

DIN EN 419241-2:2019-05 (E)

Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing

| Contents | | Page |
|-------------------------|---|-------------|
| EUROPEAN FOREWORD | | 4 |
| INTRODUCTION | | 5 |
| 1 | SCOPE | 6 |
| 2 | NORMATIVE REFERENCES | 6 |
| 3 | TERMS, DEFINITIONS, SYMBOLS AND ABBREVIATIONS | 6 |
| 3.1 | TERMS AND DEFINITIONS | 6 |
| 3.2 | SYMBOLS AND ABBREVIATIONS | 7 |
| 4 | INTRODUCTION | 7 |
| 4.1 | GENERAL | 7 |
| 4.2 | PROTECTION PROFILE REFERENCE | 7 |
| 4.3 | PROTECTION PROFILE OVERVIEW | 7 |
| 4.4 | TOE OVERVIEW | 7 |
| 5 | CONFORMANCE CLAIM | 11 |
| 5.1 | CC CONFORMANCE CLAIM | 11 |
| 5.2 | PP CLAIM | 12 |
| 5.3 | CONFORMANCE RATIONALE | 12 |
| 5.4 | CONFORMANCE STATEMENT | 12 |
| 6 | SECURITY PROBLEM DEFINITION | 12 |
| 6.1 | ASSETS | 12 |
| 6.2 | SUBJECTS | 14 |
| 6.3 | THREATS | 15 |
| 6.4 | RELATION BETWEEN THREATS AND ASSETS | 18 |
| 6.5 | ORGANISATIONAL SECURITY POLICIES | 19 |
| 6.6 | ASSUMPTIONS | 20 |
| 7 | SECURITY OBJECTIVES | 21 |
| 7.1 | GENERAL | 21 |
| 7.2 | SECURITY OBJECTIVES FOR THE TOE | 21 |
| 7.3 | SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT | 23 |
| 7.4 | SECURITY PROBLEM DEFINITION AND SECURITY OBJECTIVES | 25 |
| 7.5 | RATIONALE FOR THE SECURITY OBJECTIVES | 30 |
| 8 | EXTENDED COMPONENTS DEFINITIONS | 33 |
| 8.1 | CLASS FCS: CRYPTOGRAPHIC SUPPORT | 33 |
| 9 | SECURITY REQUIREMENTS | 34 |
| 9.1 | TYPOGRAPHICAL CONVENTIONS | 34 |
| 9.2 | SUBJECTS, OBJECTS AND OPERATIONS | 35 |
| 9.3 | SFRS OVERVIEW | 36 |
| 9.4 | SECURITY FUNCTIONAL REQUIREMENTS | 39 |
| 9.5 | SECURITY ASSURANCE REQUIREMENTS | 64 |
| 10 | RATIONALE | 65 |

| | | |
|------|---------------------------------------|----|
| 10.1 | SECURITY REQUIREMENTS RATIONALE | 65 |
| 10.2 | SFR DEPENDENCIES | 72 |
| 10.3 | RATIONALES FOR SARS | 74 |
| | BIBLIOGRAPHY | 75 |