fiskaly.

PKI Concept

fiskaly Security Module Application for Electronic Record-keeping Systems

TOE Version 1.0.15

Document Version 1.1.16

2025-01-23

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. In the context of this document the term PKI (and the more specific term DARZ-TSE-PKI) refer to the *Set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates as long as it concerns the root CA DARZ-TSE-ROOT-CA-01 and its associated sub CAs and entity certificates.*

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:	1.1.16
Document Status:	Released
Document built from commit:	55d0d8d75a9c9b971ffae60861decf54401c3541
Date:	2025-01-23
Author:	fiskaly GmbH
Certification-ID:	BSI-DSZ-CC-1130-V4
TOE Identification:	fiskaly Security Module Application for Electronic Record-keeping Systems
TOE Version:	1.0.15
CC Version:	CC:2022 Revision 1
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:

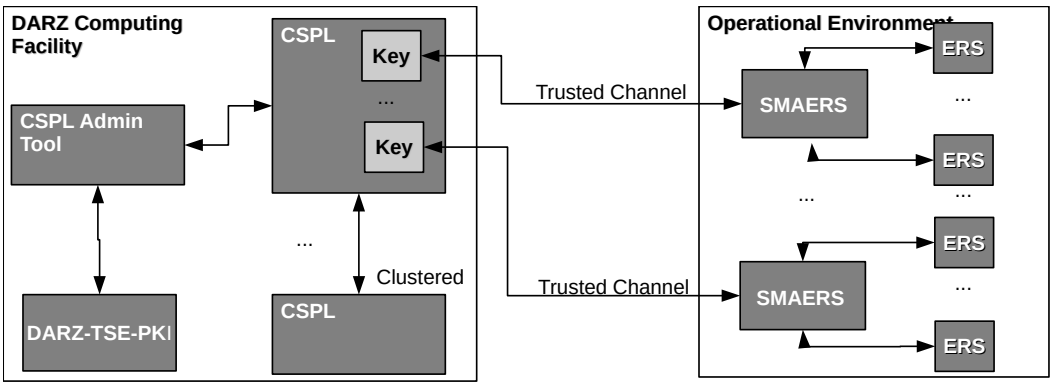

Figure 1.1: Landscape Overview

- The DARZ-TSE-PKI, operated by DARZ to issue CTSS certificates for CTSS signing keys of CTSSs. The used root CA/sub CA 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 / certificate: The sub CA key and certificate are part of the DARZ-TSE-PKI. It is used to issue the signature certificates.
- root CA key / certificate: The root CA key and certificate are part of the DARZ-TSE-PKI. It is 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 handed over personally by a representative of fiskaly GmbH who is directly authorized (in writing) by a legal representative mentioned in the Firmenbuch of Austria.
- *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 REST interface and to sign certificate requests for CTSS signature keys. It is stored in the *CSPL Admin Tool*, which is operated

via SSH-secured remote access on hardware controlled by *fiskaly* and hosted in the DARZ computing facilities. Only specially authorized employees of fiskaly GmbH have access to the *CSPL Admin Tool* via dedicated SSH keys.

- attestation key: This is a key pair, which is stored 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 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 certificate for the 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

DARZ has been certified as a PKI operator according to TR-03145-1 [4], (previously under the ID BSI-K-TR-0478-2021 and now with the certificate ID BSI-K-TR-0635-2024). 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.*

DARZ provides the root CA DARZ-TSE-ROOT-CA-01 and its sub CAs exclusively for productive certificates of CTSS products certified according to TR-03153 [1]. No other type of certificates or test certificates are being, have been, or will be issued under/from this root CA or its sub CAs. TSSs of different manufacturers have been, are, and will be distinguished by being assigned to new sub CAs under the root CA DARZ-TSE-ROOT-CA-01, e.g. DARZ-TSE-SUB-CA-01, DARZ-TSE-SUB-CA-02, and so forth. The *fiskaly Cloud Crypto Service Provider* exclusively uses the sub CA DARZ-TSE-SUB-CA-01 for the CTSS certificates of its signature keys, which are exclusively used in the context of the fiskaly CTSS. Also, the sub CA DARZ-

TSE-SUB-CA-01 exclusively issues CTSS certificates for the fiskaly CTSS (for more details, see Chapter 3).

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.

Key Generation

All CTSS signature key pairs are created in the CSPL. This is done by a *fiskaly* employee, authenticated 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* [7] 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.

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.

After its creation, the bootstrap file is exclusively in possession of fiskaly GmbH and is deployed on a tax payer machine by fiskaly GmbH personnel only for the purpose of personalization. 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.

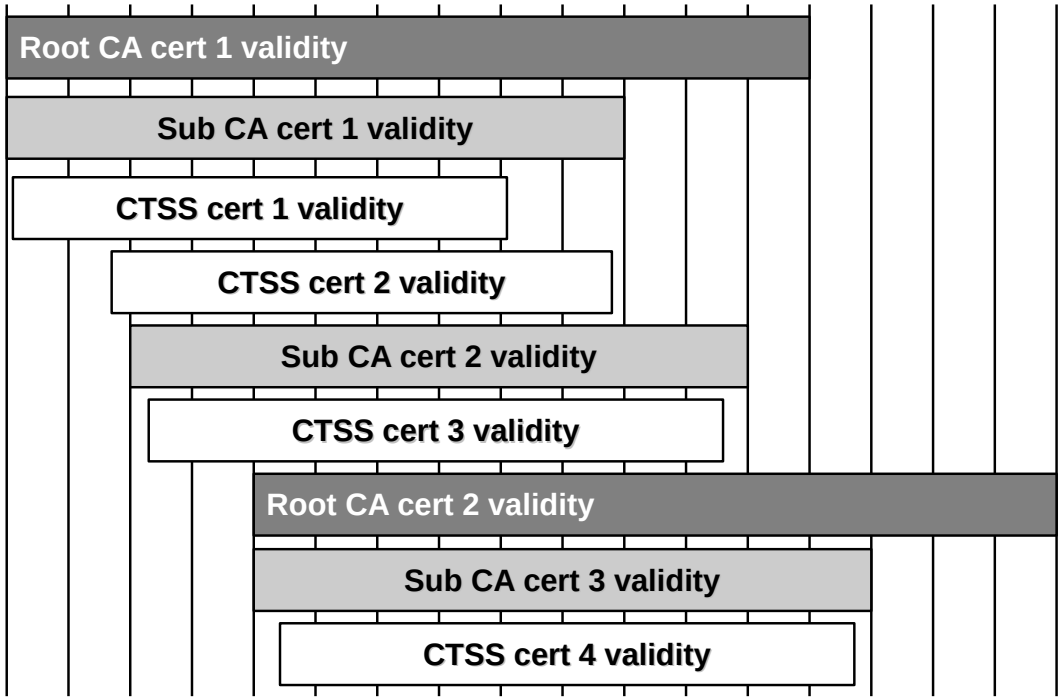

Figure 4.1: Timeline Overview

The root CA DARZ-TSE-ROOT-CA-01 will expire after 13 years, and the sub CA DARZ-TSE-SUB-CA-01 will expire after 10 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, new sub CA certificates are issued at the latest every two years, so that no CTSS certificate can be issued with a validity longer than its parent sub CA. Correspondingly, assuming a new sub CA every two years, a new root CA has to be issued at the latest every 4 years, so that it covers the validity of the sub CA certificate that has to be issued at that time, as depicted in Figure 4.1, and so on. The new CA certificates retain their name and are distinguished by incremented serial numbers. The issuing of a new sub or root CA does not affect the validity of the already issued CTSS certificates, which remain in use until their original expiration date is reached. This is also 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 the sub CA DARZ-TSE-SUB-CA-01, 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 handed over personally by a representative of fiskaly GmbH who is directly authorized (in writing) by a legal representative mentioned in the Firmenbuch of Austria. In addition, the fingerprint of the root certificate is published in the *Security Target* [10] of fiskaly SMAERS, which can be found at the BSI homepage. 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 = 1
  - C = DE
  - O = DARZ
  - CN = DARZ-TSE-ROOT-CA-01
- SubjectPublicKeyInfo
  - Named Curve: brainpoolP384r1 (1.3.36.3.3.2.8.1.1.11)

As described in Chapter 4, the serial number will be incremented upon the creation of a new root CA (at the latest by 2.6.2025).

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: yes
- 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`

IssuerAltName

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

BasicConstraints

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

AuthorityInfoAccess

- OID: 1.3.6.1.5.5.7.1.1
- 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 = 1
  - C = DE
  - O = DARZ
  - CN = DARZ-TSE-SUB-CA-01
- SubjectPublicKeyInfo
  - Named Curve: brainpoolP384r1 (1.3.36.3.3.2.8.1.1.11)

As described in Chapter 4, the serial number is incremented with the issue of new sub CAs every two years:

- 1, for CTSS certificates issued in the period 1.6.2021–1.6.2023
- 2, for CTSS certificates issued in the period 2.6.2023–2.6.2025
- and so on

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: yes
- 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=DARZ-TSE-ROOT-CA-01,O=DARZ,C=DE,SERIALNUMBER=1`, where Serial Number depends on the Serial Number in the subject of the root CA certificate (here: 1)
  - `ldap://ldap-tse-pki.da-rz.net/serialNumber=1,CN=DARZ-TSE-ROOT-CA-01,DC=DARZ,DC=DE?certificateRevocationList`, where Serial Number depends on the Serial Number in the subject of the root CA certificate (here: 1)

AuthorityInfoAccess

- OID: 1.3.6.1.5.5.7.1.1
- 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 [1], including a SHA-256 hash of the public key as SERIALNUMBER
- SubjectPublicKeyInfo
  - Named Curve: secpP256r1 (1.2.840.10045.3.1.7)

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: yes
- 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=DARZ-TSE-SUB-CA-01,O=DARZ,C=DE,SERIALNUMBER=2`, where Serial Number depends on the Serial Number in the subject of the sub CA certificate (here: 2)
  - `ldap://ldap-tse-pki.da-rz.net/serialNumber=2,CN=DARZ-TSE-SUB-CA-01,DC=DARZ,DC=DE?certificateRevocationList`, where Serial Number depends on the Serial Number in the subject of the sub CA certificate (here: 2)

AuthorityInfoAccess

- OID: 1.3.6.1.5.5.7.1.1
- 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* [9].

4.2.1 Verification of Transaction Logs

The verification of transaction logs can be performed following the description in chapter 10 of BSI TR-03153-1 (Version 1.1.1) [3].

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 an 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 an 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) failed.

4.3 Certificate Revocation

To check if certificates were revoked, DARZ – as operator of the PKI – maintains certificate revocation lists (CRLs). 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 Certificate 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 one or more CTSS certificates, the tax payer contacts fiskaly GmbH. fiskaly GmbH– as CTSS operator – will create a revocation request. Every such request is documented internally

by fiskaly GmbH in a dedicated ticket, where the information outlined in RM.Req.10 of [5] is persisted. As this information is not otherwise available, e.g., for tax inspectors, the dedicated email address 'ctss-invalidity-date-info@fiskaly.com' can be used to query it. The requesting tax payer and fiskaly GmbH have an on-going business relation, which enables fiskaly GmbH to easily check that the 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 *CSPL Admin Tool*, where a TLS client certificate is deposed that authorizes the *CSPL Admin Tool* to submit requests to the PKI API. 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.

In case the root CA is compromised, DARZ – as operator of the PKI – will inform fiskaly GmbH, who will immediately contact the BMF, related tax authorities and the manufacturer(s) of the official audit inspection tool(s) via email for the revocation of the root CA certificate. To ensure delivery, in case any of the recipients do not confirm reception within a week, the same information will be sent to them again via email and via post.

Tax inspectors and other entities interested in verifying the validity of a CTSS certificate are therefore urged to regularly consult the list of valid root CAs maintained by the BMF.

4.4 Registration / Mapping of Tax Payers and Certificates

fiskaly GmbH provides the root CA certificate 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 [9] and [8].

Bibliography

[1] Federal Office for Information Security. BSI TR-03153 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme. https://www.bsi.bund.de/dok/TR-03153.

[2] Federal Office for Information Security. Common Criteria 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, 12.11.2019.

[3] Federal Office for Information Security. BSI TR-03153-1 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme, Teil 1, Version 1.1.1. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03153/TR-03153-1_Version1-1-1.pdf, 19.12.2023.

[4] Federal Office for Information Security. BSI TR-03145 Secure CA Operation, Part 1, Version 1.1. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03145/TR03145.pdf, 27.3.2017.

[5] Federal Office for Information Security. BSI TR-03145 Secure CA Operation, Part 5, Version 1.0.1. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03145/TR03145.pdf, 5.6.2023.

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

[7] fiskaly GmbH. fiskaly Cloud Crypto Service Provider, Version 1.5.0 – Functional Specification, Version 1.4.0, 2024.

[8] fiskaly GmbH. fiskaly Security Module Application for Electronic Record-keeping Systems, Version 1.0.15 – Functional Specification, Version 1.3.0, 2025.

[9] fiskaly GmbH. fiskaly Security Module Application for Electronic Record-keeping Systems, Version 1.0.15 – Preparative Procedures & Operational User Guidance Documentation, Version 1.4.1, 2025.

[10] fiskaly GmbH. fiskaly Security Module Application for Electronic Record-keeping Systems, Version 1.0.15 – Security Target, Version 1.4.4, 2025.

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 [6], 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 [2])

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 [2])