DIN EN 419251-3:2013-06 (D)

Sicherheitsanforderungen für Geräte zur Authentisierung - Teil 3: Zusätzliche Funktionalitäten für Sicherheitsziele; Deutsche Fassung EN 419251-3:2013

Inhalt

Seite

Vorwort 6

1 Anwendungsbereich 7

2 Normative Verweisungen 7

3 Konformität 7
3.1 CC-Konformität 7
3.2 Schutzprofil-Konformität 7
3.3 Paket-Konformität 7
3.4 Begründung der Konformität 7
3.5 Konformitätsangabe 7

4 Begriffe 8

5 Symbole und Abkürzungen 10

6 Überblick über den Evaluationsgegenstand 10
6.1 EVG-Typ 10
6.2 EVG-Einsatz 11
6.3 Sicherheitsmerkmale des EVG 11
6.4 Erforderliche Nicht-EVG-Hardware und -Software 11
6.5 Schutzprofil-Nutzung 11
6.6 Gruppen 11
6.6.1 Allgemeines 11
6.6.2 Hauptgruppen 12
6.6.3 Umgebungsbezogene Gruppen 12
6.7 Konfigurationen 14
6.7.1 Allgemeines 14
6.7.2 Regeln 14
6.7.3 Mögliche Konfigurationen 15
6.8 EVG-Umgebung 17
6.8.1 Allgemeiner Überblick 17
6.8.2 Personalisierungsanwendung 18
6.8.3 Administrationsanwendung 19
6.8.4 Authentisierungsanwendung 20
6.8.5 Prüfer 21
6.8.6 Schlüsselerzeuger 21
6.8.7 Zertifizierungsinstanz 22
6.8.8 Anwendungsbeispiele 22
6.9 Lebenszyklus 24
6.9.1 Überblick 24
6.9.2 Vorpersonalisierungsphase 25
6.9.3 Personalisierungsphase 25
6.9.4 Einsatzphase 26

7 Definition des Sicherheitsproblems 28
7.1 Zu schützende Werte (Assets) 28
7.1.1 Allgemeines 28
7.1.2 „Core“-Gruppe 28
7.1.3 „KeyGen“-Gruppe 29
7.1.4 „Admin“-Gruppe 29
7.2 Benutzer 29
7.2.1 „Core“-Gruppe 29

7.2.2 „KeyImp“-Gruppe ... 30
7.2.3 „KeyGen“-Gruppe ... 30
7.2.4 „Admin“-Gruppe ... 30
7.3 Bedrohungen ... 31
7.3.1 Allgemeines ... 31
7.3.2 „Core“-Gruppe ... 31
7.3.3 „KeyGen“-Gruppe ... 32
7.3.4 „Admin“-Gruppe ... 32
7.4 Organisatorische Sicherheitsvorgaben ... 32
7.4.1 „Core“-Gruppe ... 32
7.4.2 „KeyGen“-Gruppe ... 33
7.4.3 „Admin“-Gruppe ... 33
7.5 Annahmen ... 33
7.5.1 „Core“-Gruppe ... 33
7.5.2 „KeyGen“-Gruppe ... 34
7.5.3 „Admin“-Gruppe ... 34

8 Sicherheitsziele ... 34
8.1 Allgemeines – Übertragung sensibler Daten ... 34
8.2 Sicherheitsziele für den EVG ... 35
8.2.1 „Core“-Gruppe ... 35
8.2.2 „KeyImp“-Gruppe ... 36
8.2.3 „KeyGen“-Gruppe ... 36
8.2.4 „Admin“-Gruppe ... 37
8.2.5 Untrusted PersoAppli ... 37
8.2.6 Untrusted AuthAppli ... 37
8.2.7 Untrusted Verifier ... 37
8.2.8 Untrusted CA ... 38
8.2.9 Untrusted AdminAppli ... 38
8.3 Sicherheitsziele für die Einsatzumgebung ... 38
8.3.1 „Core“-Gruppe ... 38
8.3.2 „KeyImp“-Gruppe ... 39
8.3.3 „Admin“-Gruppe ... 39
8.3.4 Trusted PersoAppli ... 39
8.3.5 Trusted AuthAppli ... 39
8.3.6 Trusted Verifier ... 39
8.3.7 Trusted CA ... 40
8.3.8 Trusted AdminAppli ... 40
8.4 Begründung für Sicherheitsziele ... 40

9 Erweiterte Komponentendefinition – Definition der Familie FCS_RNG ... 46

10 Sicherheitsanforderungen ... 47
10.1 Allgemeines ... 47
10.2 Einleitung ... 48
10.2.1 Subjekte, Objekte und Sicherheitsattribute ... 48
10.2.2 Operationen ... 49
10.3 Funktionale Sicherheitsanforderungen ... 50
10.3.1 Allgemeines ... 50
10.3.2 „Core“-Gruppe ... 50
10.3.3 „KeyImp“-Gruppe ... 59
10.3.4 „KeyGen“-Gruppe ... 62
10.3.5 „Admin“-Gruppe ... 66
10.3.6 Untrusted PersoAppli ... 71
10.3.7 Untrusted AuthAppli ... 72
10.3.8 Untrusted Verifier ... 72
10.3.9 Untrusted CA ... 73
10.3.10 Untrusted AdminAppli ... 74
10.4 Vertrauenswürdigkeitsanforderungen ... 74
10.5 SFR/Sicherheitsziele ... 74
10.6 SFR-Abhängigkeiten ... 81
10.7 Begründung für die Vertraulichkeitsanforderungen ... 83

Literaturhinweise ... 85

Stichwortverzeichnis **86**

Bilder

Bild 1 — EVG Sicherheitsmerkmale **17**
Bild 2 — Umgebung der Personalisierungsanwendung **18**
Bild 3 — Umgebung der Administrationsanwendung **19**
Bild 4 — Umgebung der Authentisierungsanwendung **20**
Bild 5 — EVG Lebenszyklus **24**

Tabellen

Tabelle 1 — Basiskonfigurationen **15**
Tabelle 2 — IDTrusted-Konfigurationen **15**
Tabelle 3 — Schutz sensibler Daten **35**
Tabelle 4 — Sicherheitsziele und Problemdefinition **41**
Tabelle 5 — Sicherheitsattribute **48**
Tabelle 6 — Core-Sicherheitsattribute **53**
Tabelle 7 — Core-Sicherheitsattribute **54**
Tabelle 8 — Core-Sicherheitsattribute – Operationen **55**
Tabelle 9 — Core-Sicherheitsattribute – Anfangswert **56**
Tabelle 10 — Core-Sicherheitsattribute – Aktualisierungen **56**
Tabelle 11 — TSF-Daten – Aktualisierungen **57**
Tabelle 12 — KeyImp-Sicherheitsattribute **59**
Tabelle 13 — KeyImp-Sicherheitsattribute – Operationen **60**
Tabelle 14 — KeyImp-Sicherheitsattribute – Aktualisierung der autorisierten Rollen **61**
Tabelle 15 — KeyImp-Sicherheitsattribute – Aktualisierung der Werte **62**
Tabelle 16 — KeyGen-Operationen **63**
Tabelle 17 — KeyGen-Sicherheitsattribute **64**
Tabelle 18 — Regeln für KeyGen-Operationen **64**
Tabelle 19 — KeyGen-Sicherheitsattribute – Aktualisierung der autorisierten Rollen **65**
Tabelle 20 — KeyGen-Sicherheitsattribute – Anfangswerte **65**
Tabelle 21 — KeyGen-Sicherheitsattribute – Aktualisierung der Werte **65**
Tabelle 22 — Admin-Sicherheitsattribute – Aktualisierung der autorisierten Rollen **69**
Tabelle 23 — Admin-Sicherheitsattribute – Anfangswerte **69**
Tabelle 24 — Admin-Sicherheitsattribute – Aktualisierung der Werte **70**
Tabelle 25 — Admin-TSF-Daten – Operationen **70**
Tabelle 26 — SFR und Sicherheitsziele **75**
Tabelle 27 — SFR-Abhängigkeiten **81**