E DIN EN 419241-2:2017-06 (D/E)

Erscheinungsdatum: 2017-05-19

Vertrauenswürdige Systeme, die Serversignaturen unterstützen - Teil 2: Schutzprofil für qualifizierte Signaturerstellungseinheiten zur Serversignierung; Deutsche und Englische Fassung prEN 419241-2:2017

Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing; German and English version prEN 419241-2:2017

Inhalt

Seite

Einleitung **5**

1 Anwendungsbereich **6**

2 Normative Verweisungen **6**

3 Begriffe, Symbole und Abkürzungen **6**
3.1 Begriffe **6**
3.2 Symbole und Abkürzungen **7**

4 Einleitung **7**
4.1 Allgemeines **7**
4.2 Schutzprofil-Referenz **7**
4.3 Schutzprofil-Übersicht — Europäische Gesetzgebung **7**
4.4 TOE Übersicht **8**
4.4.1 Allgemeines **8**
4.4.2 TOE Typ **9**
4.4.3 TOE Lebenszyklus **10**
4.4.4 Nutzung und wesentliche Sicherheitsmerkmale des TOE **10**
4.4.5 TOE-Umgebung allgemeine Übersicht **11**
4.4.6 Verfügbare nicht TOE-bezogene Hardware/Software/Firmware **11**
4.4.7 Wählbare Festlegung **11**

5 Konformitätsanspruch **12**
5.1 CC Konformitätsanspruch **12**
5.2 PP Anspruch **12**
5.3 Begründung der Konformität **12**
5.4 Konformitätsaussage **12**

6 Definition Sicherheitsproblem **12**
6.1 Werte **12**
6.2 Themen **15**
6.3 Bedrohungen **16**
6.3.1 Allgemeines **16**
6.3.2 Registrierung **16**
6.3.3 Unterzeichner-Verwaltung **17**
6.3.4 Nutzung **17**
6.3.5 System **19**
6.4 Beziehung zwischen Bedrohungen und Werten **20**
6.5 Organisatorische Sicherheitsrichtlinien **21**
6.6 Annahmen **22**

7 Sicherheitsziele **23**
7.1 Allgemeines **23**
7.2 Sicherheitsziele für das TOE **23**
7.2.1 Registrierung **23**
7.2.2 Anwenderverwaltung **24**

7.2.3 Nutzung 24
7.2.4 System 25
7.3 Sicherheitsziele für die Betriebsumgebung 26
7.3.1 Allgemeines 26
7.3.2 Definition Sicherheitsproblem und Sicherheitsziele 28
7.3.3 Begründung für die Sicherheitsziele 33
8 Erweiterte Komponenten Definitionen — Generierung von zufälligen Zahlen (FCS_RNG) 36
9 Sicherheitsanforderungen 37
9.1 Übersicht SFRs 37
9.2 Sicherheitsfunktionsanforderungen 39
9.2.1 Sicherheitsaudit (FAU) 39
9.2.2 Kryptographische Unterstützung (FCS) 40
9.2.3 Anwenderdatenschutz (FDP) 42
9.2.4 Identifizierung und Authentifizierung (FIA) 50
9.2.5 Sicherheitsverwaltung (FMT) 52
9.2.6 Schutz der TSF (FPT) 54
9.2.7 Vertrauenswürdige Pfade/Kanäle (FTP) 55
9.3 Sicherheitsbestätigungsanforderungen 57
10 Begründung 58
10.1 Sicherheitsanforderungen Begründung 58
10.1.1 Sicherheitsanforderungen Abdeckung 58
10.2 SFR-Abhängigkeiten 62
10.2.1 Allgemeines 62
10.2.2 Begründungen für SARs 64
Literaturhinweise 65