

# DIN EN 419251-2:2013-06 (En glisch)

## Security requirements for device for authentication - Part 2: Protection profile for extension for trusted channel to certificate generation application

---

<b>Contents</b>		<b>Page</b>
Foreword .....		5
1	Scope .....	6
2	Normative references .....	6
3	Conformance .....	6
3.1	CC Conformance Claim .....	6
3.2	PP Claim .....	6
3.3	Package Claim .....	6
3.4	Conformance Rationale .....	6
3.5	Conformance Statement .....	6
4	Terms and definitions .....	7
5	Symbols and abbreviations .....	9
6	Overview of the target of evaluation .....	9
6.1	TOE Type .....	9
6.2	TOE Usage .....	9
6.3	Security Features of the TOE .....	9
6.4	Examples of applications .....	11
6.4.1	E-government .....	11
6.4.2	Multiple applications .....	11
6.5	Required non-TOE Hardware and Software .....	12
6.6	Protection Profile Usage .....	12
7	TOE Environment .....	13
7.1	Overall view .....	13
7.2	Personalisation application .....	14
7.2.1	General .....	14
7.2.2	Functionalities .....	14
7.2.3	Communication .....	14
7.3	Administration application .....	15
7.3.1	General .....	15
7.3.2	Functionalities .....	15
7.3.3	Communication .....	15
7.4	Authentication application .....	16
7.4.1	General .....	16
7.4.2	Functionalities .....	16
7.4.3	Communication .....	16
7.5	Verifier .....	17
7.5.1	Functionalities .....	17
7.5.2	Communication .....	17
7.6	Key Generator .....	17
7.6.1	Functionalities .....	17
7.6.2	Communication .....	17
7.7	Certification Authority .....	18
7.7.1	Functionalities .....	18
7.7.2	Communication .....	18

8	Life Cycle .....	19
8.1	Overview .....	19
8.2	Pre-Personalisation phase .....	20
8.3	Personalisation phase .....	20
8.3.1	General .....	20
8.3.2	Personalisation application .....	21
8.4	Usage phase .....	21
8.4.1	Authentication application .....	21
8.4.2	Administration application .....	22
8.4.3	Verifier .....	23
9	Security problem definition .....	23
9.1	Assets .....	23
9.1.1	General .....	23
9.1.2	Assets protected by the TOE .....	23
9.1.3	Sensitive assets of the TOE .....	23
9.2	Users .....	24
9.3	Threats .....	25
9.4	Organisational security policies .....	27
9.4.1	Provided services .....	27
9.4.2	Other services .....	27
9.5	Assumptions .....	28
10	Security objectives .....	29
10.1	General .....	29
10.2	Security objectives for the TOE .....	29
10.2.1	Provided service .....	29
10.2.2	Authentication to the TOE .....	29
10.2.3	TOE management .....	30
10.3	Security objectives for the operational environment .....	31
10.4	Rationale for Security objectives .....	33
11	Extended component definition - Definition of the Family FCS_RNG .....	38
12	Security requirements .....	39
12.1	General .....	39
12.2	Introduction .....	40
12.2.1	Subjects Objects and security attributes .....	40
12.2.2	Operations .....	40
12.3	Security functional requirements .....	41
12.3.1	General .....	41
12.3.2	Core .....	41
12.3.3	KeyImp .....	49
12.3.4	KeyGen .....	52
12.3.5	Admin .....	55
12.3.6	Untrusted CA .....	59
12.3.7	Untrusted AdminAppli .....	60
12.4	Security assurance requirements .....	61
12.5	SFR / Security objectives .....	61
12.6	SFR Dependencies .....	67
12.7	Rationale for the Assurance Requirements .....	69
	Bibliography .....	70
	Index .....	71
	Figures Figure 1 -- TOE Security Features .....	13
	Figure 2 -- Personalisation application environment .....	14
	Figure 3 -- Administration application environment .....	15

Figure 4 -- Authentication application environment .....	16
Figure 5 -- TOE Life Cycle .....	19
Tables Table 1 -- protection of sensitive data .....	29
Table 2 -- Security objectives vs problem definition rationale .....	34
Table 3 -- Security attributes .....	40
Table 4 -- Core security attributes .....	44
Table 5 -- Core operations .....	44
Table 6 -- Core security attributes - operation .....	46
Table 7 -- Core security attributes - initial value .....	46
Table 8 -- Core security attributes - updates .....	47
Table 9 -- TSF data - updates .....	47
Table 10 -- KeyImp security attributes .....	49
Table 11 -- KeyImp security attributes - operations .....	50
Table 12 -- KeyImp security attributes - update authorised roles .....	51
Table 13 -- KeyImp security attributes - update values .....	52
Table 14 -- KeyGen operations .....	53
Table 15 -- KeyGen security attributes .....	53
Table 16 -- KeyGen operation rules .....	54
Table 17 -- KeyGen security attributes - update authorised roles .....	54
Table 18 -- KeyGen security attributes - initial values .....	55
Table 19 -- KeyGen security attributes - update values .....	55
Table 20 -- Admin security attributes - update authorised roles .....	58
Table 21 -- Admin security attributes - initial values .....	58
Table 22 -- Admin security attributes - update values .....	58
Table 23 -- Admin TSF data - operations .....	59
Table 24 -- SFR vs Security objectives rationale .....	62
Table 25 -- SFR dependencies .....	67