DIN EN 419231:2017-04 (E)

Protection Profile for trustworthy systems supporting time stamping; English version prEN 419231:2017

Contents

Page

European foreword ... 4

Introduction ... 5

1 Scope ... 6

2 Normative references ... 6

3 Terms and definitions ... 6
3.1 Definitions ... 6
3.2 Abbreviations ... 11

4 Introduction ... 12
4.1 PP reference ... 12
4.2 TOE overview ... 12
4.2.1 TOE type ... 12
4.2.2 TOE usage and major security features ... 12
4.2.3 TOE Environment general overview ... 16
4.2.4 Required non-TOE hardware/software/firmware ... 17

5 Conformance claims ... 18
5.1 CC conformance claim ... 18
5.2 PP claim ... 18
5.3 Conformance rationale ... 18
5.4 Conformance statement ... 18

6 Security problem definition ... 18
6.1 TOE assets ... 18
6.2 Threats ... 21
6.2.1 General ... 21
6.2.2 Relation between threats and assets ... 23
6.3 Organisational security policies ... 23
6.4 Assumptions ... 24

7 Security objectives ... 26
7.1 General ... 26
7.2 Security objectives for the TOE ... 26
7.3 Security objectives for the operational environment ... 27
7.4 Security objectives rationale ... 30

8 Security functional requirements ... 36
8.1 General ... 36
8.2 Subjects, objects, operations and security attributes ... 36
8.2.1 Subjects ... 36
8.2.2 Objects ... 37
8.2.3 Operations ... 37
8.2.4 Security attributes ... 37

8.3 Security requirements operations **39**
8.4 User Data Protection (FDP) **39**
8.5 Security Management (FMT) **46**
8.6 Protection of the TSF (FPT) **49**
8.7 Trusted Path/Channels (FTP) **49**
8.8 Cryptographic Support (FCS) **50**
8.9 Identification and Authentication (FIA) **51**
8.10 Security Audit (FAU) **51**

9 Security assurance requirements **52**

10 Security requirements rationale **53**
10.1 Security functional requirements rationale **53**
10.1.1 SFR dependencies rationale **53**
10.1.2 SFR vs TOE security objectives rationale **56**
10.2 Security assurance requirements rationale **59**
10.2.1 General **59**
10.2.2 Assurance level table **60**
10.2.3 EAL rationale **61**

Annex A (informative) **Revision History** **62**

Annex B (informative) **Document structure** **63**

Bibliography **64**