DIN CEN/CLC/TS 17880:2023-04 (D)

Schutzprofil für Smart Meter - Mindestsicherheitsanforderungen; Deutsche Fassung CEN/CLC/TS 17880:2022

Inhalt

Seite

Europäisches Vorwort 4

Einleitung 5

1 Anwendungsbereich 6

2 Normative Verweisungen 6

3 Begriffe 6

4 Evaluierungsgegenstand 10

5 Konformitätsansprüche 12

6 Definition des Sicherheitsproblems 12
6.1 Werte 12
6.2 Entitäten und Bedrohungsagenten 13
6.3 Bedrohungen 13
6.3.1 Allgemeines 13
6.3.2 T.NetworkDisclosure - Unbefugte Datenoffenlegung durch Netzzugang 13
6.3.3 T.DirectDisclosure - Unbefugte Datenoffenlegung durch Direktzugang 13
6.3.4 T.NetworkDataMod - Unbefugte Datenveränderung durch Netzzugang 14
6.3.5 T.DirectDataMod - Unbefugte Datenveränderung durch Direktzugang 14
6.3.6 T.Malfunction - Gefährdung von Werten aufgrund einer Fehlfunktion des TOE 14
6.4 Organisatorische Sicherheitsrichtlinien 14
6.4.1 Allgemeines 14
6.4.2 P.Logging - Protokollierung von Sicherheitsereignissen 14
6.4.3 P.Alarms - Alarmierung bei kritischen Ereignissen 15
6.5 Annahmen 15
6.5.1 A.ExternalData - Schutz von Daten außerhalb der TOE-Steuerung 15
6.5.2 A.AuditSupport - Überprüfung der Auditdaten 15
6.5.3 A.InspectionSupport - Prüfung der Integrität von Zählern 15
6.5.4 A.UniqueSubjectIDs – Subjekte haben eindeutige Identifikationsschlüssel 15

7 Sicherheitszielsetzungen 16
7.1 Allgemeines 16
7.2 Sicherheitszielsetzungen für den TOE 16
7.2.1 Allgemeines 16
7.2.2 O.Authorization – Berechtigung für den Zugriff auf TOE-Daten und -Funktionen 16
7.2.3 O.Messages – Nachrichtenschutz 16
7.2.4 O.DataAtRest – Schutz gespeicherter Daten 16
7.2.5 O.Crypto – Zugelassene kryptographische Mechanismen 16
7.2.6 O.Interfaces – Nicht-operative Schnittstellen deaktiviert 17
7.2.7 O.Resilience – Resilienz gegen Ausfälle 17
7.2.8 O.SecureUpdate – Durch digitale Signatur geschützte Updates 17
7.2.9 O.Logging – Protokollierung von Sicherheitsereignissen 17
7.2.10 O.Alarms – Alarme für kritische Ereignisse 17
7.3 Sicherheitszielsetzungen für die Operative Umgebung 17
7.3.1 OE.ExternalData – Schutz von Daten außerhalb der TOE-Steuerung 17
7.3.2 OE.AuditSupport – Überprüfung der Auditdaten 17
7.3.3 OE.InspectionSupport – Prüfungen der Integrität von Zählern 17
7.3.4 OE.UniqueSubjectIDs – Subjekte haben eindeutige Identifikationsschlüssel 18

8 Erweiterte Definitionen der Komponenten 18
8.1 Allgemeines 18
8.2 Alarm bei Sicherheitsereignissen (FAU_ARP.2) 18
8.3 Vertrauenswürdiges Software-Update (FPT_TSU.1) 19
8.4 Grundlegende TSF-Selbstprüfung (FPT_BST.1) 20
8.5 Manipulationsmeldung (FPT_TNN.1) 21
8.6 Generierung von Zufallszahlen (FCS_RNG.1) 22
8.6.1 Verhalten der Familie 22

9 Sicherheitsanforderungen 23
9.1 Typographische Konventionen 23
9.2 SFR-Architektur 23
9.3 Funktionale Sicherheitsanforderungen 26
9.3.1 Kryptographische Unterstützung 26
9.3.2 Schutz der Benutzerdaten 29
9.3.3 Identifizierung und Authentifizierung 37
9.3.4 Schutz der TSF 39
9.3.5 Sicherheitsmanagement 42
9.3.6 Sicherheitsaudit 45
9.4 Sicherheitsgewährleistungsanforderungen 50
9.4.1 Präzisierungen der Sicherheitsgewährleistungsanforderungen 51

10 Begründungen 59
10.1 Begründung für die Sicherheitszielsetzungen 59
10.1.1 Abdeckung der Sicherheitszielsetzungen 59
10.1.2 Angemessene Sicherheitszielsetzungen 60
10.2 Begründung für die Sicherheitsanforderungen 61
10.2.1 Abdeckung der Sicherheitsanforderungen 61
10.2.2 SFR-Abhängigkeiten 65
10.2.3 Begründung für SARs 68

Anhang A (informativ) Zuordnung zu Mindestsicherheitsanforderungen 69

Literaturhinweise 80