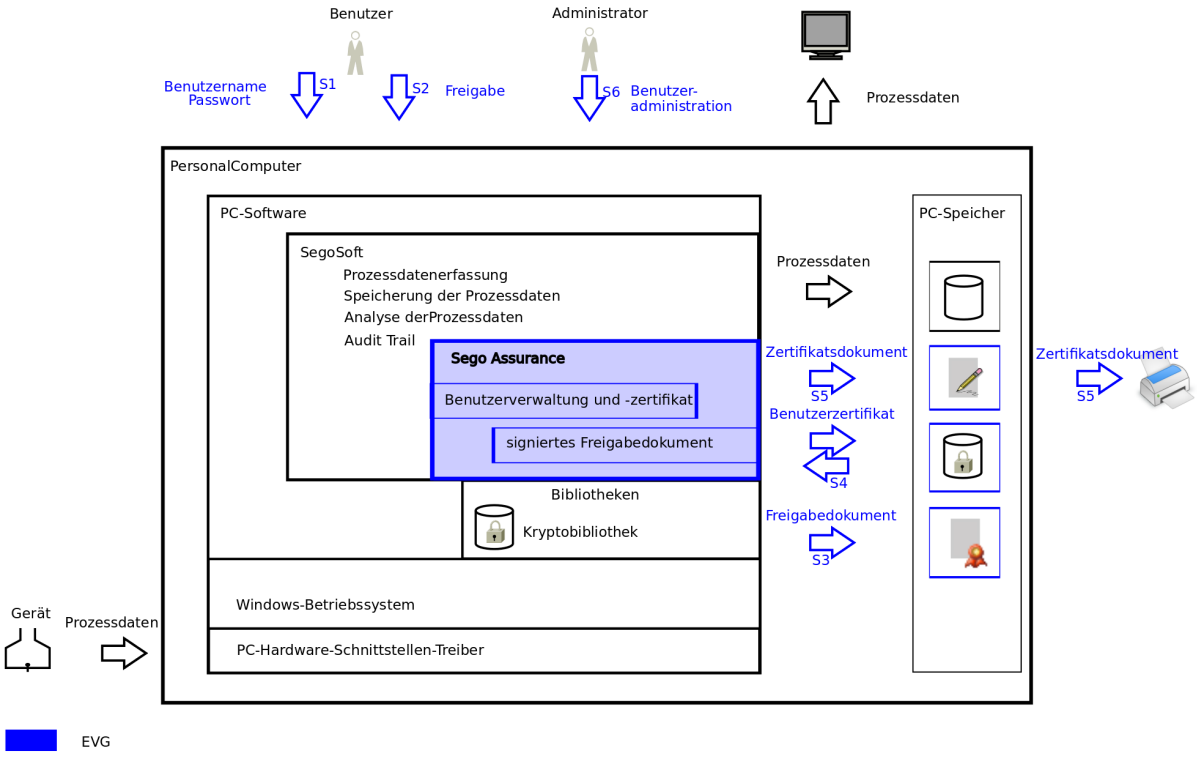


Abbildung 3: EVG in der Einsatzumgebung

SegoSoft erfasst die Prozessdaten des Aufbereitungsgeräts (Sterilisator, Desinfektor, …) und zeigt sie dem Fachpersonal grafisch als Messwertkurve am Bildschirm an (Prozessdatenerfassung, -parser). Zusätzlich werden die Prozessdaten auf der PC-Hardware gesichert (Speicherung der Prozessdaten). Bei Bedarf können die Prozessdaten mittels der von SegoSoft implementierten Mittel analysiert werden (Analyse der Prozessdaten). Die von SegoSoft durchgeführten Aktionen werden im Audit-Trail dokumentiert. Diese Funktionalitäten sind nicht Teil des Evaluierungsgegenstandes.

Die Module „Benutzerverwaltung und -zertifikat“ und „signiertes Freigabedokument“ des Evaluierungsgegenstandes werden im folgenden Kapitel beschrieben. Sie haben zur Einsatzumgebung folgende externe Schnittstellen. Diese sind in der Abbildung 3 mit blauen Pfeilen gekennzeichnet:

	Schnittstelle	**Beschreibung**
S1	Schnittstelle zum Benutzer mit Eingabe des Benutzernamens und des Passworts	Diese Schnittstelle ist unidirektional. Der Benutzer gibt Benutzername und Passwort ein.

	Schnittstelle	Beschreibung
		Diese Autorisierung des Benutzers ist sowohl für die Benutzerverwaltung als auch für die Freigabeentscheidung notwendig.
S2	Schnittstelle zum Benutzer mit Eingabe der Freigabeentscheidung	Diese Schnittstelle ist unidirektional. Der Benutzer gibt als Freigabeentscheidung ein, wie er den Prozess beurteilt und ob er die Produktfreigabe erteilt.
S3	Schnittstelle zum Freigabedokument in PC-Speicher	Diese Schnittstelle ist unidirektional. Aus der Eingabe der Freigabeentscheidung des Benutzers wird ein Freigabedokument im PDF/A-Format erzeugt und mit einer Signatur auf Basis des Benutzerzertifikats versehen. Das aus der Freigabeentscheidung erstellte und signierte Freigabedokument wird auf der PC-Hardware gespeichert.
S4	Schnittstelle zum Zertifikatscontainer in PC-Speicher	Diese Schnittstelle ist bidirektional. Das Benutzer-Zertifikat wird von der Benutzerverwaltung erzeugt, als pfx-Zertifikat im Zertifikatscontainer auf der PC-Hardware gespeichert. Für die Signatur des Freigabedokuments wird das Benutzerzertifikat aus dem Zertifikatscontainer eingelesen.
S5	Schnittstelle zum Zertifikats-Dokument	Diese Schnittstelle ist unidirektional. Nach dem Erzeugen des Benutzer-Zertifikats werden die Daten des Benutzerzertifikats als PDF/A-Dokument ausgegeben (Zertifikatsdokument) und ausgedruckt.
S6	Schnittstelle zum Administrator für die Benutzerverwaltung	Diese Schnittstelle ist bidirektional. Der Administrator kann über die Benutzerverwaltung folgende Funktionen durchführen: Anlegen, Ändern und Löschen von Benutzern sowie Organisieren von Benutzergruppen und Rechtevergabe an Benutzergruppen und Benutzer

2.2.2 Beschreibung der funktionalen Einheiten des EVG „SegoAssurance Module“

Der Evaluationsgegenstand (EVG), das „SegoAssurance Module“ (nachfolgend kurz als SegoAssurance bezeichnet), ist Teil der Prozessdokumenatations-Software SegoSoft.

SegoAssurance enthält folgende funktionale Komponenten:

- Benutzerverwaltung mit Erstellung eines eindeutigen Benutzerzertifikats auf Basis des ITU-T-Standards X.509 Version 3

- Dokumentation der Freigabeentscheidung mit einer digitalen Signatur

2.2.2.1 Benutzerverwaltung und Erstellung des Benutzerzertifikats

Die Benutzerverwaltung implementiert die Funktionen Anlegen, Ändern und Löschen von Benutzern sowie Organisieren von Benutzergruppen und Rechtevergabe an Benutzergruppen und Benutzer.

In der Benutzerverwaltung ist es möglich verschiedene Benutzer in Gruppen zu organisieren. Den Benutzergruppen und damit den zugehörigen Benutzern können verschiedene Rechte zu- oder aberkannt werden. Die für das EVG relevanten Rechte sind

- Freigabe des aufbereiteten Produkts
- Anlegen und Verwalten von Benutzern und Gruppenrechten

Durch die Organisation von Benutzern in Benutzergruppen ist es möglich, verschiedene Benutzerrollen an verschiedene Personenkreise zu vergeben.

Jeder Benutzer wird über die Merkmalskombination Benutzername-Passwort authentifiziert. Nach Anlegen des Benutzers wird über Funktionen in der Einsatzumgebung für den Benutzer ein digitales Zertifikat nach dem ITU-T-Standard X.509v3 erzeugt. Zur Erstellung des Benutzerzertifikats werden kryptographische Funktionen des Betriebssystems verwendet, die außerhalb des EVG liegen. Das Zertifikat wird über eine Zertifizierungshierarchie abgeleitet, das Wurzelzertifikat Root-CA wird von Comcotec zur Verfügung gestellt.

Nach Zertifikatserstellung wird der Signaturprüfschlüssel des Zertifikats zusammen mit einem Einweisungsformular ausgedruckt. Der Ausdruck enthält neben dem Benutzernamen (Zertifikatsinhaber) auch den Gültigkeitszeitraum des Zertifikats, den Public-Key, den Aussteller und den Fingerprint des Zertifikats. Das Papierdokument wird zur Sicherung der Integrität der Daten vom Prozessverantwortlichen (Administrator) und Benutzer unterschrieben. Das Zertifikat des Benutzers kann über SegoSoft angezeigt werden.

Firma

Name	Desinfektions-AG
Straße	Reinigungsstr.3
Postleitzahl	12345
Stadt	Berlin
Land	Germany (DE)

Ernennung und Einweisung
zur Beauftragten für die Sterilisationsfreigabe

Erstelldatum: 01.09.2013

Hiermit wird der/die Unterzeichnete(r) gemäß Ihrer/Seiner abgeschlossenen, beruflichen Ausbildung und/oder durch den Nachweis der erworbenen Sach- und Fachkunde nach den Empfehlungen des RKI in der aktuell gültigen Fassung damit beauftragt, die Freigabeentscheidung im Aufbereitungsprozess eigenverantwortlich, gewissenhaft und ordnungsgemäß nach den im innerbetrieblichen QM festgelegten Kriterien mit sofortiger Wirkung zu übernehmen.
Die im innerbetrieblichen QM und den relevanten Validierungsberichten hinterlegten Standardarbeitsanweisungen hat der/die Unterzeichnete(r) zur Kenntnis genommen, verstanden und diesbezüglich keine weiteren Fragen.

Für die Nutzung der Unterschriftsfunktion bei der Freigabe wird ein Passwort benötigt.
Das Passwort, darf nur dem/der Unterzeichneten bekannt sein. Es empfiehlt sich keine leicht zu erratende Zahlen/Buchstabenkombination dafür zu verwenden.
Das Passwort kann jederzeit durch den/die Unterzeichnete(n) in der SegoSoft selbst geändert werden.
Der/die Unterzeichnete(r) ist sich bewusst, dass erfolgt der Freigabe durch die Eingabe von Benutzername und Passwort eine rechtsgültige digitale Signatur leistet, die einer handschriftlichen Unterschrift gleichkommt.

Zertifikatsinformation für Steril Otto

Gültig ab	01.09.2013 03:00:00
Gültig bis	01.09.2015 03:00:00
Seriennummer	8C 03 02 2A 47 77 AF 17 79 E8
Fingerabdruck SHA1	8E 17 3C E2 A1 73 8F F1 C1 5E 03 4B A6 87 D5 85 0C 14 F3 0C
Fingerabdruck MD5	31 D1 49 B0 F4 2F 2F B7 F4 FD 58 C2 86 D5 D0 5E
Fingerabdruck SHA2	44 26 46 AB 84 92 70 71 43 78 D5 37 09 90 ED 3D 47 A0 90 A0 B2 E3 38 5C 59 04 28 77 68 9C 64 0D
Öffentlicher Schlüssel	30 82 01 0A 02 82 01 01 00 CC 71 36 9A 92 3F A5 4C 31 E8 35 6B BE E8 0C C2 D5 7C 58 17 07 38 36 24 18 48 BB D9 ED 37 5D 8E DB 56 67 7B E3 B9 6B B6 03 C9 AF 9D 72 3D E5 D4 10 75 FF 96 9C B1 A0 11 AE 07 43 22 86 D0 91 27 47 27 37 1E 71 7C B7 C1 AD 52 FD 1A 3A 9F 05 35 3D 07 57 8F 91 F2 A1 3C CC 08 F3 B1 44 A1 1B D5 7A 98 E2 FD 51 39 BD B7 42 AC 90 15 D5 E0 4A 6B 40 01 A6 B2 8E 49 3A 82 7B 5A 8C 8B 8D E5 1D E0 30 01 9E 28 19 14 73 03 C2 7E 0B 47 25 8A B2 3C D6 1F EA 28 5E 8F 67 6D DC CC 5F 85 5B 8E 84 68 BC 83 B9 BA 8D D1 80 39 2F 76 E1 F3 E0 CB 25 64 D6 DF D1 52 FF AF 85 97 23 CA 0B 9F FE 55 D6 3E DC 0D 7C BC A1 57 32 5B B5 B2 DE 67 56 8C 95 52 ED F9 3B 25 A5 0F 99 23 B4 E2 C9 D5 B5 2B C3 12 98 54 56 8F D1 0A 4D 3A 2A B1 FB C0 87 A5 40 14 28 43 D6 03 5A 3E A0 A3 FF E9 27 03 87 80 66 2D 02 03 01 00 01

Steril, Otto

Datum, Unterschrift

Datum, Unterschrift (Betreiber)

Abbildung 4: Zertifikatsdokument

2.2.2.2 Dokumentation der Freigabeentscheidung mit einer elektronischen Signatur als PDF/A-Dokument

Am Ende jedes Prozesszyklus (Aufbereitungsprozess des externen Geräts) kann der Benutzer die Freigabe des Prozesses und der aufbereiteten Produkte vornehmen. Hierfür muss er sich vor jeder Freigabeentscheidung als berechtigter Benutzer mit einem Passwort authentifizieren. Innerhalb dieser Freigabe wird der Bezug zur freigebenden Person durch Benutzername und Passwort hergestellt.

Die Freigabeentscheidung wird dokumentiert, indem hierüber ein Dokument nach der PDF/A-Spezifikation 1.5 erzeugt wird. Dieses Dokument wird vom EVG mit einer digitalen Signatur versehen, die auf dem Zertifikat des Benutzers beruht. Die Erzeugung der Signatur findet in der Einsatzumgebung statt, die hierfür notwendigen kryptographischen Funktionen sind nicht Teil des EVG. Die Einbindung der elektronischen Signatur erfolgt gemäß TechNote 0006: Digital Signatures in PDF/A-1.

Die Signatur weist den Unterzeichner mit seinem Namen sowie Datum und Uhrzeit der geleisteten Unterschrift aus. Sie wird dem erzeugten PDF/A-Dokument beigefügt (Inline-Signatur).

Bestandteil des Freigabe-Dokuments sind neben der Prozess- und Produktfreigabe auch die Prozessdaten und benutzerdefinierten Eingabefelder, die insbesondere zur Speicherung von anwenderspezifischen Chargenbezeichnungen, bzw. Gerätebeladungen und Ähnlichem dienen. Diese Daten stellen jedoch keine sicherheitsrelevanten Daten bezüglich der Freigabeentscheidung dar.

Für die Überprüfung der Signatur wird von der Comcotec Messtechnik GmbH das Wurzel-Zertifikat über die Webseite der Comcotec Messtechnik GmbH zum Download zur Verfügung gestellt. Dieses Wurzelzertifikat muss im AdobeReader zu den vertrauenswürdigen Zertifikaten hinzugefügt werden.

Im AdobeReader ab Version XI kann überprüft werden, ob das zur Signatur des Freigabedokuments verwendete Zertifikat auf dem vertrauenswürdigen Wurzel-Zertifikat der Comcotec GmbH beruht. Ebenso kann kontrolliert werden, ob das Zertifikat des Freigabedokuments mit den Daten des beim Anlegen des Benutzers ausgedruckten Zertifikatdokuments übereinstimmt.

2.2.3 Lieferumfang

Der Lieferumfang des Produktes SegoSoft besteht aus folgenden Komponenten:

- PC-Software SegoSoft (SegoSoft ab Version 7.0.7.0 mit SegoAssurance Version 1.2) zur Installation auf dem mit dem externen Gerät angeschlossenen Personal Computer

- SegoSoft Benutzerhandbuch Stand 17.06.2014:
  SegoSoft_Benutzerhandbuch – 2014-06-17.pdf

- SegoSoft Handbuch Installation und Administration Stand 13.06.2014:
  Installation und Administration SegoSoft Prozessdokumentation-2014-06-13-Deu.pdf

Bezüglich der Dokumentationssoftware SegoSoft ist nur das darin enthaltene Modul SegoAssurance Teil des EVG (siehe Abbildungen 2 und 3).

3 Sicherheitsziele für die Einsatzumgebung (Security objectives for the Operational Environment)

Der sichere Betrieb des EVG setzt voraus, dass folgende Sicherheitsziele in der Einsatzumgebung des EVG erfüllt sind:

OE.Admin Die Administratoren für den EVG und das Betriebssystem sind vertrauenswürdig. Sie sind für die Administration des EVG und des Betriebssystems geschult und halten die Vorgaben der Administrations-Handbücher ein. Insbesondere vergeben Sie die Rechte zur Benutzerverwaltung nur an geschultes Personal und weisen die Benutzer in die Verwendung der elektronischen Signatur ein.

Der Administrator stellt sicher, dass ein Benutzer sein erzeugtes Zertifikat auf einem Einweisungsformular schriftlich quittiert.

Der Administrator überprüft vor der Installation die Integrität der Software SegoSoft und stellt sicher, dass die Zertifikate sicher in das Benutzersystem eingebracht werden.

OE.User Die Benutzer des EVG sind vertrauenswürdig. Sie sind für die Nutzung des EVG geschult und halten die Vorgaben der Benutzerdokumentation ein. Insbesondere wählen sie sichere Passwörter und halten diese geheim.

Die Benutzer quittieren die für Sie erzeugten Zertifikate auf einem Einweisungsformular.

OE.Physical Die Systeme mit dem EVG sind so untergebracht, dass nur autorisierte Personen hierzu Zugang haben.

OE.Crypto Der EVG benutzt zum Erzeugen von Zertifikaten mit Schlüsselpaaren sowie für die Erstellung digitaler Signaturen Funktionen des Betriebssystems. Vom EVG werden die folgenden Funktionen des Betriebssystems über ein Application Programming Interface (API) genutzt:

- Generierung von kryptografisch sicheren RSA-Schlüsselpaaren (Schlüssellänge 2048 Bit)
- Erzeugung von X.509-Zertifikaten für öffentliche RSA-Schlüssel, Speicherung der X.509-Zertifikate (proprietäre Speicherung, Export als PKCS#7 möglich)
- Erzeugung von kryptografischen Hashwerten nach SHA-2 (SHA256)
- Erzeugung von digitalen RSA-Signaturen auf Basis o.g. X.509-Zertifikate zur Einbettung in PDF/A-Dokumente (PKCS#1 v2.1 bzw. Format des PDF/A-Standards)

OE.RND Es wird eine Crypto-Library eingesetzt, die zur Zufallszahlenerzeugung für die Schlüsselerzeugung der Zertifikate geeignet ist.

OE.Time Die vom EVG genutzte Hardware stellt über das Betriebssystem eine zuverlässige Zeitangabe zur Verfügung.

OE.OS Das Betriebssystem ist vertrauenswürdig, es sind die aktuellen Sicherheitsupdates installiert.

4 Definition zusätzlicher Komponenten (Extended Component Definition)

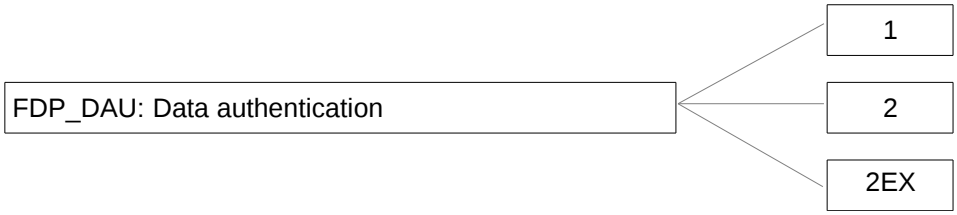
4.1 Class FDP: User data protection

4.1.1 Data authentication (FDP_DAU)

Family behaviour

The family has been extended by component FDP_DAU.2EX. It is intended to be a replacement for FDP_DAU.2 in case the validation of the evidence is not performed by the TSF, but by specific versions of Adobe Acrobat Reader. It is the responsibility of the TSF to provide the evidence in a format which can be correctly interpreted by specific versions of Adobe Acrobat Reader.

Component levelling



The components FDP_DAU.1 and FDP_DAU.2 are already described in Part 2 of the CC. Only FDP_DAU.2EX is new and described here.

Management: FDP_DAU.2EX

There are no management activities foreseen.

FDP_DAU.2EX Data Authentication with Identity of Guarantor to be validated by Adobe Acrobat Reader

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FDP_DAU.2.1EX The TSF shall provide evidence that can be used as a guarantee of the validity of documents in PDF/A format.

FDP_DAU.2.2EX The TSF shall provide such evidence in a format which can be interpreted by Adobe Acrobat Reader [assignment: list of compatible versions of Adobe Acrobat Reader] to verify the evidence of the validity of the indicated information and the identity of the user that generated the evidence.

Application Note: The evidence is not generated by the TOE, but by an external crypto library.

5 IT Sicherheitsanforderungen (IT Security Requirements)

5.1 Funktionale Sicherheitsanforderungen an den EVG (TOE Security Functional Requirements)

5.1.1 User data protection (FDP)

FDP_ACC.1 **Subset access control**

Abhängigkeiten: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the Freigabe SFP on

Subjekt	Objekt	Operation
Benutzerprozess	Freigabeentscheidung, (optional mit Prozessdaten, zusätzlich generierte Messwerte, Chargendaten, Benutzerangaben – nicht sicherheitsrelevant)	Freigabe (Erzeugung eines PDF/A-Dokuments mit einer fortschrittlichen elektronische Signatur)

.

FDP_ACF.1 **Security attribute based access control**

Abhängigkeiten: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the Freigabe SFP to objects based on the following:

Subjekt	Objekt	Attribute
Benutzerprozess	Freigabeentscheidung, (optional mit Prozessdaten, zusätzlich generierte Messwerte, Chargendaten, Benutzerangaben - nicht sicherheitsrelevant)	Benutzername, Passwort Rechte

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

Ein authentifizierter Benutzer des EVG, der das Recht „Freigabe“ besitzt, muss im Freigabedialog die Freigabe der vom EVG dargestellten Prozessdaten und der dargestellten Zusatzangaben bestätigen und sich dazu durch Eingabe seines Benutzernamens und seines Passworts identifizieren und authentifizieren.

FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: keine
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the: keine zusätzlichen Regeln

FDP_DAU.2EX	**Data Authentication with Identity of Guarantor to be validated by Adobe Acrobat Reader**
Abhängigkeiten:	FIA_UID.1 Timing of identification
FDP_DAU.2.1EX	The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of documents in PDF/A format.
FDP_DAU.2.2EX	The TSF shall provide such evidence in a format which can be interpreted by Adobe Acrobat Reader from Version XI to verify the evidence of the validity of the indicated information and the identity of the user that generated the evidence.

5.1.2 Identification and authentication (FIA)

FIA_AFL.1	**Authentication failure handling**
Abhängigkeiten:	FIA_UAU.1
FIA_AFL.1.1	The TSF shall detect when the 5 unsuccessful authentication attempts occur related to authentication for user and administration authentication.
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met, the TSF shall prevent the offending user from successfully authentication by disabling the terminal for an increasing amount of time (2 to the power of the number of unsuccessful attempts in seconds).

FIA_ATD.1	**User attribute definition**
Abhängigkeiten:	keine
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: - Benutzername - Passwort - Benutzergruppe - Rechte - Benutzerzertifikat

FIA_SOS.1	**Verification of secrets**
Abhängigkeiten:	keine
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet the following metric: The minimal password length of the administrator is 6 characters and it consists not exclusively of lower- or uppercase letters; the administrator defines the minimal password length of the user.

FIA_UAU.2	**User authentication before any action**
Abhängigkeiten:	FIA_UID.1 Timing of identification
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.2	**User identification before any action**
Abhängigkeiten:	keine
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.6	**Re-authenticating**
Abhängigkeiten:	keine
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions - ein Benutzer will ein Dokument signieren

FIA_USB.1	**User-subject binding**
Abhängigkeiten:	FIA_ATD.1 User attribute definition
FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: - Benutzername - Passwort - Benutzergruppe - Rechte - Benutzerzertifikat
FIA_USB.1.2	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: keine.
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: Nur nach Authentifizierung ist die Änderung des Passworts möglich.

5.1.3 Security management (FMT)

FMT_MSA.1/Admin	**Management of security attributes**
Abhängigkeiten:	[FDP_ACC.1 Subset access control, oder FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1/Admin	The TSF shall enforce the Freigabe_SFP to restrict the ability to query, modify, delete the security attributes Benutzername, Benutzergruppe, Rechte to Administratoren.

FMT_MSA.1/User	**Management of security attributes**
Abhängigkeiten:	[FDP_ACC.1 Subset access control, oder FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1/User	The TSF shall enforce the Freigabe_SFP to restrict the ability to modify the security attribute eigenes Passwort to Benutzer.

FMT_MSA.3	**Static attribute initialization**
Abhängigkeiten:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the Freigabe_SFP to provide restrictive default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow nobody to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1	**Specification of Management Functions**
Abhängigkeiten:	keine
FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: - Verwaltung der Benutzer und deren Rechte - Verwaltung der Benutzergruppen und deren Rechte

FMT_SMR.1	**Security roles**
Abhängigkeiten:	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles • Administrator, • Bedienungspersonal.
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

5.2 Anforderungen an die Vertrauenswürdigkeit des EVG

Der EVG erfüllt die Anforderungen der Vertrauenswürdigkeitsstufe EAL1. EAL1 umfasst die folgenden Klassen, Familien und Komponenten:

Klasse	Familie	Komponente	
Development	ADV_FSP	ADV_FSP.1	Basic functional specification
Guidance	AGD_OPE	AGD_OPE.1	Operational user guidance
	AGD_PRE	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC	ALC_CMC.1	Labelling of the TOE
	ALC_CMS	ALC_CMS.1	TOE CM coverage
Security Target	ASE_CCL	ASE_CCL.1	Conformance claims
	ASE_ECD	ASE_ECD.1	Extended components definition
	ASE_INT	ASE_INT.1	ST introduction
	ASE_OBJ	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ	ASE_REQ.1	Stated security requirements
	ASE_TSS	ASE_TSS.1	TOE summary specification
Tests	ATE_IND	ATE_IND.1	Independent testing - conformance
Vulnerability assessment	AVA_VAN	AVA_VAN.1	Vulnerability survey

6 EVG Übersichtsspezifikation (TOE Summary Specification)

Dieses Kapitel beschreibt, wie der EVG die definierten Sicherheitsanforderungen bezüglich der funktionalen Sicherheitsanforderungen aus Kapitel 5.1 und den Anforderungen an die Vertrauenswürdigkeit aus Kapitel 5.2 implementiert.

6.1 EVG-Sicherheitsfunktionen (TSF)

Die Beschreibung der Sicherheitsfunktionen nimmt die Gliederung des Kapitels 5.1. auf.

6.1.1 User data protection (FDP)

TSF_ACC.1, TSF_ACF.1:
Die Erzeugung eines Freigabe-Dokuments mit einer digitalen Signatur erfordert die Identifizierung und Authentifizierung des Benutzers mit dem Recht „Aufzeichnungen/Freigeben“.
Ein authentisierter Benutzer des EVG, der das Recht „Aufzeichnungen/Freigeben“ besitzt, muss im Freigabedialog die Freigabe der vom EVG dargestellten Prozessdaten und der dargestellten Zusatzangaben bestätigen und sich dazu durch Eingabe seines Benutzernamens und seines Passworts identifizieren und authentifizieren.

TSF_DAU.2EX: Die Freigabeentscheidung wird dokumentiert, indem hierüber ein Dokument nach der PDF/A-Spezifikation 1.5 erzeugt wird. Dieses Dokument wird mit einer digitalen Signatur versehen, die auf dem Zertifikat des Benutzers beruht. Mit dem Benutzer-Zertifikat wird das Freigabe-Dokument signiert. Dazu wird das Benutzerpasswort zum Entschlüsseln des Zertifikatscontainers (PFX-Daten) verwendet.
Mit dem Ausdruck des Signaturprüfschlüssel des Benutzerzertifikats oder Einlesen des von Comcotec zur Verfügung gestellten Wurzelzertifikat Root-CA ist eine Überprüfung der Signatur des Freigabe-Dokuments mit dem AdobeReader ab Version XI möglich.

6.1.2 Identification and authentication (FIA)

Der EVG verwendet als Authentifizierungsmechanismus ausschließlich Passworte.

TSF_AFL.1.1, TSF_AFL.1.2:
Der EVG überprüft die Anzahl der fehlgeschlagenen Authentifizierungsversuche seit der letzten erfolgreichen Authentifizierung nach Programmstart. Wird die Maximalzahl an fehlgeschlagenen Authentifizierungen erreicht, so kann der Benutzer sich für eine zunhemende Wartezeit von 2 hoch n Sekunden (n = Anzahl der fehlgeschlagenen Authentifizierungsversuchen) nicht mehr authentifizieren. Die Maximalzahl an fehlgeschlagenen Authentifizierungen beträgt 5.

TSF_ATD.1: Jeder Benutzer besitzt die eindeutigen Eigenschaften Benutzername, Passwort, Benutzergruppe, die beim Anlegen des Benutzers vom Administrator vorgegeben werden.

Über die Benutzergruppe werden dem Benutzer die sicherheitsrelevanten Rechte zugewiesen. Diese sicherheitsrelevanten Rechte sind „Aufzeichnungen/Freigeben“, „Benutzer/Erzeugen, Bearbeiten, Löschen“ (Erzeugen, Modifizieren und Löschen eines Benutzers), „Benutzereinstellungen/Bearbeiten“ (Ändern der Einstellungen des Benutzers) und „Gruppen/Erzeugen, Bearbeiten, Löschen“ (Erzeugen, Modifizieren und Löschen eines Benutzers).
Nach Anlegen des Benutzers wird vom Administrator ein Benutzerzertifikat nach dem X509v3-Standard erzeugt, das über eine Zertifikatshierachie (Root-CA, Software CA, SegoSoft-CA, SegoSoft Generic Version, Firmen-Zertifikat) abgeleitet wird. Ebenso ist die Eingabe eines Initialpassworts erforderlich.
Der EVG bietet keine Möglichkeit innerhalb der Benutzerdialog die Passwörter des Benutzers zu speichern. Die Passwörter der Benutzer werden nicht gespeichert. Die Eingabe des Benutzerpasswortes wird nur zum Entschlüsseln bzw. Verschlüsseln des Zertifikatscontainers verwendet. Geht ein Passwort verloren, kann das dazugehörige Zertifikat nicht mehr benutzt werden.

TSF_SOS.1.1 Der EVG gibt folgende Passwortregeln für die Gruppe „Administrator“ vor: Die minimale Passwortlänge beträgt 6 Zeichen, das Passwort darf nicht nur aus Klein- bzw Großbuchstaben bestehen.
Die minimale Passwortlänge der Benutzer ist vom Administrator einstellbar

TSF_UAU.2: Für die EVG-relevanten Sicherheitsfunktionen, die Erzeugung des signierten Freigabedokuments und die Benutzerverwaltung ist eine vorherige Authentifizierung (Eingabe von Benutzer und Passwort) notwendig.
Die Benutzerverwaltung ist nur nach vorheriger Authentifizierung möglich. Modifikationen eines Benutzers erfordern das Recht „Benutzer/Erzeugen, Bearbeiten, Löschen“, Änderungen der Einstellungen eines Benutzers (Passwortlänge, Logout-Zeit, Passwortaging) das Recht „Benutzereinstellungen/Bearbeiten“.
Nach Eingabe der Freigabeentscheidung wird die Authentifizierung des Benutzers gefordert. Ebenso ist das Recht „Aufzeichnungen/Freigeben“ erforderlich.
Für Aktionen außerhalb des EVG (z.B. Darstellung der Prozessdaten, Lesen der Stammdaten einschließlich Benutzerkonfiguration) nicht notwendig.

TSF_UID.2: Der Benutzer muss sich vor jeder TSF-betroffenen Aktion erneut authentifizieren.

TSF_UAU.6: Die Erzeugung jedes Freigabe-Dokuments erfordert eine Authentifizierung unabhängig davon, ob der Benutzer bereits authentifiziert ist.

TSF_USB.1: Die Modifikation des Benutzernamens oder der Benutzergruppe erfordert das Recht „Benutzer/Erzeugen, Bearbeiten, Löschen“ (Erzeugen, Modifizieren und Löschen eines Benutzers).
Die Änderung des Benutzerpassworts erfordert die Eingabe des alten Passworts. Der Benutzer kann jederzeit sein Passwort wechseln.
Mit der Benutzergruppe werden auch die Rechte des Benutzers vorgegeben. Eine Änderung in der Benutzergruppe erfordert das Recht „Gruppen/Erzeugen, Bearbeiten, Löschen“
Das Benutzerzertifikat wird nach Anlegen eines Benutzers erzeugt und kann nicht verändert werden.

6.1.3 Security management (FMT)

TSF_MSA.1/Admin:

Die Benutzerverwaltung besitzt ausgezeichnete Mitglieder, die sogenannten Administratoren (Gruppe). Diese verfügen über alle erforderlichen Rechte zur Manipulation anderer Benutzer. Ein Benutzer der Gruppe „Administrator“ besitzt alle sicherheitsrelevanten Rechte, d.h. die Rechte „Aufzeichnungen/Freigeben“, „Benutzer/Erzeugen, Bearbeiten, Löschen“, „Benutzereinstellungen/Bearbeiten“, und
„Gruppen/Erzeugen, Bearbeiten, Löschen“.
Die Rechte der Gruppe „Administrator“ können nicht verändert werden.

TSF_MSA.1/User:

Ein Benutzer der Gruppe „Bedienungspersonal“ besitzt hinsichtlich der Modifikation seiner Benutzerattribute die alleinige Möglichkeit sein Passwort zu ändern.

TSF_MSA.3: Beim Anlegen eines Benutzers mit Zertifikat muss der Vor- und Nachname und ein Passwort angegeben werden. Diese Angaben müssen verpflichtet erfolgen.

Nach Anlegen des Benutzers wird für den Benutzer ein digitales Zertifikat nach dem ITU-T-Standard X.509v3 erzeugt. Das Zertifikat wird über eine Zertifizierungshierarchie abgeleitet, das Wurzelzertifikat Root-CA wird von Comcotec zur Verfügung gestellt.

Das Benutzer-Zertifikat wird ohne weitere Optionen erstellt, die Sicherheitskonfiguration (z. B. Schlüssellänge) wird durch SegoSoft fest vorgegeben.

Die generierten Zertifikate inklusive privatem und öffentlichen Schlüssel werden in der Datei "Sego.usr" verschlüsselt als PFX-Daten (Zertifikatsconainer) abgespeichert. Dazu werden Methoden aus der Microsoft Crypto-API benutzt.

Nach der Zertifikatserstellung für einen Benutzer wird der Signaturprüfschlüssel des Zertifikats ausgedruckt. Der Ausdruck enthält neben dem Benutzernamen (Zertifikatsinhaber) auch den Gültigkeitszeitraum des Zertifikats, den Public-Key, den Aussteller und den Fingerprint des Zertifikats.

Mit dem Recht „Benutzereinstellungen/Bearbeiten“ können die Anforderungen an den Benutzer bezüglich der Passwortlänge, der Logout-Zeit und der Gültigkeit des Passwort (Passwortaging) vorgegeben werden. Es werden keine Default-Einstellungen vom EVG bezüglich der Logout-Zeit und der Gültigkeit des Passworts vorgegeben.
Die Rechte der Gruppe „Bedienungspersonal“ und „Administrator“ können nicht verändert werden.

TSF_SMF.1: Die Verwaltung der Rechte der Benutzer erfolgt über die Zuweisung des Benutzers zu einer Gruppe. Für jede Gruppe mit Ausnahme der Initialgruppen „Administrator“ und „Bedienungspersonal“ können die sicherheitsrelevanten Rechte („Aufzeichnungen/Freigeben“,
„Benutzer/Erzeugen, Bearbeiten, Löschen“,
„Benutzereinstellungen/Bearbeiten“ und „Gruppen/Erzeugen, Bearbeiten,

Löschen“) aktiviert/deaktiviert werden. Für die Modifikation der Gruppen ist das Recht „Gruppen/Erzeugen, Bearbeiten, Löschen“ erforderlich.

TSF_SMR.1: Der EVG gibt die Benutzergruppen „Administrator“ und „Bedienungspersonal“ vor. Deren Rechte können nicht verändert werden.
Jeder Benutzer kann nur einer Benutzergruppe zugewiesen werden.

7 Erklärungen

7.1 Erklärung der Sicherheitsanforderungen

7.1.1 Abbildung der Sicherheitsziele für den EVG auf Sicherheitsanforderungen

In diesen Sicherheitsvorgaben wurden keine Sicherheitsziele für den EVG identifiziert (low assurance Security Target). Dadurch ergibt sich keine Notwendigkeit der Abbildung der Sicherheitsziele für den EVG auf Sicherheitsanforderungen.

7.1.2 Erfüllung der Abhängigkeiten

7.1.2.1 Erfüllung der Abhängigkeiten der SFRs

Die nachfolgende Tabelle zeigt auf, dass alle Abhängigkeiten vom EVG aufgelöst sind.

Komponente	Abhängigkeit	aufgelöst durch	Kommentar
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	
FDP_ACF.1	FDP_ACC.1	FDP_ACC.1	
	FMT_MSA.3	FMT_MSA.3	
FDP_DAU.2EX	FIA_UID.1	FIA_UID.2	hierarchisch
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2	hierarchisch
FIA_ATD.1	keine		
FIA_UAU.2	FIA_UID.1	FIA_UID.2	hierarchisch
FIA_UID.2	keine		
FIA_UID.6	keine		
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	
FMT_MSA.1 /Admin	FDP_ACC.1 oder FDP_IFC.1	FDP_ACC.1	
	FMT_SMR.1	FMT_SMR1	
	FMT_SMF.1	FMT_SMF.1	
FMT_MSA.1 /User	FDP_ACC.1 oder FDP_IFC.1	FDP_ACC.1	
	FMT_SMR.1	FMT_SMR1	
	FMT_SMF.1	FMT_SMF.1	
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1/Admin	
		FMT_MSA.1/User	
	FMT_SMR.1	FMT_SMR1	
FMT_SMF.1	keine		
FMT_SMR.1	FIA_UID.1	FIA_UID.2	hierarchisch

7.1.2.2 Erfüllung der Abhängigkeiten der SARs

Es wurde die Vertrauenswürdigkeitsstufe EAL1 ausgewählt, ohne dass Augmentierungen vorgenommen wurden. Damit sind alle Abhängigkeiten aufgelöst.

7.2 Erklärung der Erweiterungen

Um die funktionalen Anforderungen an den EVG zu formulieren, war eine Erweiterung des CC Teil 2 [1] erforderlich: FDP_DAU.2EX. Diese Erweiterung war erforderlich, weil gegenüber FDP_DAU.2 wichtige Funktionalität (Validieren der Nachweise) nicht vom EVG, sondern von der Einsatzumgebung (Adobe Acrobat Reader) wahrgenommen werden.

Es waren keine Erweiterungen des CC Teil 3 [2] erforderlich.

Anhang

Anhang A Abkürzungen

API	Application Programming Interface
ASR	Assurance Security Requirement
CC	Common Criteria
EAL	Evaluation Assurance Level
EVG	Evaluierungsgegenstand
ISO	International Standardisation Organisation
MS	Microsoft
PDF, PDF/A	Portable Document Format
PP	Protection Profile
RSA	Rivest, Shamir, Adleman
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SigG	Signatur-Gesetz
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

Anhang B Glossar

Prozessbeurteilung

Beurteilung des dokumentierten Prozesses des Gerätes.
Diese Beurteilung ist abhängig vom Gerät, Gerätetyp und dessen Verwendung.

Produktfreigabe

Benutzerbeurteilung, ob das durch den Geräteprozess aufbereitete Produkt (z.B. sterilisierte oder desinfizierte Produkt), für die spätere Verwendung geeignet/freigegeben ist.

Freigabedokument

PDF/A-Dokument zum Nachweis der Freigabeentscheidung

elektronische Signaturen (SigG)

Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen,

fortgeschrittene elektronische Signaturen (SigG):

elektronische Signaturen, die
a) ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
b) die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
c) mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und
d) mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann,

Signaturschlüssel (SigG)

einmalige elektronische Daten wie private kryptographische Schlüssel, die zur Erstellung einer elektronischen Signatur verwendet werden,

Signaturprüfschlüssel (SigG)

elektronische Daten wie öffentliche kryptographische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden,

Zertifikate (SigG)

elektronische Bescheinigungen, mit denen Signaturprüfschlüssel einer Person zugeordnet werden und die Identität dieser Person bestätigt wird,

Signaturschlüssel-Inhaber (SigG)

natürliche Personen, die Signaturschlüssel besitzen; bei qualifizierten elektronischen Signaturen müssen ihnen die zugehörigen Signaturprüfschlüssel durch qualifizierte Zertifikate zugeordnet sein,

Zertifikatsdokument:

PDF/A-Dokument über ein Zertifikat mit den Angaben zum Signaturschlüssel-Inhaber, Gültigkeitszeitraum, öffentlicher Schlüssel, Aussteller, Fingerprint (MDH5, SHA1 und SH2)

pfx-Zertifikatsdatei:

Datei nach dem Standard PKCS#12 (Personal Information Exchange Syntax Standard), in der die Informationen, aus denen ein X.509-Zertifikat aufgebaut ist, passwortgeschützt gespeichert sind.

Anhang C Literaturverzeichnis

[3] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, September 2012, Version 3.1, Revision 4, CCMB-2012-09-001

[4] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-002

[5] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-003

[6] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2012, Version 3.1, Revision 4, CCMB-2012-09-004