T · · Systems · · ·

Zertifizierungsreport

T-Systems-DBZ-ITSEC-01111-2004

NCA-Schlüsselgenerator, Version 1.00

Kraftfahrt-Bundesamt

Zertifizierungsreport T-Systems-DBZ-ITSEC-01111-2004

Für weitere Auskünfte ist die Zertifizierungsstelle wie folgt erreichbar:

✉ Zertifizierungsstelle der T-Systems
c/o T-Systems GEI GmbH
BU ITC Security
Rabinstr.8, 53111 Bonn

☎ 0228/9841-0, Fax: 0228/9841-60

💻 www.t-systems-zert.com

Die Zertifizierungsstelle der T-Systems

bestätigt hiermit, dass

das System

NCA-Schlüsselgenerator, Version 1.00

des

Kraftfahrt-Bundesamtes
Fördestraße 16, 24944 Flensburg-Mürwik

nach den Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC) und dem Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM) gegen spezifische Sicherheitsvorgaben evaluiert wurde und folgendes Prüfergebnis erzielte:

Sicherheitsfunktionen:	**Schlüsselgenerierung, Schlüsselsicherung auf Backup- und Release-Cards**
Vertrauenswürdigkeitsstufe:	**E3**
Mindeststärke der Sicherheitsmechanismen:	**hoch**

Dieses Zertifikat gilt nur in Verbindung mit dem vollständigen Zertifizierungsreport zur unten angegebenen Registriernummer und für die darin aufgeführten Konfigurationen und Einsatzumgebungen. Die Empfehlungen und Hinweise im Zertifizierungsreport sind zu beachten. Die Sicherheitsvorgaben, die Basis der Evaluierung waren, sind im Zertifizierungsreport aufgeführt. Kopien des Zertifikats und des Zertifizierungsreports sind beim Auftraggeber und – mit Zustimmung des Auftraggebers - bei der Zertifizierungsstelle erhältlich.

Registrierungsnummer: Bonn, den 07.06.2004

T-Systems-
DBZ-ITSEC-01111-2004

Dr. Heinrich Kersten
Leiter der Zertifizierungstelle

Zertifizierungsstelle der T-Systems
c/o T-Systems GEI GmbH, BU ITC Security, Rabinstr.8, 53111 Bonn
☎ 0228/9841-0, Fax: 0228/9841-60 Internet: www.t-systems-zert.com
Akkreditiert nach DIN EN 45011 durch DATech e.V.

DAT-ZE-015/98-01

(Diese Seite ist beabsichtigterweise leer.)

Inhaltsverzeichnis

Titelblatt 1
Copyright 2
Zertifikat 3
Inhaltsverzeichnis 5
Abkürzungen 7
Referenzen 8
Glossar 9
Erläuterungen zu den Sicherheitskriterien 13

Antragsteller und Evaluationsgegenstand 17
Maßgebende Prüfgrundlagen 17
Evaluierung 17
Zertifizierung 18
Zusammenfassung der Ergebnisse 20
Anwendung der Ergebnisse 21

Anhang: Sicherheitsvorgaben zu „NCA-Schlüsselgenerator, Version 1.00“

(Diese Seite ist beabsichtigterweise leer.)

Abkürzungen

AIS	Anwendungshinweise und Interpretationen zum Schema (Verfahren des BSI)
BGBl	Bundesgesetzblatt
BS	British Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
DAR	Deutscher Akkreditierungsrat
DATech	Deutsche Akkreditierungsstelle Technik e.V.
DIN	Deutsches Institut für Normung e.V.
ETR	Evaluation Technical Report (Evaluierungsbericht)
EVG	Evaluationsgegenstand
ISO	International Organization for Standardization
IT	Informationstechnik
ITSEC	Information Technology Security Evaluation Criteria (ITSEC)
ITSEF	IT Security Evaluation Facility: Prüflabor
ITSEM	Information Technology Security Evaluation Manual (ITSEM)
JIL	Joint Interpretation Library
RegTP	Regulierungsbehörde für Telekommunikation und Post
SigG	(deutsches) Signaturgesetz
SigV	(deutsche) Signaturverordnung

Referenzen

/AISx/ Anwendungshinweise und Interpretationen zum Schema, Bundesamt für Sicherheit in der Informationstechnik, gültige Fassungen

/ALG/ Geeignete Kryptoalgorithmen, veröffentlicht im Bundesanzeiger durch die Regulierungsbehörde für Telekommunikation und Post, gültige Fassung

/BS7799/ BS7799-1:2000 Information technology - Code of practice for information security management (ISO/IEC 17799:2000)
BS7799-2:2002 Information security management systems - Specification with guidance for use

/CC/ Common Criteria: Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (ISO 15408), August 1999
Teil1: Einführung und allgemeines Modell
Teil2: Funktionale Sicherheitsanforderungen
Teil3: Anforderungen an die Vertrauenswürdigkeit

/CEM/ Common Methodology for Information Technology Security Evaluation,
Part1: Introduction and general model, Version 0.6, January 1997
Part2: Evaluation Methodology, Version 1.0, August 1999

/EU-DIR/ Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13.Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen

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

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

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

/SiGAK/ Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten: Arbeitsgrundlage für Entwickler/Hersteller und Prüf-/Bestätigungsstellen, Regulierungsbehörde für Telekommunikation und Post, Version 1.1, Stand: 15.12.2003

/SigG/ Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz – SigG) vom 16.05.2001 (BGBl. I, S. 876 ff.)

/SigV/ Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I., S. 3074 ff.)

Glossar

Das Glossar erläutert Begriffe aus dem Zertifizierungsschema der T-Systems, erhebt allerdings keinerlei Anspruch auf Vollständigkeit oder Allgemeingültigkeit. Der Begriff *Sicherheit* meint hier stets Sicherheit im Kontext der Informationstechnik.

Akkreditierung	Von einem Akkreditierungsgeber durchgeführtes Verfahren zum Nachweis, dass eine Prüfstelle [bzw. Zertifizierungsstelle] den Anforderungen der maßgebenden Norm ISO 17025 [bzw. DIN EN 45011] entspricht.
Audit	Verfahren des Sammelns objektiver Nachweise dafür, dass ein Prozess so abläuft wie vorgegeben.
Bestätigungsstelle	Stelle, die mit Anerkennung durch die Regulierungsbehörde für Telekommunikation und Post und im Einklang mit SigG und SigV Sicherheitsbestätigungen für technische Komponenten und für die Umsetzung von Sicherheitskonzepten bei Trust Centern (Zertifizierungsdiensteanbietern 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 sind.
Dienstleistung	Hier: Eine von einem Unternehmen angebotene, durch Geschäftsprozesse erbrachte und durch Nutzer in Anspruch nehmbare Leistung.
Evaluation Technical Report	Schlussbericht einer Prüfstelle über den Ablauf und die Ergebnisse einer Evaluation.
Evaluationsgegenstand	Ein IT-Produkt oder IT-System, das in Verbindung mit seinen (Administrations- und Benutzer-) Handbüchern Gegenstand einer Evaluierung ist.
Evaluationsstufe	Stufe der Vertrauenswürdigkeit, die aus einer Evaluierung gewonnen wird; Element eines Bewertungssystems in Sicherheitskriterien ITSEC / CC; Höhe des Vertrauens, dass der EVG seine Sicherheitsvorgaben erfüllt.
Evaluator	Prüfer/in in einer Prüfstelle.

Evaluierung	Prüfung eines IT-Produktes, IT-Systems oder einer IT-Dienstleistung auf der Basis von IT-Sicherheitskriterien.
Integrität	Klassisches Sicherheitsziel: Daten sollen nur von Befugten geändert werden können.
IT-Dienstleistung	Dienstleistung, die sich bei ihrer Erbringung auf IT-Systeme abstützt.
IT-Produkt	Software und / oder Hardware, die bei einem Anbieter (Hersteller, Vertreiber) erworben werden kann.
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.
Lizenzvereinbarung	Vereinbarung zwischen einer Prüfstelle und einer Zertifizierungsstelle - den Ablauf und die Verantwortlichkeiten bei einer Prüfung / 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 von IT-Produkten.
Prozess	Abfolge vernetzter Tätigkeiten (Prozesselemente) in einer gegebenen Prozessumgebung – mit dem Gesamtziel, eine bestimmte Dienstleistung zu erbringen.
Prüfbegleitung	Verfahren der Zertifizierungsstelle, um die Ordnungsmäßigkeit (Kriterienkonformität, einheitliche Vorgehensweise und Bewertungen, etc.) einer Evaluierung zu überprüfen.
Prüfstelle	Stelle, die Evaluierungen durchführt (ITSEF).
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.

Security for Business	Sicherheitsinitiative, die Service-Bausteine (Basissicherheit, Standardsicherheit, Professionelle Sicherheit) in puncto IT-Sicherheit für Unternehmen anbietet. Die Bausteine beinhalten Beratung, Analysen, Penetrationstests, Audits sowie nach erfolgreicher Abnahme Verfahren der Registrierung, Siegelvergabe und Zertifizierung. Details sind den Web-Seiten der Initiative zu entnehmen. (www.s4b.org)
Sicherheitsbestätigung	SigG: Eine Bescheinigung, die die Erfüllung von Anforderungen des Signaturgesetzes bestätigt.
Sicherheitsfunktion	Funktionen zur Abwehr bestimmter Bedrohungen.
Sicherheitskriterien	Dokument mit Sicherheitsanforderungen an Produkte, Systeme und / oder Dienstleistungen und / oder deren Evaluierung.
Sicherheitsvorgaben	Dokument, das einen Satz von Sicherheitsanforderungen and Spezifikationen enthält, die als Basis einer Evaluierung eines speziellen EVG dienen.
Sicherheitszertifikat	s. Zertifikat
System-Zertifizierung	Zertifizierung von installierten IT-Systemen.
Trust Center	s. Zertifizierungsdiensteanbieter
Unternehmensprozess	s. Prozess
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.
Vertraulichkeit	Klassisches Sicherheitsziel: Daten sollen nur durch Befugte zur Kenntnis genommen werden können.
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.
Zertifizierungsdiensteanbieter	Stelle, die die Zugehörigkeit von Signaturschlüsseln zu einer Person durch ein (elektronisches) Zertifikat bestätigt - im Signaturgesetz als „Zertifizierungsdiensteanbieter“ bezeichnet.

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.

Erläuterungen zu den Sicherheitskriterien

Dieses Kapitel gibt einen Überblick über die angewendeten Sicherheitskriterien und deren Bewertungsmaßstäbe. Textpassagen innerhalb „...“ stellen Zitate aus den ITSEC bzw. den ITSEM dar.

- Grundbegriffe

Sicherheit ist nach dem Verständnis der ITSEC dann gegeben, wenn ausreichendes Vertrauen darin besteht, dass der Evaluationsgegenstand (EVG) seine *Sicherheitsziele* erfüllt.

Sicherheitsziele setzen sich in der Regel aus Forderungen nach Vertraulichkeit, Verfügbarkeit und / oder Integrität von bestimmten Datenobjekten zusammen. Solche Sicherheitsziele werden durch den Auftraggeber der Evaluierung festgelegt. Normalerweise ist dies bei einem IT-Produkt der Entwickler oder Vertreiber, bei einem IT-System der Betreiber.

Den festgelegten Sicherheitszielen stehen prinzipielle *Bedrohungen* gegenüber, nämlich der Verlust der Vertraulichkeit, der Verlust der Verfügbarkeit, der Verlust der Integrität bestimmter Datenobjekte.

Aus solchen prinzipiellen Bedrohungen werden *Angriffe*, wenn Subjekte unerlaubt Datenobjekte mitlesen oder abhören, Dritten vorenthalten oder unbefugt ändern.

Sicherheitsfunktionen des EVG sollen solche *Angriffe* abwehren.

Es stellen sich dabei zwei Grundfragen: Funktionieren die Sicherheitsfunktionen korrekt? Sind die Sicherheitsfunktionen wirksam?

Vertrauen in die Erfüllung der Sicherheitsziele kann man dann haben, wenn *Korrektheit* und *Wirksamkeit* geprüft (*evaluiert*) worden sind.

- Evaluationsstufen

Eine Evaluierung kann nur mit begrenztem Aufwand und in begrenzter Zeit durchgeführt werden. Die mögliche Tiefe einer Evaluierung ist also stets begrenzt. Das Angemessenheitsprinzip verbietet es andererseits, bei geringem Sicherheitsbedarf eine extrem aufwändige Prüfung durchzuführen; ebenso unangemessen wäre es, bei höchstem Sicherheitsbedarf nur „oberflächlich“ zu prüfen.

Es ist deshalb sinnvoll, unterschiedliche Prüftiefen (und damit Prüfaufwände) festzulegen: In den ITSEC werden 6 Evaluationsstufen zur Prüfung von Korrektheit und Wirksamkeit definiert. E1 bezeichnet die niedrigste, E6 die höchste Stufe.

Die Vertrauenswürdigkeit eines EVG kann also in diesen Stufen „gemessen“ werden.

Die folgenden Auszüge aus den ITSEC lassen erkennen, welche Prüfaspekte im Rahmen einer Evaluierung behandelt werden und welche Prüftiefe welcher E-Stufe entspricht.

E1 „Auf dieser Stufe müssen für den EVG die Sicherheitsvorgaben und eine informelle Beschreibung des Architekturentwurfs vorliegen. Durch funktionale Tests muss nachgewiesen werden, dass der EVG die Anforderungen der Sicherheitsvorgaben erfüllt.“

E2 „Zusätzlich zu den Anforderungen für die Stufe E1 muß hier eine informelle Beschreibung des Feinentwurfs vorliegen. Die Aussagekraft der funktionalen Tests muß bewertet werden. Ein Konfigurationskontrollsystem und ein genehmigtes Distributionsverfahren müssen vorhanden sein.“

E3 „Zusätzlich zu den Anforderungen für die Stufe E2 müssen der Quellcode bzw. die Hardware-Konstruktionszeichnungen, die den Sicherheitsmechanismen entsprechen, bewertet werden. Die Aussagekraft der Tests dieser Mechanismen muß bewertet werden.“

E4 „Zusätzlich zu den Anforderungen für die Stufe E3 muß ein formales Sicherheitsmodell Teil der Sicherheitsvorgaben sein. Die sicherheitsspezifischen Funktionen, der Architekturentwurf und der Feinentwurf müssen in semiformaler Notation vorliegen.“

E5 „Zusätzlich zu den Anforderungen für die Stufe E4 muß ein enger Zusammenhang zwischen dem Feinentwurf und dem Quellcode bzw. den Hardware-Konstruktionszeichnungen bestehen.“

E6 „Zusätzlich zu den Anforderungen für die Stufe E5 müssen die sicherheitsspezifischen Funktionen und der Architekturentwurf in einer formalen Notation vorliegen, die konsistent mit dem zugrundeliegenden formalen Sicherheitsmodell ist.“

In allen E-Stufen müssen darüber hinaus Wirksamkeitsaspekte nach folgendem Schema untersucht werden:

„Die Bewertung der Wirksamkeit erfordert die Betrachtung der folgenden Aspekte des EVG:

a) die Eignung der sicherheitsspezifischen Funktionen des EVG, den in den Sicherheitsvorgaben aufgezählten Bedrohungen zu widerstehen;

b) die Fähigkeit der sicherheitsspezifischen Funktionen und Mechanismen des EVG, in einer Weise zusammenzuwirken, daß sie sich gegenseitig unterstützen und ein integriertes, wirksames Ganzes bilden;

c) die Fähigkeit der Sicherheitsmechanismen des EVG, einem direkten Angriff zu widerstehen;

d) ob bekannte Sicherheitsschwachstellen in der Konstruktion des EVG in der Praxis die Sicherheit des EVG kompromittieren können;

e) daß der EVG nicht in einer Weise konfiguriert werden kann, die unsicher ist, aber von der ein Systemverwalter oder ein Endnutzer vernünftigerweise glauben könnte, daß sie sicher ist;

f) ob bekannte Sicherheitsschwachstellen beim Betrieb des EVG in der Praxis die Sicherheit des EVG kompromittieren können."

- Sicherheitsfunktionen und Sicherheitsmechanismen

Sicherheitsfunktionen in einem EVG dienen der Abwehr von Bedrohungen.

Solche Sicherheitsfunktionen können in einer typischen Kombination („Funktionalitätsklasse") vorkommen. Beispiel: Die Funktionalitätsklasse F-C2 setzt sich aus den Funktionen *Identifikation und Authentisierung*, *Zugriffskontrolle*, *Beweissicherung*, *Protokollauswertung* und *Wiederaufbereitung* zusammen. Diese Klasse ist bei vielen kommerziellen Betriebssystemen gegeben.

Jede Sicherheitsfunktion kann auf unterschiedlichste Weise realisiert werden. Beispiel: Die Funktion *Identifikation und Authentisierung* kann unter anderem durch ein Paßwort-Verfahren, durch Verwendung von Chipkarten mit Challenge-Response Verfahren oder durch biometrische Verfahren realisiert sein. Jede Realisierung dieser Art heißt *(Sicherheits-)Mechanismus* der Sicherheitsfunktion *Identifikation und Authentisierung*. Für andere Sicherheitsfunktionen gilt sinngemäß das gleiche.

Die Widerstandskraft eines Sicherheitsmechanismus gegenüber direkten Angriffen wird als *Stärke* des Mechanismus bezeichnet.

In den ITSEM werden zwei Arten von Mechanismen unterschieden: Typ B und Typ A.

Typ B „Ein Mechanismus vom Typ B ist ein Sicherheitsmechanismus, der bei perfekter Konzipierung und Implementierung keine Schwächen aufweist. Ein Mechanismus vom Typ B kann als nicht durch einen direkten Angriff überwindbar betrachtet werden, gleichgültig, wie groß der Aufwand an Ressourcen, Fachkenntnissen und entsprechenden Gelegenheiten ist. ...

Mechanismen vom Typ B können jedoch durch indirekte Angriffe überwunden werden, mit denen sich andere Wirksamkeitsanalysen befassen.“

Typ A „Ein Mechanismus vom Typ A ist ein Sicherheitsmechanismus mit einer potentiellen Schwachstelle in seinem Algorithmus, seinen Prinzipien oder seinen Eigenschaften, aufgrund derer er durch Einsatz ausreichender Ressourcen, Fachkenntnisse und entsprechender Gelegenheiten mit einem direkten Angriff überwunden werden kann. ... Mechanismen vom Typ A bedienen sich häufig eines ‚Geheimnisses‘ wie etwa eines Passwortes oder eines kryptographischen Schlüssels.“

„Alle Mechanismen vom Typ A ... haben eine Stärke, die dem Aufwand an Ressourcen, Fachkenntnissen und Gelegenheiten, zur Gefährdung der Sicherheit durch einen direkten Angriff auf den Mechanismus entspricht.“

Wie wird bei Mechanismen vom Typ A die Stärke definiert?

„Alle kritischen Sicherheitsmechanismen (d.h. diejenigen, deren Versagen eine Sicherheitslücke hervorrufen würde), werden hinsichtlich ihrer Fähigkeit bewertet, einem direkten Angriff zu widerstehen. Die Mindeststärke jedes kritischen Mechanismus wird entweder als niedrig, mittel oder hoch bewertet.“

niedrig: „Damit die Mindeststärke eines kritischen Mechanismus als niedrig eingestuft werden kann, muß erkennbar sein, daß er Schutz gegen zufälliges unbeabsichtigtes Eindringen bietet, während er durch sachkundige Angreifer überwunden werden kann.“

mittel: „Damit die Mindeststärke eines kritischen Mechanismus als mittel eingestuft werden kann, muß erkennbar sein, daß er Schutz gegen Angreifer mit beschränkten Gelegenheiten oder Betriebsmitteln bietet.“

hoch: „Damit die Mindeststärke eines kritischen Mechanismus als hoch eingestuft werden kann, muß erkennbar sein, daß er nur von Angreifern überwunden werden kann, die über sehr gute Fachkenntnisse, Gelegenheiten und Betriebsmittel verfügen, wobei ein solcher erfolgreicher Angriff als normalerweise nicht durchführbar beurteilt wird.“

1 Antragsteller und Evaluationsgegenstand

1 Antragsteller der Zertifizierung war das Kraftfahrt-Bundesamt, Fördestraße 16, 24944 Flensburg-Mürwik.

2 Ziel der Antragstellung war das Gebiet „Zertifikate nach ITSEC/CC“.

3 Evaluationsgegenstand (EVG) war das System „NCA-Schlüsselgenerator für das Trustcenter des Kraftfahrt-Bundesamtes, Version 1.00“, im Folgenden kurz bezeichnet als: NCA-Schlüsselgenerator, Version 1.00.

4 Seitens des Antragstellers sind Sicherheitsvorgaben für den EVG in deutscher Sprache bereitgestellt worden. Die Sicherheitsvorgaben, letzte Version 1.04 vom 30.04.2004, werden im Anhang wiedergegeben.

5 Die Sicherheitsvorgaben referenzieren als Prüfkriterien die ITSEC und als Evaluationsstufe E3, für die Mindeststärke der Sicherheitsmechanismen wird „hoch“ angegeben.

2 Maßgebende Prüfgrundlagen

6 Die Evaluierung des EVG erfolgte antragsgemäß gegen die

- Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC) /ITSEC/.

7 Für die Evaluierung und Zertifizierung waren weiterhin folgende Dokumente maßgebend:

- Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM) /ITSEM/,
- Joint Interpretation Library /JIL/,
- Anwendungshinweise und Interpretationen zum Schema, Bundesamt für Sicherheit in der Informationstechnik /AIS/,
- Arbeitsanweisung „Zertifikate nach ITSEC/CC“ der T-Systems GEI GmbH, BU ITC Security (gültige Fassung).

3 Evaluierung

8 Die Evaluierung des EVG wurde durch das Kraftfahrt-Bundesamt bei der Prüfstelle für IT-Sicherheit der T-Systems GEI GmbH beauftragt.

9 Die Prüfstelle ist nach ISO 17025 akkreditiert und besitzt eine gültige Lizenz der Zertifizierungsstelle und des BSI für das hier vorliegende Prüfgebiet.

10 Die Evaluierung erfolgte im Zertifizierungsschema der T-Systems.

11 Die Evaluierung wurde durch die Zertifizierungsstelle kriteriengemäß begleitet.

12 Das Ergebnis der Evaluierung ist im Evaluation Technical Report (ETR) der Prüfstelle dargestellt. Der ETR trägt die Versionsnummer 1.11 und das Datum 27.05.2004.

13 Die Evaluierung des EVG wurde am 28.05.2004 beendet.

4 Zertifizierung

14 Das Zertifizierungsschema der T-Systems ist auf den entsprechenden Web-Seiten der Zertifizierungsstelle veröffentlicht (www.t-systems-zert.com).

15 Die Zertifizierungsstelle der T-Systems arbeitet im Einklang mit der DIN EN 45011 und ist im Hinblick auf diese Norm bei der DATech e.V. für Prüfungen nach den ITSEC und den Common Criteria akkreditiert (DAR-Registriernummer DAT-ZE-015/98-01).

16 Die Zertifizierung des EVG erfolgte wie beantragt gemäß Verfahrenstyp 01: „Zertifikate nach ITSEC/CC“.

17 Dem Zertifizierungsverfahren wurde die Registriernummer T-Systems-DBZ-ITSEC-01111-2004 zugewiesen.

18 Für die Zertifizierung des EVG sind Auflagen und Empfehlungen maßgebend; näheres enthält das Kapitel 5.

19 Eine Kurzfassung der Ergebnisse enthält das Sicherheitszertifikat T-Systems-DBZ-ITSEC-01111-2004 vom 07.06.2004 auf der Seite 3 dieses Zertifizierungsreports.

20 Das Zertifikat und der Zertifizierungsreport sind auf den Web-Seiten (www.t-systems-zert.com) der Zertifizierungsstelle veröffentlicht.

21 Hiermit wird bestätigt, dass

- die am Verfahren beteiligten Evaluatoren und Zertifizierer weder an der Entwicklung, dem Vertrieb noch an einer Anwendung des EVG beteiligt waren,
- alle Regeln des Zertifizierungsschemas, des speziellen Verfahrenstyps und der maßgebenden Kriterien eingehalten wurden.

Klaus-Werner Schröder	Dr. Heinrich Kersten
(Zertifizierer)	(Leiter der Zertifizierungsstelle)

5 Zusammenfassung der Ergebnisse

22 Evaluiert wurde die folgende Konfiguration des EVG:

Der EVG besitzt nur eine, nicht mehr änderbare Konfiguration.

23 Das Evaluierungsergebnis gilt nur für diese Konfiguration(en) des EVG.

24 Entsprechend den Sicherheitsvorgaben und dem Ergebnis der Evaluierung besitzt der EVG folgende Sicherheitsfunktionen:

- Schlüsselgenerierung, Schlüsselsicherung auf Backup- und Release-Cards

25 Die Evaluierung hat ergeben, dass der EVG allen Anforderungen der Evaluationsstufe E3 der ITSEC genügt, d.h. alle Anforderungen an die Korrektheit und Wirksamkeit in dieser Stufe sind erfüllt. Dies sind:

ITSEC E3.1 bis E3.37 für die Korrektheit mit den Phasen

Konstruktion - Entwicklungsprozess:
Anforderungen, Architekturentwurf, Feinentwurf, Implementierung

Konstruktion - Entwicklungsumgebung:
Konfigurationskontrolle, Programmiersprachen und Compiler, Sicherheit beim Entwickler

Betrieb - Betriebsdokumentation:
Benutzerdokumentation, Systemverwalter-Dokumentation

Betrieb - Betriebsumgebung:
Auslieferung und Konfiguration, Anlauf und Betrieb

ITSEC 3.12 bis 3.37 für die Wirksamkeit mit den Aspekten

Wirksamkeitskriterien - Konstruktion:
Eignung der Funktionalität, Zusammenwirken der Funktionalität, Stärke der Mechanismen, Bewertung der Konstruktionsschwachstellen

Wirksamkeitskriterien - Betrieb:
Benutzerfreundlichkeit, Bewertung der operationellen Schwachstellen

26 Hinsichtlich der Sicherheitsmechanismen lautet das Ergebnis der Evaluierung:

Die folgenden Mechanismen des EVG sind kritische Mechanismen: M1 (Ver-/Entschlüsselung mit DES3), M9 (Schlüsselerzeugung gemäß SigG/SigV), M10 (Erzeugung einer zufälligen Zahl fester Länge), M11 (Abarbeitung des Scripts aus der Image-Card), M12 (PIN-Änderung).

Die folgenden Mechanismen sind vom Typ A und haben eine Mindeststärke gemäß der Stufe hoch: M1, M9, M10.

Die folgenden Mechanismen sind vom Typ B: M11 und M12.
Für Mechanismen des Typs B ist gemäß den zugrunde liegenden Kriterien keine Mechanismenstärke anzugeben. Im Rahmen der Schwachstellenanalyse konnte jedoch festgestellt werden, dass selbst unter Zugrundelegung eines Aufwands gemäß der Stufe hoch bei den angenommenen Einsatzbedingungen keine ausnutzbare Schwachstelle erkennbar ist.

27 Die Auslieferung des Systems erfolgt entsprechend den Angaben des Auftraggebers nach folgendem Verfahren:

Die Auslieferung des Systems an den Nutzer erfolgt direkt durch den Hersteller ohne Beteiligung Dritter.

Dieses Auslieferungsverfahren entspricht den Vorgaben der nationalen Zertifizierungsbehörde für die Stufe E3 der ITSEC.

28 Folgende zusätzlichen Hinweise sind für den sicherheitsgerechten Einsatz des EVG zu beachten:

Die Benutzerdokumentation und die Sicherheitsvorgaben beinhalten alle relevanten Informationen für die sichere Benutzung des EVG.

6 Anwendung der Ergebnisse

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

30 Der Zertifizierungsreport dient dem Auftraggeber als Nachweis der durchgeführten Evaluierung und dem Nutzer als eine Grundlage für die sichere Nutzung des EVG.

31 Für die sichere Nutzung des EVG enthalten insbesondere die folgenden Stellen im Zertifizierungsreport wichtige Informationen:

- Kapitel 1: die genaue Bezeichnung des Systems einschließlich der Versionsangabe:

Zertifikat und Zertifizierungsreport gelten nur für dieses System und diese spezielle Version.

- Kapitel 5: Angaben zum Auslieferungsverfahren des EVG.
  Andere Auslieferungsverfahren können unter Umständen nicht die für die Stufe E3 erforderliche Sicherheit bieten.

- Kapitel 5: Angaben zu evaluierten Konfigurationen des EVG.
  Der EVG gilt nur in diesen Konfigurationen als zertifiziert.

- Kapitel 5: Hinweise für den Nutzer des EVG.
  Die Sicherheit bei der Anwendung des EVG kann ggf. nicht mehr gegeben sein, wenn diese Hinweise nicht beachtet werden.

- Anhang: Sicherheitsvorgaben zum EVG.
  Hier sind insbesondere die Informationen zur Art der Nutzung des EVG, zum Lieferumfang, zu seinen Sicherheitszielen bzw. den betrachteten Bedrohungen und zur Einsatzumgebung zu beachten.

32 Falls Anforderungen aus diesem Report nicht eingehalten werden, gilt das Evaluationsergebnis nur noch bedingt. In einem solchen Fall ist eine ergänzende Analyse erforderlich, um festzustellen, ob und in welchem Umfang der EVG auch unter den geänderten Bedingungen noch Sicherheit bieten kann. Die Prüfstelle und die Zertifizierungsstelle können bei der Analyse unterstützen.

33 Bei Änderungen an dem EVG, an seinem Auslieferungsverfahren oder seiner Einsatzumgebung kann eine Re-Zertifizierung erfolgen. Die Ergebnisse solcher nach den Verfahrensregeln der Zertifizierungsstelle durchgeführten Re-Zertifizierungen werden in entsprechenden technischen Anhängen zu diesem Zertifizierungsreport dokumentiert.

34 Bei neuen Erkenntnissen über die Sicherheit des EVG können ebenfalls technische Anhänge zum Zertifizierungsreport herausgegeben werden.

35 Den Web Seiten (www.t-systems-zert.com) der Zertifizierungsstelle ist zu entnehmen, ob

- technische Anhänge zu diesem Zertifizierungsreport herausgegeben worden sind (die Anhänge werden fortlaufend nummeriert: T-Systems-DBZ-ITSEC-01111-2004/1, .../2,...),

- neue Versionen des EVG sich in der Evaluierung befinden bzw. bereits zertifiziert worden sind.

Ende des Zertifizierungsreports zu T-Systems-DBZ-ITSEC-01111-2004.

Anhang: Sicherheitsvorgaben zu „NCA-Schlüsselgenerator, Version 1.00“

(Diese Seite ist beabsichtigterweise leer.)

T · · TeleSec ·

SICHERHEITSVORGABEN

NCA-SCHLÜSSELGENERATOR

Dokumentenkennung:	IT.SGNCA.EVL.SV.104
Dateiname:	SV_SG_11.doc
Stand:	30.04.2004
Version:	1.04
Autor:	T-Systems International GmbH

(Diese Seite ist beabsichtigterweise leer.)

Inhaltsverzeichnis

1. Beschreibung des Evaluationsgegenstandes 4
1.1. Beschreibung des „NCA-Schlüsselgenerator-Systems“ 4
1.2. Beschreibung des Evaluierungsgegenstandes 6
1.2.1. Genaue Bezeichnung des EVG 6
1.2.2. Auslieferungsumfang des EVG 6
2. System-Sicherheitspolitik 7
2.1. Bedrohungen 7
2.2. Sicherheitsziele des Systems 7
2.3. Externe Sicherheitsmaßnahmen 8
2.3.1. Sicherheitseigenschaften von Komponenten des NCA-Schlüsselgenerators 8
2.3.2. Gesicherte Einsatzumgebung des NCA-Schlüsselgenerators 8
2.3.3. Inbetriebnahme 8
2.3.4. Wirkbetrieb 9
2.4. Sicherheitsfunktionalität des EVG 11
2.4.1. Sicherheitsziele des EVG 11
2.4.2. Sicherheitsfunktionen des EVG 11
3. Zweckmäßigkeit der Sicherheitsmaßnahmen 13
4. Evaluationsziel 14
4.1. Angestrebte Evaluationsstufe 14
4.2. Mindeststärke der Mechanismen 14
5. Glossar 15
6. Tabellenverzeichnis 16
7. Literatur 17

1. Beschreibung des Evaluationsgegenstandes

1.1. Beschreibung des „NCA-Schlüsselgenerator-Systems“

Zweck des Systems

Das NCA-Schlüsselgenerator-System stellt für die National Certification Authority (NCA) des Kraftfahrtbundesamtes (KBA) die NCA-Schlüsselpaare für das Signieren von Zertifikaten der NCA auf Signatur-Chipkarten und für die Gewährleistung der Verfügbarkeit auf Backup-Karten bereit. Es unterstützt die Erstellung beliebig vieler NCA-Schlüsselpaare. Jedes NCA-Schlüsselpaar kann auf beliebig vielen Signatur- und Backup-Karten gespeichert werden. Dabei soll der Evaluationsgegenstand (EVG) im Zusammenwirken mit der Einsatzumgebung die Anforderungen der vorgegebenen Richtlinien von EU (europäische Policy) und Bund (nationale Policy) erfüllen.

Die NCA-Schlüsselpaare bestehen aus je einem privaten Schlüssel (privater Exponent und Modul) und einem öffentlichen Schlüssel (öffentlicher Exponent und Modul) für das asymmetrische Kryptosystem RSA mit einer Modullänge von 1024 Bit. Das NCA-Schlüsselgenerator-System gewährleistet die kryptographische Sicherheit der NCA-Schlüsselpaare.

Jede NCA-Chipkarte enthält genau ein NCA-Schlüsselpaar. Der private NCA-Schlüssel wird auf den Signatur-Karten so gespeichert, dass das Signieren von Zertifikaten mit der NCA-Karte erst nach Authentisierung des Benutzers mit einer sechsstelligen PIN möglich ist. Der private NCA-Schlüssel wird auf den Backup-Karten so gespeichert, dass ein Auslesen des privaten Schlüssels erst nach Authentisierung der Benutzer mit zwei sechsstelligen PIN‘s möglich ist. Der öffentliche NCA-Schlüssel kann von einer NCA-Karte jederzeit ausgelesen werden.

Art der Nutzung

Das „NCA-Schlüsselgenerator-System“ realisiert 3 Prozesse:

1. Die Generierung eines NCA-Schlüsselpaares und dessen Speicherung auf einer KBA-Backup-Card.

2. Das Duplizieren eines NCA-Schlüsselpaares von einer KBA-Backup-Card auf eine fest gelegte Anzahl weiterer KBA-Backup-Clone-Cards.

3. Die Herstellung einer fest gelegten Anzahl Signatur-Karten (KBA-Release-Cards) unter Nutzung einer Backup-Karte.

Das „NCA-Schlüsselgenerator-System“ wird in einer gesicherten Umgebung der NCA des KBA betrieben.

Lieferumfang des „NCA-Schlüsselgenerator-Systems“

Das „NCA-Schlüsselgenerator-System“ wird in folgenden Komponenten geliefert:

(1) Schlüsselgeneratorrechner
Der Schlüsselgeneratorrechner dient der Erzeugung der KBA-Schlüsselpaare. Er besteht aus einem Personalcomputer mit CD-ROM und einer seriellen Schnittstelle zum Schlüsselbearbeitungsrechner, aber abgeklemmter Tastatur- und Monitorschnittstelle mit physikalischem Zugangsschutz und Versiegelung sowie ohne nicht-flüchtigen Datenspeicher. Er verfügt außerdem über eine physikalische Rauschquelle (TSM95-PCMCIA-Steckkarte). Auf dem Schlüsselgeneratorrechner werden MS-DOS (Version 6.22), TSM-Software und die EVG-Komponente Schlüsselgenerierungssoftware ausgeführt.

(2) Schlüsselbearbeitungsrechner
Der Schlüsselbearbeitungsrechner besteht aus einem Personalcomputer mit CD-ROM, internem Lautsprecher, drei seriellen Schnittstellen zu den Bediener- und Backup-Chipkartenlesern und der Umschalte-Hardware und einer parallelen Schnittstelle zur Umschalte-Hardware, aber abgeklemmter Tastatur- und Monitorschnittstelle mit physikalischem Zugangsschutz und Versiegelung sowie ohne nicht-flüchtigen Datenspeicher. Auf dem Schlüsselbearbeitungsrechner werden MS-DOS (Version 6.22) und die EVG-Komponente Schlüsselbearbeitungssoftware ausgeführt.

(3) Initialisierungsrechner
Der Initialisierungsrechner ist ein Standard-Personalcomputer unter Windows NT 4.0 mit CD-ROM, Festplatte, Tastatur, Monitor sowie einer seriellen und einer parallelen Schnittstelle zur Umschalte-Hardware. An den Initialisierungsrechner ist ein E2/hoch evaluierter Klasse-3-Chipkartenleser für eine Benutzer-Authentisierung über PIN-Pad angeschlossen. Auf dem Initialisierungsrechner läuft Software zur Initialisierung der TCOS-Karten, zur Steuerung- und Information des Bedieners und die EVG-Komponente PIN-Änderungssoftware.

(4) Umschalte-Hardware
Die Umschalte-Hardware verfügt über eine Kontaktiereinheit für Chipkarten, die über eine Umschalte-Logik an zwei Chipkartenleser an die seriellen Schnittstellen des Schlüsselbearbeitungsrechner bzw. des Initialisierungsrechner angeschlossen sind, sowie über zwei parallele Schnittstellen zur Steuerung der Umschaltens zwischen Schlüsselbearbeitungsrechner und Initialisierungsrechner.

(5) Bediener-Chipkartenleser
Der Chipkartenleser nach B1-Spezifikation der TeleSec besitzt eine serielle Schnittstelle zum Schlüsselbearbeitungsrechner und die erforderliche Kontaktierbaugruppe für die Chipkarte.

(6) Backup-Chipkartenleser
Der Chipkartenleser ist ein E2/hoch evaluierter Klasse-3-Chipkartenleser für eine Benutzer-Authentisierung über PIN-Pad mit serieller Schnittstelle zum Schlüsselbearbeitungsrechner, Kontaktierbaugruppe für die Chipkarte, Anzeige und Tastatur (PIN-Pad).

(7) Bediener-Chipkarten
Die Bediener-Chipkarten Operator-Card, Command-Card, Image-Card und Session-Card sind Chipkarten mit dem Betriebssystem TCOS 2.0 Release 3 und spezifischen Dateien für die Steuerung des NCA-Schlüsselgenerators.

(8) TCOS-Chipkarten
Die Chipkarten sind mit den ROM-Codeanteilen des Betriebssystems TCOS 2.0 Release 3 versehen. Die Chipkarte befindet sich im nicht-initialisierten Zustand, d.h. für den operationellen Betrieb sind Teile des Betriebssystems und die Filestruktur in das EEPROM zu laden.

(9) NCA-Schlüsselgenerator
Der NCA-Schlüsselgenerator umfasst die spezielle Software und Betriebsdokumentation zur Erstellung der Signatur- und Backup-Karten. Er bildet den EVG der vorliegenden Evaluierung. Die EVG-Komponenten sind im Abschnitt 1.2.2 Auslieferungsumfang des EVG beschrieben.

Das KBA als Betreiber des Systems ergreift materielle, personelle und organisatorische Maßnahmen zur Gewährleistung der Integrität des NCA-Schlüsselgenerator-Systems und Geheimhaltung der im Betriebsprozess verarbeiteten Daten. (s. 2.3 Externe Sicherheitsmaßnahmen).

1.2. Beschreibung des Evaluierungsgegenstandes

1.2.1. Genaue Bezeichnung des EVG

Der Evaluierungsgegenstand ist der NCA-Schlüsselgenerator, Version 1.00.

1.2.2. Auslieferungsumfang des EVG

Komponente	Bezeichnung	Version	Auslieferungsform
Schlüsselgenerierungssoftware	TRUST_SG.EXE	Version: 1.02	CD-ROM
Schlüsselbearbeitungssoftware	SB.EXE	Version: 1.10	CD-ROM
PIN-Änderungssoftware	BCTNPINSET.EXE	Version: 1.10	Software
Bedienerdokumentation	BD_SG_11.DOC	Version: 1.04	Dokument
Systemverwalterdokumentation	SD_SG_11.DOC	Version: 1.03	Dokument
Script	KBA_BACKUP.TXT	Version: 1.00	Image-Card
Script	KBA_BATCH.TXT	Version: 1.00	Image-Card
Script	KBA_ BACKUPCOPY.TXT	Version: 1.00	Image-Card
Script	KBA_RELEASE.TXT	Version: 1.00	Image-Card

Anmerkung:
Die Image-Card ist eine Chipkarte mit TCOS 2.0 Release 3, auf der die entsprechenden Scripte als EVG-Komponente gespeichert sind.

2. System-Sicherheitspolitik

Die Sicherheitspolitik des „NCA-Schlüsselgenerator-Systems“ lässt sich zusammenfassend wie folgt formulieren:

„Es müssen geeignete NCA-Schlüsselpaare für RSA-Signaturen erzeugt werden. Die NCA-Schlüsselpaare müssen auf den Signatur-Karten und Backup-Karten gesichert gespeichert werden. Die Nutzung des privaten NCA-Schlüssels zur Signaturerzeugung kann von einer autorisierten Person erfolgen. Ein Duplizieren der NCA-Schlüsselpaare mittels Backup-Karte kann ausschließlich von zwei autorisierten Personen erfolgen. Der Betrieb des NCA-Schlüsselgenerators erfolgt in einer gesicherten Umgebung.“

Autorisierte Personen im Sinne der Sicherheitspolitik sind Personen, die im Besitz der Bediener- sowie ggf. Backup-Karten sind, in Kenntnis entsprechender geheim gehaltener PIN sind und Zugang zu dem NCA-Schlüsselgenerator-System haben.

2.1. Bedrohungen

B1 Offenbarung der privaten NCA-Schlüssel durch Abhören des Produktionsprozesses außerhalb der geschützten Einsatzumgebung, durch Manipulation und Auswertung der Daten des Produktionsprozesses im NCA-Schlüsselgenerator-System.

B2 Signaturerzeugung auf der Grundlage kryptographisch schwacher KBA-Schlüsselpaare durch Ausnutzung systemeigener Schwachstellen oder durch Manipulation des NCA-Schlüsselgenerator-Systems unabhängig von den KBA-Karten.

B3 Signaturerzeugung mit einem privaten NCA-Schlüssel durch Missbrauch der KBA-Karten durch Unbefugte (d.h. Personen ohne Kenntnis der Benutzer-PIN).

B4 Offenbarung der privaten NCA-Schlüssel auf den KBA-Karten durch unbefugtes Kopieren, d.h. von einer beliebigen Signatur-Karte oder von einer Backup-Karte ohne Kenntnis beider Benutzer-PIN‘s. Diese Bedrohung schließt insbesondere eine Manipulation des NCA-Schlüsselgenerator-Systems oder der KBA-Karten ein.

2.2. Sicherheitsziele des Systems

SZ1 Schutz der Vertraulichkeit und Integrität der Daten des Produktionsprozesses im NCA-Schlüsselgenerator-System und der Integrität des NCA-Schlüsselgenerator-Systems vor Manipulation.

SZ2 Die Einmaligkeit des generierten Schlüsselpaars ist mit an Sicherheit grenzender Wahrscheinlichkeit gewährleistet. Aus einem öffentlichen NCA-Schlüssel darf der dazu gehörige geheime NCA-Schlüssel nicht abgeleitet werden können.

SZ3 Ein Signieren mit einem auf einer Signatur-Karte gespeicherten privaten NCA-Schlüssel ist nur bei Kenntnis einer Benutzer-PIN möglich. Eine anderweitige Verwendung des privaten NCA-Schlüssels auf der Signatur-Karte ist auszuschliessen.

SZ4 Ein Lesen des privaten NCA-Schlüssels von einer Backup-Karten ist nur bei Kenntnis zweier Benutzer-PIN‘s möglich. Eine anderweitige Verwendung des privaten NCA-Schlüssels auf der Backup-Karten ist auszuschliessen.

2.3. Externe Sicherheitsmaßnahmen

2.3.1. Sicherheitseigenschaften von Komponenten des NCA-Schlüsselgenerators

Der Betreiber des NCA-Schlüsselgenerator-Systems verwendet für Signatur-Karten (KBA-Release-Cards) und Backup-Karten (KBA-Backup-Cards und KBA-Backup-Clone-Cards) nur authentische TCOS-Karten im Initialisierungszustand, die er direkt vom Hersteller Telesec bezieht.

Es werden folgende Sicherheitseigenschaften der Komponenten des Systems NCA-Schlüsselgenerator vorausgesetzt:

(1) Der TSM des Schlüsselgeneratorrechners ist als externe physikalische Zufallsquelle nach ITSEC E3 hoch evaluiert.

(2) Der Chip SLE66CX320P / m1421b25 der TCOS-Chipkarten gewährleistet die physische Sicherheit der gespeicherten NCA-Schlüsselpaare. Er ist unter BSI-DSZ-ITSEC-0175-2002 nach ITSEC E4 hoch zertifiziert.

(3) Das Betriebssystem TCOS 2.0, Release 3, der TCOS-Chipkarten gewährleistet die Zugriffskontrolle für Kommandos gemäß [4]. Das Betriebssystem ist nach ITSEC E4 hoch evaluiert.

(4) Die eingesetzten Klasse-3-Chipkartenlesegeräte (Backup-Kartenleser am Schlüsselbearbeitungsrechner u. Bedienerkartenleser am Initialisierungsrechner) sind E2/hoch evaluiert und gewährleisten, dass die Identifikationsdaten, welche zur Chipkarte gesendet werden, weder gespeichert noch preisgegeben werden.

2.3.2. Gesicherte Einsatzumgebung des NCA-Schlüsselgenerators

Der Raum, in dem sich der EVG befindet, im folgenden SG-Raum genannt, ist durch eine Zutrittskontrollanlage vor unbefugtem Zutritt gesichert. Der SG-Raum, darf nur für autorisierte Personen zugänglich sein. Zum Öffnen der Sicherheitstüren sind zwei Personen erforderlich, die vom Zutrittskontrollsystem zugelassen sind.

Der SG-Raum muss so beschaffen sein, dass von außerhalb des Raumes keine Einflussnahme auf die in seinem Inneren befindlichen Prozesse möglich ist. Es dürfen keine Informationen über die im Betriebsprozess verarbeiteten Daten von außen erfassbar sein.

2.3.3. Inbetriebnahme

Vor der Inbetriebnahme des EVGs werden die vertrauenswürdig erzeugten CD-ROMs, Operator-Cards, Command Cards, Image-Cards und Session-Cards sowie TCOS-Chipkarten durch den Hersteller an den Anwender übergeben.

Während der Inbetriebnahme sind mindestens eine Person des Lieferanten und eine Person des Betreibers anwesend. Dabei werden die CD-ROMs eingelegt, und die notwendigen Chipkarten an die Bediener des Systems übergeben.

Die Anwesenden überzeugen sich davon, dass

(1) die CD-ROM der Schlüsselbearbeitung die öffentlichen Schlüssel der Operator-Cards und der Session-Cards sowie die Kartennummern der entsprechenden Operator- und Session-Cards enthält,

(2) die auf den Operator-Cards befindlichen privaten Schlüssel nicht ausgelesen werden können,

(3) die auf den Session-Cards befindlichen privaten Schlüssel nicht ausgelesen werden können,

(4) die Command-Card für die Aufnahme der Anzahl der zu beschlüsselnden TCOS-Chipkarten bzw. zu erzeugenden Backup-Chipkarten und die Kennung des zu verwendenden Scripts bereit ist,

(5) die Image-Card lediglich die Scripte des EVG unveränderbar enthält,

(6) die Operator-Cards, Session-Cards, Image-Cards, Command-Cards und TCOS-Chipkarten vertrauenswürdig an die Operatoren übergeben werden,

(7) ausschließlich die oben beschriebenen Dateien und Verzeichnisse auf den CDs befindlich sind,

(8) die CD-ROMs in die Laufwerke des Schlüsselgeneratorrechner und des Schlüsselbearbeitungsrechners eingelegt und die CD-ROM-Laufwerke versiegelt werden,

(9) die Rechnergehäuse, die Umschalte-Hardware, die Chipkartenleser und die Leitung zwischen den Komponenten des NCA-Schlüsselgenerator-Systems versiegelt werden und

(10) alle Prüf-/Kontrollschritte als erledigt protokolliert werden.

2.3.4. Wirkbetrieb

Der Betreiber ergreift materielle, personelle und organisatorische Sicherheitsmaßnahmen zum sicheren Betrieb des NCA-Schlüsselgenerator-Systems.

(1) Die für den Betrieb benötigten Karten sind im Besitz eines klar begrenzten Personenkreises, den Bedienern. Die Operator-Cards, die Command-Cards, die Image-Cards und die Session-Cards sind so auf die berechtigten Personen aufzuteilen, dass der Wirkbetrieb die Anwesenheit und Tätigkeit von zwei Bedienern erfordert.

(2) Es wird gewährleistet, dass mindestens zwei für die Verwendung der Backup-Karten befugte Personen während des Betriebs des Systems NCA-Schlüsselgenerator, insbesondere des EVGs, anwesend sind. Für die Erstellung von Signatur-Karten muss eine für die Signatur-Karten befugte Person anwesend sein. Die anwesenden Personen haben sich während des Betriebs im SG-Raum gegenseitig in der korrekten Durchführung der Prozesse entsprechend der Betriebsdokumentation zu überwachen.

(3) Ein Bediener stellt die authentischen TCOS-Chipkarten im Initialisierungszustand für die zu erzeugende KBA-Backup-Card, KBA-Backup-Clone-Card oder KBA-Release-Card zur Verfügung. Das KBA-System (Init-Rechner) führt unmittelbar vor der Beschlüsselung der zu produzierenden Karte eine Komplettierung durch (Komplettierung von TCOS im EEPROM, Anlegen des MFs).

(4) Die Bediener überzeugen sich vor Betriebsaufnahme von dem ordnungsgemäßen Zustand

(a) des Schlüsselgeneratorrechners und des Schlüsselbearbeitungsrechners, einschließlich der Versiegelung und der Abdeckungen der Tastaturschnittstellen und der Monitorschnittstellen sowie der Versiegelung der Gehäuse, der CD-ROM-Laufwerke, der seriellen Schnittstellen und der parallelen Schnittstellen,

(b) der Umschalte-Hardware, einschließlich der Versiegelung des Gehäuses,

(c) des Bediener-Chipkartenleser und des Backup-Chipkartenlesers,

(d) der Leitung zwischen dem Schlüsselgeneratorrechner, dem Schlüsselbearbeitungsrechner, der Umschalte-Hardware und dem Initialisierungsrechner

und protokollieren dies.

(5) Ein Bediener authentisiert sich mit seiner persönlichen Berechtigungskarte (TIKS/NetKey) und zugehöriger PIN gegenüber der Software auf dem Initialisierungsrechner. Jeder Bediener hält seine PIN geheim und schützt seine Berechtigungskarte vor Missbrauch.

(6) Die Bediener wählen für jede Backup-Karte (d.h. KBA-Backup-Card oder KBA-Backup-Clone-Card) und jede der Signatur-Karte (KBA-Release-Card) zufällige PIN für die Sicherung des Zugriffs der privaten NCA-Schlüssel. Jeder Bediener hält die von ihm gewählte PIN geheim.

(7) Der Betreiber ergreift Maßnahmen zur Gewährleistung der Verfügbarkeit der Backup-Karten im Bedarfsfall. Der Betreiber ergreift Maßnahmen zur Gewährleistung der Geheimhaltung und der Verfügbarkeit dieser PIN unter den Bedingungen der langfristigen Benutzung der Chipkarten.

(8) Der Betreiber ergreift organisatorische Maßnahmen zur Sicherstellung des Übergangs der Backup- und Backup-Clone-Karten aus dem Null-PIN Status in einen Status, in dem ein Auslesen des geheimen Schlüssels nur durch Eingabe zweier gültiger und geheimer PIN‘s möglich ist. Diese organisatorischen Maßnahmen haben im Falle der Backup- und der Backup-Clone-Karte unmittelbar nach der Kartenproduktion am Initialisierungsrechner zu erfolgen.

(9) Der Betreiber ergreift organisatorische Maßnahmen zur Sicherstellung des Übergangs der Release-Karte aus dem Null-PIN Status in einen Status, in dem eine gültige und geheime PIN den geheimen Schlüssel vor unerlaubter Verwendung schützt. Diese organisatorischen Maßnahmen haben im Falle der Release-Karten unmittelbar nach der Kartenproduktion durch Anmeldung der Karten am RA-System zu erfolgen.

2.4. Sicherheitsfunktionalität des EVG

2.4.1. Sicherheitsziele des EVG

Der EVG verwirklicht die Sicherheitsziele SZ2, SZ3 und SZ4 unter der Bedingung, dass die externen Sicherheitsmassnahmen des Betreibers des NCA-Schlüsselgenerator-Systems das SZ1 durchsetzt.

2.4.2. Sicherheitsfunktionen des EVG

SF1 Schlüsselgenerierung

Der EVG erzeugt mit der Sicherheitsfunktion SF1 NCA-Schlüsselpaare, die den Anforderungen an geeignete Kryptoalgorithmen für qualifizierte Signaturen des SigG/SigV entsprechen [5].

Die Sicherheitsfunktion SF1 nutzt den TSM unter den im Abschnitt 2.3.1 Sicherheitseigenschaften von Komponenten des NCA-Schlüsselgenerators, Punkt (1), genannten Voraussetzungen als externe Zufallsquelle für einen internen deterministischen Zufallsgenerator. Die SF1 unterzieht den TSM einem Online-Test und verwendet die gelesenen Zufallsbytes nur nach erfolgreichem Online-Test.

Die Sicherheitsfunktion SF1 erzeugt die Primzahlen *p* und *q* derart, dass

- Die Primfaktoren *p* und *q* werden unter Beachtung der genannten Nebenbedingungen unabhängig voneinander zufällig erzeugt.
- Der zugrunde liegende Modulus $n = pq$ eine Bitlänge von mindestens 1024 haben ($log_2 (n) \geq 1023$) hat:

$$log_2(n) = log_2(p) + log_2(q) \geq 1023$$

- Die Primfaktoren *p* und *q* von n ungefähr gleich groß sind, aber nicht zu dicht beieinander liegen, d. h. konkret

$$\mathbf{0.5 < \left|\log_2(p) - \log_2(q)\right| < 30}$$

- Der öffentliche Exponent *e* wird mit $\boldsymbol{ggT(e,(p-1)\cdot(q-1)) = 1}$ gewählt. Der zugehörige geheime Exponent *d* wird dann berechnet, so dass $\boldsymbol{ed \equiv 1 mod (p-1)(q-1)}$ gilt. Der EVG verwendet feste Exponenten, die je nach Anforderung des Systems, in welchem sie zum Einsatz kommen sollen, im Bereich zwischen 31 Bit und 64 Bit liegen, z. B. $e = 2^{30} + 2^7 + 1$ (31 Bit).

SF2 Sicherung des NCA-Schlüssels auf Backup-Karten

Die Sicherheitsfunktion SF2 erzeugt Backup-Karten aus TCOS-Karten unter der im Abschnitt 2.3.1 Sicherheitseigenschaften von Komponenten des NCA-Schlüsselgenerators, Punkte (2) und (3), genannten Voraussetzungen, so dass das Auslesen des gespeicherten NCA-Schlüsselpaares nur nach Authentisierung der Benutzer mit zwei sechsstelligen PIN möglich ist.

Die Sicherheitsfunktion SF2 legt die für die PIN-Authentisierung und Schlüsselspeicherung notwendigen Dateien so an, dass

(a) ein Lesen des privaten NCA-Schlüssels nur nach Benutzerauthentisierung mit zwei sechstelligen PIN möglich ist,

(b) der private NCA-Schlüssel nicht anderweitig, insbesondere nicht zur Signaturerstellung, verwendet werden kann.

KBA-Backup-Cards und KBA-Backup-Clone-Cards besitzen die gleiche Datei-Struktur.

Nach der Quelle des NCA-Schlüsselpaares, das auf die Backup-Karte gespeichert wird, unterstützt die Sicherheitsfunktion SF2 die folgenden Prozesse:

(a) Erzeugung einer KBA-Backup-Card mit einem durch die Sicherheitsfunktion SF1 gelieferten NCA-Schlüsselpaar,

(b) Erzeugung einer KBA-Backup-Clone-Card mit einem von einer Backup-Karte gelieferten NCA-Schlüsselpaar.

Die Sicherheitsfunktion SF2 unterstützt durch die Passwortanwendung auf dem Initialisierungsrechner die Festlegung der PIN der Benutzerauthentisierung auf den produzierten Backup-Karten zum Zugriff auf den NCA-Schlüssel (vgl. auch Abschnitt 2.3.4, Punkt (8)).

Anmerkung:
Die Eingabe der PIN zur Benutzerauthentiserung zum Lesen des Secret Key von den Backup-Karten zur Erstellung der KBA-Backup-Clone-Card erfolgt auf dem Backup-Chipkartenleser.

SF3 Sicherung des NCA-Schlüssels auf KBA-Release-Cards

Die Sicherheitsfunktion SF3 erzeugt KBA-Release-Cards aus TCOS-Karten unter der im Abschnitt 2.3.1 Sicherheitseigenschaften von Komponenten des NCA-Schlüsselgenerators, Punkte (2) und (3), genannten Voraussetzungen, so dass das gespeicherte NCA-Schlüsselpaar nicht auslesbar ist.

Die Sicherheitsfunktion SF3 legt die für die PIN-Authentisierung und Schlüsselspeicherung notwendigen Dateien so an, dass

(a) für die Verwendung des privaten NCA-Schlüssels eine PIN-Mechanismus angelegt wird, der jedoch noch im Null-PIN Status verbleibt,

(b) der private NCA-Schlüssel nicht ausgelesen werden kann.

Anmerkung:
Die Sicherheitsfunktion SF3 umfasst nicht den Übergang aus dem Null-PIN Status in eine gültige und geheime PIN zum Schutz des geheimen Schlüssels gegen unerlaubte Verwendung. Dieses hat unmittelbar nach der Kartenproduktion durch Anmeldung in das RA-System zu erfolgen und wird somit durch eine organisatorische Maßnahme sichergestellt (vgl. auch Abschnitt 2.3.4, Punkt (9)).

3. Zweckmäßigkeit der Sicherheitsmaßnahmen

Die Abdeckung der Bedrohungen Bx, x=1,...,4, durch die Sicherheitsziele SZy, y=1,...,4, mittels externer Sicherheitsmaßnahmen und Sicherheitsfunktionen des EVG sind in der folgenden Tabelle dargestellt.

	SZ1	SZ2	SZ3	SZ4
B1	Externe Sicherheitsmaßnahmen			
B2		SF1		
B3			SF3	
B4				SF2

Tabelle 1: Zusammenhang Bedrohungen, Sicherheitsziele, Sicherheitsfunktionen und externer Sicherheitsmaßnahmen

In Tabelle 1 ist zu erkennen, dass jeder Bedrohung mindestens eine Sicherheitsfunktion bzw. externe Sicherheitsmaßnahmen entgegenwirken.

Der Bedrohung B1 (Produktionsprozess abhören außerhalb der geschützten Einsatzumgebung) wird durch externe Sicherheitsmaßnahmen entgegengewirkt. Die externen Sicherheitsmaßnahmen bestehen in darin, das NCA-SG-System ausschließlich in einem zutrittsgeschützten Raum (4-Augen-Prinzip) zu betreiben, der so beschaffen sein muss, dass von außerhalb weder Informationen abgegriffen noch die Prozesse im Inneren manipuliert werden können (abstrahlgeschützt).

Die Sicherheitsfunktion SF1 (Schlüsselgenerierung) wirkt der Bedrohung B2 (schwache Schlüssel) entgegen, da die Schlüssellänge und die Qualität mit der die Schlüssel erzeugt werden zur Abwehr dieser Bedrohung geeignet ist.

Der Bedrohung B4 (unbefugtes Kopieren von Schlüsseln) wirkt die Sicherheitsfunktion SF2 (Sicherung des NCA-Schlüssels auf KBA-Backup-Karten) entgegen, da die Filestruktur auf den betroffenen Karten vom EVG so angelegt, dass ein Auslesen der geheimen Schlüssel nur nach erfolgreicher Benutzerauthentisierung von zwei berechtigten Personen durch Nachweis ihrer PIN möglich ist. Eine mögliche missbräuchliche Anwendung des geheimen Schlüssels auf der Karte wird durch die angelegte Filestruktur unterbunden, da der Schlüssel nicht innerhalb dieser KBA-Backup-Karte zum Signieren verwendet werden kann.

Durch die Sicherheitsfunktion SF3 (Sicherung des NCA-Schlüssels auf KBA-Release-Karten) wird der Bedrohung B3 (missbräuchliche Anwendung des NCA-Schlüssels) entgegengewirkt, da die Filestruktur auf den betroffenen Karten vom EVG so angelegt wird, dass eine Anwendung des geheimen Schlüssels nur nach erfolgreicher Benutzerauthentisierung der berechtigten Person durch ihre PIN möglich ist. Ein Auslesen des geheimen Schlüssels wird durch die angelegte Filestruktur unterbunden, da der Schlüssel nach PIN-Prüfung ausschließlich innerhalb dieser KBA-Release-Karte verwendet werden kann.

4. Evaluationsziel

4.1. Angestrebte Evaluationsstufe

Für den NCA-Schlüsselgenerator wird die ITSEC-Evaluationsstufe ***E3*** festgelegt.

4.2. Mindeststärke der Mechanismen

Die Mindeststärke aller verwendeten Mechanismen wird mit ***hoch*** postuliert.

5. Glossar

Backup-Karte	Oberbegriff für KBA-Backup-Card und KBA-Backup-Clone-Card
Initialisierungsrechner	Personalcomputer zur Initialisierung der KBA-Karten, zur Steuerung- und Information des Bedieners und zur PIN-Änderung.
KBA-Backup-Card	Chipkarte, auf die das NCA-Schlüsselpaar nach seiner Generierung zum Zweck des Backups gespeichert wird
KBA-Backup-Clone-Card	Chipkarte, auf die das NCA-Schlüsselpaar von einer KBA-Backup-Card zum Zweck des Backups kopiert wird
KBA-Karte	Oberbegriff für KBA-Release-Card, KBA-Backup-Card und KBA-Backup-Clone-Card
KBA-Release-Karten	Signatur-Chipkarte mit einem NCA-Schlüsselpaar zum Signieren von Zertifikaten der NCA, auch kurz Signatur-Karte genannt
NCA-Schlüsselgenerator	System für die Generierung der NCA-Schlüsselpaare für das auf Signatur-Chipkarten (KBA-Release-Karten) und für die Gewährleistung der Verfügbarkeit auf Backup-Karten
NCA-Schlüsselpaar	RSA-Schlüsselpaar mit der Modullänge 1024 Bit zum Signieren (mit dem privaten Schlüssel) und Prüfen (mit dem öffentlichen Schlüssel) von Zertifikaten der NCA
Schlüsselbearbeitungsrechner	Personalcomputer zum Anlegen der Dateien und zum Speichern des NCA-Schlüsselpaares auf den KBA-Karten
Schlüsselgeneratorrechner	Personalcomputer zur Erzeugung der KBA-Schlüsselpaare mit der Schlüsselgenerator-Software
Umschalte-Hardware	Kontaktiereinheit für Chipkarten zur wechselseitigen Bearbeitung der KBA-Karten durch Schlüsselbearbeitungsrechner und Initialisierungsrechner

6. Tabellenverzeichnis

TABELLE 1: ZUSAMMENHANG BEDROHUNGEN, SICHERHEITSZIELE, SICHERHEITSFUNKTIONEN UND EXTERNER SICHERHEITSMAßNAHMEN 13

7. Literatur

[1] Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC); Vorläufige Form der harmonisierten Kriterien, Version 1.2, Juni 1991

[2] Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM), Vorläufige Form der harmonisierten Methodik, Version 1.0, Juni 1991

[3] ITSEC Joint Interpretation Library (ITSEC JIL); Version 2.0, November 1998

[4] Telesec Chipcard Operating System, Betriebssystem für Chipkarten TCOS V2.0 Release3, Produktbereich T-TeleSec Deutsche Telekom AG, Version 1.07, Januar 2001

[5] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung, Bundesanzeiger Nr. 48, S. 4202-4203, v. 11.03.2003

Ende der Sicherheitsvorgaben zu
„NCA-Schlüsselgenerator, Version 1.00“.

Zertifizierungsreport T-Systems-DBZ-ITSEC-01111-2004

Hrsg.: T-Systems GEI GmbH
Adresse: Rabinstr. 8, 53111 Bonn
Telefon: 0228/9841-0
Fax: 0228/9841-60
Web: www.t-systems-ict-security.com
www.t-systems-zert.com