

E DIN EN 419111-4:2013-03 (E)

Erscheinungsdatum: 2013-03-25

Protection profiles for signature creation and verification application - Signature verification application - Part 4: Core PP; English version prEN 419111-4:2013

Inhalt	Seite
Foreword	5
1 Scope	6
2 Normative references	6
3 Terms and definitions	6
4 Symbols and abbreviations	6
5 TOE overview	6
5.1 TOE Type	6
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-validation operations	8
5.4.3 Validation operations	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 Validation status	10
7.1.2 Document	10
7.1.3 Signing certificate	10
7.1.4 Root certificate	10
7.1.5 Certification path	10
7.1.6 Signature policy	10
7.1.7 Signature attribute	10
7.2 Threats	11
7.2.1 T.Document	11
7.2.2 T.SignaturePolicy	11
7.2.3 T.Certificate	11
7.2.4 T.RootCertificate	11
7.3 Organisational security policies	11
7.4 Assumptions	11
7.4.1 A.Platform	11
7.4.2 A.Verifier	12
8 Security objectives	12
8.1 Security objectives for the TOE	12
8.1.1 OT.Certificate	12
8.1.2 OT.Certification_Path_Validation	12
8.1.3 OT.Crypto	12
8.1.4 OT.Document	12

8.1.5	OT.Root_Certificate	12
8.1.6	OT.Signature_Policy.....	12
8.2	Security objectives for the operational environment.....	13
8.2.1	OE.Checker.....	13
8.2.2	OE.Output_Device	13
8.2.3	OE.Platform	13
8.2.4	OE.Root_Certificate	13
8.2.5	OE.Verifier	13
8.3	Rationale for Security objectives	14
9	Extended component definition	15
10	Security requirements	15
10.1	Introduction	15
10.1.1	Subjects Objects and security attributes	15
10.1.2	Operations	17
10.2	Security functional requirements.....	20
10.2.1	Security functional requirements for the TOE.....	20
10.3	Security assurance requirements	31
10.4	Requirement rationales	32
10.4.1	SFR / Security objectives.....	32
10.4.2	SFR Dependencies	33
10.4.3	Rationale for the Assurance Requirements	35
10.4.4	SAR Dependencies	35
	Bibliography	37
	Index.....	38

Figures

Figure 1 — Core SVA environment	7
---------------------------------------	---

Tables

Table 1 — Rationale for security objectives	14
Table 2 — Subject security attributes.....	15
Table 3 — Object security attributes	16
Table 4 — Operations — attributes conditions and modifications	17
Table 5 — protection of sensitive data	20
Table 6 — Validation SFP – Objects and Operations.....	21
Table 7 — Validation SFP – Objects and Attributes	22
Table 8 — Verification operation rules	23
Table 9 — Checker IFF Operations	24
Table 10 — Driving application IFF Operations	24
Table 11 — Input device IFF Operations	24
Table 12 — Output device IFF Operations	24

Table 13 — Driving application IFF Operations & attributes	25
Table 14	25
Table 15 — Checker IFF Operations & attributes	25
Table 16 — Checker IO rules	26
Table 17 — Input device Operations & attributes	26
Table 18 — Input device IO rules	26
Table 19 — Output device Operations & attributes	27
Table 20 — Output device operation rules	27
Table 21 — TOE SAR.....	31
Table 22 — SFR vs Objectives on the TOE.....	32
Table 23 — SFR Dependencies	33
Table 24 — SAR dependencies	35