DIN EN 419251-3:2013-06 (E)

Security requirements for device for authentication - Part 3: Additional functionality for security targets

Contents

Page

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 7

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 10
6.4 Required non-TOE Hardware and Software 10
6.5 Protection Profile Usage 10
6.6 Groups 10
6.6.1 General 10
6.6.2 Main groups 10
6.6.3 Environment groups 11
6.7 Configurations 13
6.7.1 General 13
6.7.2 Rules 13
6.7.3 Possible Configurations 14
6.8 TOE Environment 15
6.8.1 Overall view 15
6.8.2 Personalisation application 16
6.8.3 Administration application 17
6.8.4 Authentication application 18
6.8.5 Verifier 19
6.8.6 Key Generator 19
6.8.7 Certification Authority 20
6.8.8 Examples of applications 20
6.9 Life Cycle 22
6.9.1 Overview 22
6.9.2 Pre-Personalisation phase 23
6.9.3 Personalisation phase 23
6.9.4 Usage phase 24

7 Security problem definition 26
7.1 Assets 26
7.1.1 General 26
7.1.2 Core group 26
7.1.3 KeyGen group 26

7.1.4 Admin group 27
7.2 Users 27
7.2.1 Core group 27
7.2.2 KeyImp group 28
7.2.3 KeyGen group 28
7.2.4 Admin group 28
7.3 Threats 28
7.3.1 General 28
7.3.2 Core group 29
7.3.3 KeyGen group 30
7.3.4 Admin group 30
7.4 Organisational security policies 30
7.4.1 Core group 30
7.4.2 KeyGen group 31
7.4.3 Admin group 31
7.5 Assumptions 31
7.5.1 Core group 31
7.5.2 KeyGen group 32
7.5.3 Admin group 32

8 Security objectives 32
8.1 General - Transfer of sensitive data 32
8.2 Security objectives for the TOE 33
8.2.1 Core group 33
8.2.2 KeyImp group 34
8.2.3 KeyGen group 34
8.2.4 Admin group 34
8.2.5 Untrusted PersoAppli 35
8.2.6 Untrusted AuthAppli 35
8.2.7 Untrusted Verifier 35
8.2.8 Untrusted CA 35
8.2.9 Untrusted AdminAppli 35
8.3 Security objectives for the operational environment 36
8.3.1 Core group 36
8.3.2 KeyImp group 36
8.3.3 Admin group 37
8.3.4 Trusted PersoAppli 37
8.3.5 Trusted AuthAppli 37
8.3.6 Trusted Verifier 37
8.3.7 Trusted CA 37
8.3.8 Trusted AdminAppli 37
8.4 Rationale for Security objectives 38

9 Extended component definition - Definition of the Family FCS_RNG 43

10 Security requirements 43
10.1 General 43
10.2 Introduction 44
10.2.1 Subjects Objects and security attributes 44
10.2.2 Operations 45
10.3 Security functional requirements 46
10.3.1 General 46
10.3.2 Core group 47
10.3.3 KeyImp group 55
10.3.4 KeyGen group 58
10.3.5 Admin group 61
10.3.6 Untrusted PersoAppli 65
10.3.7 Untrusted AuthAppli 66
10.3.8 Untrusted Verifier 66
10.3.9 Untrusted CA 67
10.3.10 Untrusted AdminAppli 68
10.4 Security assurance requirements 68

10.5 SFR / Security objectives 69
10.6 SFR Dependencies 74
10.7 Rationale for the Assurance Requirements 76

Bibliography 78

Index 79

Figures Figure 1 -- TOE Security Features 15

Figure 2 -- Personalisation application environment 16

Figure 3 -- Administration application environment 17

Figure 4 -- Authentication application environment 18

Figure 5 -- TOE Life Cycle 22

Tables Table 1 -- Basic configurations 14

Table 2 -- IdTrusted configurations 14

Table 3 -- Protection of sensitive data 33

Table 4 -- Security objectives vs problem definition rationale 38

Table 5 -- Security attributes 45

Table 6 -- Core security attributes 50

Table 7 -- Core operations 50

Table 8 -- Core security attributes - Operation 51

Table 9 -- Core security attributes - initial value 52

Table 10 -- Core security attributes - Updates 53

Table 11 -- TSF data - updates 53

Table 12 -- KeyImp security attributes 55

Table 13 -- KeyImp security attributes - operations 56

Table 14 -- KeyImp security attributes - update authorised roles 57

Table 15 -- KeyImp security attributes - update values 58

Table 16 -- KeyGen operations 59

Table 17 -- KeyGen security attributes 59

Table 18 -- KeyGen operation rules 60

Table 19 -- KeyGen security attributes - update authorised roles 60

Table 20 -- KeyGen security attributes - initial values 61

Table 21 -- KeyGen security attributes - update values 61

Table 22 -- Admin security attributes - update authorised roles 64

Table 23 -- Admin security attributes - initial values 64

Table 24 -- Admin security attributes - update values 64

Table 25 -- Admin TSF data - operations 65

Table 26 -- SFR vs Security objectives retionale 69

Table 27 -- SFR dependencies 74