PKI Disclosure Statement

Version: 2.3

Document Card:

Document title	PKI DISCLOSURE STATEMENT OF CCK MF CERTIFICATION POLICY
Document owner	Security Department Ministry of Finance Republic of Poland
Version	2.3
Document status	**Approved**
Date of approval	11.05.2026
Number of pages	8

approved by:

Version	Approved by
2.3	The Director of Security Department Ministry of Finance

Contents

1 TSP contact info

The contact point for handling any matters related to execution of the certification policy by Ministry of Finance (further: **MF**) Republic of Poland is:

Ministry of Finance
Security Department

Postal address, names of management staff and contact phone are published on the website:

https://www.gov.pl/web/finance/security-department
e-mail: sekretariat.dbe@mf.gov.pl

Within the CCK[1] MF certification system (see chapter **2.1)**, publicly available certificates are issued only within the following sub-systems: *CCK MF External* (Zewnętrzne) and *CCK KSeF*.

Together with the certificate, the *CCK MF External* subsystem provide the subscriber with a confidential identification code, necessary for authentication in contacts with CCK MF, including certificate revocation, suspension, suspension repealing.

To revoke a certificate issued for a given identifier in the *CCK KSeF* sub-system, you must authenticate yourself using an authentication means containing this identifier, i.e. the NIP or PESEL number, or – in the case of a qualified certificate without the NIP or PESEL number – a qualified certificate whose SHA256 hash (so-called *fingerprint*) is included in the certificate being revoked.

The details of the appropriate certificate revocation procedure can be found in the documents published in Polish on the websites:

- in case of *CCK MF External*
  https://puesc.gov.pl/uslugi/uzyskaj-lub-uniewaznij-certyfikat-celny
- in case of *CCK KSeF*
  https://ksef.podatki.gov.pl/ksef-na-okres-obligatoryjny/certyfikaty-ksef/

2 Certificate types, validation procedures and usage

2.1 Certificate types

The “CCK MF” certification system consists of Root and certification subsystems, as illustrated in the figure below:

[1] *Certification Centre*; otherwise: *CA* (Certification Authority)

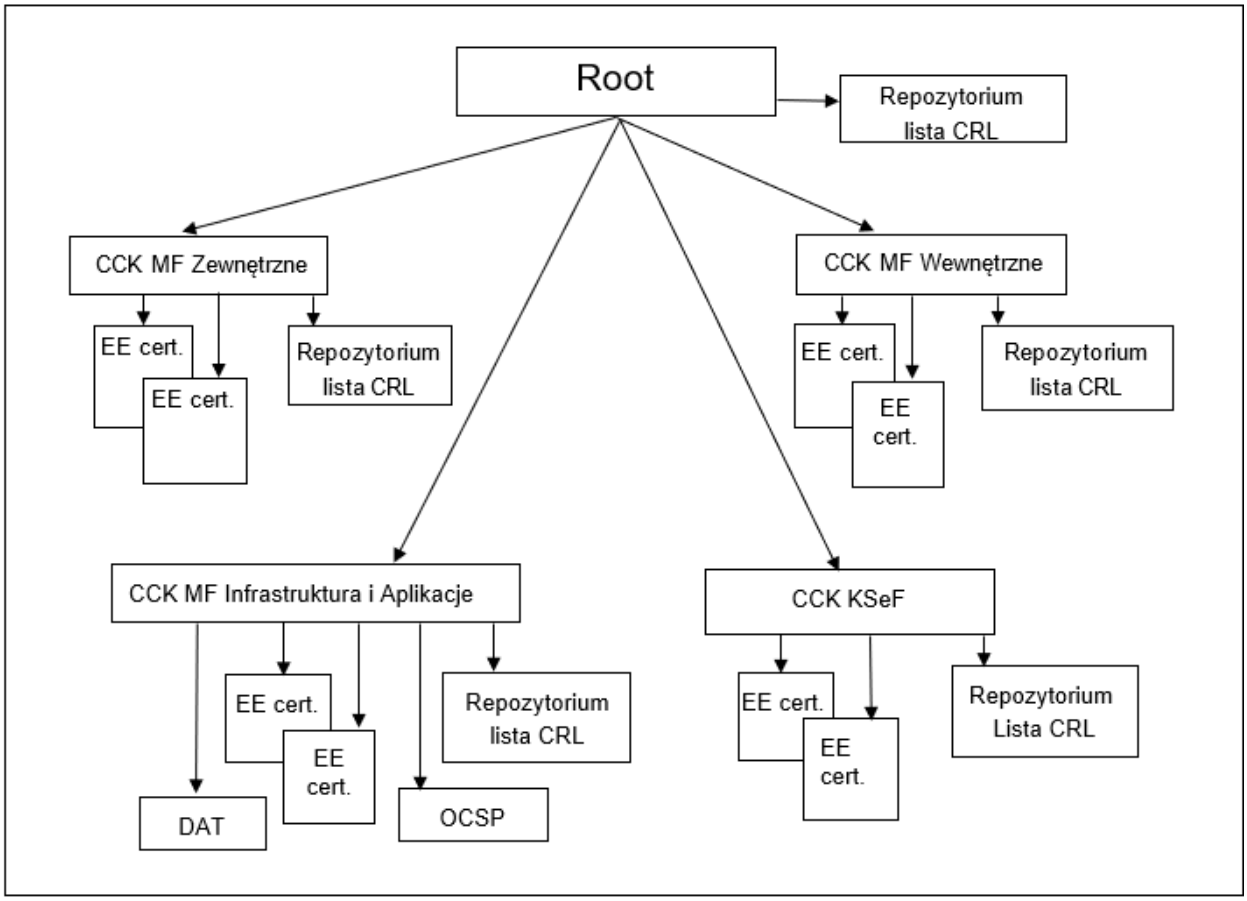

Figure 1 Logical diagram od the PKI system

Root issues *CA certificates* only:

- self-signed certificates for distribution of the trust anchor,
- cross-certificates for subCAs.

SubCA issues *EE certificates* only:

- certificates for subscribers,
- certificates for OCSP[2] Responder (Infrastructure and Application subCA only).

The subscriber of trust services within the CCK MF may be any natural person with full legal capacity or any legal person within the meaning of national law, as well as any other entity of a similar nature (an organizational unit without legal personality, a civil partnership, etc.) or - in the case of subCA Infrastructure and Applications - even a device or application.

All certificates have profile compliant with X.509 v3 standard.

Private keys for electronic signatures/seals could be generated and stored on devices such as smart cards, and may also be generated in the application and stored in a software token such as PKCS#12.

[2] *Online Certificate Status Protocol*

2.2 Identity validation procedures

In the case of internal subsystems (*CCK MF Internal* and *CCK MF Infrastructure and Applications*), identity validation is carried out based on the internal procedures of the Ministry of Finance. In the case of external systems (*CCK MF External* and *CCK KSeF*), the subscriber's identity is validated when setting up the appropriate account in the system PUESC[3] or – in the case of system KSeF[4] – in order to submit an application for a certificate, the user must authenticate and authorize himself in KSeF and then submit the application via this system.

PUESC System
Identity confirmation as part of obtaining a PUESC account with an extended scope of authorizations is possible on the basis of:

- signing the application with a qualified signature,
- signing the application with a trusted signature,
- personal appearance ("face-to-face") and identification with an identity document (identity card, passport, permanent residence card):
  - at the customs and tax office;
  - at the customs and tax office delegation or
  - at the customs branch.

In the case of citizens of a third country (outside the EU), the authenticity of the registration data can be confirmed:

- at the consulate,
- at the embassy,
- at a notary in the country of residence.

The principles of identity confirmation are described in Polish at
https://puesc.gov.pl/web/guest/uslugi/sposoby-potwierdzania-tozsamosci-osoby

KSeF System
Identity confirmation on the KSeF platform is possible based on:

- signing the application with a qualified signature (the qualified certificate must contain the PESEL number),
- sealing the application with a qualified stamp (the qualified certificate must contain the NIP or REGON number),
- signing the application with a trusted signature (verified by the ePUAP Trusted Profile)[5]
- electronic seal verified by the EE AP Peppol[6] certificate
- authentication via the National Electronic Identification Node[7] using electronic identification means with assurance level substantial or high.

Authentication may also be made basing on previous certificate (on a valid signature/seal of the person applying for the certificate). In such case a new certificate will contain the same data identifying the subscriber as the data in the previous certificate.

2.3 Certificate usage

As part of the CCK MF certification policy, the following certificates are generated for subscribers:

- the *CCK MF External* subsystem – customs certificates for signing documents sent to National

[3] The Tax and Customs Electronic Services Portal

[4] The National System of e-Invoices

[5] https://www.biznes.gov.pl/en/portal/004724

[6] https://efaktura.gov.pl/openpeppol/

[7] https://www.gov.pl/web/cyfryzacja/budowa-krajowego-wezla-identyfikacji-elektronicznej

Revenue Administration (pl. *Krajowa Administracja Skarbowa*; KAS),
- the *CCK MF Internal* subsystem – customs certificates for KAS and Ministry of Finance employees/officers (1) for signing and (2) for encryption,
- the *CCK MF Infrastructure and Applications* subsystem – certificates for services and devices, certificates for applications, certificates for securing communication and data, also in the scope of exchange with external entities, certificates for electronic seals, time stamping, OCSP,
- the *CCK KSeF* subsystem – certificates for the purpose of authentication and confirmation of invoices in KSeF offline modes.

As it results from the above, certificates issued within the CCK MF have different types of applications, **but their use is limited to the internal needs of units subordinate to the minister responsible for finance**, as well as to communication between citizens and these units in matters concerning handling matters conducted within the framework of services provided electronically. In particular, CCK MF certificates are used to authenticate documents using an advanced electronic signature verified using a customs certificate, referred to in art. 10b of the Act of 19 March 2004 "Customs Law" and in § 4 item 3 of the "Regulation of the Minister of Development and Finance of 19 September 2017 on the method of sending declarations and applications and the types of electronic signatures with which they should be provided" and CCK MF certificates are used to authenticate users and provide invoices with a verification code within KSeF.

3 Reliance limits

The CCK MF does not provide any implied guarantees, except for those that may result from the applicable provisions of common law. CCK MF does not pay compensation for damages or is liable for the lost profits of subscribers.

The CCK MF retains the following information for at least 20 years after any certificate based on these documents ceases to be valid:
- some documentation created on the occasion of acceptance of the certificate (i.e. reporting the need for correction),
- all issued certificates,
- all events related to the change of certificate status, including all issued CRL[8]s.

4 Obligations of the subscribers

The subscriber is obliged to provide his/her true data during registration. After receiving the certificate, check the correctness of the data contained in the certificate before first use. In the event of finding any irregularities, the subscriber should immediately notify the certificate issuer and apply for a new one, correcting the previously incorrect data.

The subscriber is obliged to properly protect the private key against disclosure or use by unauthorized persons. Private key for electronic signature should remain at the sole discretion of the subscriber – the natural person whose data are placed in the certificate. It is not acceptable for the key to be used by another person. Private key for electronic seal should remain at the sole discretion of the person or persons authorized by a given person/organization.

In the event of a justified suspicion of access to the private key by an unauthorized person, loss or disclosure of the private key or circumstances in which there is a risk of unauthorized use of the key, the subscriber is obliged to immediately revoke the certificate.

The CCK MF subscriber's certificates may not be used by persons or entities external to MF and

[8] *Certificate Revocation List*

subordinate units and for purposes other than transferring data to MF systems or verifying messages transmitted from these systems. In particular, certificates issued by *CCK MF External*, *CCK MF Internal*, *CCK MF Infrastructure and Applications* and *CCK KSeF* cannot be used to confirm the sender's identity in private life or in matters addressed to other entities or public administration offices, with the exception of services provided via electronic platforms of the Ministry of Finance or the National Revenue Administration and internal exchange of information in units subordinate to the minister responsible for finance.

The CCK MF certification policy does not impose an obligation to store subscriber's keys in special devices such as electronic cards.

5 Certificate status checking obligations of relying parties

The only way to confirm the subscriber's certificate validity in terms of possible revocation or suspension is to check certificate status on an appropriate CRL list or using the OCSP service, however, the OCSP service is not available in every certification subsystem.

The fact that a new CRL has not been published within a specified time cannot be the basis for concluding that the certificates have not been revoked.

In order to examine the status of the certificate revocation, it is required to:
- download the OCSP token for this certificate and check the certificate status saved in this token or
- download the CRL list issued after the time at which we examine the certificate validity and check the status of the certificate on CRL.

Verification of the correctness of signatures on certificates, OCSP tokens and CRLs must be performed on the basis of a certification path starting with the Root public key (the so-called "trust anchor").

Note that in the *CCK KSeF* subsystem, the CRL includes the critical issuingDistributionPoint extension, which allows the CRL to be segmented into smaller parts. According to section 5.2.5 of RFC 5280 (X.509), the syntax and semantics of the distributionPoint field in this extension are the same as those of the distributionPoint field in the CRLDistributionPoints extension in certificates. If the distributionPoint field is present in the issuingDistributionPoint extension, it MUST contain at least one of the names from the corresponding distributionPoint field of the cRLDistributionPoints extension of each certificate that is in scope for this CRL (the same encoding is used in the distributionPoint fields of the certificate and the CRL).

6 Limited warranty and disclaimer / Limitation of liability

The CCK MF is obligated to:
- properly protect its private keys against damage or disclosure,
- ensure access control to hardware and software used in the CCK MF,
- timely execution of certificate suspension/revocation requests,
- publish and maintain up-to-date CRL lists and OCSP tokens (the OCSP service is not implemented in all subsystems).

The CCK MF is not liable for the consequences of using a certificate issued to a subscriber in a manner inconsistent with this certification policy.

The CCK MF, providing trust services, is not responsible for the correct operation of the software used by the subscriber/relying party and the correctness and adequacy of technical and organizational security measures applied by the subscriber/relying party.

In no event shall CCK MF be liable for any damages incurred by subscribers and relying parties (or other

parties) resulting from or in any way related to the improper use or exploitation of a certificate issued by CCK MF that has been:
• revoked or expired,
• used for an unauthorized purpose,
• manipulated (its integrity has not been positively verified),
• cracked (the complementary private key has been compromised),
• omitted.

7 Applicable agreements, Certification Policy

This summary applies to the certification policy whose identifying data is included in the table below:

Policy name	Polityka certyfikacji CCK MF
Policy qualifier	none
OID (*Object Identifier*)	0.4.0.2042.1.3 itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) lcp (3)
Version	2.3
Approval data	11.05.2026
Validity	until further notice

The complete text of the certification policy document in Polish is available on the website:

https://puesc.gov.pl/pki/resource/Polityka_certyfikacji_CCK_MF.pdf
or
https://ksef.podatki.gov.pl/ksef-na-okres-obligatoryjny/certyfikaty-ksef/

8 Privacy policy

The CCK MF processes subscribers' personal data in accordance with applicable regulations regarding their protection and the requirements specified in the Personal Data Protection Policy applicable in the Finance Resort.

9 Refund policy

If a subscriber is not satisfied with the services, they may request certificate revocation. The CCK MF does not charge any fees for services provided, hence there are no refunds.

10 Applicable law, complaints and dispute resolution

The applicable law in the scope of application of this certification policy is Polish law. In matters of interpretation of any provisions, the provisions of Polish law shall apply. Any disputes that cannot be resolved through amicable negotiations shall be resolved by Polish courts.

11 TSP and repository licenses, trust marks, and audit

The CCK MF is subject to regular internal audits, conducted by persons not involved in the current management of CCK MF, as well as external audits.

Security audits are conducted while maintaining the objectivity and impartiality of the audit process, in

particular it is ensured that persons conducting the security audit are not responsible for reviewing that part of the system in which they participate as part of their official duties.

Persons conducting the security audit have appropriate qualifications, experience and knowledge in the field of security audit methodology.

Tasks related to conducting a security audit may be entrusted to an external entity ensuring:

- implementation in accordance with the standards for auditing information security management systems specified in Polish and international standards, including ISO 19011,
- qualified auditors, including the lead auditor, with certificates confirming knowledge in the field of auditing for compliance with the ISO 27001 standard,
- appropriate experience confirmed by references.

An external audit is carried out at least once every 2 years.

The internal documentation of the Ministry of Finance contains a document specifying the audit procedures.

The CCK MF is included in the Register maintained by the National Bank of Poland. That Register is kept pursuant to the provisions of Article 6 of the Act of 5 September 2016 on Trust Services and Electronic Identification (consolidated text Journal of Laws of 2024, item 1725). The minister in charge of digital affairs does not control such an entity ex ante, he/she can only order an inspection when an irregularity has been reported, pursuant to Article 17(3)(b) of the eIDAS regulation[9].

[9] Regulation of the European Parliament and the European Council (EU) No. 910/2014 of 23 July 2014 on electronic identification and trust services with regard to electronic transactions on the internal market and repealing Directive 1999/93/EC