DIN CEN/TS 419221-4:2016-10 (E)

Protection Profiles for TSP cryptographic modules - Part 4: Cryptographic m odule for CSP signing operations without backup; English version CEN/TS 419221-4:2016

Contents

Page

European foreword ... 4

Introduction ... 5

1 Scope ... 6

2 Normative references ... 6

3 Terms and definitions ... 6

4 PP Introduction ... 6
4.1 General ... 6
4.2 PP Reference ... 6
4.3 Protection Profile Overview ... 7
4.4 TOE Overview ... 8
4.4.1 TOE type ... 8
4.4.2 TOE Roles ... 9
4.4.3 Usage and major security features of the TOE ... 9
4.4.4 Available non-TOE hardware/software/firmware ... 11

5 Conformance Claim ... 11
5.1 CC Conformance Claim ... 11
5.2 PP Claim ... 11
5.3 Conformance Rationale ... 11
5.4 Conformance Statement ... 11

6 Security Problem Definition ... 12
6.1 Assets ... 12
6.1.1 General ... 12
6.1.2 TOE services ... 12
6.1.3 TOE Data ... 12
6.2 Threats ... 13
6.2.1 General ... 13
6.2.2 Threat agents ... 13
6.2.3 Threats description ... 14
6.3 Organizational Security Policies ... 17
6.4 Assumptions ... 17

7 Security Objectives ... 18
7.1 General ... 18
7.2 Security Objectives for the TOE ... 18
7.3 Security Objectives for the Operational Environment ... 20

8 Extended Components Definitions ... 21
8.1 Extended Component Definitions — Family FCS_RND ... 21

9 Security Requirements ... 22
9.1 General ... 22
9.2 Subjects, objects, security attributes and operations ... 22
9.2.1 General ... 22
9.2.2 Subjects ... 22
9.2.3 TOE Objects and security attributes ... 23
9.2.4 TOE Operations ... 23

9.3 Security Functional Requirements 24
9.3.1 General 24
9.3.2 Security audit (FAU) 24
9.3.3 Cryptographic support (FCS) 25
9.3.4 User data protection (FDP) 27
9.3.5 Identification and authentication (FIA) 29
9.3.6 Security management (FMT) 30
9.3.7 Privacy (FPR) — Unobservability (FPR_UNO.1) 32
9.3.8 Protection of the TOE Security Functions (FPT) 32
9.3.9 Trusted path (FTP) — Trusted path (FTP_TRP.1) 35
9.4 Security Assurance Requirements 35
9.5 Security Requirements Rationale 36
9.5.1 Security Problem Definition coverage by Security Objectives 36
9.5.2 Security Objectives coverage by SFRs 41
9.5.3 SFR Dependencies 45
9.5.4 Rationale for SARs 46
9.5.5 AVA_VAN.5 Advanced methodical vulnerability analysis 46

Bibliography 47