



BSI Standards Publication

Protection Profiles for TSP Cryptographic Modules

Part 5: Cryptographic Module for Trust Services

National foreword

This British Standard is the UK implementation of EN 419221-5:2018.

The UK participation in its preparation was entrusted to Technical Committee IST/17, Cards and security devices for personal identification.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 95322 4

ICS 35.240.30; 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 May 2018.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

English Version

Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services

Profils de protection pour les modules
cryptographiques de prestataires de services de
confiance - Partie 5: Module cryptographique pour les
services de confiance

Schutzprofile für kryptographische Module von
Vertrauensdiensteanbietern - Teil 5: Kryptographisches
Modul für vertrauenswürdige Dienste

This European Standard was approved by CEN on 2 March 2018.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Contents	Page
European foreword.....	5
Introduction	6
1 Scope	7
2 Normative references	7
3 Terms and definitions	8
3.1 Terms and definitions	8
3.2 Abbreviations	9
4 Protection Profile.....	9
4.1 General.....	9
4.2 Protection Profile Reference.....	10
4.3 Protection Profile Overview.....	10
4.3.1 General.....	10
4.3.2 EU Qualified Electronic Signature / Seal Creation Device	11
4.4 TOE Overview	11
4.4.1 TOE type	11
4.4.2 Usage and major security features of the TOE.....	18
4.4.3 Available non-TOE hardware/software/firmware.....	19
5 Conformance Claim	19
5.1 CC Conformance Claim	19
5.2 PP Claim	19
5.3 Conformance Rationale.....	19
5.4 Conformance Statement	20
6 Security Problem Definition.....	20
6.1 Assets.....	20
6.2 Subjects.....	20
6.3 Threats.....	20
6.3.1 General.....	20
6.3.2 T.KeyDisclose — Unauthorised disclosure of secret/private key	21
6.3.3 T.KeyDerive — Derivation of secret/private key	21
6.3.4 T.KeyMod — Unauthorised modification of a key.....	21
6.3.5 T.KeyMisuse — Misuse of a key.....	21
6.3.6 T.KeyOveruse — Overuse of a key	21
6.3.7 T.DataDisclose — Disclosure of sensitive client application data.....	21
6.3.8 T.DataMod — Unauthorised modification of client application data.....	21
6.3.9 T.Malfunction — Malfunction of TOE hardware or software	22
6.4 Organisational Security Policies.....	22
6.4.1 P.Algorithms — Use of approved cryptographic algorithms.....	22
6.4.2 P.KeyControl — Support for control of keys	22
6.4.3 P.RNG — Random Number Generation	22
6.4.4 P.Audit — Audit trail generation.....	23
6.5 Assumptions.....	23
6.5.1 A.ExternalData — Protection of data outside TOE control	23
6.5.2 A.Env — Protected operating environment.....	23
6.5.3 A.DataContext — Appropriate use of TOE functions	23

6.5.4	A.UAuth — Authentication of application users.....	24
6.5.5	A.AuditSupport — Audit data review	24
6.5.6	A.AppSupport — Application security support	24
7	Security Objectives.....	24
7.1	General	24
7.2	Security Objectives for the TOE.....	24
7.2.1	General	24
7.2.2	OT.PlainKeyConf — Protection of confidentiality of plaintext secret keys	24
7.2.3	OT.Algorithms — Use of approved cryptographic algorithms	24
7.2.4	OT.KeyIntegrity — Protection of integrity of keys	25
7.2.5	OT.Auth — Authorization for use of TOE functions and data	25
7.2.6	OT.KeyUseConstraint — Constraints on use of keys.....	25
7.2.7	OT.KeyUseScope — Defined scope for use of a key after authorization	25
7.2.8	OT.DataConf — Protection of confidentiality of sensitive client application data.....	26
7.2.9	OT.DataMod — Protection of integrity of client application data.....	26
7.2.10	OT.ImportExport — Secure import and export of keys	26
7.2.11	OT.Backup — Secure backup of user data	26
7.2.12	OT.RNG — Random number quality	27
7.2.13	OT.TamperDetect — Tamper Detection.....	27
7.2.14	OT.FailureDetect — Detection of TOE hardware or software failures	27
7.2.15	OT.Audit — Generation of audit trail.....	27
7.3	Security Objectives for the Operational Environment.....	27
7.3.1	General	27
7.3.2	OE.ExternalData — Protection of data outside TOE control	27
7.3.3	OE.Env — Protected operating environment	28
7.3.4	OE.DataContext — Appropriate use of TOE functions.....	28
7.3.5	OE.Uauth — Authentication of application users.....	28
7.3.6	OE.AuditSupport — Audit data review	28
7.3.7	OE.AppSupport — Application security support.....	29
8	Extended Components Definitions.....	29
8.1	Generation of random numbers (FCS_RNG)	29
8.1.1	General	29
8.1.2	Family behaviour	29
8.1.3	Component levelling.....	29
8.2	Basic TSF Self Testing (FPT_TST_EXT.1)	30
8.2.1	General	30
8.2.2	Family behaviour	30
8.2.3	Component levelling.....	30
9	Security Requirements	31
9.1	General	31
9.2	Typographical Conventions	31
9.3	SFR Architecture	31
9.3.1	SFR Relationships	31
9.3.2	SFRs and the Key Lifecycle	33
9.4	Security Functional Requirements.....	35
9.4.1	General	35
9.4.2	Cryptographic Support (FCS).....	35
9.4.3	Identification and authentication (FIA)	38
9.4.4	User data protection (FDP)	41
9.4.5	Trusted path/channels (FTP).....	47
9.4.6	Protection of the TSF (FPT).....	49
9.4.7	Security management (FMT)	51

9.4.8	Security audit data generation (FAU)	58
9.5	Security Assurance Requirements	60
9.5.1	General	60
9.5.2	Refinements of Security Assurance Requirements	61
10	Rationales	65
10.1	Security Objectives Rationale	65
10.1.1	Security Objectives Coverage	65
10.1.2	Security Objectives Sufficiency	66
10.2	Security Requirements Rationale	68
10.2.1	Security Requirements Coverage	68
10.2.2	SFR Dependencies	70
10.2.3	Rationale for SARs	72
10.2.4	AVA_VAN.5 Advanced methodical vulnerability analysis	73
Annex A (informative)	Mapping to Regulation (EU) 910/2014	74
Bibliography		79

Tables

Table 1 — Key Attributes Modification Table	56
Table 2 — Key Attributes Initialisation Table ⁸²	57
Table 3 — Security Assurance Requirements	61
Table 4 — Security Problem Definition mapping to Security Objectives	66
Table 5 — TOE Security Objectives mapping to SFRs	68
Table 6 — SFR Dependencies Rationale	71
Table A.1— Mapping between [Regulation, Annex II] and this PP	74

Figures

Figure 1 — Generic TOE Architecture	12
Figure 2 — Generation of Random numbers - Component Levelling	29
Figure 3 — Basic TSF Self Testing - Component Levelling	30
Figure 4 — Architecture of Key Protection SFRs	32
Figure 5 — Architecture of User, TSF Protection and Audit SFRs	33
Figure 6 — Generic Key Lifecycle and Related SFRs	34

European foreword

This document (EN 419221-5:2018) has been prepared by Technical Committee CEN/TC 224 “Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment”, the secretariat of which is held by AFNOR.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by November 2018, and conflicting national standards shall be withdrawn at the latest by November 2018.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

According to the CEN-CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

Clause 4 provides the introductory material for the Protection Profile.

Clause 5 provides the conformance claim.

Clause 6 provides the Security Problem Definition. It presents the Assets, Threats, Organisational Security Policies and Assumptions related to the TOE.

Clause 7 defines the security objectives for both the TOE and the TOE environment.

Clause 8 presents the extended components that will be used in this PP.

Clause 9 contains the functional requirements and assurance requirements derived from the Common Criteria (CC), Part 2 [CC2] and Part 3 [CC3] that are to be satisfied by the TOE.

Clause 10 provides rationales to demonstrate that:

- Security Objectives satisfy the policies and threats;
- SFR match the security Objectives;
- SFR dependencies are satisfied;
- The SARs are appropriate.

A Bibliography is provided to identify background material.

A Mapping to the EU 'Requirements For Qualified Electronic Signature Creation Devices' is provided in Annex A.

1 Scope

This part of EN 419221 specifies a Protection Profile for cryptographic modules which is intended to be suitable for use by trust service providers supporting electronic signature and electronic sealing operations, certificate issuance and revocation, time stamp operations, and authentication services, as identified by the (EU) No 910/2014 regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Regulation (EU) No 910/2014 eIDAS) in [10]. The Protection Profile also includes optional support for protected backup of keys.

The document follows the rules and conventions laid out in Common Criteria Part 1 [CC1], Annex B “Specification of Protection Profiles”.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 19790:2012, *Information technology — Security techniques — Security requirements for cryptographic modules*

Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model (Version 3.1 Revision 4, September 2012), CCMB-2012-09-001 [CC1]

Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, (Version 3.1 Revision 4, September 2012), CCMB-2012-09-002 [CC2]

Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, (Version 3.1 Revision 4, September 2012), CCMB-2012-09-003 [CC3]

3 Terms and definitions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 419221-1, Common Criteria Part 1 [CC1] and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

3.1.1

assigned key

key (usually a secret key) with the 'Assigned Flag' attribute set to 'assigned', meaning that:

- the 'Re-authorization conditions' and 'Key Usage' attributes cannot be changed;
- the Authorization Data attribute can only be changed by presentation of the current Authorization Data – it cannot be changed or reset by an Administrator;
- the key cannot be imported or exported.

Note 1 to entry: These properties of an Assigned Key support the sole control of a key that is required for secret keys used to create digital signatures.

3.1.2

Authorization Data

data, including data particular to the user, which is used to control access to (and thus use of) a key. Data particular to the user may include data derived from a secret known only by the user, data derived from a device held by the user and/or data derived from biometric features of the user. Other parts of the authorization data may include data held within the cryptographic module, data held by administrator(s) or data provided by the application

3.1.3

electronic seal

data in electronic form which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity

3.1.4

electronic timestamp

data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time

3.1.5

secret key

either a secret key used in symmetric cryptographic functions, or a private key used in asymmetric cryptographic functions

3.1.6**trust service**

electronic service which enhances trust and confidence in electronic transactions

Note 1 to entry: Such trust services are typically but not necessarily using cryptographic techniques or involving confidential material.

3.2 Abbreviations

For the purposes of this document, the abbreviations given in EN 419221-1 and the following apply.

CC	Common Criteria
DTBS	Data To Be Signed
DTBS/R	Data To Be Signed or its unique Representation
EAL	Evaluation Assurance Level
IT	Information Technology
PCIe	Peripheral Component Interconnect Express
PP	Protection Profile
RNG	Random Number Generator
SAR	Security Assurance Requirements
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSP	Trust Service Provider

4 Protection Profile**4.1 General**

This clause provides document management and overview information that is required to carry out Protection Profile registration. 4.2 “PP Reference” gives labelling and descriptive information necessary for registering the Protection Profile (PP). 4.3 “Protection Profile Overview” summarizes the PP in narrative form. 4.4 “TOE Overview” summarizes the TOE in a narrative form. As such, these subclauses give an overview to the potential user to decide whether the PP is of interest.

4.2 Protection Profile Reference

Title	Protection Profiles for TSP Cryptographic Modules – Part 5: Cryptographic Module for Trust Services
CC revision	v3.1 release 4
PP version	1.0
Authors	CEN/TC 224
Keywords	cryptographic module

4.3 Protection Profile Overview

4.3.1 General

This Protection Profile (PP) defines the security requirements for cryptographic modules used by trust service providers supporting electronic signing and sealing operations and authentication services. It includes optional support for protected backup of keys.

The Protection Profile is aimed at supporting trust services providers as identified by the proposed regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (eIDAS) in Regulation (EU) 910/2014 [7].

The Cryptographic Module, which is the Target of Evaluation (TOE), generates and/or protects secret keys and other sensitive data, and allows controlled use of these data for one or more cryptographic services in support of TSP trust services.

This PP is Common Criteria Part 2 [CC2] extended and Common Criteria Part 3 [CC3] conformant. The assurance level for this PP is EAL4, augmented with AVA_VAN.5 (Advanced methodical vulnerability analysis).

4.3.2 EU Qualified Electronic Signature / Seal Creation Device

Cryptographic Modules certified to this PP are intended to meet the security assurance requirements of Qualified Electronic Signature, and Electronic Seal, Creation Devices for use by trust service providers as specified in Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [7], although its use is not necessarily limited to such services. For further information see Annex A.

This Protection Profile is established by CEN for use by trust services including qualified trust services as identified in [7].

4.4 TOE Overview

4.4.1 TOE type

4.4.1.1 General

The TOE is a cryptographic module suitable for use by trust service providers supporting electronic signature and electronic sealing operations, certificate issuance and revocation, time stamp operations, and authentication services (including support of authentication of client applications or authorized users of secret keys, and support of authentication for electronic identification), as identified by the (EU) No 910/2014 regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (eIDAS) in [7]. The TOE may also support protected backup of keys.

The TOE provides cryptographic functions that support trust services but is not, in general, aware of the context in which a cryptographic function is used. Any such context is therefore the responsibility of client applications used by the trust service provider, and these client applications need to use the cryptographic functions in an appropriate way. In general this will be achieved by suitable configuration of the TOE and its stored data (for example: to ensure that secret keys intended for electronic signature creation are only available for use by the signatory to whom they are linked, the client application shall follow an appropriate process to generate the key pair, to maintain sole control of the secret key by the intended signatory, and to ensure that the key can only be used for signing). As well as providing cryptographic functions, the TOE manages and protects the cryptographic keys used by these functions¹.

The TOE is therefore a set of configured software and hardware. Due to the generic TOE definition in this PP, the particular hardware/software/firmware required by the TOE is not defined by this PP. A generic TOE architecture is shown in Figure 1.

¹ As described in footnote 6, this Protection Profile includes a refinement to ADV_ARC.1 to consider support keys used in the implementation of the TOE and its protection measures.

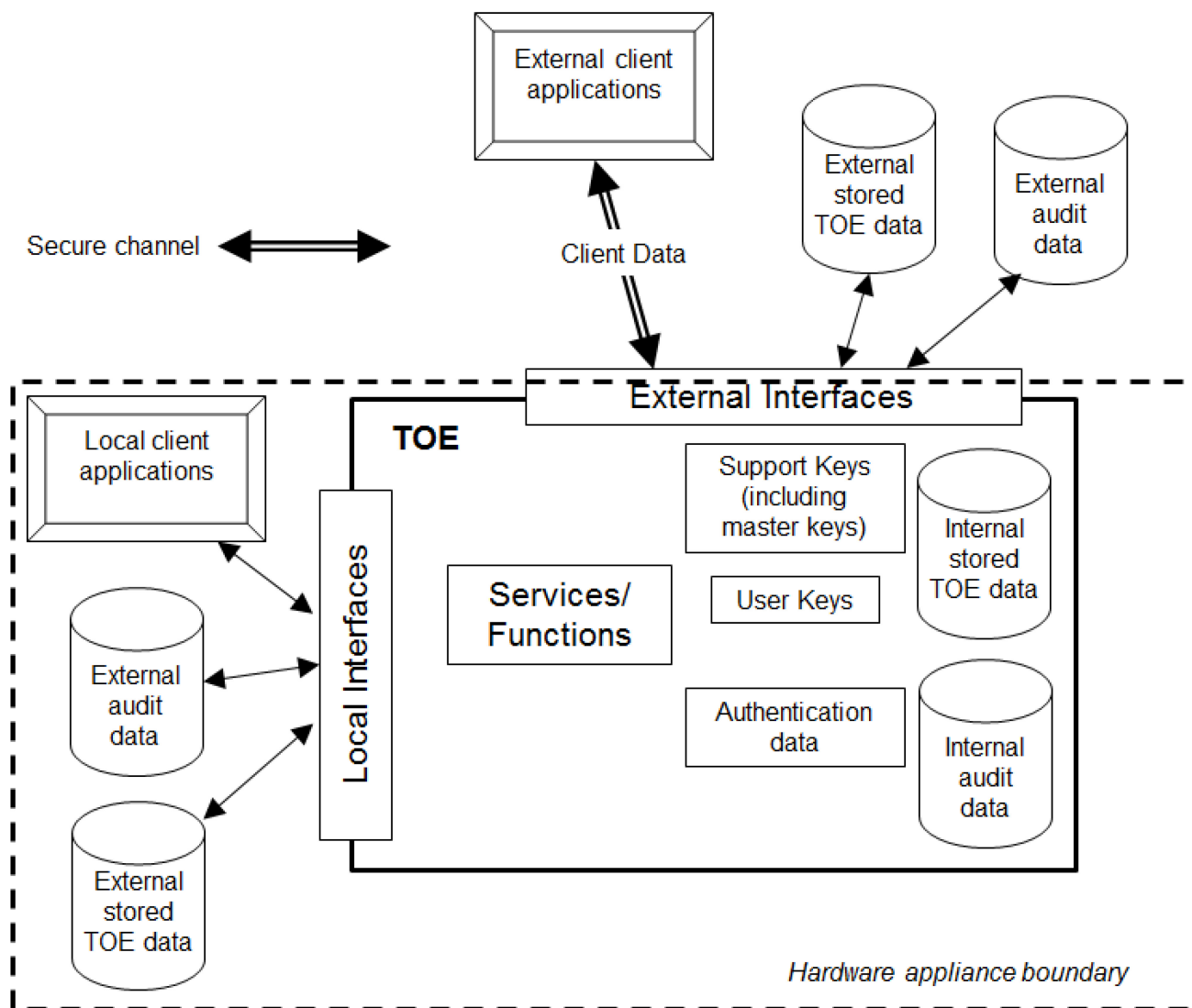


Figure 1 — Generic TOE Architecture

The hardware appliance boundary in Figure 1 represents the enclosure of the computing appliance which hosts the TOE. This can be a server, a PC or equivalent.

Local client applications reside in the same hardware appliance as the TOE, e.g. in the case of the TOE being a PCIe card inside a server, local client applications are the applications running within the same server boundary and using the TOE's services through the PCIe bus. Another example of local client application is an embedded application running inside the physical boundary of the TOE.

External client applications communicate remotely with the TOE through a network connection.

In all cases, the Client Application is outside the scope of the TOE.

A specific TOE will not necessarily include all of the elements shown in Figure 1. A TOE that comprises a PCIe card located in a server may have only local interfaces, e.g. for local client applications and storage of audit and TOE data within the server hardware boundary (which in this case is the hardware appliance boundary in Figure 1), but a dedicated cryptographic module might not include any such local storage and may use only external interfaces. The Security Target for each specific TOE is required to make clear what resources and channels are provided by that TOE.

The TOE is intended to support the provision of cryptographic functions for use by trust service providers.

The TOE implements separate authentication or authorization² of the following distinct types of entity:

- administrators of the TOE;
- application users of TOE cryptographic functions (local or external client applications, authenticated by their use of secure channels);
- users of secret keys (which in at least some cases need to have their use limited to a certain natural person or legal person³).

Acceptable authentication mechanisms include but are not limited to:

- Shared secret (e.g. password or key);
- Authentication based on asymmetric cryptography;
- Physical tokens;
- Biometrics;
- One time password.

More specific requirements on authentication may be applicable in the case of a TOE performing remote signing, as noted in 4.4.2.3, but these requirements are based on conformance with further Protection Profiles or other system security requirements directed specifically at remote signing.

If the TOE supports external client applications, then they are required to use a channel that provides authentication of its end-points and protection of confidentiality and integrity of data sent on the channel⁴. Where local client applications are connected to the TOE by a channel such as a PCIe bus within the same hardware appliance protected by measures in the physical environment, then the secure environment may be considered sufficient to provide the authentication, confidentiality and integrity protection needed for communication between the TOE and local applications. Secure channels may also exist between external and local client applications, but these are not within the scope of this Protection Profile.

Authorization as a user of a secret key is always separately required before a key can be used in a cryptographic function (or exported), regardless of any other authorization that may have been established for administrators or client applications. This requirement reflects the distinct activities that are being authorized in each case. Authorization to act as an administrator is an authorization to carry out management activities on the TOE, but not to *use* keys (in fact the requirement to be able to support sole control of a signature key means that in such cases an administrator shall not have access to use keys or to be able to access their values, unless the administrator happens also to demonstrate authorization as the owner of that key). Client applications are authorized to connect to the TOE in order to be able to invoke cryptographic functions, but the ownership of keys used in such functions

² In this document ‘authentication’ implies that the user is specifically identified, whereas ‘authorization’ implies that the authority of the user to use the key is established but the identity of the individual may not be known (e.g. where a single key is available to a number of individuals using a shared passphrase). As noted elsewhere, it is the responsibility of client applications to ensure that they use the correct mechanism for the context of the relevant keys and cryptographic functions.

³ More details of these requirements and the definitions of natural and legal persons can be found in [10].

⁴ A TOE may provide some additional channels that provide only authentication and integrity protection, but it shall provide at least one channel that is also capable of protecting confidentiality.

shall be separately controlled and checked, since the keys will in general be controlled by a variety of individual users with interests that are distinct from the client application itself (for example the client application may supply a signature service to a number of different users).

The requirement for authorization at the level of individual keys also means that a cryptographic function will only be carried out by the TOE if authorization is obtained for use with a key that can be used with that cryptographic function. Thus, a request by a client to use a specific cryptographic function may fail if the attributes of the key supplied do not allow its use for that operation. The authorization data supplied in order to use a key will vary according to the environment in which the TOE is used, and the services which it supplies. The authorization data could, for example, combine multiple factors or could itself be encrypted (requiring decryption by the TOE before use). The authorization data may reach the TOE in a variety of ways, including transmission over a secure channel or direct entry at an input device connected to the TOE.

4.4.1.2 Cryptographic Functions

The TOE provides one or more of the following cryptographic functions:

- Digital signature generation and verification;
- Message digest generation;
- Message authentication code generation and verification;
- Encryption and decryption (symmetric and asymmetric);
- Key generation;
- Key agreement and distribution;
- Key derivation;
- Generation of shared secret values;
- Cryptographic support for one time password and other non-PKI based authentication mechanisms;
- Random number generation.

These functions may also be used to support TSP system functions to create electronic seals and electronic timestamps. From the perspective of this Protection Profile, specific cryptographic purposes such as electronic signatures and electronic seals are not distinguished: they both consist of a series of cryptographic functions (such as creating message digests, or encrypting data) using specific keys⁵. A Security Target that conforms to this Protection Profile will identify the precise cryptographic operations (including details of algorithms, key lengths and modes, as appropriate) provided by a specific TOE to carry out these purposes.

⁵ Some cryptographic operations, such as creating message digests, do not require keys.

4.4.1.3 Key Management

The TOE supports the secure management of cryptographic keys⁶ necessary for its implemented cryptographic functions, including:

- Key establishment (including key generation);
- Protection of keys held within the TOE and held externally (for use by the TOE);
- Control of access and use of keys by the cryptographic functions within the TOE;
- Deletion of keys within the TOE.

The TOE supports at least one of the following techniques for establishing keys⁷:

- 1) Generation of cryptographic keys using a random number generator and implementing the key generation algorithms depending on the intended use of the keys;
- 2) Import of cryptographic keys in encrypted form or cryptographic key components using split-knowledge procedures;
- 3) Key agreement protocols establishing common secrets with external entities;
- 4) Derivation of keys from shared knowledge.

Secret keys are associated with attributes that determine their use, such that the correct association between the key and its attributes shall be protected against unauthorised modification. The specific key attributes maintained by a particular TOE are required to be specified in its Security Target. In generic terms these attributes include⁸:

- The identifier of the key (this enables it to be linked by an application to a particular owner);
- The type of the key (e.g. whether the key is a secret key of a symmetric cryptographic algorithm or the secret (commonly called private) key of an asymmetric cryptographic algorithm);
- Authorization data that enables access to the key (required only for secret keys);
- Re-authorization conditions such as determining a time period or number of uses of a key that are enabled by a single presentation of the correct authorization data for the key, after which the authorization will have to be re-presented in order to authorize any further uses of the key (re-authorization conditions are required only for secret keys, and may not be the same for all types of secret keys: the details of the re-authorization conditions for a specific TOE are described by completing the selections and assignments in FIA_UAU.6/KeyAuth in 9.4.3);

⁶ This Protection Profile distinguishes support keys from user keys, as described in the refinement to ADV_ARC.1 in 9.5.2. Requirements are placed by the Protection Profile on user keys, and support keys are considered an aspect of the TOE implementation that is therefore required to support the requirements for user keys, but where different structures and mechanisms (including aspects such as critical attributes) may be used.

⁷ SFRs are defined in Clause 9 only for random number generation and import; however a Security Target may add SFRs for additional techniques supported by the TOE.

⁸ In particular these attributes shall be sufficient to allow a secret key to be identified as one that is used to produce qualified electronic signatures and qualified electronic seals that meet the requirements of [Regulation], as interpreted for a specific TOE according to the definition in item 1 of the refinement to AGD_OPE.1 in 9.5.2.

- Key usage constraints that determine which cryptographic functions that can use the key (e.g. encryption or signature);
- Whether the key is allowed to be exported;
- Whether the key is an Assigned Key (see further discussion of assigned keys in the definition of FMT_MSA.1/AKeys in 9.4.7;
- Integrity protection data that protects the integrity of the key value, the values of the key attributes, and the binding of the key to its attributes.

Authorization to change the attributes of a key is, in general, distinct from authorization to use the key for cryptographic functions. For example, a signature key may need to require that some or all of its attributes cannot be changed after initial definition (e.g. because such changes might enable subjects beyond the signatory alone to access the key, or might allow the permitted use of the key to be changed) – this is supported by the definition of an ‘Assigned Key’ which cannot be imported or exported, for which the re-authorization conditions and key usage cannot be changed, and for which the authorization data can only be changed on successful validation of the current authorization data.

Keys may leave the TOE in one of three possible situations:

- External storage of keys

The TOE may allow external storage of keys for later use by the TOE (or another instance of the TOE within the same authorized security infrastructure operated by a TSP). This reflects the fact that when dealing with large numbers of keys then a cryptographic module may not have sufficient internal storage to hold them all internally. Keys stored in this way correspond to ‘external stored TOE data’ in Figure 1, and the form in which the key is stored shall be sufficient to protect the confidentiality (for at least secret keys) and integrity of the key and the binding of the key to its attributes (in particular the requirements of the SFRs FDP_IFF.1/KeyBasics, FDP_ACF.1/KeyUsage and FDP_SDI.2 in 9.4.4 apply to keys even when they are externally stored). The type and format of this storage for normal operational purposes may be used as part of a secure backup as described in 4.4.1.5.

- Export of keys

The TOE may allow export of keys for use by authorized client applications, provided that they are not Assigned Keys, that other key attributes do not prohibit export, and that the correct authorization data for the key has been supplied. Although the TOE checks key attributes to determine whether to allow export, the appropriate values to use for the key attributes will depend on the application context in which the key is used, and the security measures (technical, physical and procedural) that apply to that context. Keys that are exported are not included in the ‘external stored TOE data’ in Figure 1.

Keys might be imported or exported as part of providing general cryptographic functions (e.g. in support of client applications that use the TOE to support their own authentication mechanisms), but the TOE also allows individual secret keys to be identified as non-exportable. Assigned keys cannot be imported or exported, and represent a more strongly controlled type of key that is intended to be used only within the TOE for operations such as electronic signature or electronic seal generation.

- Backup

The TOE may provide facilities for secure backup and restore of the TSF state, as described in 4.4.1.5.

A distinction is drawn between export of keys (as a means of storing for future use by the TOE, or for passing to client applications) and creation of backups: the TOE may use separate mechanisms for these operations.

The TOE supports at least one of the acceptable authentication mechanisms in 4.4.1.1 above to be used as a basis for authorization to access and use secret keys.

4.4.1.4 Cryptographic Algorithms

Only algorithms and algorithm parameters (e.g. key length) approved for the identified purpose shall be used by the TOE to carry out cryptographic operations for trust services. The Security Target author should therefore consult the notified body or the relevant national certification body for the admissible algorithms, cryptographic key sizes and other parameters for algorithms, and standards for trust services.

An exemplary list of algorithms and parameters can be found in ETSI/TS 119 312 [8] or SOG-IS-Crypto [11].

4.4.1.5 Backup

The TOE may support backup and restoration of the TSF state necessary to re-establish an operational state after failure. This is not a mandatory capability of the TOE, but if a backup mechanism is provided then it shall preserve the security requirements on keys. Backups may include their own copies of keys, or may make use of a copy of the externally stored form of the keys (i.e. 'external stored TOE data' in Figure 1). The TOE will protect the confidentiality of the backup data and detect loss of the integrity of the backup data (including the attributes of the keys). It is assumed that the availability is supported by the IT environment outside the scope of the TOE. The TOE shall also ensure that any backup data supports the necessary controls over access to secret keys (including *use* of the key) as required for the intended use (i.e. the application context) of the key⁹.

Because the TOE is intended to operate as part of a TSP system that operates under strong environmental and procedural controls, there is a requirement that, if the TOE provides a backup capability, then the corresponding 'restore' operation can only be carried out under at least dual person control, i.e. the restore shall be approved by at least two separate administrators.

4.4.1.6 Audit

The cryptographic module is assumed to be part of a larger system that manages audit data for the system as a whole (integrating audit records from a number of individual components). The TOE therefore logs audit records for its own actions, and it is assumed that these are collected, maintained and reviewed in the larger system. Hence there is no separate auditor role within the cryptographic module TOE, but the role of System Auditor is assumed to exist in the larger system. An example of the audit process would be for the cryptographic module TOE to export audit data to a separate audit server that is monitored and controlled by the System Auditor.

⁹ The TOE may provide a single protection method for backups, provided that this is consistent with the other requirements on protection of keys, or may provide different methods according to differences in the controls needed for keys.

4.4.2 Usage and major security features of the TOE

4.4.2.1 General

In most cases the TOE will be a separate component with its own hardware and software, communicating via a well-defined physical and logical interface with the client application in the TSP system. Examples of physical interfaces that may be used to connect the TOE to client applications include the PCI bus, the SCSI bus, USB or Ethernet. Several instances of a TOE may be combined in a single domain under a common infrastructure, but the nature of this combination and common infrastructure is beyond the scope of this Protection Profile.

The threat environment the TOE is designed for is one of high threat of network compromise, and low threat of physical compromise (for example, a Certification Authority facility with a high degree of physical protection, but an operational requirement to be connected to an untrusted network such as the internet).

The environment is assumed to prevent prolonged unauthorised physical access to the TOE (including theft). The TOE provides physical protection mechanisms to deter undetected compromise of its security functions by low attack potential individuals that do have physical access to the TOE (for example disgruntled employees with legitimate access to the TOE).

The TOE is responsible for protecting the keys against logical attacks that would result in disclosure, compromise and unauthorised modification, and for ensuring that the TOE services are only used in an authorized way.

Client applications request cryptographic functions from the TOE, typically using a key managed by the TOE¹⁰, once the appropriate authorization has been provided.

Two distinct use cases for the deployment of a cryptographic module conforming to this Protection Profile are described below. These are not necessarily the only use cases for which a cryptographic module certified against the PP will be suitable, but these are the ones that have been considered in developing this PP.

4.4.2.2 Use Case 1: Local signing

This use case is aimed at trust service providers applying its own electronic signatures or seals. Examples include TSPs issuing certificates and time-stamps, as well as TSPs supporting application services such as e-Invoicing and registered e-mail where the TSP applies its own seal / signature.

The TOE performs local cryptographic operations, and associated key management, which can be used by a client application to create qualified electronic signatures and qualified electronic seals for a natural or legal person representing a TSP. The same TSP is responsible for the security of the environment in which the TOE is used and managed (including the client application, which is outside the TOE). The signing / sealing request is passed from a signature / seal creation client application under control of the TSP and executing on an appliance in the same local operational environment as the TOE (i.e. all communications involved in creating, receiving and executing the signing / sealing request take place within the network environment controlled by the TSP, and do not involve uncontrolled networks). Apart from its support keys (e.g. to protect local secure channels to the signature creation application), the TOE generates, stores and uses only keys that belong to and represent the TSP (e.g. for signing other keys). In this use case the TOE by itself is intended to be used as a qualified electronic signature creation, or seal, device compliant to Annex II of Regulation EU 910/2014 [7]. See Annex A for further details.

¹⁰ All cryptographic operations in the scope of this Protection Profile are carried out using keys managed by the TOE, and therefore any use of other keys is outside the scope of the Protection Profile.

4.4.2.3 Use Case 2: Support for Remote Server Signing

This use case is aimed at TSPs supporting requirements for remote signing, or sealing, as specified in Regulation 910/2014. In this case the TOE on its own is not intended to meet the requirements for QSCDs in the context of remote signing set out in Annex II of (EU) No 910/2014. It is expected that the TOE would be used in conjunction with the Protection Profile to be defined in EN 419241-2 [10], and any other related Protection Profiles, to meet the requirements for Sole Control Assurance Level 2 as defined in EN 419241-1 [9]. These security requirements may govern aspects such as the definition of specific user identification and authentication methods (e.g. multi-factor authentication) used within the signing system and may affect the type and form of the authorization data that is passed to the cryptographic module in order to authorize use of a key.

The TOE performs local cryptographic operations, and associated key management, which can be used by an application using server signing, as defined in EN 419241-1 [9], to create qualified electronic signatures and qualified electronic seals on behalf of a legal or natural person which is distinct from and remote from the TSP which manages the TOE. The TOE generates, stores and uses signing / sealing keys in a way that maintains the remote control of an identified signatory or seal creator who operates through the use of a client application. The TOE deals with ensuring the security of keys and their use for signature or seal creation. Non-cryptographic functionality concerned with assuring sole control of these keys, for example authentication, is provided by other ensured functionality outside the scope of the TOE.

4.4.3 Available non-TOE hardware/software/firmware

The TOE is a Cryptographic Module comprising its own hardware and software, though it may be supported by additional non-TOE hardware (e.g. a surrounding hardware appliance, physical authentication factors) and non-TOE software (e.g. utilities, management software or interface libraries).

5 Conformance Claim

5.1 CC Conformance Claim

This Protection Profile is conformant to Common Criteria version 3.1 revision 4.

More precisely, this Protection Profile is:

- CC Part 1 [CC1];
- CC Part 2 extended [CC2];
- CC Part 3 conformant [CC3].

The assurance requirement of this Protection Profile is **EAL4 augmented**.

Augmentation results from the selection of:

- AVA_VAN.5 Advanced methodical vulnerability analysis.

5.2 PP Claim

This PP does not claim conformance to any another Protection Profile.

5.3 Conformance Rationale

Since this Protection Profile is not claiming conformance to any other Protection Profile, no rationale is necessary here.

5.4 Conformance Statement

This Protection Profile requires strict conformance of any Security Target or Protection Profile that claims conformance to this Protection Profile.

6 Security Problem Definition

6.1 Assets

The assets that need to be protected by the TOE are identified below.

R.SecretKey: secret keys used in symmetric cryptographic functions and private keys used in asymmetric cryptographic functions, managed and used by the TOE in support of the cryptographic services that it offers. This includes user keys, owned and used by specific users, and support keys used in the implementation and operation of the TOE. The asset also includes copies of such keys made for external storage and/or backup purposes. The confidentiality and integrity of these keys shall be protected.

R.PubKey: public keys managed and used by the TOE in support of the cryptographic services that it offers (including user keys and support keys). This asset includes copies of keys made for external storage and/or backup purposes. The integrity of these keys shall be protected.

R.ClientData: data supplied by a client for use in a cryptographic function. Depending on the context, this data may require confidentiality and/or integrity protection.

R.RAD: reference data held by the TOE that is used to authenticate an administrator (hence to control access to privileged administrator functions such as TOE backup, export of audit data) or to authorize a user for access to secret and private keys (R.SecretKey). This asset includes copies of authentication/authorization data made for external storage and/or backup purposes. The integrity of the RAD shall be protected; its confidentiality shall also be protected unless the authentication method used means that the RAD is public data (such as a public key).

6.2 Subjects

The types of subjects identified in this PP are:

S.Application: a client application, or process acting on behalf of a client application and that communicates with the TOE over a local or external interface. Client applications will in some situations be acting directly on behalf of end users (see S.User).

S.User: an end user of the TOE who can be associated with secret keys and authentication/authorization data held by the TOE. An end user communicates with the TOE by using a client application (S.Application).

S.Admin: an administrator of the TOE. Administrators are responsible for performing the TOE initialisation, TOE configuration and other TOE administrative functions.

Each type of subject may include many individual members, for example a single TOE will generally have many users who are all included as members of the type S.User.

6.3 Threats

6.3.1 General

The following threats are defined for the TOE. The attacker (i.e. the 'threat agent') described in each of the threats is a subject who is not authorized for the relevant action, but who may present themselves as either a completely unknown user, or as one of the subjects in 6.2 (but in this case the attacker will not have access to the authentication or authorization data for the subject).

6.3.2 T.KeyDisclose — Unauthorised disclosure of secret/private key

An attacker obtains unauthorised access to the plaintext form of a secret key (R.SecretKey), enabling either direct reading of the key or other copying into a form that can be used by the attacker as though the key were their own. This access may be gained during generation, storage, import/export, use of the key, or backup if supported by the TOE.

6.3.3 T.KeyDerive — Derivation of secret/private key

An attacker derives a secret key (R.SecretKey) from publicly known data, such as the corresponding public key or results of cryptographic functions using the key or any other data that is generally available outside the TOE.

6.3.4 T.KeyMod — Unauthorised modification of a key

An attacker makes an unauthorised modification to a secret or public key (R.SecretKey or R.PubKey) while it is stored in, or under the control of, the TOE, including export and backups if supported. This includes replacement of a key as well as making changes to the value of a key, or changing its attributes such as required authorization, usage constraints or identifier (changing the identifier to the identifier used for another key would allow unauthorised substitution of the original key with a key known to the attacker). The threat therefore includes the case where an attacker is able to break the binding between a key and its critical attributes¹¹.

6.3.5 T.KeyMisuse — Misuse of a key

An attacker uses the TOE to make unauthorised use of a secret key (R.SecretKey) that is managed by the TOE (including the unauthorised use of a secret key for a cryptographic function that is not permitted for that key¹²), without necessarily obtaining access to the value of the key.

6.3.6 T.KeyOveruse — Overuse of a key

An attacker uses a key (R.SecretKey) that has been authorized for a specific use (e.g. to make a single signature) in other cryptographic functions that have not been authorized.

6.3.7 T.DataDisclose — Disclosure of sensitive client application data

An attacker gains access to data that requires protection of confidentiality (R.ClientData, and possibly R.RAD) supplied by a client application during transmission to or from the TOE or during transmission between physically separate parts of the TOE.

6.3.8 T.DataMod — Unauthorised modification of client application data

An attacker modifies data (R.ClientData such as DTBS/R, authentication/authorization data, or a public key (R.PubKey)) supplied by a client application during transmission to the TOE or during transmission between physically separate parts of the TOE, so that the result returned by the TOE (such as a signature or public key certificate) does not match the data intended by the originator of the request.

¹¹ See OT.KeyIntegrity in 7.2.4 for further discussion of critical attributes of a key.

¹² This therefore means that the threat includes unauthorised use of a cryptographic function that makes use of a key.

6.3.9 T.Malfunction — Malfunction of TOE hardware or software

The TOE may develop a fault that causes some other security property to be weakened or to fail. This may affect any of the assets and could result in any of the other threats being realized. Particular causes of faults to be considered are:

- Environmental conditions (including temperature and power);
- Failures of critical TOE hardware components (including the RNG);
- Corruption of TOE software.

6.4 Organisational Security Policies

6.4.1 P.Algorithms — Use of approved cryptographic algorithms

The TOE offers key generation functions and other cryptographic functions provided for users that are endorsed by recognized authorities as appropriate for use by TSPs.

Application Note 1

The relevant authorities and endorsements are determined by the context of the client applications that use the TOE. For digital signatures within the European Union this is as indicated in Regulation 910/2014 [7] and an exemplary list of algorithms and parameters is given in ETSI/TS 119 312 [8] or SOG-IS-Crypto [11] (see also 4.4.1.4).

6.4.2 P.KeyControl — Support for control of keys

The life cycle of the TOE and any secret keys that it manages (where such keys are associated with specific entities, such as the signature creation data associated with a signatory or the seal creation data associated with a seal creator¹³), shall be implemented in such a way that the secret keys can be reliably protected by the legitimate owner against use by others, and in such a way that the use of the secret keys by the TOE can be confined to a set of authorized cryptographic functions.

Application Note 2

This policy is intended to ensure that the TOE can be used for qualified electronic seals and qualified electronic signatures as in Regulation 910/2014 [7], but recognizes that not all keys are used for such purposes. Therefore, although the TOE needs to be able to support the necessary strong controls over keys in order to create such seals and signatures, not all keys need the same level and type of control.

6.4.3 P.RNG — Random Number Generation

The TOE is required to generate random numbers that meet a specified quality metric, for use by client applications. These random numbers shall be suitable for use as keys, authentication/authorization data, or seed data for another random number generator that is used for these purposes.

¹³ A seal creator may be a *legal person* (see [Regulation]) rather than a *natural person*, and seal creation data may therefore be authorised for use by a number of natural persons, depending on the nature and requirements of the trust service provided.

6.4.4 P.Audit — Audit trail generation

The TOE is required to generate an audit trail of security-relevant events, recording the event details and the subject associated with the event.

Application Note 3

The cryptographic module TOE is assumed to be part of a larger system that manages audit data. The TOE therefore logs audit records, and it is assumed that these are collected, maintained and reviewed in the larger system. Hence there is no separate auditor role within the cryptographic module TOE, but the role of System Auditor is assumed to exist in the larger system – cf. A.AuditSupport in 6.5.5.

6.5 Assumptions

6.5.1 A.ExternalData — Protection of data outside TOE control

Where copies of data protected by the TOE are managed outside of the TOE, client applications and other entities shall provide appropriate protection for that data to a level required by the application context and the risks in the deployment environment.

In particular, any backups of the TOE and its data are maintained in a way that ensures appropriate controls over making backups, storing backup data, and using backup data to restore an operational TOE. The number of sets of backup data does not exceed the minimum needed to ensure continuity of the TSP service. The ability to restore a TOE to an operational state from backup data requires at least dual person control (i.e. the participation and approval of more than one authenticated administrator).

6.5.2 A.Env — Protected operating environment

The TOE operates in a protected environment that limits physical access to the TOE to authorized Administrators. The TOE software and hardware environment (including client applications) is installed maintained by Administrators in a secure state that mitigates against the specific risks applicable to the deployment environment.

6.5.3 A.DataContext — Appropriate use of TOE functions

Any client application using the cryptographic functions of the TOE will ensure that the correct data are supplied in a secure manner (including any relevant requirements for authenticity, integrity and confidentiality). For example, when creating a digital signature over a DTBS the client application will ensure that the correct (authentic, unmodified) DTBS/R is supplied to the TOE, and will correctly and securely manage the signature received from the TOE; and when certifying a public key the client application will ensure that necessary checks are made to prove possession of the corresponding private key. The client application may make use of appropriate secure channels provided by the TOE to support these security requirements. Where required by the risks in the operational environment a suitable entity (possibly the client application) performs a check of the signature returned from the TOE, to confirm that it relates to the correct DTBS.

Client applications are also responsible for any required logging of the uses made of the TOE services, such as signing (or sealing) events.

Similar requirements apply in local use cases where no client application need be involved, but in which the TOE and its user data (such as keys used for signatures) need to be configured in ways that will support the need for security requirements such as sole control of signing keys.

Appropriate procedures are defined for the initial creation of data and continuing operation of the TOE according to the specific risks applicable to the deployment environment and the ways in which the TOE is used.