PKI Concept

fiskaly Security Module Application for Electronic Record-keeping Systems

TOE Version 1.0.5

Document Version 1.1.6

2021-04-21

fiskaly GmbH

Contents

Chapter 1

Introduction

This document is the PKI Concept for the fiskaly CTSS and its SMAERS, the fiskaly Security Module Application for Electronic Record-keeping Systems (fiskaly SMAERS). It covers the key creation in the *fiskaly Cloud Crypto Service Provider*, which is the CSPL used by the fiskaly CTSS. fiskaly Security Module Application for Electronic Record-keeping Systems and *fiskaly Cloud Crypto Service Provider* are developed and maintained by fiskaly GmbH. In addition, this document deals with the communication with the PKI operated by DARZ and the structure of the certificates used. The following section gives a brief overview over the involved components and key features of their configuration.

1.1 Document and TOE Reference

Document Type:	PKI Concept
Document Version:	1.1.6
Document built from commit:	1481a077d7c6137ff154ab572b2957641a0c0eca
Date:	2021-04-21
Author:	fiskaly GmbH
Certification-ID:	BSI-DSZ-CC-1130
TOE Identification:	fiskaly Security Module Application for Electronic Record-keeping Systems
TOE Version:	1.0.5
CC Version:	3.1 Revision 5
Assurance Level:	EAL2 augmented with ALC_LCD.1 and ALC_CMS.3
PP Conformance:	BSI-CC-PP-0105-V2-2020 including the package *Trusted Channel between TOE and CSP* from BSI-CC-PP-0105-V2-2020

1.2 Overview

Overview: Landscape

The solution landscape is depicted in Figure 1.1. It shows four major kinds of entities:

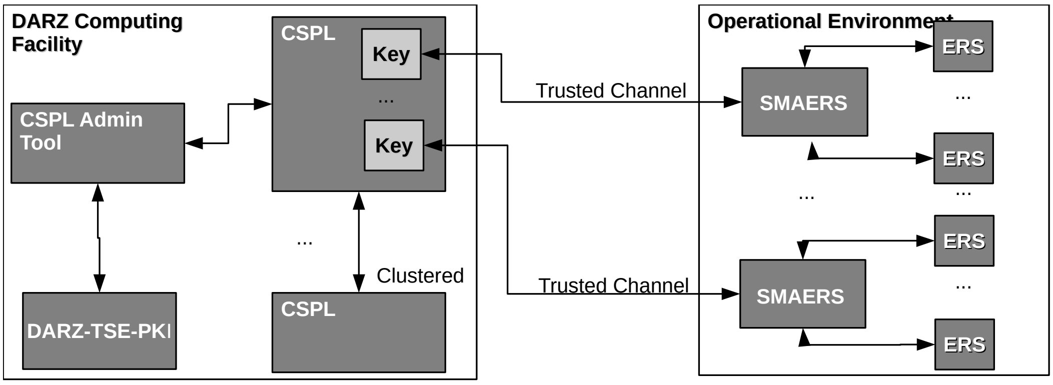

Figure 1.1: Landscape Overview

- The DARZ-TSE-PKI, operated by DARZ to issue CTSS certificates for CTSS signing keys of CTSSs. The PKI only serves this purpose. See Chapter 2 for details.
- CSPLs, operated by fiskaly GmbH, which contain the private CTSS signing keys of CTSSs. The CSPLs are operated in a cluster in the same data operation center as the DARZ-TSE-PKI, but under the control of *fiskaly*. Each CSPL holds multiple CTSS signing keys for multiple CTSSs. Each key is used by at most one CTSS.
- multiple CTSS, which each contain one SMAERS. Each CTSS uses exactly one CTSS signing key of one CSPL (up to clustering) to sign log messages. Each CTSS might be used by multiple Electronic Record-keeping Systems of the same tax payer. Note that multiple tax payers cannot share one CTSS.
- multiple ERS, each operated by exactly one tax payer. Note that one tax payer might operate multiple ERS, but no ERS can be operated by multiple tax payers.

In addition, Figure 1.1 shows the keys in the CSPLs, as well as the *CSPL Admin Tool*. They are included to make the mapping of SMAERS units to keys visible in the picture and show the communication channels between the components.

Note that DARZ is on the one hand the operator of the PKI, on the other hand DARZ operates the secure computing facility, which hosts the CSPL Admin Tool and the CSPLs. For the *CSPL Admin Tool* and the CSPL, fiskaly provides and controls the hardware, which executes both. Here DARZ is only the provider of the computing facility. This allows to operate CSPL, *CSPL Admin Tool* and the PKI in the same secure environment but separates the responsibility and control between DARZ as PKI operator and fiskaly as operator of the CSPL (and *CSPL Admin Tool*).

Overview: Involved Keys

The following list gives a brief overview over the keys, which are involved to create CTSS certificates for fiskaly Security Module Application for Electronic Record-keeping Systems:

- CTSS signature key(s) / CTSS certificate: These are the keys in the CSPL, which are used to sign log messages. Their certificates are included in each TAR file being exported from a CTSS.
- sub CA key(s) / certificate: The sub CA keys and certificate are part of the DARZ-TSE-PKI. They are used to issue the signature certificates.
- root CA key(s) / certificate: The root CA keys and certificate are part of the DARZ-TSE-PKI. They are used to issue the sub CA certificates. The certificate of the root CA is provided to the BMF following the requirements of the transmission given by BSI. The certificate is provided via De-Mail by a contractor of fiskaly who has been directly authorized by the GM of fiskaly for this transmission.
- *fiskaly* key pair / certificate: This is a key pair, being generated by fiskaly GmbH. The key pair is a 256-bit ECC key pair on curve secp256r1 and was generated with openssl. The public key of the key pair was provided to DARZ via a s/mime (signed and encrypted) email and DARZ created a certificate for it. In addition, the fingerprint of the public key was compared by phone between two employees of the involved parties, which know each other. fiskaly GmbH uses it to access the PKI's RESTinterface and to sign certificate requests for CTSS signature keys. It is stored in the *CSPL Admin Tool*, which is operated on hardware being controlled by fiskaly and hosted in the DARZ computing facilities.
- attestation key: This is a key pair, which is hard-coded in the CSPL. It is the same for all CSPL instances (of the same CSPL version). The key pair is a 256-bit ECC key pair on curve secp256r1 and was generated by *fiskaly* on an air-gapped laptop of *fiskaly*. It is generated with openssl. The key is stored in the git repository of the CSPL and access is restricted to entitled *fiskaly* employees. The key is used exclusively to create the attestation signature of the certificate requests for keys, which are generated and stored within the CSPL. The exclusive use is guaranteed by organizational means (access control of the repository). The public key of the attestation key pair was provided to DARZ via s/mime (signed and encrypted) email. In addition, the fingerprint of the public key was compared by phone between two employees of the involved parties, which know each other.

Their detailed role will become clear in the following chapters.

Chapter 2

The DARZ-TSE-PKI

The PKI, which issues the CTTS certificate for the CTSS signature keys of the CTSS of fiskaly GmbH is the DARZ-TSE-PKI. It is operated by DARZ:

DARZ GmbH
Julius-Reiber-Str. 11
D-64293 Darmstadt
Amtsgericht Darmstadt, HRB 86495

To operate the PKI, DARZ uses the software MTG PKI, which is developed and maintained by MTG:

MTG AG
Dolivostraße 11
D-64293 Darmstadt
Amtsgericht Darmstadt, HRB 9801

The PKI has been certified according to TR-03145 [2]. The certificate number is BSI-K-TR-0294-2018. The data processing center, which hosts the PKI has been certified in accordance with ISO27001:2013. This certificate with certificate number 01 153 1400758 has been issued by TÜV Rheinland Cert GmbH. The *Geltungsbereich* of the ISO27001-certification is *Gesamtunternehmen inkl. aller Produkte und Services der DARZ GmbH als FULL-IT-Serviceprovider mit eigenem Hochsicherheitsrechenzentrum und redundantem Glasfaserring zu Frankfurter Rechenzentren.*

This is the only PKI, which produces certificates for signature keys of *fiskaly Cloud Crypto Service Provider*, which uses the keys only for CTSSs. This way, the PKI issues end entity certificates only for CTSSs. In addition, *fiskaly Cloud Crypto Service Provider* is the only CSPL (and CSP) which fiskaly Security Module Application for Electronic Record-keeping Systems uses. Therefore, all certificates for signing keys of fiskaly SMAERS are issued by this PKI.

Chapter 3

Key Generation and Certificate Creation

This chapter covers the process from the generation of a CTSS signature key pair to the CTSS certificate to be created. This is a process between PKI and CSPL. It is supported by the *CSPL Admin Tool*, which guides the process. The *CSPL Admin Tool* is used to manage the CSPL and developed by fiskaly GmbH. It eases the PKI communication and key generation in the CSPL, but it is not part of the certification scope.

Key Generation

All CTSS signature key pairs are created in the CSPL. This is done by a *fiskaly* employee, authentication to the CSPL as Crypto Officer. The CSPL itself generates the keys using its deterministic random number generator and the interface, which is documented in *Functional Specification Documentation* [6] and part of the Common Criteria Certification of the *fiskaly Cloud Crypto Service Provider* of fiskaly GmbH.

After the generation of the key pair, it can be used through the CSPL's documented and certified interface.

CTSS Certificate (Request) Creation

To trigger the creation of a CTSS certificate, the PKI offers a REST interface, which is protected by TLS. To request a CTSS certificate, a certificate request has to be created and transmitted to this REST interface of the PKI. fiskaly GmbH creates this request using its *CSPL Admin Tool*, which again uses the documented CSPL interface. The *CSPL Admin Tool* is operated at the DARZ facility, i.e., close to the PKI and CSPL. It creates a request as required by the MTG PKI software. The request is signed three times by fiskaly GmbH:

- one signature with the attestation key of the CSPL, being created within the CSPL

- one signature with the *fiskaly* key, being created by the *CSPL Admin Tool*
- one signature with the CTSS signature key for which the CTSS certificate is requested

In addition, the signed request contains an *AttestationNonce*, which is requested from the PKI upfront. Afterwards the *CSPL Admin Tool* transmits the request to the REST-API of the PKI and the PKI's sub CA creates the CTSS certificate. After creation, the *CSPL Admin Tool* fetches the CTSS certificate from the REST-API of the PKI and activates it afterwards. The activation is the invocation of a REST command, which signals the CA that the created CTSS certificate was successful retrieved. This completes the creation process of CTSS certificates. In this process, *fiskaly* also retrieves the revocation password for the CTSS certificate, which *fiskaly* stores in case, the certificate has to be revoked later on.

Then, the CTSS certificate and signature key pair can be assigned to a CTSS. To do so, *CSPL Admin Tool* creates a *bootstrap-file*, that is used to personalize a SMAERS software and allows the SMAERS software to access and use the CTSS signature key and CTSS certificate. This forms the CTSS, which a tax payer can then initialize and use.

The bootstrap file will never be handed over to the tax payer. After use, the bootstrap file will be directly deleted from all machines by using the "shred -u" command (the default setting of shred is used which will overwrite the file three times). Please note that the bootstrap file can only be used once for the personalization of SMAERS. If a bootstrap file would be used again, the CSPL will return an error in the course of the personalization process.

Chapter 4

Certificates

This chapter covers the CTSS certificates and the certificate chain, which allows to verify the CTSS certificates. In addition, it briefly refers to the signature verification procedure and refers to the detailed description.

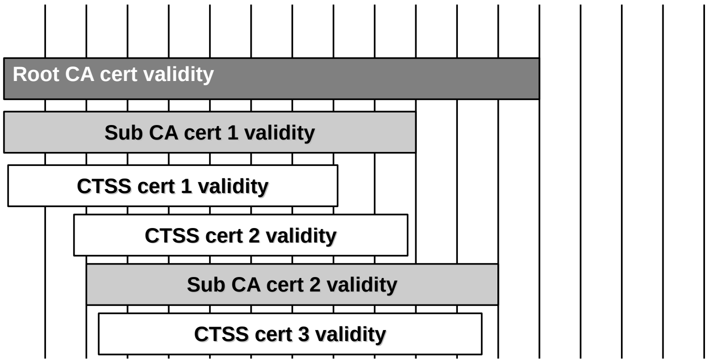

Figure 4.1: Timeline Overview

Note that the root CA key has a private key usage of 3 years and the root CA certificate has a validity of 13 years. The sub CA key has a private key usage of 2 years and the sub CA certificate is valid for 10 years. Finally, the CTSS signature keys have a private key usage of 8 years and the CTSS certificates are valid for 8 years. Accordingly, sub CA certificates are issued after two years and the root CA has to be renewed after 3 years. This is depicted in Figure 4.1. Here the vertical lines separate the validity into chunks of one year.

4.1 Certificate Structure

The CTSS certificates are signed by a sub CA of DARZ, which again is signed by the root CA. The following three sections detail the structure of each of the three types of certificates involved, while the last covers the extensions, which are part of the different types of certificates.

4.1.1 Root CA Certificate

This is the root of trust for the certificate chain of the fiskaly Security Module Application for Electronic Record-keeping Systems. To be able to check that the correct root certificate was obtained or returned by fiskaly SMAERS in a TAR file, the certificate of the root CA is provided to the BMF following the requirements of BSI. The certificate is provided via De-Mail by an contractor of fiskaly who has been directly authorized by the GM of fiskaly for this transmission. In addition, the fingerprint of the root certificate is published in the *Security Target* [8] of fiskaly SMAERS, which can be found at the BSI homepage after successful completion of the Common Criteria Certification process. Note that the certificate that is submitted to BMF is the actual anchor of trust. The root CA certificate looks as follows:

- Version
  - „v3“
- SerialNumber
  - random, 126 bit entropy
- Signature
  - ECDSAwithSHA384 (1.2.840.10045.4.3.3)
- Issuer
  - equals Subject
- Validity
  - 13 years
- Subject
  - SERIALNUMBER = currently 1, increased by 1 for each new root CA certificate
  - C = DE
  - O = DARZ
  - CN = DARZ-TSE-ROOT-CA
- SubjectPublicKeyInfo
  - Named Curve: brainpoolP384r1 (1.3.36.3.3.2.8.1.1.11)

In addition, the certificate contains the following extensions:

SubjectKeyIdentifier

- OID: 2.5.29.14
- critical: no
- value: SHA-1 hash of the public key of this certificate

KeyUsage

- OID: 2.5.29.15
- critical: no
- value:
  - keyCertSign, cRLSign

CertificatePolicies

- OID: 2.5.29.32
- critical: no
- value:
  - OID of the Certificate Policy: 1.3.6.1.4.1.51695.1.3
  - Policy Qualifier Id: CPS
  - Qualifier: `https://www.da-rz.de/de/ueber-darz/unternehmen/pki/`

SubjectAltName

- OID: 2.5.29.17
- critical: no
- value:
  - RFC822 Name: tse-root-ca@da-rz.de
  - URL: `https://www.da-rz.de/de/ueber-darz/unternehmen/pki/`

IssuerAltName

- OID: 2.5.29.35
- critical: no
- value:
  - RFC822 Name: tse-root-ca@da-rz.de
  - URL: `https://www.da-rz.de/de/ueber-darz/unternehmen/pki/`

BasicConstraints

- OID: 2.5.29.19
- critical: yes
- value:
  - root CA certificate: pathLenConstraint, 1

AuthorityInfoAccess

- OID: 1.3.6.1.5.5.5.7.1.1
- critical: no
- value:
  - Access Method: Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
  - Alternative Name
    - URL: `https://www.da-rz.de/de/ueber-darz/unternehmen/pki/`

4.1.2 Sub CA Certificate

- Version
  - „v3“
- SerialNumber
  - random, 126 bit entropy
- Signature
  - ECDSAwithSHA384 (1.2.840.10045.4.3.3)
- Issuer
  - equals Subject of the Root CA certificate
- Validity
  - 10 years
- Subject
  - SERIALNUMBER = currently 1, increased by 1 for each new sub CA certificate
  - C = DE
  - O = DARZ
  - CN = DARZ-TSE-SUB-CA
- SubjectPublicKeyInfo
  - Named Curve: brainpoolP384r1 (1.3.36.3.3.2.8.1.1.11)

This certificate contains in addition the following extensions:

AuthorityKeyIdentifier

- OID: 2.5.29.35
- critical: no
- value: SHA-1 hash of the public key of the issuer

SubjectKeyIdentifier

- OID: 2.5.29.14
- critical: no
- value: SHA-1 hash of the public key of this certificate

KeyUsage

- OID: 2.5.29.15
- critical: no
- value:
  - keyCertSign, cRLSign

CertificatePolicies

- OID: 2.5.29.32
- critical: no
- value:
  - OID of the Certificate Policy: 1.3.6.1.4.1.51695.1.3
  - Policy Qualifier Id: CPS
  - Qualifier: `https://www.da-rz.de/de/ueber-darz/unternehmen/pki/`

SubjectAltName

- OID: 2.5.29.17
- critical: no
  - RFC822 Name: tse-root-ca@da-rz.de
  - URL: `https://www.da-rz.de/de/ueber-darz/unternehmen/pki/`

IssuerAltName

- OID: 2.5.29.35
- critical: no
- value: equals SubjectAltName of the issuer certificate

BasicConstraints

- OID: 2.5.29.19
- critical: yes
- value:
  - cA: yes
  - pathLenConstraint: 0

CRLDistributionPoints

- OID: 2.5.29.31
- critical: no
- value:
  - `http://tse-pki.da-rz.net/tse-pki/crl?issuerDN=CN%3DDARZ-TSE-ROOT-CA%2CO%3DDARZ%2CC%3DDE%2CSERIALNUMBER%3D1`, where Serial Number depends on the Serial Number in the subject of the root CA certificate
  - `ldap://ldap-tse-pki.da-rz.net/serialNumber=1,CN=DARZ-TSE-ROOT-CA,DC=DARZ,DC=DE?certificateRevocationList`, where Serial Number depends on the Serial Number in the subject of the root CA certificate

AuthorityInfoAccess

- OID: 1.3.6.1.5.5.5.7.1.1
- critical: no
- value:
  - Access Method: Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
  - Alternative Name
    - URL: `https://www.da-rz.de/de/ueber-darz/unternehmen/pki/`

4.1.3 CTSS Certificate

- Version
  - „v3“
- SerialNumber
  - random, 126 bit entropy
- Signature
  - ECDSAwithSHA384 (1.2.840.10045.4.3.3)

- Issuer
  - equals Subject of the Sub CA certificate
- Validity
  - 8 years
- Subject
  - as specified by TR-03153 [3], including a SHA-256 hash of the public key as SERIALNUMBER
- SubjectPublicKeyInfo
  - Named Curve: secpP256r1 (1.2.840.10045.3.1.7) or brainpoolP256r1 (1.3.36.3.3.2.8.1.1.7)

This certificate contains in addition the following extensions:

AuthorityKeyIdentifier

- OID: 2.5.29.35
- critical: no
- value: SHA-1 hash of the public key of the issuer

KeyUsage

- OID: 2.5.29.15
- critical: no
- value:
  - digitalSignature

CertificatePolicies

- OID: 2.5.29.32
- critical: no
- value:
  - OID of the Certificate Policy: 1.3.6.1.4.1.51695.1.3
  - Policy Qualifier Id: CPS
  - Qualifier: `https://www.da-rz.de/de/ueber-darz/unternehmen/pki/`

IssuerAltName

- OID: 2.5.29.35
- critical: no
- value: equals SubjectAltName of the issuer certificate

BasicConstraints

- OID: 2.5.29.19
- critical: yes
- value:
  - cA: false

CRLDistributionPoints

- OID: 2.5.29.31
- critical: no
- value:
  - `http://tse-pki.da-rz.net/tse-pki/crl?issuerDN=CN%3DDARZ-TSE-SUB-CA%2CO%3DDARZ%2CC%3DDE%2CSERIALNUMBER%3D10`, where Serial Number depends on the Serial Number in the subject of the sub CA certificate
  - `ldap://ldap-tse-pki.da-rz.net/serialNumber=1,CN=DARZ-TSE-SUB-CA,DC=DARZ,DC=DE?certificateRevocationList`, where Serial Number depends on the Serial Number in the subject of the sub CA certificate

AuthorityInfoAccess

- OID: 1.3.6.1.5.5.5.7.1.1
- critical: no
- value:
  - Access Method: Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
  - Alternative Name
    - URL: `https://www.da-rz.de/de/ueber-darz/unternehmen/pki/`

4.2 Signature Verification

The following two sections are a copy of the instructions regarding the verification of log messages and the certificate chain. They are provided in section 4.1 of the document *Preparative Procedures & Operational User Guidance Documentation - fiskaly Security Module Application for Electronic Record-keeping Systems* [7].

4.2.1 Verification of Transaction Logs

To verify the integrity of one log message, proceed as follows:

- Extract the root CA certificate from the exported TAR-file
- Retrieve the root CA certificate for the CTSS from the BMF and compare it to the certificate from the TAR-file. Make sure they are equal.
- Extract the sub CA certificate and CTSS certificate from the TAR-file
- Verify the signature of the log message with the CTSS certificate
- Verify that the CTSS certificate was valid at signature time. To do so, check that at that point of time all certificates in the certificate chain from CTSS certificate to the root CA certificate as trust anchor were valid. In addition, check the CTSS certificate was issued by the sub CA certificate and check that the sub CA certificate was issued by the root CA certificate. To do so verify the signatures in the CTSS certificate and sub CA certificate with the public key of the issuing certificate, i.e., with the public key of the sub CA certificate for the CTSS certificate and with the public key of the root CA certificate for the sub CA certificate
- Check that none of the involved certificates was revoked using the revocation mechanism, given in the certificates. In case the certificate(s) got revoked after signature creation time, the revocation reason has to be considered to decide, if the revocation influences the validity of the signature

This allows to verify signature of log messages successfully for 10 years (or more) even after the validity period of the CTSS certificate ended. To be able to do so is required by law. The goal of this hybrid verification model is to verify that the signature was valid at signature creation time (and the certificates did not get revoked afterwards).

4.2.2 Verification of Tar files

To verify a TAR file, each log message within the file has to be checked. How to do so can be found in section 4.2.1.

In addition, the following has to be checked:

- check that the timestamps of the log messages are plausible (with respect to time adjustments of the CSP)
- check that the transaction counters of the log messages are plausible, i.e.
  - they form a increasing sequence, i.e., no two transactions have the same transaction counter
  - no gaps appear (in case of an unfiltered export)
  - the transaction counters increase according to the time stamps of the start transaction messages

- check that the signature counters of the log messages are plausible, i.e.
  - they form a increasing sequence, i.e., no two signatures have the same signature counter
  - there are no gaps in the sequence of signature counters
  - the sequence of signature counters fits to the associated time stamps and to the transaction counters of the start transaction messages

In case any of these checks fails, the TAR file has to be analyzed in more detail to understand, why the check(s) did fail.

4.3 Certificate Revocation

To check if certificates were revoked, DARZ -as operator of the PKI- maintains certificate revocation lists (CRL). There is one revocation list for the root CA and one list for the sub CA. Both are publicly available via URLs, which are encoded as the value of the corresponding extension in the sub CA Certificates and in the CTSS certificates. Note that all CRLs are available for at least ten additional years after the end of the validity period of the certificates involved. See section 4.1.2 and section 4.1.3 to find the corresponding URLs. This ensures, that everybody, especially tax payers and tax inspectors are able to inspect revocation information as required in section 4.2.

To revoke a CTSS certificate, the tax payer contacts fiskaly GmbH. fiskaly GmbH-as CTSS operator- will create a revocation request. Be aware that tax payer and fiskaly GmbH have an on-going business relation, which enables fiskaly GmbH to easily check that the requesting tax payer is indeed entitled to revoke the specific CTSS certificate. Here fiskaly GmbH is constantly aware, which tax payers use which CTSS certificates. To authorize towards DARZ -as CRL maintainer- fiskaly GmbH uses the revocation password, which fiskaly GmbH received, when the CTSS certificate was issued. Then fiskaly GmbH transmits the request to the PKI and ensures that the CTSS certificate in question gets revoked.

Note that revoked CTSS certificates remain on the CRL for at least ten years after the end of the validity period of the revoked certificate.

4.4 Registration / Mapping of Tax Payers and Certificates

Fiskaly GmbH provides the root CA certificate(s) for its CTSSs to the BMF, following the requirements of BSI. This action establishes the trust anchor(s) for the cryptographic verification of log messages of the fiskaly CTSSs.

Tax Payers are by law required to register the CTSS and the associated CTSS certificate at the financial authorities. This registration process is not part of the certified CTSS of fiskaly GmbH.

The tax payer is required to perform the registration on its own.

The ERS manufacturer might include this process in the ERS software or create features in their ERS software to support and guide the tax payer in the registration process. All required information from the CTSS can be exported easily as documented in [7] and [5].

Bibliography

[1] Common Criteria. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1, Revision 5, April 2017. `https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf`.

[2] Federal Office for Information Security. BSI TR-03145 Secure Certification Authority operation Version 1.1. `https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03145/TR-03145_node.html`.

[3] Federal Office for Information Security. BSI TR-03153 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme Version 1.0.1. `https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03153/tr03153_node.html`.

[4] Federal Office for Information Security. Protection Profile Cryptographic Service Provider Light (CSPL) Version 1.0, BSI-CC-PP-0111-2019. `https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0111.html`.

[5] fiskaly GmbH. Functional Specification – Security Module Application for Electronic Record-Keeping Systems, Version 1.1.3, 2021.

[6] fiskaly GmbH. Functional Specification, fiskaly Cloud Crypto Service Provider Version 1.2.8, 2021.

[7] fiskaly GmbH. Preparative Procedures & Operational User Guidance Documentation – fiskaly Security Module Application for Electronic Record-Keeping Systems, Version 1.1.4, 2021.

[8] fiskaly GmbH. Security Target, – fiskaly Security Module Application for Electronic Record-Keeping Systems, Version 1.1.4, 2021.

Keywords

Term	**Description**
authentication reference data	data used by the TOE to verify the authentication attempt of a user
authentication verification data	data used by the user to authenticate themselves to the TOE
authenticity	the property that ensures that the identity of a subject or resource is the one claimed (cf. ISO/IEC 7498-2:1989)
cluster	a system of TOE samples initialized by an administrator and communication through trusted channels in order to manage known users and to share the cryptographic keys
cryptographic key	a variable parameter which is used in a cryptographic algorithm or protocol
data integrity	the property that data has not been altered or destroyed in an unauthorized manner (cf. ISO/IEC 7498-2:1989)
firmware	executable code that is stored in hardware and cannot be dynamically written or modified during execution while operating on a non-modifiable or limited execution platform, cf. ISO/IEC 19790
hardware	physical equipment or comprises the physical components used to process programs and data or to protect physically the processing components, cf. ISO/IEC 19790
Issuer of update code package	Trusted authority issuing an update code package (UCP) and holding the signature private key for signing the UCP and corresponding to the public key implemented in the TOE for verification of the UCP. The issuer is typically the TOE manufacturer. The issuer of an UCP is identified by the security attribute Issuer of the UCP.
Platform guidance	All documentation provided by the hardware manufacturer, or software platform manufacturer, that provides information on how to securely implement functionality.

private key	confidential key used for asymmetric cryptographic mechanisms like decryption of cipher text, signature-creation or authentication proof, where it is difficult for the adversary to derive the confidential private key from the known public key
public key	public known used for asymmetric cryptographic mechanisms like encryption of cipher text, signature-verification or authentication verification, where it is difficult for the adversary to derive the confidential private key from the known public key
secret key	key of symmetric cryptographic mechanisms, using two identical keys with the same secret value or two different values, where one may be easy calculated from the other one, for complementary operations like encryption / decryption, signature-creation / signature-verification, or authentication proof / authentication verification
secure channel	a trusted channel which is physically protected and logical separated communication channel between the TOE and the user, or is protected by means of cryptographic mechanisms
software	executable code that is stored on erasable media which can be dynamically written and modified during execution while operating on a modifiable execution platform, cf. ISO/IEC 19790
trusted channel	a means by which a TSF and another trusted IT product can communicate with necessary confidence (cf. CC part 1 [1], paragraph 97)
update code package	code if implemented changing the TOE implementation at the end of the TOE life time

Table 4.1: Glossary (Table 8 in Base-PP [4])

Abbreviations

Acronym	**Term**
A.xxx	Assumption
CC	Common Criteria
CSP	Cryptographic Service Provider
CSPLight	Cryptographic Service Provider Light
ECC	Elliptic curve cryptography
HMAC	Keyed-Hash Message Authentication Code
KDF	Key derivation function
MAC	Message Authentication Code
n. a.	Not applicable
O.xxx	Security objective for the TOE
OE.xxx	Security objective for the TOE environment
OSP.xxx	Organisational security policy
PACE	Password Authenticated Connection Establishment
PKI	Public key infrastructure
PP	Protection profile
SAR	Security assurance requirements
SFR	Security functional requirement
T.xxx	Threat
TOE	Target of Evaluation
TSF	TOE security functionality
UCP	update code package

Table 4.2: Abbreviations (Table 9 in Base-PP [4])