debis

Services by DaimlerChrysler

Zertifizierungsreport

Hicom Xpress@LAN, Version 1.1

Siemens AG

debisZERT-DSZ-CC-04053-2000

debis IT Security Services

Die Dienstleister der Moderne

Vorwort

Das Produkt Hicom Xpress@LAN, Version 1.1 der Siemens AG wurde gegen die *Common Criteria for Information Technology Security Evaluation* evaluiert. Die Evaluierung wurde im Rahmen des Zertifizierungsschemas debisZERT der debis IT Security Services durchgeführt. Die Zertifizierung erfolgte im Dienstleistungsbereich 4: *Zertifikate mit Anerkennung durch das BSI*.

Das Ergebnis lautet:

EVG Sicherheitsfunktionen:	Identifikation und Authentisierung, regelbasierte Zugriffskontrolle und Sicherheitsprotokollierung
Stufe der Vertrauenswürdigkeit:	EAL1
Stärke der Sicherheitsfunktionen:	- ohne -

Die Ordnungsmäßigkeit der Evaluierung wird hiermit bestätigt.

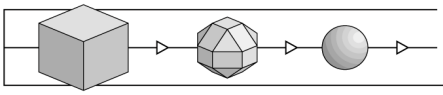
Bonn, den 14. November 2000

Zertifizierer: Leiter der Zertifizierungsstelle:

Dr. Hans-Reinhard Baader Dr. Heinrich Kersten

Für weitere Auskünfte und Kopien dieses Reports ist die Zertifizierungsstelle wie folgt erreichbar:

✉ debis IT Security Services, - Zertifizierungsstelle -, Rabinstr. 8, 53111 Bonn
☎ 0228/9841-0, Fax: 0228/9841-60
💻 Email: debiszert@itsec-debis.de, Internet: www.debiszert.de



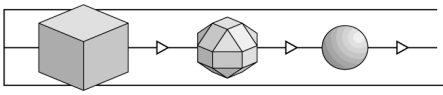
Revisionsliste

Die nachfolgende Revisionsliste gibt Auskunft über den Erstellungsprozeß für die Erstausgabe des Zertifizierungsreports.

Re-Zertifizierungen aufgrund von Produktänderungen sind in Kapitel 6 aufgeführt.

Revision	Datum	Vorgang
0.9	31.10.2000	Vorversion (nach Musterreport 1.5)
1.0	14.11.2000	Ersterstellung (nach Musterreport 1.5)

Inhalt



1 Überblick

1.1 Evaluierung

1 Die Evaluierung wurde durch Siemens AG, ICN EN HO SE, Brauckstraße 14, D-58449 Witten beauftragt.

2 Die Evaluierung wurde durchgeführt von der Prüfstelle IT-Sicherheit der debis IT Security Services und am 14.11.2000 beendet.

3 Die Evaluierung wurde gegen die *Common Criteria for Information Technology Security Evaluation* /CC/ durchgeführt. Eine Übersicht über die grundlegenden Strukturen der CC und ihre Terminologie enthält /CC/ Part 1: Introduction and General Model.

4 Da zur Zeit noch kein offizielles Evaluationshandbuch für die CC existiert, wurden entsprechende Entwürfe /CEM/ und - soweit sinnvollerweise anwendbar - die Evaluationsmethodologie in /ITSEM/ verwendet.

5 Die der Evaluierung zugrunde liegenden Sicherheitsvorgaben (Security Target), Version 1.1 vom 18.08.2000, sind seitens des Auftraggebers in deutscher Sprache bereitgestellt worden.

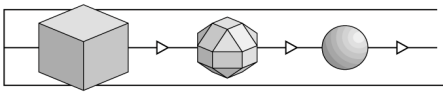
1.2 Zertifizierung

6 In den zur Zeit diskutierten Entwürfen eines Evaluationshandbuchs für die CC werden die Begriffe „overseer“ und „evaluation summary report“ (ESR) verwendet. Entsprechend der Terminologie von debisZERT meint „overseer“ stets „Zertifizierer“ und „evaluation summary report“ ist identisch mit „Zertifizierungsreport“; weiterhin wird der Prozeß, bestehend aus Prüfbegleitung, Produktion, Freigabe und Veröffentlichung des ESR, als „Zertifizierung“ bezeichnet.

7 Die Zertifizierung wurde gemäß den Regeln des Zertifizierungsschemas debisZERT der debis IT Security Services durchgeführt. Die Zertifizierungsstelle arbeitet im Einklang mit der DIN EN 45011 und ist im Hinblick auf diese Norm bei der Deutsche Akkreditierungsstelle Technik e.V. (DATech) akkreditiert (DAR-Registriernummer DIT-ZE-005/98-00).

8 Die Zertifizierungsstelle der debis IT Security Services hat das Zertifizierungsverfahren nach Maßgabe folgender Dokumente durchgeführt:

- /Z01/ Zertifizierungsschema
- /V04/ Zertifikate mit Anerkennung durch das BSI



1.3 Zertifizierungsreport

9 Dieser Zertifizierungsreport gibt die Ergebnisse der Evaluierung von Hicom Xpress@LAN, Version 1.1 wieder - im folgenden als EVG = Evaluationsgegenstand bezeichnet.

10 Der Zertifizierungsreport gilt nur für die angegebene Version(en) des EVG. Er kann jedoch auf neue bzw. andere Versionen ausgedehnt werden, sobald eine erfolgreiche Re-Evaluierung stattgefunden hat.

11 Die numerierten Paragraphen in diesem Zertifizierungsreport sind formelle Aussagen der Zertifizierungsstelle. Unnumerierte Paragraphen enthalten Aussagen des Auftraggebers (Sicherheitsvorgaben) oder ergänzendes Material.

12 Der Zertifizierungsreport dient

- dem Auftraggeber als Nachweis der durchgeführten Evaluierung und
- dem Nutzer als Grundlage für den sicherheitsgerechten Einsatz von Hicom Xpress@LAN, Version 1.1.

13 Der Zertifizierungsreport enthält die Seiten 1 bis 56. Kopien des Zertifizierungsreports können beim Auftraggeber oder bei der Zertifizierungsstelle angefordert werden.

14 Der Zertifizierungsreport kann einerseits durch Nachweise über erfolgte Re-Zertifizierungen, andererseits durch Anhänge zu besonderen technischen Problemen ergänzt werden. Solche Nachweise bzw. Anhänge werden im Internet unter der URL

- http://www.debiszert.de

  im Abschnitt „Deutsches IT-Sicherheitszertifikat“ veröffentlicht.

1.4 Zertifikat

15 Eine Kurzfassung der Ergebnisse enthält das Sicherheitszertifikat debisZERT-DSZ-CC-04053-2000.

16 Das Zertifikat wird im Internet unter der URL

- http://www.debiszert.de

  im Abschnitt „Deutsches IT-Sicherheitszertifikat“ veröffentlicht.

17 Das Zertifikat („Deutsches IT-Sicherheitszertifikat“) wird durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) anerkannt, das seinerseits die Gleichwertigkeit des Zertifikats zu seinen eigenen Zertifikaten im internationalen Kontext bestätigt.

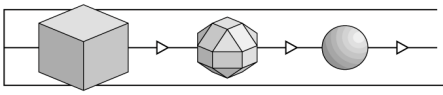
1.5 Anwendung der Ergebnisse

18 Die Prozesse der Evaluierung und Zertifizierung werden nach dem Stand der Technik durchgeführt, können aber keine *absolute* Garantie dafür geben, dass das zertifizierte Objekt frei von Schwachstellen ist. Mit steigender Evaluationsstufe verringert sich allerdings die Wahrscheinlichkeit erheblich, dass ausnutzbare Schwachstellen unentdeckt bleiben.

19 Um die Ergebnisse der Evaluierung sinnvoll nutzen zu können, wird dringend empfohlen, den Zertifizierungsreport aufmerksam zu lesen. Insbesondere die Informationen zur Art der Nutzung des zertifizierten Objektes, zu den betrachteten Bedrohungen, zur Einsatzumgebung und zu den geprüften Konfigurationen sind wichtige Vorgaben für die Praxis.

20 Das Evaluierungsergebnis gilt nur unter der Voraussetzung, dass alle Vorgaben aus dem Zertifizierungsreport beachtet werden.

Sofern von diesen Vorgaben abgewichen wird, gilt das Evaluierungsergebnis nur noch bedingt. In einem solchen Fall ist eine ergänzende Analyse erforderlich, um festzustellen, ob und in welchem Umfang das zertifizierte Objekt auch unter den geänderten Bedingungen noch Sicherheit bieten kann. Die genannte Prüfstelle und die Zertifizierungsstelle können bei der Analyse unterstützen.



(Diese Seite ist beabsichtigterweise leer.)

2 Wesentliche Ergebnisse der Evaluierung

2.1 Grundlegendes

21 Das Ergebnis der Evaluierung ist im ETR (Evaluation Technical Report of the Hicom Xpress@LAN, Version 1.1, 14.11.2000) dargestellt. Die Evaluierung erfolgte gegen die im Kapitel 3 dieses Zertifizierungsreports wiedergegebenen Sicherheitsvorgaben.

22 Der evaluierte und getestete EVG hat folgende Bestandteile:

1. Baugruppen-Software (Sachnummer: P30300-P1538-A1-08) mit Binderstand APS-Nummer: HE210I.08.435 (Firmware, wird bereits vorinstalliert auf der Baugruppe ausgeliefert),

2. Hicom 150 E Office Administrationsanleitung für Hicom Xpress@LAN, Stand 2000 (Sachnummer: A31003-K5020-B811-2-19),

3. Hicom 150 E Office Sicherheitstechnische Ergänzung zur Administrationsanleitung für Hicom Xpress@LAN, Stand September 2000 (Sachnummer: A31003-K5020-X100-1-20),

4. Assistant für Xpress@LAN auf Diskette (Sachnummer: P30300-P1562-A1-05) (Software).

23 Der EVG wurde in folgender Einsatzumgebung getestet:

- Baugruppe Voice / Data für Hicom 150 E Office pro (Sachnummer: S30810-Q2930-X000-06),

- Hicom 150 E Office pro als Siemens-Nebenstellenanlage,

- PC (kompatibel zum Industriestandard) mit WinNT 4.0 als Betriebssystem.

2.2 Zusammenfassung zum EVG

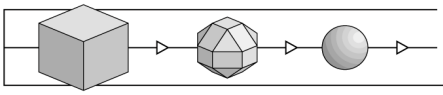
24 Der EVG ist das Produkt

Hicom Xpress@LAN, Version 1.1.

25 Der EVG ist ein Software-Produkt, das aus zwei Teilen besteht:

- Ein Teil ist die Firmware, die auf einer speziellen Einsteckkarte (Baugruppe) für eine Siemens-Nebenstellenanlage der Hicom 150 E-Familie läuft, und

- der zweite Teil ist das Anwendungsprogramm zur Administration, das auf einem PC des Industriestandards unter Windows 95 / 98 / NT läuft.



Der EVG wird benutzt, um Verbindungs- und Kommunikationsdienste zwischen einem LAN und der analogen oder digitalen Telekommunikationswelt (WAN) zur Verfügung zu stellen.

Der EVG wurde durch die

Siemens AG, ICN EN HO SE 8

für die Evaluierung bereitgestellt.

2.3 Ergebnis

26 Die Prüfstelle kommt zu folgendem Ergebnis:

- Die Sicherheitsvorgaben erfüllen die Anforderungen der entsprechenden Klasse ASE (Security Target Evaluation) der Common Criteria.

- Der EVG genügt den Anforderungen der Evaluationsstufe EAL1 der Common Criteria. Diese Stufe beinhaltet die folgenden Assurance Components:

Assurance class	Assurance components	
Configuration management	**ACM_CAP.1**	**Version numbers**
Delivery and operation	**ADO_IGS.1**	**Installation, generation, and start-up procedures**
Development	**ADV_FSP.1**	**Informal functional specification**
	ADV_RCR.1	**Informal correspondence demonstration**
Guidance documents	**AGD_ADM.1**	**Administrator guidance**
	AGD_USR.1	**User guidance**
Tests	**ATE_IND.1**	**Independent testing – conformance**

- Die Sicherheitsfunktionen des EVG bzw. ihre Mechanismen wurden hinsichtlich ihrer Stärke nicht bewertet, da eine solche Bewertung für die Stufe EAL1 nicht vorgesehen ist.

2.4 Hinweise

27 Die Prüfstelle hat für den evaluierten EVG keine Auflagen an den Hersteller auszusprechen.

28 Die Prüfstelle hat folgende Auflagen an den Anwender auszusprechen:

- Der Anwender soll die vom Hersteller bereitgestellte Dokumentation, insbesondere die dort gegebenen Sicherheitshinweise, beachten. Diese Dokumentation richtet sich sowohl an den Administrator als auch an den Endnutzer.

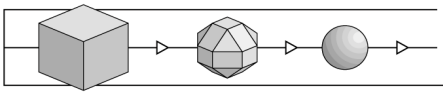
- Der Anwender soll die Installationsdiskette für den Assistant für Xpress@LAN so aufbewahren, dass sie nicht für Personen zugänglich ist, die keine Administratorrechte haben.

- Der Anwender soll den Assistant für Xpress@LAN nur auf einem solchen PC (Admin-PC) installieren, dessen Betriebssystem die Nutzeridentifikation und –authentisierung zwingend verlangt, wobei die Anzahl der Fehlversuche gezählt wird.

- Der Anwender soll die Benutzung des Fehlversuchszählers des Betriebssystems des Admin-PCs einschalten.

- Der Administrator soll als Authentisierungsprotokoll das PAP nicht benutzen.

- Der Administrator soll bei der Firewall-Funktionalität (Sicherheitsfunktionen SF-3a, SF-3b und SF-3c) nur richtungsunabhängige Kommunikation erlauben.



(Diese Seite ist beabsichtigterweise leer.)

3 Sicherheitsvorgaben

3.1 ST-Einführung

Sicherheitsvorgaben im Sinne der CC enthalten die IT-Sicherheitsanforderungen und spezifizieren die funktionalen und vertrauenschaffenden Sicherheitsmaßnahmen zur Erfüllung dieser Sicherheitsanforderungen.

Der Begriff **Sicherheitsvorgaben** wird hier als deutsche Übertragung des englischen Fachbegriffes „Security Target“ (abgekürzt ST) benutzt. Da die Abkürzung „ST“ allgemein verbreitet ist, wird sie gleichbedeutend mit dem Begriff „Sicherheitsvorgaben“ benutzt.

3.1.1 ST-Identifikation

Dieses Dokument

Sicherheitsvorgaben für Hicom Xpress@LAN, Version 1.1,

Version 1.1 vom 18.08.2000,

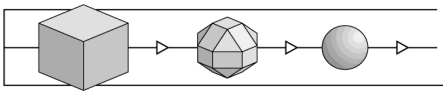
beschreibt die Sicherheitseigenschaften des IT-Produktes Hicom Xpress@LAN, Version 1.1 der Firma Siemens AG, Berlin und München. Dieses IT-Produkt besteht aus den in Abschnitt 3.2.2 genannten Komponenten mit den dort angegebenen Versionsnummern und Auslieferungsständen. Der EVG besteht aus den ebenfalls dort genauer bezeichneten Bestandteilen.

Dieses Dokument ist Grundlage einer Evaluierung von Hicom Xpress@LAN, Version 1.1 nach EAL1 der CC [4].

3.1.2 ST-Übersicht

Gegenwärtig existieren zwei Kommunikationsnetze parallel zueinander, Computernetze und Telekommunikationsnetze. Da inzwischen die Telekommunikationsnetze weitestgehend unter Benutzung moderner Informationstechnik betrieben werden, besteht die Möglichkeit, beide Kommunikationsnetze miteinander zu verbinden. Dies kann zum Beispiel durch Erweiterung einer Telefonvermittlungsanlage um eine geeignete Zusatzbaugruppe geschehen, so dass ein lokales Computernetz für Weitverkehrsverbindungen das Telekommunikationsnetz benutzen kann.

Bei der Integration beider Netze, des Telekommunikationsnetzes und des Computernetzes, ergeben sich nicht nur neue Funktionalitäten, sondern auch die Sicherheitsprobleme beider Bereiche werden miteinander verknüpft.



Dieses ST definiert die sicherheitsrelevanten Aspekte und zeigt auf, wie sie durch den EVG gelöst werden. Als Ergänzung zu einer Siemens-Nebenstellenanlage[1] stellt der EVG folgende Sicherheitsfunktionalität zur Verfügung:

- Identifikation und Authentisierung,
- regelbasierte Zugriffskontrolle und
- Protokollierung.

3.1.3 CC-Konformität

Diese Sicherheitsvorgaben folgen der Standardgliederung gemäß CC Teil 1 (vergl. [1]). Die funktionalen Anforderungen an den EVG sind konform zu Teil 2 (vergl. [2]), die Anforderungen an die Vertrauenswürdigkeit des EVGs konform zu Teil 3, EAL1 (vergl. [4]) der CC.

Alle Referenzen zu den Common Criteria for Information Technology Security Evaluation (CC) beziehen sich auf die Version 2.0 der CC vom Mai 1998, die in deutscher Übersetzung als

> „Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik“

am 15. November 1999 als gültige IT-Sicherheitskriterien im Sinne des BSI-Errichtungsgesetzes im Bundesanzeiger veröffentlicht wurden.

3.2 EVG-Beschreibung

3.2.1 Typ des EVG

Beim Hicom Xpress@LAN, Version 1.1 handelt sich um ein IT-Produkt, dessen wesentliche Funktionalität die Protokollumsetzung zwischen der TCP/IP-Welt oder IPX/SPX-Welt einerseits und der analogen oder digitalen Telekommunikationswelt andererseits ist. Die Verbindung zur analogen und digitalen Telekommunikationswelt wird über eine Siemens-Nebenstellenanlage hergestellt, die Verbindung zur TCP/IP- oder IPX/SPX-Welt über einen 10/100BaseT-Anschluß.

Der EVG kann nur zusammen mit und als Erweiterung zu bestimmten Nebenstellenanlagen der Siemens AG eingesetzt werden.

---

[1] Das Produkt Hicom Xpress@LAN, Version 1.1 kann in eine der folgenden Siemens-Nebenstellenanlagen eingebaut werden: Hicom 150 E OfficeCom, Hicom 150 E OfficePoint, Hicom 150 E OfficePro (jeweils ab Software-Version 2.2). Der Begriff „Siemens-Nebenstellenanlage“ bezeichnet in diesen Sicherheitsvorgaben eine dieser Hicom 150 E Office-Anlagen.

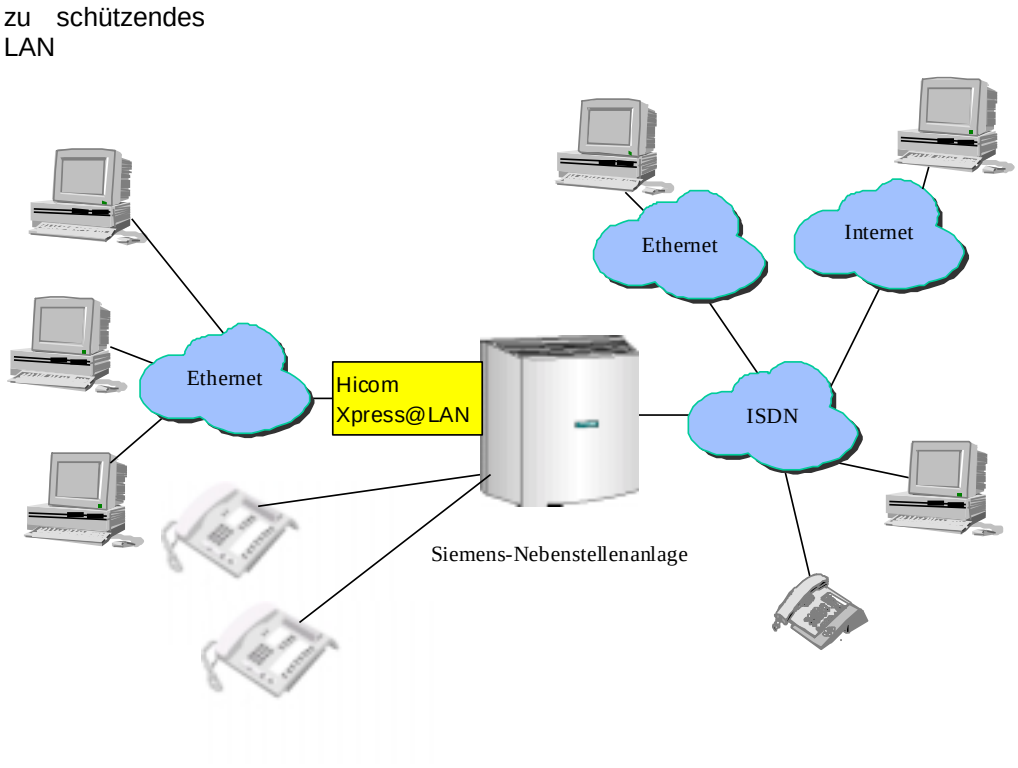


Abbildung 1: Anbindung der Hicom Xpress@LAN an ein Computernetz und eine Siemens-Nebenstellenanlage

3.2.2 Umfang und Abgrenzung

Ein ausgeliefertes Hicom Xpress@LAN, Version 1.1-Produkt besteht aus folgenden Objekten:

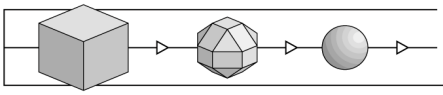
1. Baugruppen-Software (Sachnummer: P30300-P1538-A1-08) mit Binderstand APS-Nummer: HE210I.08.435, Bestandteil des EVGs,

2. Hicom 150 E Office Administrationsanleitung für Hicom Xpress@LAN, Stand 2000 (Sachnummer: A31003-K5020-B811-2-19), Bestandteil des EVGs,

3. Sicherheitstechnische Ergänzung zur Administrationsanleitung für Hicom Xpress@LAN, Stand September 2000 (Sachnummer: A31003-K5020-X100-1-20), Bestandteil des EVGs,

4. Assistant für Xpress@LAN auf Diskette (Sachnummer: P30300-P1562-A1-05), Bestandteil des EVGs,

    - Hicom 150 E Office Servicehandbuch für Hicom Xpress@LAN, Stand 2000 (Sachnummer: A31003-K5020-S100-3-20),



- vCAPI client auf Diskette (Sachnummer: P30300-P1561-A1-04),

- Hicom-Einsteckkarte (vier verschiedene Baugruppen, von denen jeweils eine ausgeliefert wird):
  Voice / Data für Hicom 150 E Office com / point (Sachnummer: S30810-Q2931-X000-05),
  Data only für Hicom 150 E Office com / point (Sachnummer: S30810-Q2931-X100-03)
  Voice / Data für Hicom 150 E Office pro (Sachnummer: S30810-Q2930-X000-06)
  Data only für Hicom 150 E Office com / point (Sachnummer: S30810-Q2930-X100-03).

Genau die unter 1. bis 4. genannten Bestandteile gehören zum EVG. Die Hicom-Einsteckkarte gehört nicht zum EVG. Zur IT-Umgebung des EVGs gehören

- die Hicom-Einsteckkarte,

- das zum Betreiben des Assistant für Xpress@LAN vorausgesetzte Betriebssystem (Windows 95, 98, NT) sowie jeder der Administrations-PCs, auf denen der Assistant für Xpress@LAN läuft,

- das jeweilige LAN (Ethernet über 10 / 100BaseT-Anschluß, TCP / IP- oder IPX / SPX als Protokolle),

- die auf den externen Schnittstellen des EVG aufsetzenden Applikationen (z. B. vCAPI-Clients, H.323-Clients, Hicom Xpress @LAN-Clients, SNMP-Tools) und

- die jeweilige Siemens-Nebenstellenanlage.

3.2.3 Zweck, Einsatzart und Funktionalität

Die Baugruppen-Software läuft auf der Einsteckkarte für bestimmte Siemens-Nebenstellenanlagen und dient der Verbindung zwischen einem TCP / IP- oder IPX / SPX-basierten LAN und der TK-Welt. Zur Administration der Baugruppe (s. Glossar) dient der im Lieferumfang enthaltene Assistant für Xpress@LAN, der auf PCs des Industriestandards mit Windows 95 / 98 / NT als Betriebssystem ablauffähig ist.

Die Baugruppe muss nach Auslieferung und Installation in die entsprechende Siemens-Nebenstellenanlage für die Nutzung vorbereitet werden (Administration). Dies geschieht mit dem Assistant für Xpress@LAN. Im weiteren Betrieb ist jederzeit eine erneute Administration möglich.

Der EVG unterstützt folgende Funktionen:

- Voice over LAN,

- Routing und LAN-LAN-Kopplung / RAS,
- vCAPI-Unterstützung für Telematik-Dienste,
- Internet-Zugang,
- Kanalbündelung (PPP-Multilink),
- Unterstützung für externe Gatekeeper (Bereitstellung von ISDN-Merkmalen für H.323-Clients),
- Authentisierung, Zugangskontrolle,
- Administration über PC-Programm Assistant für Xpress@LAN.

Dabei werden nicht alle der vorgenannten Funktionalitäten direkt vom EVG bereitgestellt, vielmehr können Leistungsmerkmale der Siemens-Nebenstellenanlage transparent genutzt werden. Die vom EVG bereitgestellte Sicherheitsfunktionalität wird weiter unten aufgeführt (vgl. Abschnitt 3.6).

3.2.4 Betriebsmodi und verarbeitete Daten

Die Baugruppe kennt nach der Erstinbetriebnahme nur einen Betriebsmodus (den Wirkbetrieb). Im Wirkbetrieb können zwei Aktivitäten parallel durchgeführt werden, die Nutzung der Funktionalität der Baugruppe und die Administration der Baugruppe auf einem Admin-PC. Beim Einspielen einer neuen Konfiguration werden alle bestehenden Verbindungen abgebaut, und es wird ein startup der Baugruppe mit der neuen Konfiguration durchgeführt. Anschließend wird der Wirkbetrieb auf der Grundlage der neuen Konfiguration fortgesetzt, vgl. auch [6], [7].

Die Baugruppe nimmt Daten entgegen, verarbeitet sie und gibt sie weiter. Dabei liegen die zu übertragenden Daten auf der LAN-Seite im TCP / IP-Format oder IPX / SPX-Format vor, auf der ISDN-Seite im ISDN-Format. Bei der Verarbeitung der Daten findet eine Protokollumsetzung statt.

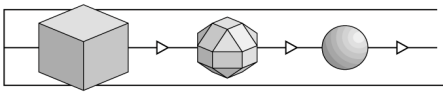
3.2.5 Topologie und EVG-interne Kommunikation

Der EVG besteht logisch aus zwei Komponenten, der Baugruppe und dem Assistant für Xpress@LAN. Der Assistant für Xpress@LAN kommuniziert mit der Baugruppe unter Benutzung des zu schützenden LANs. Ferner können Baugruppe und Assistant für Xpress@LAN auch über eine SLIP-Verbindung miteinander kommunizieren.

3.2.6 Voreingestellte EVG-Nutzer und ihre Rollen

Im Wirkbetrieb kennt der EVG drei Personengruppen (Rollen), die potentiell (logischen) Zugriff auf den EVG haben:

USER: entweder Personen, die einen autorisierten Hicom Xpress@LAN-Client benutzen oder autorisierte Endgeräte (i. a. PCs), auf denen



(mindestens) ein Internet-Dienst (Ebene 4 und tiefer im ISO/OSI-Schichtenmodell) oder ein H.323-Client oder ein vCAPI-Client installiert ist

ADMIN: Personen, die den Assistant für Xpress@LAN zur Administration benutzen

UNBEFUGTE alle anderen Personen oder Endgeräte

Bei der Administration unterscheidet der Assistant für Xpress@LAN vier Rollen, denen jeweils unterschiedliche Informationen und Einstellmöglichkeiten angeboten werden:

- Revision (Level[2] 2),
- Administration Kunde (Level 4),
- Eigenwarter / Service (Level 5),
- Entwicklung (Level 6).

3.3 Die Sicherheitsumgebung des EVG

Die Baugruppe benötigt eine bestimmte Siemens-Nebenstellenanlage, mit der zusammen sie betrieben werden kann (vgl. auch [6]). Die Administrationssoftware Assistant für Xpress@LAN läuft auf PCs des Industriestandards unter Windows 95 / 98 / NT.

3.3.1 Subjekte, Objekte und Zugriffsarten

Der EVG unterscheidet folgende Subjekte:

S_USER befugte Benutzer einer schützenswerten Funktionalität (siehe oben USER),

S_ADMIN befugte Benutzer des Assistant für Xpress@LAN (Level 2, 4, 5 oder 6),

S_UNBEF UNBEFUGTE.

Folgende Objekte werden als schützenswert durch den EVG und seine Umgebung definiert:

V_KONF Konfigurationsdaten des EVGs auf der Baugruppe (auch Kundendaten-speicher genannt, KDS),

---

[2] Die Bezeichnung „Level n“ wurde von der Siemens-Nebenstellenanlage übernommen. Die Zahl n entspricht dabei der Rückmeldung, die von der Siemens-Nebenstellenanlage bei der erfolgreichen Authentisierung gegeben wird. Nicht erfolgreiche Authentisierung wird durch Rückgabe der „0“ signalisiert.

V_DATA Daten im LAN (Filterfunktion, Abweisung unbefugter Zugriffe von außerhalb),

V_EVG die Baugruppe,

V_FUNC schützenswerte Funktionalität (gegen unbefugte Nutzung): H.323-Client, Hicom Xpress@LAN-Client, vCAPI-Client, Internet-Dienste.

Als Zugriffsarten sind relevant:

Z_READ lesen, empfangen,

Z_MODIFY ändern, erzeugen, schreiben, senden,

Z_USE nutzen, ausführen.

3.3.2 Annahmen

3.3.2.1 Infrastrukturelle Annahmen

A_ORT Die Siemens-Nebenstellenanlage mit der installierten Baugruppe wird in einem zutrittsgeschützten Raum aufgestellt. Der Zutritt unbefugter Personen wird verhindert.

3.3.2.2 Vernetzungsspezifische Annahmen

A_PATH Alle Verbindungen zwischen dem zu schützenden LAN einerseits und dem Internet oder dem Telefonnetz andererseits gehen nur über die Baugruppe in Verbindung mit der Siemens-Nebenstellenanlage.

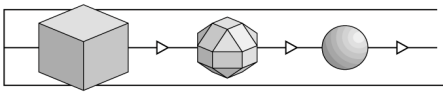
A_TRUST Die während der Administration bestehende Verbindung zwischen Admin-PC und Baugruppe ist vertrauenswürdig.

3.3.2.3 Personelle Annahmen

A_PERS Die Personen, die die Rollen Revision (Level 2), Administration Kunde (Level 4), Eigenwarter / Service (Level 5) und Entwicklung (Level 6) besetzen, sind fachlich kompetent und vertrauenswürdig.

3.3.3 Bedrohungen

T_CONF UNBEFUGTE (S_UNBEF) können die sicherheitsrelevanten Konfigurationsdaten V_KONF auf der Baugruppe lesen (Z_READ) und sie ggf. ändern (Z_MODIFY).
Die angegriffenen Werte sind die Konfigurationsdaten V_DATA auf der Baugruppe.
Angreifer sind S_UNBEF im LAN oder ISDN.



Angegriffen werden die externen Schnittstellen der Baugruppe mit frei erhältlichen, einfach zu bedienenden Softwaretools.

T_READ S_UNBEF außerhalb des zu schützenden LANs erhalten Kenntnis (Z_READ) von den Daten V_DATA im LAN.
Die angegriffenen Werte sind die Daten V_DATA im LAN.
Angreifer sind S_UNBEF, die nicht im zu schützenden LAN sitzen.
Angegriffen wird auf der ISDN-Schnittstelle mit handelsüblichen Softwaretools.

T_MODIF S_UNBEF außerhalb des zu schützenden LANs können Daten V_DATA im LAN ändern oder erzeugen (Z_MODIFY).
Die angegriffenen Werte sind die Daten V_DATA im LAN.
Angreifer sind UNBEFUGTE im ISDN.
Angegriffen wird auf der ISDN-Schnittstelle mit handelsüblichen Softwaretools.

T_FUNC S_UNBEF nutzen (Z_USE) schützenswerte Funktionalität V_FUNC.
Die angegriffenen Werte sind die in Abschnitt 3.1 aufgeführten Funktionalitäten V_FUNC.
Angreifer sind S_UNBEF im LAN oder im ISDN.
Angegriffen wird auf der ISDN-Schnittstelle mit handelsüblichen Softwaretools.

T_DOS Der durch die LAN-Benutzer[3] erzeugte Netzverkehr führt zu einer Überlastung der Baugruppe (V_EVG) und so zur Gefährdung ihrer Verfügbarkeit.
Der „angegriffene“ Wert ist die Baugruppe bezüglich ihrer Verfügbarkeit für die Erfüllung ihrer Funktionalität.
„Angreifer“ sind die Endgeräte im LAN, die Netzverkehr zur Baugruppe erzeugen.
„Angegriffen“ wird auf der LAN-Schnittstelle mit den installierten handelsüblichen Applikationen.

3.3.4 Organisatorische Sicherheitspolitik

- keine -

[3] Dabei ist es nicht entscheidend, ob es sich beim LAN-Benutzer um einen Befugten (S_USER), einen Administrator (S_ADMIN) oder einen Unbefugten (S_UNBEF) handelt.

3.4 Sicherheitsziele

3.4.1 Sicherheitsziele für den EVG

O_CONF Die Konfigurationsdaten V_KONF des EVGs auf der Baugruppe sind gegen Kenntnisnahme und Änderung durch S_UNBEF oder S_USER zu schützen.

O_FUNC Die Nutzung schützenswerter Funktionalität V_FUNC durch UNBEFUGTE (S_UNBEF) ist zu verhindern.

O_DATA Die Daten V_DATA im zu schützenden LAN sind gegen Zugriffe (lesen, ändern oder erzeugen, Z_READ oder Z_MODIFY) von UNBEFUGTEn (S_UNBEF) aus dem Telefonnetz oder dem Internet zu schützen.

O_PROT Versuche, unbefugt schützenswerte Funktionalität V_FUNC zu nutzen (Z_USE) oder unbefugt auf V_DATA zuzugreifen (Z_READ oder Z_MODIFY), müssen erkannt werden.

O_DOS Eine Überlastung der Baugruppe muss verhindert und ihre Verfügbarkeit damit gesichert werden.

3.4.2 Sicherheitsziele für die Umgebung

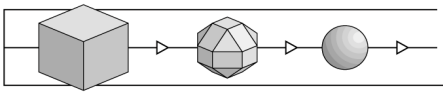
Im laufenden Betrieb (ohne Administration) benötigt die Baugruppe für ihre korrekte Funktion keine anderen Produkte außer der Siemens-Nebenstellenanlage.

Zum Zweck der Administration verlässt sich der EVG jedoch auf die Ergebnisse der Identifikation und Authentisierung des Administrators durch die Siemens-Nebenstellenanlage. Deshalb müssen in der Umgebung des EVGs folgende Ziele erreicht werden, um die vom EVG bereitgestellten Sicherheitsmerkmale zu unterstützen.

O_NSTA Der Verantwortliche für den EVG muss sicherstellen, dass die Siemens-Nebenstellenanlage baugruppenkonform konfiguriert wird. Sie muss alle Passwörter vertraulich halten. Ihre Sicherheitsfunktionen (insbesondere die Identifizierung und Authentisierung) müssen korrekt und zuverlässig arbeiten.

O_PATH Der Verantwortliche für den EVG muss sicherstellen, dass alle Verbindungen ins Internet oder ins Telefonnetz nur über die Baugruppe in Verbindung mit der Siemens-Nebenstellenanlage gehen.

O_ADMIN Der Verantwortliche für den EVG muss sicherstellen, dass Installation, Administration und Wartung nur durch geschultes und vertrauenswürdiges Personal über eine vertrauenswürdige Verbindung in einer Weise erfolgen, die die Sicherheit aufrecht erhält.



O_PHYS Der Verantwortliche für den EVG muss sicherstellen, dass die Aufstellung der Siemens-Nebenstellenanlage mit der Baugruppe in einem zutrittsgeschützten Raum erfolgt, in dem die Betriebsbedingungen für die Siemens-Nebenstellenanlage eingehalten werden.

3.5 Anforderungen an die IT- Sicherheit

3.5.1 Funktionale Sicherheitsanforderungen an den EVG

Die funktionalen Anforderungen an den EVG werden unter ausschließlicher Verwendung von funktionalen Komponenten aus Teil 2 der CC [2] formuliert. Die Abhängigkeiten funktionaler Komponenten untereinander werden berücksichtigt. Wenn eine Abhängigkeit nicht erfüllt wird, ist eine Begründung angegeben. Weitere Abhängigkeiten bestehen nicht.

Im einzelnen werden folgende Komponenten gefordert:

3.5.1.1 Komponente FIA_UID.2 Benutzeridentifikation vor jeglicher Aktion

FIA_UID.2.1 Die TSF müssen erfordern, dass sich jeder Benutzer identifiziert, bevor für diesen jegliche andere TSF-vermittelte Aktionen erlaubt werden.

3.5.1.2 Komponente FIA_UAU.2 Benutzerauthentisierung vor jeglicher Aktion

FIA_UAU.2.1 Die TSF müssen erfordern, dass jeder Benutzer erfolgreich authentisiert wurde, bevor diesem jegliche andere TSF-vermittelte Aktionen erlaubt werden.

3.5.1.3 Komponente FPT_STM.1 Verlässliche Zeitstempel

FPT_STM.1.1 Die TSF sollen einen verlässlichen Zeitstempel für den Eigengebrauch bereitstellen.

3.5.1.4 Komponente FAU_ARP.1 Sicherheitsalarme

FAU_ARP.1.1 Die TSF müssen [Zuweisung: *Liste der am wenigsten störenden Aktionen*] bei Erkennen einer potentiellen Sicherheitsverletzung ausführen.

Verfeinerung: [Zuweisung: *Liste der am wenigsten störenden Aktionen*] die Protokollierung

FAU_ARP.1.1 Die TSF müssen die Protokollierung bei Erkennen einer potentiellen Sicherheitsverletzung ausführen.

3.5.1.5 Komponente FAU_GEN.1 Generierung der Protokolldaten

FAU_GEN.1.1 Die TSF müssen in der Lage sein, für folgende protokollierbaren Ereignisse eine Protokollaufzeichnung zu generieren:
a) Starten und Beenden der Protokollierungsfunktionen;
b) Alle protokollierbaren Ereignisse für den Protokollierungsgrad [Auswahl: *Minimal, Einfach, Detailliert, nicht angegeben*]; und
c) [Zuweisung: *sonstige speziell festgelegte protokollierbare Ereignisse*].

Schritt 1: [Auswahl: *Minimal, Einfach, Detailliert, nicht angegeben*] nicht angegeben
[Zuweisung: *sonstige speziell festgelegte protokollierbare Ereignisse*] Einspielung einer neuen Konfiguration

FAU_GEN.1.1 Die TSF müssen in der Lage sein, für folgende protokollierbaren Ereignisse eine Protokollaufzeichnung zu generieren:
a) Starten und Beenden der Protokollierungsfunktionen;
b) alle protokollierbaren Ereignisse für den Protokollierungsgrad nicht angegeben; und
c) Einspielung einer neuen Konfiguration.

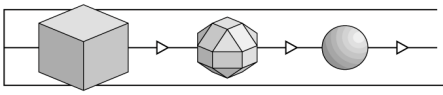
Schritt 2: editorische Verfeinerung: Die Wortgruppe „für den Protokollierungsgrad nicht angegeben“ wird gestrichen.

FAU_GEN.1.1 Die TSF müssen in der Lage sein, für folgende protokollierbaren Ereignisse eine Protokollaufzeichnung zu generieren:
a) Starten und Beenden der Protokollierungsfunktionen;
b) alle protokollierbaren Ereignisse; und
c) Einspielung einer neuen Konfiguration.

FAU_GEN.1.2 Die TSF müssen innerhalb jeder Aufzeichnung mindestens die folgenden Informationen speichern:
a) Datum und Uhrzeit des Ereignisses, Art des Ereignisses, Identität des Subjekts und das Ergebnis (Erfolg oder Misserfolg) des Ereignisses;
und
b) basierend auf den Definitionen der in PP/ST eingebundenen protokollierbaren Ereignisse, für jede Art von Protokollierungsereignissen [Zuweisung: *sonstige protokollierungsrelevante Information*].

Verfeinerung: [Zuweisung: *sonstige protokollierungsrelevante Information*] keine weiteren Informationen

FAU_GEN.1.2 Die TSF müssen innerhalb jeder Aufzeichnung mindestens die folgenden Informationen speichern:
a) Datum und Uhrzeit des Ereignisses, Art des Ereignisses, Identität des Subjekts und das Ergebnis (Erfolg oder Misserfolg) des Ereignisses; und
b) basierend auf den Definitionen der in PP/ST eingebundenen



protokollierbaren Ereignisse, für jede Art von Protokollierungsereignissen keine weiteren Informationen.

3.5.1.6 Komponente FAU_SAR.1 Durchsicht der Protokollierung

FAU_SAR.1.1 Die TSF müssen für [Zuweisung: *autorisierte Benutzer*] die Fähigkeit bereitstellen, [Zuweisung: *Liste der Protokollinformationen*] aus den Protokollaufzeichnungen zu lesen.

Verfeinerung: Zuweisungen

autorisierte Benutzer : Administratoren
Liste der Protokollinformationen : alle erzeugten Protokollinformationen

FAU_SAR.1.1 Die TSF müssen für Administratoren die Fähigkeit bereitstellen, alle erzeugten Protokollinformationen aus den Protokollaufzeichnungen zu lesen.

FAU_SAR.1.2 Die TSF müssen die Protokollaufzeichnungen in einer für die Interpretation der Informationen durch den Benutzer geeigneten Art und Weise bereitstellen.

3.5.1.7 Komponente FAU_SAR.2 Eingeschränkte Durchsicht der Protokollierung

FAU_SAR.2.1 Die TSF müssen allen Benutzern Zugriff zum Lesen der Protokollaufzeichnungen verbieten, mit Ausnahme derjenigen Benutzer, denen der Lesezugriff explizit gewährt wurde.

3.5.1.8 Komponente FAU_STG.1 Geschützte Speicherung des Protokolls

FAU_STG.1.1 Die TSF müssen die gespeicherten Protokollaufzeichnungen gegen nichtautorisiertes Löschen schützen.

FAU_STG.1.2 Die TSF müssen Modifizierungen der Protokollaufzeichnungen [Auswahl: *verhindern, erkennen*] können.

Verfeinerung: Auswahl *verhindern, erkennen :* verhindern

FAU_STG.1.2 Die TSF müssen Modifizierungen der Protokollaufzeichnungen verhindern können.

3.5.1.9 Komponente FTA_TSE.1 EVG-Sitzungseinrichtung

FTA_TSE.1.1 Die TSF müssen in der Lage sein, basierend auf [Zuweisung: *Attribute*] eine Sitzungseinrichtung zu verweigern.

Verfeinerung: Zuweisung *Attribute :* der MAC-Adresse, der IP / IPX-Adresse oder der Port-Adresse

FTA_TSE.1.1 Die TSF müssen in der Lage sein, basierend auf der MAC-Adresse, der IP / IPX-Adresse oder der Port-Adresse eine Sitzungseinrichtung zu verweigern.

3.5.1.10 Komponente FRU_RSA.1 Maximale Quote

FRU_RSA.1.1 Die TSF müssen maximale Quoten für folgende Betriebsmittel [Zuweisung: *kontrollierte Betriebsmittel*], die [Auswahl: *ein einzelner Benutzer, eine festgelegte Benutzergruppe, Subjekte*] [Auswahl: *gleichzeitig, über eine spezifizierte Zeitspanne*] benutzen können, durchsetzen.

Verfeinerung: Zuweisung und Auswahl

Zuweisung: folgende Betriebsmittel *kontrollierte Betriebsmittel:* der interne Speicher der Baugruppe
Ersetzung *ein einzelner Benutzer, eine festgelegte Benutzergruppe, Subjekte:* Subjekte
Auswahl: [*gleichzeitig, über eine spezifizierte Zeitspanne*] über eine spezifizierte Zeitspanne

FRU_RSA.1.1 Die TSF müssen maximale Quoten für den internen Speicher der Baugruppe, der von Subjekten über eine spezifizierte Zeitspanne benutzt werden kann, durchsetzen.

3.5.1.11 Komponente FAU_SAA.1 Analyse von möglichen Verletzungen

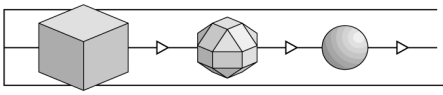
FAU_SAA.1.1 Die TSF müssen in der Lage sein, beim Überwachen der protokollierten Ereignisse eine Menge von Regeln anzuwenden und auf Grundlage dieser Regeln eine potentielle Verletzung der TSP anzuzeigen.

FAU_SAA.1.2 Die TSF müssen zur Überwachung von protokollierten Ereignissen die folgenden Regeln durchsetzen:
a) Eine Häufung oder Kombination von [Zuweisung: *Teilmenge von festgelegten protokollierbaren Ereignissen*], die bekanntermaßen eine potentielle Sicherheitsverletzung anzeigen;
b) [Zuweisung: *beliebige andere Regeln*].

Schritt 1: Zuweisung:

b) [Zuweisung: *beliebige andere Regeln*]: Jedes Auftreten eines Ereignisses, das zu einer zur Protokollierung ausgewählten Ereignisgruppe gehört, muss protokolliert werden.

FAU_SAA.1.2 Die TSF müssen zur Überwachung von protokollierten Ereignissen die folgenden Regeln durchsetzen:
a) Eine Häufung oder Kombination von [Zuweisung: *Teilmenge von festgelegten protokollierbaren Ereignissen*], die bekanntermaßen eine potentielle Sicherheitsverletzung anzeigen;



b) Jedes Auftreten eines Ereignisses, das zu einer zur Protokollierung ausgewählten Ereignisgruppe gehört, muss protokolliert werden.

Schritt 2: Verfeinerung:

Die Komponente, die eine Anwendung der Regeln a) oder b) zuläßt, wird so verfeinert, dass nur die Regel b) angewendet wird.[4]

FAU_SAA.1.2 Die TSF müssen zur Überwachung von protokollierten Ereignissen die folgenden Regeln durchsetzen:
Jedes Ereignis, das zu einer zur Protokollierung ausgewählten Ereignisgruppe gehört, muss protokolliert werden.

3.5.2 Anforderungen an die Vertrauenswürdigkeit des EVG

Die Anforderungen an die Vertrauenswürdigkeit des EVGs sind gemäß der Stufe EAL1 der CC [4] festgelegt.

Im einzelnen sind dies:

Vertrauenswürdigkeitsklasse Konfigurationsmanagement

ACM_CAP.1 Versionsnummern

Vertrauenswürdigkeitsklasse Auslieferung und Betrieb

ADO_IGS.1 Installations-, Generierungs- und Anlaufprozeduren

Vertrauenswürdigkeitsklasse Entwicklung

ADV_FSP.1 Informelle funktionale Spezifikation

ADV_RCR.1 Informeller Nachweis der Übereinstimmung

Vertrauenswürdigkeitsklasse Handbücher

AGD_ADM.1 Systemverwalterhandbuch

AGD_USR.1 Benutzerhandbuch

Vertrauenswürdigkeitsklasse Testen

ATE_IND.1 Unabhängiges Testen – Übereinstimmung

---

[4] Bemerkung: Bei genauerer Betrachtung stellt man fest, dass die Regel b) die Regel a) umfaßt.

3.5.3 Sicherheitsanforderungen an die IT Umgebung

In Übereinstimmung mit dem Ziel O_NSTA wird gefordert, dass die Siemens-Nebenstellenanlage die Funktionen Identifizierung und Authentisierung für Administration und Service korrekt und vertrauenswürdig bereitstellt. Daher ist an die IT-Umgebung des EVGs folgende Sicherheitsanforderung zu stellen (beachte: mit den TSF sind die TSF der Siemens-Nebenstellenanlage gemeint):

FIA_ATD.1.1 Die TSF müssen die folgende Liste von Sicherheitsattributen, die zu einzelnen Benutzern gehören, erhalten[5]: [Zuweisung: *Liste der Sicherheitsattribute*].

Verfeinerung: [Zuweisung: *Liste der Sicherheitsattribute*]: (Level 0; S_UNBEF), (Level 2; S_ADMIN aus Revision), (Level 4; S_ADMIN aus Administration Kunde), (Level 5; S_ADMIN aus Eigenwarter / Service) oder (Level 6; S_ADMIN aus Entwicklung)

FIA_ATD.1.1 Die TSF müssen die folgende Liste von Sicherheitsattributen, die zu einzelnen Benutzern gehören, erhalten: (Level 0; S_UNBEF), (Level 2; S_ADMIN aus Revision), (Level 4; S_ADMIN aus Administration Kunde), (Level 5; S_ADMIN aus Eigenwarter / Service) oder (Level 6; S_ADMIN aus Entwicklung).

3.6 EVG-Übersichtsspezifikation

3.6.1 Spezifikation der EVG-Sicherheitsfunktionen

Der EVG stellt folgende Sicherheitsfunktionen bereit, mit denen die in Abschnitt 5.1 aufgeführten funktionalen Sicherheitsanforderungen an den EVG erfüllt werden:

SF-1: Authentisierung von Administratoren (Assistant für Xpress@LAN)

SF-2: Zugriffskontrolle auf Datenbankelemente (nur Assistant für Xpress@LAN) der Konfigurationsdaten V_KONF

SF-3a: MAC-Adress-Filter

SF-3b: IP / IPX-Adress-Filter

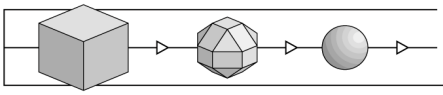
SF-3c: Port-Adress-Filter

SF-4: Protokollierung durch SNMP-Traps

SF-5: Protokollierung abgewiesener und angenommener Verbindungen (Kunden-Trace)

---

5 Im englischen Original wird das Verb „maintain“ verwendet, „erhalten“ ist daher im Sinne von „pflegen“ zu verstehen.



SF-6: Authentisierung der voice clients vom Typ OptiC55 (auf der Baugruppe)

SF-7: Herstellen authentischer Verbindungen (Identifikation durch Rückruf)

SF-8: Authentisierung der remote user an der Baugruppe

SF-9: Zeitstempel

SF-10: Überlastsicherung des LAN-Adapters

Außer SF-1 und SF-2 sind alle anderen TSF auf der Baugruppe realisiert.

Die oben genannten Sicherheitsfunktionen wirken wie folgt:

SF-1: Unmittelbar nach dem Start des Assistant für Xpress@LAN wird der Benutzer nach Name und Passwort gefragt. Diese Aktion ist die erste, die der Benutzer ausführen muss, bevor er irgend eine andere Funktion von Assistant für Xpress@LAN nutzen kann. Weitere Aktionen mit Assistant für Xpress@LAN sind erst möglich, nachdem sich der Benutzer erfolgreich identifiziert und authentisiert hat.
Das Passwort wird vom Assistant für Xpress@LAN an die Siemens-Nebenstellenanlage (über die Verbindung zum EVG) zur Prüfung gesandt. Das Prüfergebnis geht an Assistant für Xpress@LAN zurück. Anhand des Ergebnisses lehnt Assistant für Xpress@LAN den Benutzer ab (Returncode = 0) oder weist dem authentisierten Administrator seinen Level zu. Anschließend an die erfolgreiche Authentisierung wird der Kundendatensatz (KDS, identisch mit V_KONF) aus der Baugruppe geladen.

SF-2: Nach erfolgreicher Authentisierung eines Administrators stellt Assistant für Xpress@LAN diesem den KDS zur Bearbeitung bereit. Dabei werden nur solche Daten zur Bearbeitung angezeigt und bearbeitet, die dem eingestellten Level entsprechen. Nach erfolgter Bearbeitung wird der bearbeitete KDS an die Baugruppe gesandt und dort gespeichert.
SF-2 sorgt ferner dafür, dass die Log-Informationen der Baugruppe nur von Administratoren heruntergeladen werden können.

SF-3: (SF-3a, SF-3b, SF-3c) Die Filter sind auf der Baugruppe als Software realisiert. Sie werden durch den KDS konfiguriert, wirken nach dem Prinzip „Was nicht explizit erlaubt ist, ist verboten“ und filtern nach IP-Adressen, MAC-Adressen und Portnummern. Eine Filterung nach Diensten erfolgt nicht.

SF-4: Die auf der Baugruppe laufende Software beinhaltet einen SNMP-Server. Dieser erkennt bestimmte Zustände und Ereignisse auf der Baugruppe und ist in der Lage, Informationen dazu zu erzeugen (SNMP-Traps), vgl. [7], S. 97f. Die generierten SNMP-Traps werden auf der Baugruppe als strukturierte ASCII-Datei gespeichert. Es besteht auch die Möglichkeit, die generierten Traps an eine festgelegte Adresse zu senden. Dies muss im KDS konfiguriert werden.
Einmal durch SF-4 geschriebene Informationen können auf der Baugruppe nicht

modifiziert werden. Da die Speicher als Ringspeicher organisiert sind, können bei unachtsamer Administration höchstens Protokollinformationen mit neuen Protokollinformationen überschrieben werden.

SF-5: Die auf der Baugruppe laufende Software ist in der Lage, sicherheitskritische Ereignisse, die sich auf den PPP-Verbindungsaufbau und den ISDN-Verbindungsaufbau beziehen, zu erkennen und Protokollinformationen als strukturierte ASCII-Datei zu generieren, die Auskunft über diese Ereignisse geben, vgl. [7], S. 147ff. Dies muss im KDS konfiguriert werden.
Einmal durch SF-5 geschriebene Informationen können auf der Baugruppe nicht modifiziert werden. Da die Speicher als Ringspeicher organisiert sind, können bei unachtsamer Administration höchstens Protokollinformationen mit neuen Protokollinformationen überschrieben werden.

SF-6: Voice clients vom Typ OptiC55 müssen sich vor dem Verbindungsaufbau bei der Baugruppe authentisieren. Dazu gibt der Benutzer in seiner Applikation (Teil der IT-Umgebung des EVGs) seine Rufnummer und sein Passwort an. Die Baugruppe prüft die Angaben und nimmt im Erfolgsfall weitere Aufträge an. H.323-Clients müssen sich ebenfalls authentisieren.

SF-7: Im KDS ist konfigurierbar, ob bei einem eingehenden Ruf eine Verbindung aufgebaut wird oder der Verbindungswunsch abgelehnt und die im KDS konfigurierte Rufnummer aktiv gewählt wird.

SF-8: Die Authentisierung entfernter Nutzer erfolgt mittels eines nutzerspezifischen Passwortes. Zur Abwicklung des notwendigen Datenverkehrs werden die Protokolle PAP / CHAP (vgl. folgende RFCs: PAP / CHAP: 1334; CHAP: 1994; MS-CHAP: 2433 und 2759) genutzt.

SF-9: Die Baugruppe verfügt über einen eigenen Uhrenschaltkreis, der Datum und Uhrzeit für EVG-interne Zwecke bereitstellt.

SF-10: Die Baugruppe verfügt über einen Mechanismus, der den LAN-Adapter für die Annahme von Paketen sperrt, wenn ein bestimmter Auslastungsgrad der Baugruppe erreicht oder überschritten ist.

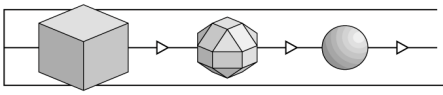
Weitere Informationen zu den Sicherheitsfunktionen finden sich in den Handbüchern [6] und [7] und in den angegebenen RFCs.

3.6.2 Spezifikation der Maßnahmen zur Vertrauenswürdigkeit des EVG

Zur Erfüllung der Anforderungen an die Vertrauenswürdigkeit des EVGs wurden gemäß der Stufe EAL1 der CC [4] folgende Maßnahmen getroffen:

Vertrauenswürdigkeitsklasse Konfigurationsmanagement

ACM_CAP.1.1M Der Entwickler vergibt für den EVG einen eindeutigen Namen, der sicherstellt, dass Mehrdeutigkeit darüber ausgeschlossen ist, welche Version des EVG geprüft und bewertet wird.



ACM_CAP.1.2M Der Entwickler kennzeichnet den EVG mit seinem eindeutigen Namen.

Vertrauenswürdigkeitsklasse Auslieferung und Betrieb

ADO_IGS.1M Der Entwickler stellt eine Beschreibung der Installations-, Generierungs- und Anlaufprozeduren bereit, vgl. [6] und [7].

Vertrauenswürdigkeitsklasse Entwicklung

ADV_FSP.1M Der Entwickler stellt eine informelle funktionale Spezifikation der TSF des EVGs bereit, die alle externen Schnittstellen vollständig definiert und das Verhalten der TSF beschreibt.

ADV_RCR.1M Der Entwickler stellt eine Analyse der Übereinstimmung von Security Target und funktionaler Spezifikation der TSF bereit.

Vertrauenswürdigkeitsklasse Handbücher

AGD_ADM.1M Der Entwickler stellt ein Systemverwalterhandbuch bereit, vgl. [7].

AGD_USR.1M Der Entwickler stellt ein Benutzerhandbuch[6] bereit, vgl. [6].

Vertrauenswürdigkeitsklasse Testen

ATE_IND.1M Der Entwickler stellt den EVG für den Evaluator bereit, damit dieser ihn testen kann. Darüber hinaus stellt der Entwickler dem Evaluator geeignete Testhilfsmittel bereit, die den Evaluator bei seiner Tätigkeit unterstützen.

3.7 PP-Postulate

Dieses Security Target nimmt nicht Bezug auf ein Protection Profile.

Alle EVG-Ziele und –Anforderungen sind in den vorangehenden Abschnitten vollständig dargestellt.

---

6 Das Benutzerhandbuch [6] richtet sich an den Betreiber der Hicom Xpress@LAN, d. h. der Benutzer des EVGs ist hier der Betreiber.

3.8 Erklärung (Rationale)

3.8.1 Erklärung der Sicherheitsziele

3.8.1.1 Rückführung der Sicherheitsziele für den EVG auf Bedrohungen

Der EVG schützt gegen fünf explizit genannte Bedrohungen, indem er entsprechende Sicherheitsziele erreicht. Die folgende Tabelle 1 zeigt die Korrespondenz zwischen Bedrohungen und Sicherheitszielen.

Sicherheitsziel	Bedrohung
O_CONF	T_CONF
O_DATA	T_READ, T_MODIF
O_PROT	(T_READ, T_MODIF, T_FUNC)
O_FUNC	T_FUNC
O_DOS	T_DOS

Tabelle 1: Sicherheitsziele für den EVG und Bedrohungen

Nachfolgend werden die einzelnen Korrespondenzen begründet.

O_CONF

Die Konfigurationsdaten V_KONF des EVGs auf der Baugruppe sind gegen Kenntnisnahme und Änderung durch S_UNBEF oder S_USER zu schützen.

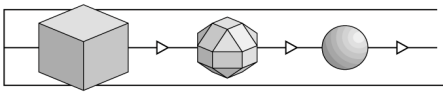
Dieses Sicherheitsziel ist gegen die entsprechende Bedrohung gerichtet, dass die Konfigurationsdaten des EVGs (auch KDS genannt) unbefugt zur Kenntnis genommen oder geändert werden können.

O_DATA

Die Daten V_DATA im zu schützenden LAN sind gegen Zugriffe (lesen, ändern oder erzeugen) von S_UNBEF aus dem Telefonnetz oder dem Internet zu schützen.

Dieses Sicherheitsziel ist gegen die Bedrohung gerichtet, die Daten im zu schützenden LAN unbefugt aus dem Telefonnetz oder dem Internet zu lesen (T_READ).

Dieses Sicherheitsziel ist ferner gegen die Bedrohung gerichtet, die Daten im zu schützenden LAN unbefugt aus dem Telefonnetz oder dem Internet zu ändern oder zu erzeugen (T_MODIF).



O_PROT

Versuche, unbefugt schützenswerte Funktionalität V_FUNC zu nutzen oder unbefugt auf V_DATA zuzugreifen (Z_READ oder Z_MODIFY), müssen erkannt werden.

Anhand der eingestellten Konfiguration V_KONF lässt der EVG Verbindungen zu oder weist sie ab. Hinter abgewiesenen Verbindungswünschen können sich Angriffe verbergen. Um derartige Angriffsversuche erkennen und darauf reagieren zu können, ist eine Protokollierung von Versuchen, unbefugt schützenswerte Funktionalität V_FUNC zu nutzen oder unbefugt auf V_DATA zuzugreifen, notwendig. Indem solche Versuche protokolliert (und ausgewertet) werden, werden potentielle Angriffe erkennbar. Indirekt wird daher den Bedrohungen T_READ, T_MODIF und T_FUNC entgegengewirkt.

O_FUNC

Die Nutzung schützenswerter Funktionalität V_FUNC durch UNBEFUGTE (S_UNBEF) ist zu verhindern.

Dieses Sicherheitsziel ist gegen die Bedrohung T_FUNC gerichtet, dass V_FUNC durch S_UNBEF aus dem LAN oder dem ISDN genutzt wird.

O_DOS

Eine Überlastung der Baugruppe muss verhindert und ihre Verfügbarkeit damit gesichert werden.

Dieses Sicherheitsziel ist gegen die Bedrohung gerichtet, die Baugruppe durch den erzeugten Netzverkehr im LAN zu überlasten und so ihre Verfügbarkeit zu gefährden.

3.8.1.2 Rückführung der Sicherheitsziele für den EVG auf Elemente der Sicherheitspolitik

Da die Sicherheitsziele einzig auf die Bedrohungen und die Annahmen zurückgeführt werden, wurde eine organisatorische Sicherheitspolitik nicht angegeben. Es sind hier folglich keine Elemente der Sicherheitspolitik zu betrachten.

3.8.1.3 Rückführung der Sicherheitsziele für die EVG-Umgebung auf Annahmen oder Bedrohungen

Es gibt vier Sicherheitsziele für die Umgebung des EVGs (O_NSTA, O_PATH, O_ADMIN und O_PHYS), die aus folgenden Gründen aufgestellt werden:

Sicherheitsziel	Annahme oder Bedrohung
O_NSTA	T_CONF, (T_READ, T_MODIF, T_FUNC)
O_PATH	A_PATH, (T_READ, T_MODIF, T_FUNC)

Sicherheitsziel	Annahme oder Bedrohung
O_ADMIN	A_PERS, A_ORT, A_TRUST
O_PHYS	A_ORT

Tabelle 2: Sicherheitsziele für die Umgebung und Bedrohungen und Annahmen

O_NSTA

Der Verantwortliche für den EVG muss sicherstellen, dass die Siemens-Nebenstellenanlage baugruppenkonform konfiguriert wird. Sie muss alle Passwörter vertraulich halten. Ihre Sicherheitsfunktionen (insbesondere die Identifizierung und Authentisierung) müssen korrekt und zuverlässig arbeiten.

Bei der Authentisierung eines Administrators (Level 2, 4, 5, oder 6) verlässt sich der EVG auf das Authentisierungsergebnis, das ihm von der Siemens-Nebenstellenanlage mitgeteilt wird. Auf der Grundlage dieser Authentisierung wird dem Benutzer des Assistant für Xpress@LAN die Möglichkeit gegeben, den KDS zu bearbeiten. Eine falsche Authentisierung eröffnet daher die Möglichkeit, die Sicherheitsfunktionen des EVGs auszuschalten oder zu umgehen. O_NSTA wirkt folglich gegen die Bedrohungen T_CONF, indirekt jedoch auch gegen T_READ, T_MODIF und T_FUNC.

O_PATH

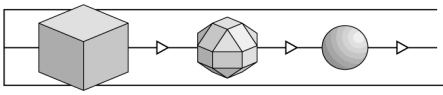
Der Verantwortliche für den EVG muss sicherstellen, dass alle Verbindungen ins Internet oder ins Telefonnetz nur über die Baugruppe in Verbindung mit der Siemens-Nebenstellenanlage gehen.

Gibt es außer dem geschützten Zugang zum Internet über den EVG noch weitere Zugänge zum Internet, über die Sicherheitslücken eingeführt werden, so können die Bedrohungen (ggf. außer T_CONF und T_DOS) insgesamt nicht abgewehrt werden, da sich ein Angreifer stets den „Weg des geringsten Widerstandes“ wählen wird. Das Ziel O_PATH wird durch die Annahme A_PATH abgedeckt.

O_ADMIN

Der Verantwortliche für den EVG muss sicherstellen, dass Installation, Administration und Wartung nur durch geschultes und vertrauenswürdiges Personal über eine vertrauenswürdige Verbindung in einer Weise erfolgen, die die Sicherheit aufrecht erhält.

Dieses Ziel ist abgedeckt durch die personelle Annahme A_PERS für die fachliche Kompetenz und Vertrauenswürdigkeit der Administratoren, durch die Annahme A_ORT, indem das Risiko unbefugten physischen Zugriffs bekämpft wird, und durch die Annahme A_TRUST, durch die die vertrauenswürdige Verbindung gewährleistet wird.



O_PHYS

Der Verantwortliche für den EVG muss sicherstellen, dass die Aufstellung der Siemens-Nebenstellenanlage mit der Baugruppe in einem zutrittsgeschützten Raum erfolgt, in dem die Betriebsbedingungen für die Siemens-Nebenstellenanlage eingehalten werden.

Dieses Ziel ist abgedeckt durch die Annahme A_ORT.

3.8.1.4 Eignung der Sicherheitsziele zur Bekämpfung der Bedrohungen

Die folgende Tabelle 3 zeigt die Beziehung zwischen Bedrohungen und Sicherheitszielen:

Bedrohung	Sicherheitsziele
T_CONF	O_CONF, O_NSTA
T_READ	O_DATA, O_PATH, (O_PROT, O_NSTA)
T_MODIFY	O_DATA, O_PATH, (O_PROT, O_NSTA)
T_FUNC	O_FUNC, O_PATH, (O_PROT, O_NSTA)
T_DOS	O_DOS

Tabelle 3: Sicherheitsziele, die zur Abwehr von Bedrohungen beitragen

T_CONF

T_CONF wird abgewehrt, wenn der Zugriff auf die Konfigurationsdaten V_KONF nur Befugten gestattet wird. O_CONF ist daher ein zur Abwehr von T_CONF geeignetes Ziel. Indem auch der physische Zugriff auf die Baugruppe mittels O_NSTA beschränkt wird, ist sichergestellt, dass Unbefugte nur über die logischen Schnittstellen der Baugruppe angreifen können. Folglich ist auch O_NSTA ein zur Abwehr von T_CONF geeignetes Ziel.

T_READ

T_READ wird abgewehrt, wenn V_DATA vor dem lesenden Zugriff durch S_UNBEF aus dem Internet oder dem Telefonnetz geschützt sind. O_DATA ist daher zur Abwehr von T_READ geeignet und angemessen. Damit es nicht möglich ist, den EVG und seine Schutzwirkung zu umgehen, muss jeder Weg eines Unbefugten aus dem Internet oder dem Telefonnetz in das zu schützende LAN über die Baugruppe führen. Folglich ist O_PATH ebenfalls angemessen und geeignet, T_READ abzuwehren. Das Ziel O_PROT dient der Überwachung von Sicherheitsfunktionen der Baugruppe und ist daher grundsätzlich angemessen und geeignet, der Bedrohung T_READ indirekt entgegenzuwirken. Die Eignung und Angemessenheit von O_NSTA zur Bekämpfung von T_READ wurde bereits in Abschnitt 3.8.1.3 dargelegt.

T_MODIFY

T_MODIFY wird abgewehrt, wenn V_DATA vor dem Zugriff Z_MODIFY durch S_UNBEF aus dem Internet oder dem Telefonnetz geschützt sind. Dies ist einer der Inhalte des Zieles O_DATA. Mit analoger Begründung wie für T_READ ist O_DATA daher auch zur Abwehr von T_MODIFY angemessen und geeignet. Die Analogie gilt ebenfalls für O_PATH, O_PROT und O_NSTA.

T_FUNC

T_FUNC wird abgewehrt, wenn das komplementäre Ziel O_FUNC erreicht wird, weshalb es angemessen und geeignet ist. Für Eignung und Angemessenheit von O_PATH, O_PROT und O_NSTA gelten analoge Begründungen wie unter T_READ dargestellt.

T_DOS

O_DOS ist das zur Bedrohung T_DOS komplementäre Ziel und daher geeignet und angemessen, T_DOS zu bekämpfen.

3.8.2 Erklärung der Sicherheitsanforderungen

3.8.2.1 Innere Konsistenz und gegenseitige Unterstützung der funktionalen Anforderungen

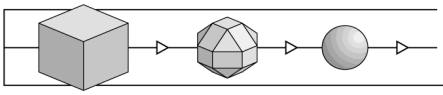
Die funktionalen Sicherheitsanforderungen wurden aus den CC, Teil 2 ([2]) ausgewählt. Sie entsprechend damit vordefinierten CC-Komponenten. Es wurden die nach CC zulässigen Operationen Verfeinerung, Zuweisung, Auswahl und Iteration benutzt. Zusätzliche Komponenten wurden nicht verwendet. Hierarchien und Abhängigkeiten der vordefinierten Komponenten untereinander wurden beachtet. Aus den vorgenannten Gründen bilden die funktionalen Anforderungen ein sich gegenseitig unterstützendes Ganzes.

3.8.2.2 Vollständige Abdeckung der Sicherheitsziele

3.8.2.2.1 Ziele und Anforderungen für den EVG

Die folgende Tabelle 4 zeigt, welche Beziehungen zwischen funktionalen Komponenten und Sicherheitszielen für den EVG bestehen.

	O_CONF	O_FUNC	O_DATA	O_PROT	O_DOS
FIA_UID.2.1	X	X	X		
FIA_UAU.2.1	X	X	X		
FPT_STM.1.1				X	
FAU_ARP.1.1				X	
FAU_GEN.1.1				X	



	O_CONF	O_FUNC	O_DATA	O_PROT	O_DOS
FAU_GEN.1.2				X	
FAU_SAR.1.1				X	
FAU_SAR.1.2				X	
FAU_SAR.2.1				X	
FAU_STG.1.1				X	
FAU_STG.1.2				X	
FTA_TSE.1.1		X	X		
FRAU_RSA.1.1					X
FAU_SAA.1.1				X	
FAU_SAA.1.2				X	

Tabelle 4: Sicherheitsziele für den EVG und funktionale Anforderungen

Ein Kreuz in der Tabelle 4 zeigt an, dass die in der jeweiligen Zeile angegebene funktionale Komponente vom in der jeweiligen Spalte angegebenen Sicherheitsziel benötigt wird. Es ist zu erkennen, dass es kein Sicherheitsziel gibt, dem nicht mindestens eine funktionale Komponente zugeordnet wäre. Darüber hinaus gibt es keine funktionale Komponente, die nicht auf mindestens ein Ziel zurückgeführt würde.

Erklärung der Tabelle 4

O_CONF

O_CONF wird durch die Sicherheitsanforderungen für den EVG FIA_UID.2.1 und FIA_UAU.2.1 abgedeckt. Die Konfigurationsdaten V_KONF liegen auf der Baugruppe. Sie können dort jedoch nicht bearbeitet werden, da eine entsprechende Funktionalität fehlt. Das Lesen der V_KONF setzt sogar voraus, dass die V_KONF von der Baugruppe auf einen PC heruntergeladen werden. Daher ist genau diese Funktionalität gegen Missbrauch zu schützen. Die Anforderung FIA_UAU.2.1 verlangt gerade die Authentisierung (hier: der Administratoren). Die abhängige Komponente FIA_UID.1 wird nicht gefordert. Statt dessen wird die stärkere Anforderung FIA_UID.2.1 gestellt, die hierarchisch dazu ist. Die Forderungen FIA_UID.2.1 und FIA_UAU.2.1 zu stellen ist aber auch ausreichend, da Kenntnisnahme und Änderung von V_KONF auf diese Weise erst nach erfolgreicher Identifikation und Authentisierung möglich werden.

O_FUNC

O_FUNC wird durch die funktionalen Sicherheitsanforderung FIA_UID.2.1, FIA_UAU.2.1 und FTA_TSE.1.1 abgedeckt, die zum Teil aus Gründen der Abhängigkeit aufgenommen wurden.

Wenn bestimmte Benutzer von der Inanspruchnahme einer Funktionalität ausgenommen werden sollen, so muss der EVG in der Lage sein, zwischen verschiedenen Benutzern authentisch zu unterscheiden. Daher wurde FIA_UAU.2.1

ausgewählt. Als abhängige Komponente ist dann FIA_UID.1 auszuwählen. Hier wurde entschieden, die stärkere Anforderung FIA_UID.2.1 auszuwählen, die hierarchisch zu FIA_UID.1 ist. Die Authentisierung von Benutzern mit Ausnahme der Administratoren (vgl. dazu die Beschreibung der SF-1 in Abschnitt 3.6.1) erfolgt auf der Baugruppe. Da die Benutzer entfernte Rechner benutzen, wird ein Authentisierungsprotokoll (PAP oder CHAP) angewendet.

Da die bereitzustellende Funktionalität des EVGs die Verweigerung von Zugriffen aus dem Internet oder ins Internet einschließt und dies im Rahmen der Einrichtung entsprechender Sitzungen oder ihrer Verweigerung geschieht, ist die Anforderung FTA_TSE.1.1 auszuwählen, die gerade dies fordert.

Die drei funktionalen Sicherheitsanforderung FIA_UID.2.1, FIA_UAU.2.1 und FTA_TSE.1.1 zu stellen, ist zur Umsetzung des Zieles O_FUNC ausreichend, da der Nutzung einer schützenswerten Funktionalität, die verbindungsorientiert genutzt wird, die Identifikation und Authentisierung vorangestellt werden, während schützenswerte Funktionalität, die verbindungslos genutzt wird, vor unbefugter Nutzung durch die Verweigerung der Einrichtung einer Sitzung geschützt wird.

O_DATA

Die funktionalen Sicherheitsanforderungen FIA_UID.2.1, FIA_UAU.2.1 und FTA_TSE.1.1 unterstützen das Sicherheitsziel O_DATA mit folgender Begründung:

Da zwischen autorisierten und nicht autorisierten Benutzern unterschieden werden soll, ist FIA_UAU.2 auszuwählen und als abhängige Komponente FIA_UID.1, wobei hier jedoch stärker FIA_UID.2 gewählt wurde (beachte: **vor jeder anderen Interaktion**). Die Authentisierung von Benutzern mit Ausnahme der Administratoren (vgl. dazu die Beschreibung der SF-1 in Abschnitt 3.6.1) erfolgt auf der Baugruppe. Da die Benutzer entfernte Rechner benutzen, wird ein Authentisierungsprotokoll (PAP oder CHAP) angewendet.

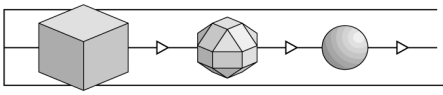
Da die bereitzustellende Funktionalität des EVGs die Verweigerung von Zugriffen aus dem Internet einschließt und dies im Rahmen der Einrichtung entsprechender Sitzungen oder ihrer Verweigerung geschieht, ist die Anforderung FTA_TSE.1.1 auszuwählen, die gerade dies fordert.

FIA_UID.2.1, FIA_UAU.2.1 und FTA_TSE.1.1 sind als Anforderungen für O_DATA ausreichend. Die Begründung ergibt sich analog zur Begründung unter O_FUNC.

O_PROT

O_PROT wird durch die Anforderungen FPT_STM.1.1, FAU_ARP.1.1, FAU_GEN.1.1, FAU_GEN.1.2, FAU_SAR.1.1, FAU_SAR.1.2, FAU_SAR.2.1, FAU_STG.1.1, FAU_STG.1.2, FAU_SAA.1.1 und FAU_SAA.1.2 unterstützt, die zum Teil aus Gründen der Abhängigkeit aufgenommen wurden.

Um Angriffsversuche erkennen und darauf reagieren zu können, ist eine Protokollierung von Versuchen, unbefugt schützenswerte Funktionalität V_FUNC zu nutzen oder



unbefugt auf V_DATA zuzugreifen, notwendig. Daher ist FAU_ARP.1 auszuwählen, die gerade dies fordert. FAU_ARP.1 hängt von der Komponente FAU_SAA.1 ab, diese von FAU_GEN.1, diese wiederum von FPT_STM.1. Es ist ferner nötig, die erfassten Protokolldaten auch auszuwerten. Dies wird gerade von FAU_SAR.1 gefordert. Da Protokolldaten indirekten Aufschluss über Angriffsversuche geben, muss der Zugriff auf befugte Nutzer beschränkt werden. Dies fordert FAU_SAR.2. Schließlich wird FAU_STG.1 gefordert, damit die Zuverlässigkeit der aus den Protokollaufzeichnungen gewonnenen Schlüsse nicht durch Unvollständigkeit oder Fehlerhaftigkeit leidet.

Das Ziel O_PROT ist ausreichend abgedeckt durch die Anforderungen FPT_STM.1.1, FAU_ARP.1.1, FAU_GEN.1.1, FAU_GEN.1.2, FAU_SAR.1.1, FAU_SAR.1.2, FAU_SAR.2.1, FAU_STG.1.1, FAU_STG.1.2, FAU_SAA.1.1 und FAU_SAA.1.2, denn FAU_ARP.1.1 fordert, dass potentielle Sicherheitsverletzungen überhaupt protokolliert werden. Als davon abhängige Komponenten müssen FAU_SAA.1.1, FAU_SAA.1.2, FAU_GEN.1.1, FAU_GEN.1.2 und FPT_STM.1.1 gefordert werden. Das Erfordernis, protokollierte Informationen auch auswerten zu können, wird durch die Anforderungen FAU_SAR.1.1, FAU_SAR.1.2 und FAU_SAR.2.1 abgedeckt, wobei die Beschränkung des Lesens auf autorisierte Personen der missbräuchlichen Verwendung von Protokollinformationen entgegenwirkt. Wegen der Zuverlässigkeit der Informationen, die aus den Protokollaufzeichnungen entnommen werden können, werden schließlich die Forderungen FAU_STG.1.1 und FAU_STG.1.2 gestellt.

O_DOS

O_DOS wird einzig durch FRU_RSA.1.1 unterstützt. Die Überlastung der Baugruppe wird verhindert, wenn für die Bearbeitung der von der Baugruppe angenommenen Datenpakete jeweils genug Ressourcen an Rechenzeit und Speicherkapazität bereitstehen. Die aktuell zur Verfügung stehende Speicherkapazität bestimmt, ob die Datenpakete, die bereits von der Baugruppe angenommen wurden, auch ordnungsgemäß bearbeitet werden können. Daher ist es sinnvoll und angemessen, eine Beschränkung der maximalen Belegung für den internen Speicher der Baugruppe zu fordern. Dies verlangt genau FRU_RSA.1.1. Alle Subjekte werden gleichbehandelt, da es sich um ein verbindungsloses Protokoll handelt. Alle bereits in Bearbeitung befindlichen Datenpakete können ordnungsgemäß bearbeitet werden, da stets genügend Speicherplatz und Bearbeitungszeit zur Verfügung stehen, und es werden nur so viele neue Datenpakete angenommen, wie in unmittelbarer Zukunft auch bearbeitet werden können. Folglich fordert FRU_RSA.1.1 genau das richtige.

3.8.2.2.2 Ziele und Anforderungen für die IT-Umgebung des EVGs

Für die IT-Umgebung ist eine Sicherheitsanforderung angegeben: FIA_ATD.1.1. Diese Anforderung wird gestellt, damit die TSF die Information erhalten, welche Person (d. h. welche Rolle) sich zur Administration angemeldet hat. Diese Information kann nur dann bereitgestellt werden, wenn das Sicherheitsziel O_NSTA an die IT-Umgebung erfüllt wird.

Das Sicherheitsziel O_PATH an die IT-Umgebung lässt sich nicht durch eine funktionale Anforderung an die IT-Umgebung realisieren, hier sind vielmehr Installationen weiterer externer Netzzugänge zu unterlassen.

3.8.2.3 Angemessenheit der Anforderungen an die Vertrauenswürdigkeit

Die Anforderungen an die Vertrauenswürdigkeit des EVG wurden aus Teil 3 der CC ausgewählt. Es wurden alle Anforderungen gemäß EAL 1 ausgewählt, weitere Anforderungen an die Vertrauenswürdigkeit wurden nicht gestellt.

Der EVG soll dem Benutzer die Überzeugung vermitteln, dass seine Sicherheitsfunktionen korrekt arbeiten. Die Bedrohungen, gegen die der EVG schützt, werden nicht als besonders schwerwiegend angesehen. Das unterstellte Angriffspotential geht nicht von gezielten Angriffen durch Experten aus, sondern unterstellt allenfalls ungeschulte „Angreifer“ mit frei verfügbaren Tools, denen die Handbücher, die mit dem EVG ausgeliefert werden, zur Verfügung stehen. Die Evaluierung soll daher zeigen, dass der EVG seine Sicherheitsfunktionen in der beschriebenen Weise bereitstellt, und dass diese Sicherheitsfunktionen korrekt arbeiten und gegen die beschriebenen Bedrohungen wirken.

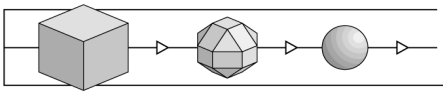
Diesen Anforderungen ist die Evaluierung gemäß EAL 1 der CC angemessen.

3.8.2.4 Erklärung der Maßnahmen zur Vertrauenswürdigkeit

Die in Abschnitt 5.2 gestellten Anforderungen an die Vertrauenswürdigkeit werden durch die in Abschnitt 6.2 niedergelegten Maßnahmen zur Vertrauenswürdigkeit mit folgender Begründung erfüllt:

Jede Anforderungen an die Vertrauenswürdigkeit wird durch (mindestens) eine Maßnahme zur Vertrauenswürdigkeit abgedeckt.

Anforderungen an die Vertrauenswürdigkeit	Maßnahmen zur Vertrauenswürdigkeit
ACM_CAP.1	ACM_CAP.1.1M, ACM_CAP.1.2M
ADO_IGS.1	ADO_IGS.1M
ADV_FSP.1	ADV_FSP.1M
ADV_RCR.1	ADV_RCR.1M
AGD_ADM.1	AGD_ADM.1M
AGD_USR.1	AGD_USR.1M
ATE_IND.1	ATE_IND.1M



Die Maßnahmen zur Vertrauenswürdigkeit wurden so gewählt, dass

- alle für die Evaluierung gemäß EAL1 geforderten Dokumente bereitgestellt werden,
- die bereitgestellten Dokumente alle geforderten und erwarteten Inhalte zur Verfügung stellen,
- die Eindeutigkeits- und Kennzeichnungsforderungen erfüllt werden und
- die notwendigen Unterstützungen für die Durchführung von unabhängigen Evaluatortests, einschließlich der Bereitstellung des EVGs und einer geeigneten Testumgebung, gegeben werden.

3.8.3 Erklärung der EVG-Übersichtsspezifikation

Zwischen den funktionalen Sicherheitsanforderungen und den Sicherheitsfunktionen des EVGs besteht beiderseitige Abdeckung. Im Detail gilt:

Sicherheits-anforderung	Sicherheitsfunktionen									
	SF-1	SF-2	SF-3	SF-4	SF-5	SF-6	SF-7	SF-8	SF-9	SF-10
FIA_UID.2.1	X	X				X	X	X		
FIA_UAU.2.1	X	X				X	X	X		
FPT_STM.1.1									X	
FAU_ARP.1.1				X	X					
FAU_GEN.1.1				X	X					
FAU_GEN.1.2				X	X				X	
FAU_SAR.1.1		X								
FAU_SAR.1.2				X	X					
FAU_SAR.2.1	X									
FAU_STG.1.1	X									
FAU_STG.1.2				X	X					
FTA_TSE.1.1			X							
FRU_RSA.1.1										X
FAU_SAA.1.1				X	X					
FAU_SAA.1.2				X	X					

Tabelle 5: Sicherheitsanforderungen an den EVG und Sicherheitsfunktionen des EVGs

Jede funktionale Sicherheitsanforderung des EVGs wird durch mindestens eine Sicherheitsfunktion realisiert. Darüber hinaus ist keine EVG-Sicherheitsfunktion implementiert, für die keine funktionale Sicherheitsanforderung bestünde.

FIA_UID.2.1

Die verlangte Identifikation vor jeder anderen Interaktion mit dem EVG wird von den Sicherheitsfunktionen SF-1, SF-2, SF-6, SF-7 und SF-8 umgesetzt, wobei SF-1 und SF-2 für die Administratoren angewendet werden, SF-6, SF-7 und SF-8 für die sonstigen Benutzer des EVGs.

FIA_UAU.2.1

Die verlangte Authentisierung vor jeder anderen Interaktion mit dem EVG wird von den Sicherheitsfunktionen SF-1, SF-2, SF-6, SF-7 und SF-8 umgesetzt, wobei SF-1 und SF-2 für die Administratoren angewendet werden, SF-6, SF-7 und SF-8 für die sonstigen Benutzer des EVGs.

FPT_STM.1.1

Die verlangten verlässlichen Zeitstempel werden von der SF-9 bereitgestellt.

FAU_ARP.1.1

Potentielle Sicherheitsverletzungen können im Rahmen von Management-Aktivitäten der Baugruppe (SNMP-Traps) oder von normalen Funktionsabläufen (Kundentraces) auftreten. SF-4 und SF-5 setzen die verlangte Erkennung und Protokollierung um.

FAU_GEN.1.1

Die Anforderungen gemäß FAU_GEN.1.1 werden ebenfalls von SF-4 und SF-5 umgesetzt, wobei das Einspielen einer neuen Konfiguration nur durch SF-5 erfolgt. Dies reicht aus, da die SNMP-Traps Bestandteil des KDS sind, d. h. SF-5 protokolliert auch das Einspielen einer neuen „SNMP-Konfiguration“.

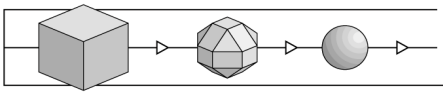
FAU_GEN.1.2

Diese Anforderungen werden durch SF-4 und SF-5 realisiert, wobei die erforderlichen Zeitstempel von SF-9 bereitgestellt werden.

FAU_SAR.1.1

Nur die am Assistant für Xpress@LAN authentisierten Administratoren können Protokollinformationen erhalten. Diese Forderung wird durch die SF-2 wie folgt umgesetzt:

SF-2 sorgt dafür, dass die Log-Informationen der Baugruppe nur von Administratoren heruntergeladen werden können.



FAU_SAR.1.2

SF-4 und SF-5 erzeugen die Log-Informationen als ASCII-Texte, der sich leicht interpretieren lässt.

FAU_SAR.2.1

Da SF-2 erst wirksam wird, nachdem SF-1 einen Administrator authentisiert hat, sind die Protokollinformationen der Baugruppe nur von Administratoren herunterladbar. Ein direktes Lesen der Log-Informationen von der Baugruppe ohne Benutzung des Assistant für Xpress@LAN wird nicht unterstützt (keine entsprechende Funktionalität vorhanden). Für die SNMP-Traps muss eine Konfiguration eingestellt werden, die die Traps nur an Administratoren sendet. Dies geschieht durch entsprechenden Eintrag im KDS.

FAU_STG.1.1

Die Log-Informationen auf der Baugruppe können nur durch Administratoren (Feststellung durch SF-1) gelöscht werden. Dies geschieht durch Freigabe des benutzten Speicherplatzes im Anschluss an das Herunterladen. Implizit erfolgt eine teilweise Löschung auf der Baugruppe immer dann, wenn der vorgesehene Speicher voll ist (Ringspeicher).

FAU_STG.1.2

Einmal durch SF-4 oder SF-5 geschriebene Informationen können auf der Baugruppe nicht modifiziert werden. Da die Speicher als Ringspeicher organisiert sind, können bei unachtsamer Administration höchstens Protokollinformationen mit neuen Protokollinformationen überschrieben werden.

FTA_TSE.1.1

Diese Anforderung wird durch die Filter SF-3a, SF-3b und SF-3c realisiert.

FRU_RSA.1.1

Die Quoten für die Anzahl der innerhalb einer spezifizierten Zeitspanne angenommener Pakete werden durch die Sicherheitsfunktion SF-10 realisiert.

FAU_SAA.1.1

Die Sicherheitsfunktionen SF-4 und SF-5 wenden zur Entscheidung, ob Ereignisse protokolliert werden, Regeln an, die durch entsprechende Einträge in KDS repräsentiert werden. Nähere Informationen dazu finden sich in [7], 63f, 66, 97f, 147f.

FAU_SAA.1.2

SF-4 und SF-5 setzen diese Forderung auf der Basis der Konfiguration im KDS um.

3.8.4 Erklärung der PP-Postulate

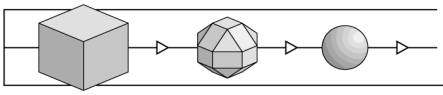
Dieser Abschnitt entfällt, da keine Postulate der Übereinstimmung mit irgend einem Protection Profile erhoben werden.

3.9 A N H A N G (zu den Sicherheitsvorgaben)

3.9.1 Abkürzungen

Bemerkung: Weitere Abkürzungen mit Erklärung finden sich in [6], S. 153f.

Abb.	Abbildung(en)
A_NNN	Annahme, durch „NNN“ näher qualifiziert
CC	Common Criteria
EAL	Evaluationsstufe (evaluation assurance level)
EVG	Evaluationsgegenstand
HW	Hardware
IT	Informationstechnik, -technologie
Kap.	Kapitel
PP	Protection Profile(s)
RFC	(Internet) Request for Comment
SNMP	Simple Network Management Protocol
SF	Sicherheitsfunktion
SFR	Security Functional Requirement(s)
SLIP	Serial Line Interconnection Protocol (V.24)
SOF	Mechanismenstärke (strength of function)
ST	Security Target (synonym gebraucht wie SV)
SV	Sicherheitsvorgaben
SW	Software
Sekt.	Sektion(en), Abschnitt(e)



Tab.	Tabelle(n)
TOE	Target of evaluation (hier: EVG)
TSF	TOE Security Function(s)

3.9.2 Glossar

Administrator	eine Person, die für die Aufrechterhaltung der Betriebsbereitschaft verantwortlich ist
Baugruppe	Kurzbezeichnung für die Baugruppen-Software und die jeweilige Hicom-Einsteckkarte (vgl. Abschnitt 2.2)
(End-)nutzer	eine Person, die Kontakt zu einem in Betrieb befindlichen EVG hat und dessen Dienstleistungen und Funktionen nutzt
Siemens-Nebenstellen-anlage	eine der folgenden Nebenstellenanlagen (jeweils ab Software-Version 2.2): Hicom 150 E OfficeCom, Hicom 150 E OfficePoint, Hicom 150 E OfficePro; abkürzend wird auch die Schreibweise „Hicom 150 E Office“ verwendet

3.9.3 Quellen

[1] "Common Criteria for Information Technology Security Evaluation (CC)", Part 1, Version 2.1, August 1999

[2] "Common Criteria for Information Technology Security Evaluation (CC)", Part 2, Version 2.1, August 1999

[3] "Common Criteria for Information Technology Security Evaluation (CC)", Annex to Part 2, Version 2.1, August 1999

[4] "Common Criteria for Information Technology Security Evaluation (CC)", Part 3, Version 2.1, August 1999

[5] „Guide for Production of PPs and STs“, Version 0.5, March 1998, ISO/IEC JTC 1/SC 27/WG 3, N422

[6] Hicom 150 E Office – Hicom Xpress@LAN Release 1.1 – Servicehandbuch, Siemens AG 2000, Bestellnummer A31003-K5020-S100-3-20

[7] Hicom 150 E Office – Administrationsanleitung für Hicom Xpress@LAN, Siemens AG 2000, Bestellnummer A31003-K5020-B811-2-19

[8] Sicherheitstechnische Ergänzung zur Administrationsanleitung für Hicom Xpress@LAN, Siemens AG, September 2000, Bestellnummer A31003-K5020-X100-1-20

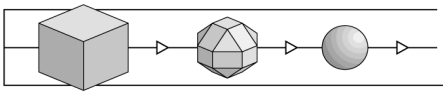
[9] Lloyd, B. and W. Simpson, "PPP Authentication Protocols", RFC 1334, October 1992

[10] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996

[11] Zorn, G. and Cobb, S., "Microsoft PPP CHAP Extensions", RFC 2433, October 1998

[12] Zorn, G., "Microsoft PPP CHAP Extensions, Version 2", RFC 2759, January 2000

[13] U.S. Department of Commerce / National Bureau of Standards: Data Encryption Standard, FIPS PUB 46, 1977 January 15



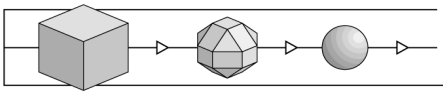
(Diese Seite ist beabsichtigterweise leer.)

4 Hinweise und Empfehlungen zum zertifizierten Objekt

29 Die Ausführungen in Kapitel 2 sind als Ergebnis der Evaluierung zu beachten.

30 Bei der Zertifizierung haben sich folgende weitergehenden Hinweise oder Empfehlungen für den Anwender ergeben (als Erläuterung zu Abschnitt 2.4, letzter Spiegelstrich).

Die Regeln für die Firewall-Funktionalität können richtungsabhängig definiert werden. Dadurch ist es prinzipiell möglich, in Richtung vom LAN zum WAN andere Filterregeln zu definieren als in Richtung vom WAN zum LAN. Von dieser Möglichkeit soll im praktischen Betrieb **nicht** Gebrauch gemacht werden.



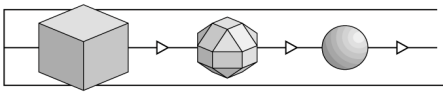
(Diese Seite ist beabsichtigterweise leer.)

5 Anhang

5.1 Glossar

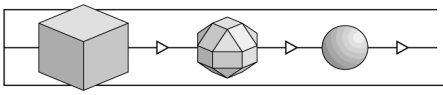
Das Glossar erläutert die in dieser Broschüre verwendeten Begriffe, erhebt allerdings keinerlei Anspruch auf Vollständigkeit oder Allgemeingültigkeit. Der Begriff *Sicherheit* meint hier stets Sicherheit im Kontext der Informationstechnik.

Akkreditierung	Verfahren zum Nachweis, daß eine Prüfstelle den Anforderungen der Norm DIN EN 45001 entspricht. Eine Akkreditierung wird durch eine *Akkreditierungsstelle* durchgeführt. Allgemein anerkannt sind Akkreditierungen von Akkreditierungsstellen, die im Deutschen Akkreditierungsrat (DAR) vertreten sind.
Anerkennung	Ausdruck und Bestätigung der Gleichwertigkeit (von Zertifikaten und Lizenzen).
Assoziiertes Labor	Ein per Vertrag mit debisZERT kooperierendes Entwicklungslabor, das optimierte Verfahren zur Vorbereitung von Evaluierungen einsetzt.
Auftraggeber	Eine natürliche oder juristische Person, die einen Auftrag (hier:) zur Zertifizierung oder Evaluierung erteilt; sie muß eine ausreichende Verfügungsberechtigung über das zu zertifizierende bzw. zu evaluierende Objekt besitzen.
Bestätigungsstelle	Stelle, die im Einklang mit SigG und SigV Sicherheitsbestätigungen für technische Komponenten und für die Umsetzung von Sicherheitskonzepten bei Trust Centern (Zertifizierungsstellen nach SigG) herausgibt.
Bestätigungsverfahren	Verfahren mit dem Ziel einer Sicherheitsbestätigung
Common Criteria	Sicherheitskriterien, die aus dem amerikanischen Orange Book / den Federal Criteria, den europäischen ITSEC und den kanadischen CTCPEC hervorgegangen sind und ein weltweit akzeptierter Sicherheitsstandard werden sollen.
debisZERT	Name des Zertifizierungsschemas von debis IT Security Services.
Dienstleistung	Hier: Eine durch ein Unternehmen angebotene, durch (Unternehmens-)Prozesse erbrachte und durch Nutzer in Anspruch nehmbare Leistung.
Dienstleistungsbereich	Bezeichnung für einen bestimmten Typ von Verfahren innerhalb von debisZERT.
DIN EN 45000	Normen-Reihe, die einschlägige Standards insbesondere für Prüf- und Zertifizierungsstellen enthält.



Einzelbericht	Bericht einer Prüfstelle zu einzelnen Prüfaspekten bei einer Evaluierung
Erst-Zertifizierung	Erstmalige Zertifizierung eines IT-Produkts, IT-Systems oder einer IT-Dienstleistung.
Evaluationsstufen	s. Sicherheitsstufen.
Evaluator	Prüfer / in in einer Prüfstelle.
Evaluierung	Prüfung eines IT-Produktes, IT-Systems oder einer IT-Dienstleistung auf der Basis von IT-Sicherheitskriterien oder einer IT-Sicherheitsnorm.
Evaluierungsbericht	Einzelbericht (s.d.) oder Abschlußbericht einer Prüfstelle über Ablauf und Ergebnis einer Evaluierung. (Name „ETR“ im ITSEC-Kontext)
Hersteller-Laboratorium	Bei dem Hersteller eines Produkts / Systems oder bei dem Anbieter von Dienstleistungen angesiedelte Organisationseinheit, die Evaluierungen durchführt.
Integrität	Klassisches Sicherheitsziel: Daten sollen nur von Befugten geändert werden können.
IT-Dienstleistung	Dienstleistung, die sich bei ihrer Erbringung auf IT-Produkte und IT-Systeme abstützt.
IT-Komponente	Sicherheitskriterien: funktional abgrenzbarer Teil eines IT-Produkts / eines IT-Systems.
IT-Produkt	Software und / oder Hardware, die bei einem Anbieter (Hersteller, Vertreiber) erworben werden kann.
ITSEC	Information Technology Security Evaluation Criteria (ITSEC) [Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)]: Europäischer de facto Standard für die Evaluierung von IT-Produkten und IT-Systemen.
ITSEM	Information Technology Security Evaluation Manual (ITSEM) [Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM)]: Handbuch zu den ITSEC, das vor allem die Durchführung von Evaluierungen beschreibt.
(IT-) Sicherheits-management	Ein Unternehmensprozeß, dessen Ziel die Einrichtung und Aufrechterhaltung der (IT-)Sicherheit in einem Unternehmen ist.
IT-System	Eine in sich funktionsfähige Kombination von IT-Produkten. (ITSEC:) Eine reale Installation von IT-Produkten mit einer bekannten Einsatzumgebung.

Komponente nach SigG	Eine logische Funktionseinheit in IT-Systemen, die in SigG / SigV definierte Aufgaben erfüllt (Anzeigekomponente, Komponente zur Schlüsselerzeugung, etc.)
Lizenz (persönliche)	Bestätigung einer persönlichen Qualifikation (hier im Kontext von debisZERT, s. zertifizierter Ingenieur)
Lizenzierter Ingenieur	Eine Person, die im Zusammenhang mit Evaluierungen Qualifizierungsverfahren bei debisZERT durchlaufen hat (s. Lizenz).
Lizenzierung	Verfahren der Überprüfung von Organisation und Qualifikation einer Prüfstelle im Hinblick auf den möglichen Abschluß einer Lizenzvereinbarung.
Lizenzvereinbarung	Vereinbarung zwischen einer Prüfstelle und einer Zertifizierungsstelle – den Ablauf und die Verantwortlichkeiten bei einer Evaluierung und Zertifizierung betreffend.
Meilensteinplan	Projekt- / Terminplan für die Durchführung einer Evaluierung und Zertifizierung
Problembericht	Bericht einer Prüfstelle an die Zertifizierungsstelle über besondere Probleme bei einer Evaluierung, z.B. die Interpretation der Sicherheitskriterien betreffend.
Produkt-Zertifizierung	Zertifizierung eines IT-Produktes.
Prozeß (Unternehmens~)	Abfolge vernetzter Tätigkeiten (Prozeßelemente) in einer gegebenen Prozeßumgebung – mit dem Gesamtziel, eine bestimmte Dienstleistung zu erbringen.
Prüfbegleiter	Mitarbeiter / in der Zertifizierungsstelle, führt die Prüfbegleitung durch.
Prüfbegleitung	Verfahren der Zertifizierungsstelle, um die Ordnungsmäßigkeit (Kriterienkonformität, einheitliche Vorgehensweise und Bewertungen, etc.) einer Evaluierung zu überprüfen.
Prüfbericht	Einzelbericht oder Evaluierungsbericht
Prüfstelle	Stelle, die Evaluierungen durchführt.
Regulierungsbehörde	die nach §66 Telekommunikationsgesetz (TKG) zuständige Regulierungsbehörde für Telekommunikation und Post
Re-Zertifizierung	Nach Änderungen am zertifizierten Objekt notwendig werdende Zertifizierung der geänderten Version; kann auch bei Wechsel von Werkzeugen, Produktions- und Auslieferungsprozessen, Sicherheitskriterien erforderlich werden.
Sicherheitsbestätigung	In debisZERT eine juristisch verbindliche Bestätigung von Sicherheitseigenschaften; z.B. eine Bescheinigung, die die Erfüllung der Anforderungen des Signaturgesetzes bestätigt.

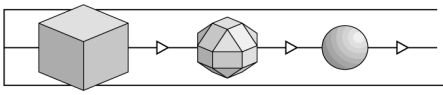


Sicherheitsfunktion	Funktionen eines IT-Produktes oder IT-Systems zur Abwehr bestimmter Bedrohungen.
Sicherheitskriterien	Dokument, das technische Anforderungen an Produkte, Systeme und / oder Dienstleistungen enthalten kann, zumindest aber die Evaluierung solcher Anforderungen beschreibt.
Sicherheitsnorm	Anforderungen an Produkte, Systeme oder Dienstleistungen die Sicherheit betreffend.
Sicherheitsstandard	Zusammenfassender Begriff für Sicherheitskriterien und Sicherheitsnormen.
Sicherheitsstufen	In Sicherheitskriterien definierte Stufen, die aufgrund unterschiedlicher Anforderungen an das zu zertifizierende Objekt und an die Tiefe der Prüfung eine unterschiedlich hohe Sicherheit ausdrücken.
Sicherheitszertifikat	s. Zertifikat
Signaturgesetz – SigG	§3 des Informations- und Kommunikationsdienstegesetzes (IuKDG)
Signaturverordnung - SigV	Amtliche Ausführungsbestimmungen zum Signaturgesetz.
System-Akkreditierung	Freigabe eines IT-Systems oder einer IT-Dienstleistung zur Nutzung (hier unter dem Blickwinkel ausreichender Sicherheit).
System-Zertifizierung	Zertifizierung eines IT-Systems (hier unter dem Blickwinkel ausreichender Sicherheit).
Trust Center	Stelle, die die Zugehörigkeit von Signaturschlüsseln zu einer Person durch ein (elektronisches) Zertifikat bestätigt - im Signaturgesetz als „Zertifizierungsstelle“ bezeichnet.
Unternehmensprozeß	s. Prozeß
Verfahrenskennung	Code-Bezeichnung für ein Bestätigungsverfahren
Verfügbarkeit	Klassisches Sicherheitsziel: Daten sollen Befugten stets zur Verfügung stehen, d.h. nicht von Unbefugten vorenthalten werden können oder aufgrund technischer Defekte nicht verfügbar sein.
Verfügungsberechtigung	hier: Berechtigung, alle mit einer Evaluierung und Zertifizierung verbundenen Inspektionen an einem Produkt, System oder einer Dienstleistung zulassen zu können.
Vertraulichkeit	Klassisches Sicherheitsziel: Daten sollen nur durch Befugte zur Kenntnis genommen werden können.

Vor-Zertifizierung	Bestätigung der Ergebnisse einer Voruntersuchung einer produkt- bzw. prozeßspezifischen Sicherheitsnorm oder eines sicherheitsrelevanten Werkzeugs (im Hinblick auf spätere Zertifizierungen).
Zertifikat	Zusammenfassende (Kurz-)Darstellung eines Zertifizierungsergebnisses; wird durch die Zertifizierungsstelle ausgestellt.
Zertifizierer	Mitarbeiter / in einer Zertifizierungsstelle, die eine Zertifizierung durchführt.
Zertifizierung	Unabhängige Bestätigung der Ordnungsmäßigkeit einer Evaluierung. Auch Bezeichnung für das Gesamtverfahren bestehend aus Evaluierung, Prüfbegleitung und Ausstellung von Zertifikaten und Zertifizierungsreports.
Zertifizierungskennung	Code-Bezeichnung für ein Zertifizierungsverfahren.
Zertifizierungsreport	Bericht über Gegenstand, Ablauf und Ergebnis eines Zertifizierungsverfahrens; wird durch die Zertifizierungsstelle ausgestellt.
Zertifizierungsschema	Zusammenfassung aller Grundsätze, Regeln und Verfahren einer Zertifizierungsstelle.
Zertifizierungsstelle	Stelle, die Zertifizierungen durchführt. (s. auch *Trust Center* für eine zweite Bedeutung.)
ZKA-Kriterien	Sicherheitskriterien des Zentralen Kreditausschusses.

5.2 Referenzen

/ A00 /	Lizenzierungsschema, debisZERT, Version 1.6, 31.03.2000, http: / / www.debiszert.de /
/ ALG /	Anhang zu „Bekanntmachung zur digitalen Signatur nach Signaturgesetz und Signaturverordnung vom 09.02.98 im Bundesanzeiger Nr. 31 v. 14.02.98“ , (http: / / www.regtp.de / Fachinfo / Digitalsign / start.htm)
/ BSIG /	Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz - BSIG), BGBl. I. vom 17. Dezember 1990, Seite 2834 ff.
/ CC /	Common Criteria for Information Technology Security Evaluation, Version 2.1, Part 1 (Introduction and general model), Part 2 (Security functional requirements), Part 2 : Annexes, Part 3 (Security assurance requirements) , August 1999, http: / / csrc.nist.gov / cc / info / infolist.htm
/ CEM /	Common Methodology for Information Technology Security Evaluation, Part 1 (Introduction and general model), version 0.6, January 1997, Part 2 (Evaluation Methodology), version 1.0, August 1999, http: / / csrc.nist.gov / cc / info / infolist.htm



/EBA/ Kriterien für die sicherheitstechnische Bewertung und Konstruktion von CIR-Netzkomponenten, Eisenbahn-Bundesamt, Version 1.0 vom 8.2.94

/ITSEC/ Information Technology Security Evaluation Criteria (ITSEC), Version 1.2 (1991), ISBN 92-826-3004-8

(deutsche Übersetzung:) Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), Version 1.2 (1991), Bundesanzeiger-Verlag Köln, ISBN 92-826-3003-X

(französische Übersetzung:) Critères d'Évaluation de la Sécurité des Systèmes Informatiques (ITSEC), Version 1.2 (1991), ISBN 92-826-3005-6

/ITSEM/ Information Technology Security Evaluation Manual (ITSEM), Version 1.0 (1993), ISBN 92-826-7087-2

(deutsche Übersetzung:) Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM), Version 1.0 (1993), Bundesanzeiger Verlag Köln, ISBN 92-826-7078-2

/IuKDG/ Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG), BGBl. I. vom 28. Juli 1997, Seite 1870 ff.

/JIL/ Joint Interpretation Library, Version 2.0, Nov. 1998

/Mkat12/ Maßnahmenkatalog nach §12 Abs. 2, RegTP, http://www.RegTp.de/Fachinfo/DigitalSign/start.htm

/Mkat16/ Maßnahmenkatalog nach §16 Abs. 6, RegTP, http://www.RegTp.de/Fachinfo/DigitalSign/start.htm

/SigG/ Artikel 3 von /IuKDG/

/SIGV/ Verordnung zur digitalen Signatur (Signaturverordnung - SigV), BGBl. I. vom 27.10.1997, Seite 2498 ff.

/TKG/ Telekommunikationsgesetz (TKG), BGBl. I. vom 25.7.1996, Seite 1120

/V01/ Zertifikate gemäß ITSEC/CC, Dienstleistungsbereich 1 von debisZERT, Version 1.5, 30.06.1999, http://www.debiszert.de/

/V02/ Sicherheitsbestätigungen für Komponenten gemäß dem Signaturgesetz, Dienstleistungsbereich 2 von debisZERT, Version 1.5, 30.06.1999, http://www.debiszert.de/

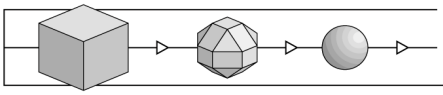
/V03/ Sicherheitsbestätigungen für Zertifizierungsstellen gemäß dem Signaturgesetz, Dienstleistungsbereich 3 von debisZERT, Version 1.0, 29.10.1999, http://www.debiszert.de/

/V04/ Zertifikate mit Anerkennung durch das BSI, Dienstleistungsbereich 4 von debisZERT, Version 1.5, 30.06.1999, http://www.debiszert.de/

/Z01/ Zertifizierungsschema, debisZERT, Version 1.5, 30.06.1999, http://www.debiszert.de/

5.3 Abkürzungen

AA	Arbeitsanweisungen
AIS	Anforderung einer Interpretation von Sicherheitskriterien
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Errichtungsgesetz
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CTCPEC	Canadian Trusted Computer Products Evaluation Criteria
DAR	Deutscher Akkreditierungsrat
DBAG	Deutsche Bahn AG
debisZERT	Zertifizierungsschema der debis IT Security Services
DATech	Deutsche Akkreditierungsstelle Technik e.V.
DLB	Dienstleistungsbereich
EBA	Eisenbahn-Bundesamt
ETR	Evaluation Technical Report (Evaluierungsbericht)
EVG	Evaluationsgegenstand
IT	Informationstechnik
ITSEC	Information Technology Security Evaluation Criteria (ITSEC)
ITSEF	IT Security Evaluation Facility (s. CLEF)
ITSEM	Information Technology Security Evaluation Manual (ITSEM)
IuKDG	Informations- und Kommunikationsdienstegesetz
RegTP	Regulierungsbehörde für Telekommunikation und Post
SigG	Signaturgesetz
SigV	Signaturverordnung
TKG	Telekommunikationsgesetz
ZKA	Zentraler Kreditausschuß



(Diese Seite ist beabsichtigterweise leer.)

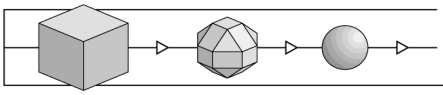
6 Re-Zertifizierungen

31 Bei Änderungen an dem zertifizierten Objekt kann nach Maßgabe der Verfahrensregeln von debisZERT eine Re-Zertifizierung erfolgen. Die hier in zeitlicher Reihenfolge erscheinenden Anhänge beschreiben die Art der Änderungen, die neue Produktversion und den Zertifizierungsstatus.

32 Bei neuen Erkenntnissen über die Sicherheit des zertifizierten Objektes kann ein technischer Anhang zum Zertifizierungsreport herausgegeben werden.

33 Re-Zertifizierungen und neue technische Anhänge werden in der Druckschrift /Z02/ und über WWW angekündigt.

34 Die Anhänge sind forlaufend numeriert.



Ende der Erstausgabe des Zertifizierungsreports.