DIN EN 419241-1:2018-09 (D)

Vertrauenswürdige Systeme, die Serversignaturen unterstützen - Teil 1: Allgemeine Systemsicherheitsanforderungen; Deutsche Fassung EN 419241-1:2018

Inhalt

Seite

Europäisches Vorwort ... 4

Einleitung ... 6

1 Anwendungsbereich ... 7
1.1 Allgemeines ... 7
1.2 Außerhalb des Anwendungsbereichs ... 7
1.3 Zielgruppe ... 8

2 Normative Verweisungen ... 8

3 Begriffe ... 8

4 Symbole und Abkürzungen ... 10

5 Beschreibung vertrauenswürdiger Systeme, die Serversignaturen unterstützen ... 11
5.1 Allgemeines ... 11
5.2 Ziele der Signaturerstellung und der Serversignatur ... 11
5.3 An eine natürliche Person gebundene Signatur oder an eine juristische Person gebundenes Siegel ... 11
5.4 Alleinige Kontrolle Sicherheitsniveaus ... 11
5.5 Serversignaturen im Stapel ... 12
5.6 Signierschlüssel und Verschlüsselungsmodul ... 12
5.7 Authentifizierung des Unterzeichners ... 13
5.7.1 Elektronische Identifizierungsmittel ... 13
5.7.2 Authentifizierungsmechanismus ... 13
5.7.3 Authentifizierungsziel ... 13
5.7.4 Authentifizierungsübertragung an eine externe Partei ... 13
5.8 Signatur-Aktivierungsdaten ... 14
5.9 Signatur-Aktivierungsprotokoll ... 14
5.10 Interaktionskomponente des Unterzeichners ... 15
5.11 Signatur-Aktivierungsmodul ... 15
5.12 Umgebungen ... 16
5.12.1 Eingriffsgeschützte Umgebung ... 16
5.12.2 TSP-geschützte Umgebung ... 16
5.12.3 Umgebung des Unterzeichners ... 16
5.13 Funktionsmodell ... 17
5.13.1 Allgemeines ... 17
5.13.2 Anwendungsbereich der Anforderungen ... 17
5.13.3 Signatur-Aktivierungsmechanismus ... 18
5.13.4 TW4S-Komponenten ... 20

6 Sicherheitsanforderungen ... 21
6.1 Allgemeines ... 21
6.2 Allgemeine Sicherheitsanforderungen (SRG) ... 21
6.2.1 Verwaltung (SRG_M) ... 21
6.2.2 Systeme und Betriebsabläufe (SRG_SO) ... 22
6.2.3 Identifizierung und Authentifizierung (SRG_IA) ... 23
6.2.4 System-Zugriffskontrolle (SRG_SA) ... 24
6.2.5 Schlüsselverwaltung (SRG_KM) ... 24
6.2.6 Prüfung (SRG_AA) ... 27

6.2.7 Archivierung (SRG_AR) **28**
6.2.8 Backup und Wiederherstellung (SRG_BK) **29**
6.3 Kernkomponenten-Sicherheitsanforderungen (SRC) **29**
6.3.1 Signierschlüssel-Einrichtung (SRC_SKS) - Kryptografischer Schlüssel (SRC_ SKS.1) **29**
6.3.2 Unterzeichner-Authentifizierung (SRC_SA) **30**
6.3.3 Erstellung der digitalen Signatur (SRC_DSC) - Verschlüsselungsvorgang (SRC_DSC.1) **30**
6.4 Zusätzliche Sicherheitsanforderungen für SCAL2 (SRA) **30**
6.4.1 Allgemeines **30**
6.4.2 Signatur-Aktivierungsprotokoll und Signatur-Aktivierungsdaten (SRA_SAP) **31**
6.4.3 Signierschlüsselverwaltung (SRA_SKM) **32**

Anhang A (normativ) Anforderungen an elektronische Identifizierungsmittel, Merkmale und Ausführung **34**
A.1 Registrierung **34**
A.1.1 Beantragung und Eintragung **34**
A.1.2 Nachweis und Verifizierung der Identität (natürliche Person) **34**
A.1.3 Nachweis und Verifizierung der Identität (juristische Person) **37**
A.1.4 Verknüpfung von elektronischen Identifizierungsmitteln von natürlichen und juristischen Personen **39**
A.2 Elektronische Identifizierungsmittel und Authentifizierung **40**
A.2.1 Merkmale und Ausführung elektronischer Identifizierungsmittel **40**
A.2.2 Authentifizierungsmechanismus **40**

Literaturhinweise **42**