DIN EN 419251-1:2013-05 (E)

Security requirements for device for authentication - Part 1: Protection profile for core functionality

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 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 10
6.4.1 E-government 10
6.4.2 Multiple applications 11
6.5 Required non-TOE Hardware and Software 11
6.6 Protection Profile Usage 11

7 TOE Environment 12
7.1 Overall view 12
7.2 Personalisation application 13
7.2.1 General 13
7.2.2 Functionalities 13
7.2.3 Communication 13
7.3 Authentication application 14
7.3.1 General 14
7.3.2 Functionalities 14
7.3.3 Communication 14
7.4 Verifier 15
7.4.1 Functionalities 15
7.4.2 Communication 15
7.5 Key Generator 15
7.5.1 Functionalities 15
7.5.2 Communication 15
7.6 Certification Authority Functionalities 15

8 Life Cycle 16
8.1 Overview 16
8.2 Pre-Personalisation phase 17
8.3 Personalisation phase 18
8.3.1 General 18
8.3.2 Personalisation application 18

8.4 Usage phase Authentication application 18
8.4.1 General 18
8.4.2 Verifier 19

9 Security problem definition 19
9.1 Assets 19
9.1.1 General 19
9.1.2 Assets protected by the TOE 19
9.1.3 Sensitive assets of the TOE 19
9.2 Users 20
9.3 Threats 21
9.4 Organisational security policies 22
9.4.1 Provided services 22
9.4.2 Other services 22
9.5 Assumptions 23

10 Security objectives 24
10.1 General 24
10.2 Security objectives for the TOE 24
10.2.1 Provided service 24
10.2.2 Authentication to the TOE 24
10.2.3 TOE management 24
10.3 Security objectives for the operational environment 25
10.4 Rationale for Security objectives 26

11 Extended component definition 30

12 Security requirements 30
12.1 General 30
12.2 Introduction 31
12.2.1 Subjects Objects and security attributes 31
12.2.2 Operations 31
12.3 Security functional requirements 32
12.3.1 General 32
12.3.2 Core 32
12.3.3 KeyImp 40
12.4 Security assurance requirements 43
12.5 SFR / Security objectives 43
12.6 SFR Dependencies 46
12.7 Rationale for the Assurance Requirements 48
12.7.1 EAL.4 methodically designed, tested, and reviewed 48
12.7.2 AVA_VAN.5 Advanced methodical vulnerability analysis 48
12.7.3 ALC_DVS.2 Sufficiency of security measures 48

Bibliography 49

Index 50

Figures Figure 1 -- TOE Security Features 12

Figure 2 -- Personalisation application environment 13

Figure 3 -- Authentication application environment 14

Figure 4 -- TOE Life Cycle 16

Tables Table 1 -- Protection of sensitive data 24

Table 2 -- Security objectives vs problem definition rationale 27

Table 3 -- Security attributes 31

Table 4 -- Core security attributes 35

Table 5 -- Core operations 35

Table 6 -- Core security attributes - Operation 36

Table 7 -- Core security attributes - Initial value 37

Table 8 -- Core security attributes - updates 38

Table 9 -- TSF data - Updates 38

Table 10 -- KeyImp security attributes 40

Table 11 -- KeyImp security attributes - operations 41

Table 12 -- KeyImp security attributes - update authorised roles 42

Table 13 -- KeyImp security attributes - Update values 43

Table 14 -- SFR vs Security objectives retionale 44

Table 15 -- SFR dependencies 46