

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

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

---

| <b>Contents</b>  | <b>Page</b> |
|--|-------------|
| 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          |

|              |  |           |
|--------------|--|-----------|
| <b>9.3</b>   | <b>Security Functional Requirements</b> .....                            | <b>24</b> |
| <b>9.3.1</b> | <b>General</b> .....   | <b>24</b> |
| <b>9.3.2</b> | <b>Security audit (FAU)</b> .....  | <b>24</b> |
| <b>9.3.3</b> | <b>Cryptographic support (FCS)</b> .....                                 | <b>25</b> |
| <b>9.3.4</b> | <b>User data protection (FDP)</b> .....                                  | <b>27</b> |
| <b>9.3.5</b> | <b>Identification and authentication (FIA)</b> .....                     | <b>29</b> |
| <b>9.3.6</b> | <b>Security management (FMT)</b> .....                                   | <b>30</b> |
| <b>9.3.7</b> | <b>Privacy (FPR) — Unobservability (FPR_UNO.1)</b> .....                 | <b>32</b> |
| <b>9.3.8</b> | <b>Protection of the TOE Security Functions (FPT)</b> .....              | <b>32</b> |
| <b>9.3.9</b> | <b>Trusted path (FTP) — Trusted path (FTP_TRP.1)</b> .....               | <b>35</b> |
| <b>9.4</b>   | <b>Security Assurance Requirements</b> .....                             | <b>35</b> |
| <b>9.5</b>   | <b>Security Requirements Rationale</b> .....                             | <b>36</b> |
| <b>9.5.1</b> | <b>Security Problem Definition coverage by Security Objectives</b> ..... | <b>36</b> |
| <b>9.5.2</b> | <b>Security Objectives coverage by SFRs</b> .....                        | <b>41</b> |
| <b>9.5.3</b> | <b>SFR Dependencies</b> .....  | <b>45</b> |
| <b>9.5.4</b> | <b>Rationale for SARs</b> .....  | <b>46</b> |
| <b>9.5.5</b> | <b>AVA_VAN.5 Advanced methodical vulnerability analysis</b> .....        | <b>46</b> |
|              | <b>Bibliography</b> .....  | <b>47</b> |