NISZ

National Infocommunications Services Company
Limited by Shares

GovCA
PKI Disclosure Statement

OID: 0.2.216.1.200.1100.100.42.3.1.19
Effective date: 28 April, 2025
Version: 1.7

Adorján István

Digitálisan aláírta:
Adorján István
Dátum: 2025.03.27
08:49:19 +01'00'

Important Notice about this Document

This document is the PKI Disclosure Statement (herein after referred as the PDS. This document does not substitute or replace the Certificate Policy (CP) / Certification Practice Statement (CPS) under which certificates for electronic signature issued by NISZ are issued. You must read the CP (BR-MTT) / CPS (BSZ-MTT) at https://hiteles.gov.hu/szabalyzatok before you apply for or rely on a certificate issued by NISZ.

The purpose of this document is to summarize the key points of the CP/CPS for the benefit of Subscribers and Relying Parties.

This document is not intended to create contractual relationship between NISZ National Infocommunication Services Company Limited by Shares (herein after referred as Trusted Service Provider or TSP) and any other person or organization. Any person seeking to rely on certificates or participate within the NISZ PKI must do it so pursuant to definitive contractual documentation. This version of the PDS has been approved for use by the NISZ Policy Management Group and is subject to amendment and change in accordance with the policies and guidelines adopted, from time to time, by the Policy Management Group. The date on which this version of the PDS becomes effective is indicated on this document.

Content

1. TSP CONTACT INFO

NISZ National Infocommunications Services Company Limited by Shares
Registered seat: Róna street 52-80, Budapest H-1149, HUNGARY
Website: https://hiteles.gov.hu

Customer Service Office:
Address: Vaskapu street 30/b, Budapest H-1097, HUNGARY
Phone: +36 1 795-7200
Email: info@hiteles.gov.hu

HelpDesk:
Phone: +36 1 795-7300
Email: helpdesk@nisz.hu

2. CERTIFICATE TYPE, VALIDATION PROCEDURES AND USAGE

Certificate type

RSA environment

The TSP under the name of "Minősített Tanúsítványkiadó v2 – GOV CA" issues qualified certificate, that contains RSA keys with a length of 2048 bits, for electronic signatures or seals for legal persons or entities without legal personality in public registers. Certificate profile is compliant with EN 319 412. The applied policy and security requirements are compliant with EN 319 411 and EN 319 401.

CA Name	CA Certificate	Subject Key Identifier
Minősített Tanúsítványkiadó v2 - GOV CA	http://qca.hiteles.gov.hu/cer/GOVCA-Qv2.cer	F4 A3 3B 8F 29 7A 31 28 CF 6B C8 86 F8 26 A8 CB DD 27 88 80

ECC environment

The TSP under the name of "GovCA Minősített Tanúsítványkiadó", "GovCA Minősített Tanúsítványkiadó 2024" and „GovCA Minősített Közigazgatási Tanúsítványkiadó" issues qualified certificate, that contains ECC keys (or in the case of such special order RSA keys with a length of 3072 bits), for electronic signatures or seals for legal persons or entities without legal personality listed in public registers. The qualified certificates issued by „GovCA Minősített Közigazgatási Tanúsítványkiadó" can be used for the provision of digital services or for official document issuance. The certificate used by an individual authorized to issue official documents includes the technical object identifier 0.2.216.1.200.1100.100.42.3.7. Certificate profile is compliant with EN 319 412 standard. The applied policy and security requirements are compliant with EN 319 411 and EN 319 401 standards.

CA Name	CA Certificate	Subject Key Identifier
GovCA Minősített Tanúsítványkiadó	http://qca.hiteles.gov.hu/ecc/cer/govca-ecc-q.cer	BC F7 B1 51 B4 7A C9 B5 0D FB 6E 52 2D DB 0B B6 41 33 B3 C9
GovCA Minősített Tanúsítványkiadó 2024	http://qca.hiteles.gov.hu/ecc/cer/govca-ecc-q2024.cer	CC 72 1D C9 25 B0 12 B2 2E DC 12 7E 63 22 10 07 7B C4 1B 42
GovCA Minősített Közigazgatási Tanúsítványkiadó	http://qca.hiteles.gov.hu/ecc/cer/govca-ecc-qket.cer	31 8F 35 00 31 8E 6A 4A F6 B6 E1 21 EE 4C 2C 8F 07 92 A0 11

Certificate application

The subscriber may apply for the certificate by entering into the Subscriber Agreement and filling the Certificate Request Form. The registration process of the certificates issued for the provision of digital services is compliant with the 322/2024 (XI. 6.) Government Regulation of Hungary.

Certificate usage

The private key associated to the certificate can be used only for creating electronic signatures or seals, the certified public key can be used only for validating electronic signatures or seals.

Certificate validity period

The validity period of the certificate is usually three years, or can be less based on a special order.

Certificate suspension and revocation

Certificate suspension may be requested by the subscriber, the authorized representative of the organization or by the subscriber's contact person by telephone at the Phone Help Desk (7/24) by announcing the suspension password. The certificate is suspended for up to 5 calendar days - or if the last calendar day is not a working day, the next business day.

Certificate revocation may be requested by the signatory, the authorized representative of the organization or by the subscriber contact in person or by post with hand signature at the Customer Relationship Office or by sending an electronically signed document.

3. RELIANCE LIMITS

Refer to section 9.8 of the CP/CPS for reliance limits. The TSP undertakes the liability for breach of its obligations pursuant to the CP/CPS.

Retention period

All events involved in the generation of CA key pairs, certificate generation and issuance, certificate revocation and every event having significant importance on security are recorded. Audit logs are retained as archive records for a period no less than twelve (12) years and no less than ten (10) years for certificate issuance data after expiration of validity of the certificate.

4. OBLIGATIONS OF SUBSCRIBERS

By applying for the certificate issuance and entering into the Subscriber Agreement, the subscriber to enter the certification system on the conditions stated in the Agreement, CP and CPS.
Subscriber is committed to:

- comply with the rules of the agreement made with the TSP;
- submit complete and accurate information in connection with an application for the certificate and will promptly update such information from time to time as necessary to maintain such completeness and accuracy;
- immediately inform the TSP about any errors, defects or changes in the certificate;
- exercise sole and complete control and use of the private key that corresponds to the certificate public key;
- secure the private key and take all reasonable and necessary precautions to prevent the theft, tampering, compromise, loss, damage, interference, disclosure or unauthorized use of the private key (including the QSCD holding the private key and the certificate, or other activation data used to control access the private key);

- immediately notify the TSP and start the procedure of revocation in the event that their private key is compromised, or if they reason to believe or suspect or ought reasonably to suspect that the private key has been lost, damaged, modified or accessed by another person, or compromised in any other way whatsoever;
- use the private key and the associated certificate only and exclusively within the validity period of the certificate;
- forthwith upon revocation of the certificate, cease use of the private key and the certificate absolutely;
- use the certificate and the corresponding private key only for the purpose stated in the certificate;
- at all times utilize the certificate in accordance with all applicable laws and regulations.

5. CERTIFICATE STATUS CHECKING OBLIGATIONS OF RELYING PARTIES

A relying party can be any entity who accept an electronic document relying on the validation of the electronic signature or seal.

A relying party is committed to:

- verify that the electronic signature/seal was created using the private key corresponding to the public key certified in the certificate issued by the TSP;
- verify that the certificate is valid at the time of signing/sealing;
- perform certificate path building and validation using the TSP CA Certificates listed on the Hungarian Trusted List as trust anchors, and accept the certificate and the related electronic signature or seal only if the validation yields a positive result;
- check that the certificate has not been revoked by using the OCSP (Online Certificate Status Protocol) service provided or CRL (Certificate Revocation List) issued by the TSP;
- verify that neither the signed or sealed document nor the certificate has been altered after the signature or seal was created;
- carry out cryptographic operations accurately and correctly, using reliable and secure software, devices and IT environment;
- consider the electronic signature/seal or the certificate as invalid if the applied software is unable to determine their validity or if the verification result is negative;
- trust the certificate respectively the signed document only if it is used in accordance with the declared purpose and in transactions where the amount does not exceed the transaction limit (`QcStatements` / `QcLimitValue`) stated in the certificate.

6. LIMITED WARRANTY AND DISCLAIMER / LIMITATION OF LIABILITY

The TSP does not take any responsibility for the actions of third parties, subscribers and other parties not associated with the TSP. In particular, the TSP does not bear the responsibility:

- damages arising from force majeure;
- damages arising from inappropriate usage of issued certificate (term inappropriate understood, use of revoked or expired certificate, etc.);
- damages arising from electronic signed documents used in transactions where the transaction amount exceeds the transaction limit declared in the certificate.

7. APPICABLE AGREEMENTS, CPS, CP

The following documents are available online at https://hiteles.gov.hu/szabalyzatok:

- BR-MTT Certificate Policy;
- BSZ-MTT Certification Practice;
- General Terms and Conditions of NISZ (ÁSZF-GOVCA).

8. PRIVACY POLICY

The TSP shall not make the subscriber's certificate available to relying parties without the subject express consent. In this case, data contained in the published certificates are considered public information. Personal data obtained during the registration process will not be released, unless required otherwise by law or fulfil requirements of the CP/CPS (e.g., TSP termination). The related document ("Privacy Policy for GOVCA Services") is available online at https://hiteles.gov.hu/szabalyzatok.

9. REFUND POLICY

The subscriber may request a refund by notifying the Customer Service office in writing within 30 calendar days of the issuance of the certificate. The TSP handles the refund request within 15 calendar days.

10. APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION

Operating of the TSP is based on the general rules stated in the CPS and it is in accordance with the superior legal acts in force in Hungary.

Complaints and dispute resolution

Complaints related to the TSP services can be made in writing to the Customer Service Office. A receipt acknowledge will be sent after arrival. An answer will be provided within 30 working days following the arrival of the complaint.

Before resorting to any dispute resolution mechanism including adjudication or any type of alternative dispute resolution) the complaining party agree to notify the TSP the dispute in an effort to seek dispute resolution. All disputes associated with the TSP services will be resolved according to the Hungarian law.

11. TSP AND REPOSITORY LICENSES, TRUST MARKS AND AUDIT

Information on the conformity assessment of the Provider pursuant to Article 20 of Regulation (EU) No 910/2014:

- Name of the conformity assessment body: Hunguard Kft.
- Conformity assessment report identifier: C299-07/PF01-2024

The TSP is entitled to use the EU trust mark set out in Article 23 of Regulation 910/2014/EU.

The TSP and the service covered by this PDS are listed on the Hungarian Trusted List available at:

http://www.nmhh.hu/tl/pub/HU_TL.xml (machine processable format)
http://www.nmhh.hu/tl/pub/HU_TL.pdf (human readable format)