

DIN CEN/TS 419221-3:2016-10 (E)

Protection Profiles for TSP Cryptographic modules - Part 3: Cryptographic module for CSP key generation services; English version CEN/TS 419221-3:2016

Contents	Page
European foreword.....	3
0 Introduction.....	4
0.1 General.....	4
0.2 Document Structure.....	5
1 Scope.....	6
2 Normative references.....	6
3 Terms and definitions	6
4 General.....	6
4.1 PP reference.....	6
4.2 TOE overview.....	6
4.2.1 TOE usage and major security features	6
4.2.2 TOE type	8
4.2.3 Available non-TOE hardware/firmware/software.....	8
5 Conformance Claims	8
5.1 CC conformance claim	8
5.2 PP claim	9
5.3 Conformance rationale	9
5.4 Conformance statement.....	9
6 Security Problem Definition.....	9
6.1 TOE assets	9
6.2 Threats	10
6.3 Organizational security policies	12
6.4 Assumptions.....	13
7 Security Objectives	13
7.1 General.....	13
7.2 Security objectives for the TOE	13
7.3 Security objectives for the operational environment.....	15
7.4 Security objectives rationale	16
8 Security Requirements.....	21
8.1 Security functional requirements	21
8.1.1 Subjects, objects, security attributes and operations	21
8.1.2 Security requirements operations.....	22
8.1.3 Security Audit (FAU)	23
8.1.4 Cryptographic Support (FCS)	24
8.1.5 User Data Protection (FDP)	25
8.1.6 Identification and Authentication (FIA)	28
8.1.7 Security Management (FMT).....	29
8.1.8 Privacy (FPR)	30
8.1.9 Protection of the TSF (FPT)	31
8.1.10 Trusted path/channels (FTP)	33
8.2 Security assurance requirements	33
8.3 Security requirements rationale	34
8.3.1 Security functional requirements rationale.....	34
8.3.2 Security assurance requirements rationale.....	40
Bibliography.....	41