

DIN EN 419241-2:2019-05 (D)

Vertrauenswürdige Systeme, die Serversignaturen unterstützen - Teil 2: Schutzprofil für qualifizierte Signaturerstellungseinheiten zur Serversignierung; Deutsche Fassung EN 419241-2:2019

Inhalt	Seite
Europäisches Vorwort.....	4
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.....	7
4.3.1 Europäische Gesetzgebung.....	7
4.4 EVG: Übersicht.....	8
4.4.1 Allgemeines.....	8
4.4.2 EVG-Typ	10
4.4.3 EVG-Lebenszyklus	10
4.4.4 Nutzung und wesentliche Sicherheitsmerkmale des EVG	10
4.4.5 EVG-Umgebung: allgemeine Übersicht.....	11
4.4.6 Verfügbare nicht EVG-bezogene Hardware/Software/Firmware	11
4.4.7 Wählbare Festlegung.....	12
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 Subjekte.....	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.....	18
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 den EVG.....	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
7.4	Definition des Sicherheitsproblems und Sicherheitsziele.....	28
7.5	Begründung für die Sicherheitsziele.....	33
7.5.1	Allgemeines.....	33
7.5.2	Bedrohungen und Ziele	33
7.5.3	Organisatorische Sicherheitsrichtlinien und Ziele	35
7.5.4	Annahmen und Ziele	36
8	Definitionen der erweiterten Komponenten	36
8.1	Klasse FCS: Kryptographische Unterstützung.....	36
8.1.1	Allgemeines.....	36
8.1.2	Generierung von zufälligen Zahlen (FCS_RNG).....	37
9	Sicherheitsanforderungen	38
9.1	Typographische Festlegungen	38
9.2	Subjekte, Objekte und Vorgänge	38
9.3	Übersicht SFRs.....	40
9.4	Sicherheitsfunktionsanforderungen	42
9.4.1	Sicherheitsaudit (FAU)	42
9.4.2	Kryptographische Unterstützung (FCS).....	43
9.4.3	Anwenderdatenschutz (FDP)	45
9.4.4	Identifizierung und Authentifizierung (FIA).....	59
9.4.5	Sicherheitsverwaltung (FMT)	61
9.4.6	Schutz der TSF (FPT)	65
9.4.7	Vertrauenswürdige Pfade/Kanäle (FTP).....	66
9.5	Sicherheitsbestätigungsanforderungen	68
10	Begründung.....	69
10.1	Begründung der Sicherheitsanforderungen	69
10.2	SFR-Abhängigkeiten	74
10.2.1	Allgemeines.....	74
10.3	Begründungen für SARs	76
	Literaturhinweise	77