DIN EN 419221-5:2018-07 (E)

Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services; English version EN 419221-5:2018

Contents Page

European foreword ... 5

Introduction ... 6

1 Scope ... 7

2 Normative references ... 7

3 Terms and definitions ... 8
3.1 Terms and definitions ... 8
3.2 Abbreviations ... 9

4 Protection Profile ... 9
4.1 General ... 9
4.2 Protection Profile Reference ... 10
4.3 Protection Profile Overview ... 10
4.3.1 General ... 10
4.3.2 EU Qualified Electronic Signature / Seal Creation Device ... 11
4.4 TOE Overview ... 11
4.4.1 TOE type ... 11
4.4.2 Usage and major security features of the TOE ... 18
4.4.3 Available non-TOE hardware/software/firmware ... 19

5 Conformance Claim ... 19
5.1 CC Conformance Claim ... 19
5.2 PP Claim ... 19
5.3 Conformance Rationale ... 19
5.4 Conformance Statement ... 20

6 Security Problem Definition ... 20
6.1 Assets ... 20
6.2 Subjects ... 20
6.3 Threats ... 20
6.3.1 General ... 20
6.3.2 T.KeyDisclose — Unauthorised disclosure of secret/private key ... 21
6.3.3 T.KeyDerive — Derivation of secret/private key ... 21
6.3.4 T.KeyMod — Unauthorised modification of a key ... 21
6.3.5 T.KeyMisuse — Misuse of a key ... 21
6.3.6 T.KeyOveruse — Overuse of a key ... 21
6.3.7 T.DataDisclose — Disclosure of sensitive client application data ... 21
6.3.8 T.DataMod — Unauthorised modification of client application data ... 21
6.3.9 T.Malfunction — Malfunction of TOE hardware or software ... 22
6.4 Organisational Security Policies ... 22
6.4.1 P.Algorithms — Use of approved cryptographic algorithms ... 22
6.4.2 P.KeyControl — Support for control of keys ... 22
6.4.3 P.RNG — Random Number Generation ... 22
6.4.4 P.Audit — Audit trail generation ... 23
6.5 Assumptions ... 23
6.5.1 A.ExternalData — Protection of data outside TOE control ... 23
6.5.2 A.Env — Protected operating environment ... 23
6.5.3 A.DataContext — Appropriate use of TOE functions ... 23

6.5.4 A.UAuth — Authentication of application users 24
6.5.5 A.AuditSupport — Audit data review 24
6.5.6 A.AppSupport — Application security support 24

7 Security Objectives 24
7.1 General 24
7.2 Security Objectives for the TOE 24
7.2.1 General 24
7.2.2 OT.PlainKeyConf — Protection of confidentiality of plaintext secret keys 24
7.2.3 OT.Algorithms — Use of approved cryptographic algorithms 24
7.2.4 OT.KeyIntegrity — Protection of integrity of keys 25
7.2.5 OT.Auth — Authorization for use of TOE functions and data 25
7.2.6 OT.KeyUseConstraint — Constraints on use of keys 25
7.2.7 OT.KeyUseScope — Defined scope for use of a key after authorization 25
7.2.8 OT.DataConf — Protection of confidentiality of sensitive client application data 26
7.2.9 OT.DataMod — Protection of integrity of client application data 26
7.2.10 OT.ImportExport — Secure import and export of keys 26
7.2.11 OT.Backup — Secure backup of user data 26
7.2.12 OT.RNG — Random number quality 27
7.2.13 OT.TamperDetect — Tamper Detection 27
7.2.14 OT.FailureDetect — Detection of TOE hardware or software failures 27
7.2.15 OT.Audit — Generation of audit trail 27
7.3 Security Objectives for the Operational Environment 27
7.3.1 General 27
7.3.2 OE.ExternalData — Protection of data outside TOE control 27
7.3.3 OE.Env — Protected operating environment 28
7.3.4 OE.DataContext — Appropriate use of TOE functions 28
7.3.5 OE.Uauth — Authentication of application users 28
7.3.6 OE.AuditSupport — Audit data review 28
7.3.7 OE.AppSupport — Application security support 29

8 Extended Components Definitions 29
8.1 Generation of random numbers (FCS_RNG) 29
8.1.1 General 29
8.1.2 Family behaviour 29
8.1.3 Component levelling 29
8.2 Basic TSF Self Testing (FPT_TST_EXT.1) 30
8.2.1 General 30
8.2.2 Family behaviour 30
8.2.3 Component levelling 30

9 Security Requirements 31
9.1 General 31
9.2 Typographical Conventions 31
9.3 SFR Architecture 31
9.3.1 SFR Relationships 31
9.3.2 SFRs and the Key Lifecycle 33
9.4 Security Functional Requirements 35
9.4.1 General 35
9.4.2 Cryptographic Support (FCS) 35
9.4.3 Identification and authentication (FIA) 38
9.4.4 User data protection (FDP) 41
9.4.5 Trusted path/channels (FTP) 47
9.4.6 Protection of the TSF (FPT) 49
9.4.7 Security management (FMT) 51

9.4.8 Security audit data generation (FAU) **58**
9.5 Security Assurance Requirements **60**
9.5.1 General **60**
9.5.2 Refinements of Security Assurance Requirements **61**
10 Rationales **65**
10.1 Security Objectives Rationale **65**
10.1.1 Security Objectives Coverage **65**
10.1.2 Security Objectives Sufficiency **66**
10.2 Security Requirements Rationale **68**
10.2.1 Security Requirements Coverage **68**
10.2.2 SFR Dependencies **70**
10.2.3 Rationale for SARs **72**
10.2.4 AVA_VAN.5 Advanced methodical vulnerability analysis **73**
Annex A (informative) **Mapping to Regulation (EU) 910/2014** **74**
Bibliography **79**

Tables

Table 1 — Key Attributes Modification Table **56**
Table 2 — Key Attributes Initialisation Table [82] **57**
Table 3 — Security Assurance Requirements **61**
Table 4 — Security Problem Definition mapping to Security Objectives **66**
Table 5 — TOE Security Objectives mapping to SFRs **68**
Table 6 — SFR Dependencies Rationale **71**
Table A.1— Mapping between [Regulation, Annex II] and this PP **74**

Figures

Figure 1 — Generic TOE Architecture **12**
Figure 2 — Generation of Random numbers - Component Levelling **29**
Figure 3 — Basic TSF Self Testing – Component Levelling **30**
Figure 4 — Architecture of Key Protection SFRs **32**
Figure 5 — Architecture of User, TSF Protection and Audit SFRs **33**
Figure 6 — Generic Key Lifecycle and Related SFRs **34**