

E DIN EN 419111-2:2013-03 (E)

Erscheinungsdatum: 2013-03-25

Protection profiles for signature creation and verification application - Signature creation application - Part 2: Core PP; English version prEN 419111-2:2013

Inhalt	Seite
Foreword	5
1 Scope	6
2 Normative references	6
3 Terms and definitions	6
4 Symbols and abbreviations	6
5 TOE overview	7
5.1 TOE Type	7
5.2 TOE Usage	7
5.3 TOE Environment	7
5.3.1 Overview	7
5.3.2 External entities	8
5.3.3 Other Entities	8
5.4 TOE operations	8
5.4.1 Introduction	8
5.4.2 Pre-signature operations	8
5.4.3 Signature computation	8
5.5 TOE-environment operations	9
6 Conformance claims	9
6.1 CC Conformance Claim	9
6.2 PP Claim	9
6.3 Package Claim	9
6.4 Conformance Rationale	9
6.5 Conformance Statement	9
7 Security problem definition	10
7.1 Assets	10
7.1.1 Document	10
7.1.2 Certificate	10
7.1.3 Certificate path	10
7.1.4 Signature policy	10
7.1.5 Signature attribute	10
7.2 Threats	10
7.2.1 T.Document	10
7.2.2 T.Signature_Policy	10
7.2.3 T.Certificate	11
7.2.4 T.Signer_consent	11
7.2.5 T.Digital_Signature	11
7.3 Organisational security policies	11
7.4 Assumptions	11
7.4.1 A.Platform	11
7.4.2 A.SSCD	12
7.4.3 A.Signer	12
7.4.4 A.CSP	12
8 Security objectives	12
8.1 Security objectives for the TOE	12
8.1.1 OT.Signer_Control	12
8.1.2 OT.Document	12
8.1.3 OT.Certificate	12

8.1.4	OT.Signature_Attributes	13
8.1.5	OT.Signature_Policy.....	13
8.1.6	OT.Crypto	13
8.1.7	OT.Sig_Verify	13
8.2	Security objectives for the operational environment.....	13
8.2.1	OE.Platform	13
8.2.2	OE.SSCD	14
8.2.3	OE.SSCD_communication_protected.....	14
8.2.4	OE.Signer_Presence	14
8.2.5	OE.Output_Device	14
8.2.6	OE.Checker.....	14
8.2.7	OE.Signer.....	14
8.2.8	OE.CSP	15
8.3	Rationale for Security objectives	15
9	Extended component definition	16
10	Security requirements	16
10.1	General.....	16
10.2	Security requirements for the TOE	17
10.2.1	Introduction	17
10.3	Security assurance requirements for the TOE	35
10.4	Security Requirement rationales.....	36
10.4.1	Security Functional Requirement rationale	36
10.4.2	Rationale for SFR Dependencies	38
10.4.3	Security Assurance Requirements Rationale.....	40
10.4.4	Security requirements – internal consistency	40
	Bibliography	41
	Index.....	42

Figures

Figure 1 — TOE environment	7
----------------------------------	---

Tables

Table 1 — Rationale for security objectives	15
Table 2 — Subject security attributes.....	17
Table 3 — Object security attributes	17
Table 4 — Operations - attributes conditions and modifications.....	18
Table 5 — Protection of sensitive data.....	21
Table 6 — Signature SFP – Objects and Operations	23
Table 7 — Signature SFP – subjects, objects and attributes	24
Table 8 — Signature operation rules	24
Table 9 — SSCD IFF Operations	25
Table 10 — Driving Application IFF Operations	25
Table 11 — Checker IFF Operations	26

Table 12 — Input device IFF Operations	26
Table 13 — Output device IFF Operations	26
Table 14 — SSCD IFF Operations & attributes	27
Table 15 — SSCD IFF Operations & conditions	27
Table 16 — Driving Application IFF Operations & attributes	27
Table 17 — Driving Application IFF Operations & conditions	28
Table 18 — Checker IFF Operations & attributes	28
Table 19 — Checker IFF Operations & conditions	28
Table 20 — Input device IFF Operations & attributes	29
Table 21 — Input device IFF Operations & conditions	29
Table 22 — Output device IFF Operations & attributes	30
Table 23 — Output device IFF Operations & conditions	30
Table 24 — TOE SAR.....	35
Table 25 — SFR vs Objectives on the TOE.....	36
Table 26 — SFR dependencies	38