

DIN EN 419251-1:2013-05 (D)

Sicherheitsanforderungen für Geräte zur Authentisierung - Teil 1: Schutzprofil für Kernfunktionalitäten; Deutsche Fassung EN 419251-1:2013

Inhalt	Seite
Vorwort	5
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Konformität	6
3.1 CC-Konformität	6
3.2 Schutzprofil-Konformität	6
3.3 Paket-Konformität	6
3.4 Begründung der Konformität	6
3.5 Konformitätsangabe	6
4 Begriffe	7
5 Symbole und Abkürzungen	9
6 Überblick über den Evaluationsgegenstand	9
6.1 EVG-Typ	9
6.2 EVG-Einsatz	9
6.3 Sicherheitsmerkmale des EVG	10
6.4 Anwendungsbeispiele	11
6.4.1 E-Government	11
6.4.2 Sonstige Anwendungen	11
6.5 Erforderliche Nicht-EVG-Hardware und -Software	11
6.6 Schutzprofil-Nutzung	12
7 EVG-Umgebung	12
7.1 Allgemeiner Überblick	12
7.2 Personalisierungsanwendung	13
7.2.1 Allgemeines	13
7.2.2 Funktionalitäten	13
7.2.3 Kommunikation	13
7.3 Authentisierungsanwendung	14
7.3.1 Allgemeines	14
7.3.2 Funktionalitäten	14
7.3.3 Kommunikation	14
7.4 Prüfer	15
7.4.1 Funktionalitäten	15
7.4.2 Kommunikation	15
7.5 Schlüsselerzeuger	15
7.5.1 Funktionalitäten	15
7.5.2 Kommunikation	15
7.6 Zertifizierungsinstanz — Funktionalitäten	16
8 Lebenszyklus	17
8.1 Überblick	17
8.2 Vorpersonalisierungsphase	18
8.3 Personalisierungsphase	19
8.3.1 Allgemeines	19
8.3.2 Personalisierungsanwendung	19
8.4 Einsatzphase — Authentisierungsanwendung	19
8.4.1 Allgemeines	19
8.4.2 Prüfer	20

9	Definition des Sicherheitsproblems	20
9.1	Zu schützende Werte (Assets)	20
9.1.1	Allgemeines	20
9.1.2	Vom EVG geschützte Werte.....	20
9.1.3	Sensible Werte des EVG	20
9.2	Benutzer.....	21
9.3	Bedrohungen.....	22
9.4	Organisatorische Sicherheitsvorgaben	23
9.4.1	Bereitgestellte Dienste	23
9.4.2	Sonstige Dienste.....	23
9.5	Annahmen	24
10	Sicherheitsziele.....	24
10.1	Allgemeines.....	24
10.2	Sicherheitsziele für den EVG.....	25
10.2.1	Bereitgestellter Dienst.....	25
10.2.2	Authentisierung gegenüber dem EVG.....	25
10.2.3	EVG-Management	25
10.3	Sicherheitsziele für die Einsatzumgebung	26
10.4	Begründung für Sicherheitsziele	27
11	Erweiterte Komponentendefinition	32
12	Sicherheitsanforderungen	32
12.1	Allgemeines	32
12.2	Einleitung.....	32
12.2.1	Subjekte, Objekte und Sicherheitsattribute	32
12.2.2	Operationen.....	33
12.3	Funktionale Sicherheitsanforderungen.....	33
12.3.1	Allgemeines	33
12.3.2	Core	33
12.3.3	KeyImp	43
12.4	Vertrauenswürdigkeitsanforderungen	47
12.5	SFR/Sicherheitsziele	47
12.6	SFR-Abhängigkeiten	52
12.7	Begründung für die Vertraulichkeitsanforderungen.....	53
12.7.1	EAL4, methodisch entwickelt, getestet und überprüft	53
12.7.2	AVA_VAN.5, fortgeschrittene methodische Schwachstellenanalyse	53
12.7.3	ALC_DVS.2, Angemessenheit der Sicherheitsmaßnahmen.....	54
	Literaturhinweise	55
	Stichwortverzeichnis	56

Bilder

Bild 1 — EVG Sicherheitsmerkmale.....	12
Bild 2 — Umgebung der Personalisierungsanwendung.....	13
Bild 3 — Umgebung der Authentisierungsanwendung	14
Bild 4 — EVG Lebenszyklus	17

Tabellen

Tabelle 1 — Schutz sensibler Daten	25
Tabelle 2 — Sicherheitsziele und Problemdefinition	28
Tabelle 3 — Sicherheitsattribute	33

Tabelle 4 — Core-Sicherheitsattribute	37
Tabelle 5 — Core-Sicherheitsattribute	37
Tabelle 6 — Core-Sicherheitsattribute – Operationen.....	39
Tabelle 7 — Core-Sicherheitsattribute – Anfangswert	40
Tabelle 8 — Core-Sicherheitsattribute – Aktualisierungen.....	41
Tabelle 9 — TSF-Daten – Aktualisierungen	42
Tabelle 10 — KeyImp-Sicherheitsattribute	44
Tabelle 11 — KeyImp-Sicherheitsattribute – Operationen	44
Tabelle 12 — KeyImp-Sicherheitsattribute – Aktualisierung der autorisierten Rollen	46
Tabelle 13 — KeyImp-Sicherheitsattribute – Aktualisierung der Werte	46
Tabelle 14 — SFR und Sicherheitsziele	48
Tabelle 15 — SFR-Abhängigkeiten	52