

# DIN EN 419251-2:2013-06 (D)

Sicherheitsanforderungen für Geräte zur Authentisierung - Teil 2: Schutzprofil für Erweiterung für vertrauenswürdigen Kanal zur Zertifikaterzeugungsanwendung; Deutsche Fassung EN 419251-2:2013

---

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 .....	10
6.3 Sicherheitsmerkmale des EVG .....	10
6.4 Anwendungsbeispiele .....	11
6.4.1 E-Government .....	11
6.4.2 Sonstige Anwendungen .....	12
6.5 Erforderliche Nicht-EVG-Hardware und -Software .....	12
6.6 Schutzprofil-Nutzung .....	12
7 EVG-Umgebung .....	13
7.1 Allgemeiner Überblick .....	13
7.2 Personalisierungsanwendung .....	14
7.2.1 Allgemeines .....	14
7.2.2 Funktionalitäten .....	14
7.2.3 Kommunikation .....	14
7.3 Administrationsanwendung .....	15
7.3.1 Allgemeines .....	15
7.3.2 Funktionalitäten .....	15
7.3.3 Kommunikation .....	15
7.4 Authentisierungsanwendung .....	16
7.4.1 Allgemeines .....	16
7.4.2 Funktionalitäten .....	16
7.4.3 Kommunikation .....	16
7.5 Prüfer .....	17
7.5.1 Funktionalitäten .....	17
7.5.2 Kommunikation .....	17
7.6 Schlüsselerzeuger .....	17
7.6.1 Funktionalitäten .....	17
7.6.2 Kommunikation .....	17
7.7 Zertifizierungsinstanz .....	18
7.7.1 Funktionalitäten .....	18

7.7.2	Kommunikation .....	18
8	Lebenszyklus .....	19
8.1	Überblick .....	19
8.2	Vorpersonalisierungsphase .....	20
8.3	Personalisierungsphase .....	21
8.3.1	Allgemeines .....	21
8.3.2	Personalisierungsanwendung .....	21
8.4	Einsatzphase .....	22
8.4.1	Authentisierungsanwendung .....	22
8.4.2	Administrationsanwendung .....	22
8.4.3	Prüfer .....	23
9	Definition des Sicherheitsproblems .....	23
9.1	Zu schützende Werte (Assets) .....	23
9.1.1	Allgemeines .....	23
9.1.2	Vom EVG geschützte Werte .....	23
9.1.3	Sensible Werte des EVG .....	23
9.2	Benutzer .....	24
9.3	Bedrohungen .....	26
9.4	Organisatorische Sicherheitsvorgaben .....	27
9.4.1	Bereitgestellte Dienste .....	27
9.4.2	Sonstige Dienste .....	27
9.5	Annahmen .....	28
10	Sicherheitsziele .....	29
10.1	Allgemeines .....	29
10.2	Sicherheitsziele für den EVG .....	30
10.2.1	Bereitgestellter Dienst .....	30
10.2.2	Authentisierung gegenüber dem EVG .....	30
10.2.3	EVG-Management .....	30
10.3	Sicherheitsziele für die Einsatzumgebung .....	32
10.4	Begründung für Sicherheitsziele .....	33
11	Erweiterte Komponentendefinition - Definition der Familie FCS_RNG .....	40
12	Sicherheitsanforderungen .....	41
12.1	Allgemeines .....	41
12.2	Einleitung .....	41
12.2.1	Subjekte, Objekte und Sicherheitsattribute .....	41
12.2.2	Operationen .....	42
12.3	Funktionale Sicherheitsanforderungen .....	43
12.3.1	Allgemeines .....	43
12.3.2	Core .....	43
12.3.3	KeyImp .....	51
12.3.4	KeyGen .....	55
12.3.5	Admin .....	58
12.3.6	Nicht vertrauenswürdige CA .....	63
12.3.7	Nicht vertrauenswürdige Administrationsanwendung .....	64
12.4	Vertrauenswürdigkeitsanforderungen .....	65
12.5	SFR/Sicherheitsziele .....	65
12.6	SFR-Abhängigkeiten .....	72
12.7	Begründung für die Vertraulichkeitsanforderungen .....	74
	Literaturhinweise .....	76
	Stichwortverzeichnis .....	77

Bilder

<b>Bild 1 -- EVG Sicherheitsmerkmale .....</b>	<b>13</b>
<b>Bild 2 -- Umgebung der Personalisierungsanwendung .....</b>	<b>14</b>
<b>Bild 3 -- Umgebung der Administrationsanwendung .....</b>	<b>15</b>
<b>Bild 4 -- Umgebung der Authentisierungsanwendung .....</b>	<b>16</b>
<b>Bild 5 -- EVG Lebenszyklus .....</b>	<b>19</b>
<b>Tabellen</b>	
<b>Tabelle 1 -- Schutz sensibler Daten .....</b>	<b>29</b>
<b>Tabelle 2 -- Sicherheitsziele und Problemdefinition .....</b>	<b>34</b>
<b>Tabelle 3 -- Sicherheitsattribute .....</b>	<b>42</b>
<b>Tabelle 4 -- Core-Sicherheitsattribute .....</b>	<b>46</b>
<b>Tabelle 5 -- Core-Sicherheitsattribute .....</b>	<b>46</b>
<b>Tabelle 6 -- Core-Sicherheitsattribute - Operationen .....</b>	<b>47</b>
<b>Tabelle 7 -- Core-Sicherheitsattribute - Anfangswert .....</b>	<b>48</b>
<b>Tabelle 8 -- Core-Sicherheitsattribute - Aktualisierungen .....</b>	<b>49</b>
<b>Tabelle 9 -- TSF-Daten - Aktualisierungen .....</b>	<b>50</b>
<b>Tabelle 10 -- KeyImp-Sicherheitsattribute .....</b>	<b>52</b>
<b>Tabelle 11 -- KeyImp-Sicherheitsattribute - Operationen .....</b>	<b>52</b>
<b>Tabelle 12 -- KeyImp-Sicherheitsattribute - Aktualisierung der autorisierten Rollen .....</b>	<b>54</b>
<b>Tabelle 13 -- KeyImp-Sicherheitsattribute - Aktualisierung der Werte .....</b>	<b>54</b>
<b>Tabelle 14 -- KeyGen-Operationen .....</b>	<b>56</b>
<b>Tabelle 15 -- KeyGen-Sicherheitsattribute .....</b>	<b>56</b>
<b>Tabelle 16 -- Regeln für KeyGen-Operationen .....</b>	<b>56</b>
<b>Tabelle 17 -- KeyGen-Sicherheitsattribute - Aktualisierung der autorisierten Rollen .....</b>	<b>57</b>
<b>Tabelle 18 -- KeyGen-Sicherheitsattribute - Anfangswerte .....</b>	<b>57</b>
<b>Tabelle 19 -- KeyGen-Sicherheitsattribute - Aktualisierung der Werte .....</b>	<b>58</b>
<b>Tabelle 20 -- Admin-Sicherheitsattribute - Aktualisierung der autorisierten Rollen .....</b>	<b>61</b>
<b>Tabelle 21 -- Admin-Sicherheitsattribute - Anfangswerte .....</b>	<b>61</b>
<b>Tabelle 22 -- Admin-Sicherheitsattribute - Aktualisierung der Werte .....</b>	<b>62</b>
<b>Tabelle 23 -- Admin-TSF-Daten - Operationen .....</b>	<b>62</b>
<b>Tabelle 24 -- SFR und Sicherheitsziele .....</b>	<b>65</b>
<b>Tabelle 25 -- SFR-Abhängigkeiten .....</b>	<b>72</b>