

DIN CEN/TS 419221-2:2016-10 (E)

Protection Profiles for TSP cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup; English version CEN/TS 419221-2:2016

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	12
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.....	14
6.2.1 General.....	14
6.2.2 Threat agents.....	14
6.2.3 Threats description	15
6.2.4 Threats vs Threat agents.....	17
6.3 Organizational Security Policies.....	18
6.4 Assumptions.....	18
7 Security Objectives	19
7.1 General.....	19
7.2 Security Objectives for the TOE.....	19
7.3 Security Objectives for the Operational Environment	21
8 Extended Components Definitions	22
8.1 Extended Component Definitions	22
8.1.1 Family FCS_RND	22
8.1.2 Family FDP_BKP.....	23
9 Security Requirements.....	25
9.1 General.....	25
9.2 Subjects, objects, security attributes and operations	25
9.2.1 General.....	25

9.2.2	Subjects	25
9.2.3	TOE Objects and security attributes	25
9.2.4	TOE Operations	26
9.3	Security Functional Requirements.....	27
9.3.1	General	27
9.3.2	Security audit (FAU)	27
9.3.3	Cryptographic support (FCS).....	29
9.3.4	User data protection (FDP)	31
9.3.5	Identification and authentication (FIA)	35
9.3.6	Security management (FMT)	36
9.3.7	Privacy (FPR).....	37
9.3.8	Protection of the TOE Security Functions (FPT).....	39
9.3.9	Trusted path (FTP) — Trusted path (FTP_TRP.1)	42
9.4	Security Assurance Requirements	42
9.5	Security Requirements Rationale.....	43
9.5.1	Security Problem Definition coverage by Security Objectives.....	43
9.5.2	Security Objectives coverage by SFRs	49
9.5.3	SFR Dependencies	54
9.5.4	Rationale for SARs.....	54
9.5.5	AVA_VAN.5 Advanced methodical vulnerability analysis	54
	Bibliography	55