Kővári Ferenc
Digitálisan aláírta: Kővári Ferenc
Dátum: 2021.08.30 11:22:54 +02'00'

NISZ

National Infocommunications Services Company Limited by Shares

Certification Practice Statement for website authentication certificates

Version	3.3.
OID	0.2.216.1.200.1100.100.42.3.6.25.3.3
Date of effect	06.04.2021
Document category	public

Version history

version	date	description of the	prepared by	controlled by	approved by
1.0.	24.06.2017	Version submitted to authorities for registration	Polysys Kft.	Ferenc Kővári	Attila Ferencz
2.0	31.07.2017	Version modified based on NMHH's suggestions	Eszter Papp	Ferenc Kővári	Attila Ferencz
3.0	31.08.2018	Reviewed version, key generation by TSP deleted	Ferenc Kővári	Eszter Papp	Attila Ferencz
3.1	12.08.2019	Modification of the Client Relations Office's address	Ferenc Kővári	Eszter Papp	Attila Ferencz
3.2	12.09.2019	Changes base on EN standards, and on WebTrust audit suggestions	Polysys Kft. Ferenc Kővári	Ferenc Kővári	Attila Ferenc
3.3	04.03.2021	New PKI ÜKI place for certificate handover	Ferenc Kővári	Ferenc Kovács Dr.	István Adorján

In case there is a deviation between the original Hungarian version of this document and this translation, the Hungarian version shall prevail.

Table of contents

1 INTRODUCTION

This document is the Certification Practice Statement of NISZ, National Infocommunications Services Company Limited by Shares (hereinafter: the Service Provider), which is applicable to its services related to non-qualified website authentication certificates (hereinafter: BSZ-WOT).

This Certification Practice Statement describes the procedural and operational rules for the management (creation, issue, publication, revocation, hereinafter jointly: Services) of certificates issued.

The Service Provider provides its Services to its clients under contract, but it provides access to certain service elements for relying parties controlling the authenticity of websites.

1.1. Overview

The purpose of the Certification Practice Statement is to summarize all the information that the Parties involved in the Services provided by the Service Provider need to know or are recommended to know. It ensures the transparency of the Service Provider's operation for the recipients and enables them to determine how much the presented practice of providing services and the issued certificates, certificate revocation lists, real-time certificate status responses with their expectations.

This Certification Practice Statement applies to the Services provided under the "Certificate Policy for website authentication certificates" (BR-WOT).

After reading this document and the laws, standards and technical specifications referred to in Chapter 1.6.3 as well as the Service Provider's public documents listed in Chapter 1.6.3.3, the users of certificates, certificate revocation lists, real-time certificate status responses have a clear understanding of the method of managing thereof, the level of security guaranteed by those and the technical, business and financial warranties as well as legal liabilities applicable to them.

This Certification Practice Statement is based on the international recommendation {Sz1} RFC 3647, strictly following it in structure and contents. In order to strictly follow the structure thereof, it also includes chapters where no requirements are specified; in such chapters the "No requirement" text is included.

The Service Provider reported the Services provided under this Certification Practice Statement to the Supervision on the 7th of July 2017. The Supervisory Body's relevant database is available at: http://webpub-ext.nmhh.hu/esign2016/

1.2 Document name and identification

Full name of this certificate policy: "NISZ Ltd. Certification Practice Statement for Website Authentication Certificates".

Short name of the Service Regulation: BSZ-WOT.

The object identifier and version number of the service regulation are indicated on the front page.

This BSZ-WOT contains the detailed rules regarding the issue and use of the certificates issued under the BR-WOT. For the effective date and termination of this Certification Practice Statement, see Chapter 9.10.

Only the copy of this BSZ-WOT with the Service Provider's electronic stamp or the electronic signature shall be regarded as original.

1.2.1. Certification Policies

The Service Provider operation and the issuance of certificates based on this Certificate Policy complies with the actual version of the Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates issued by {Sz21} CA/Browser Forum, which is available at https://cabforum.org/baseline-requirements-documents/. If there is a conflict between this Certification Practice Statement and the Baseline requirements, then the requirements of the BRG shall be followed.

The BR-WOT Certificate Policy conforms to the `organization-validated` certificate policy specified in Chapter 1.2 of {Sz21} Baseline requirements:

```
joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140)
certificate-policies(1) baseline-requirements(2) organization-validated(2)
```

Additionally, the BR-WOT Certificate Policy conforms to the OVCP certificate policy specified in Chapter 5.3 f) of standard {Sz3} EN 319 411-1:

```
OVCP: Organizational Validation Certificate Policy
itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042)
policy-identifiers(1) ovcp (7)
```

The BR-WOT Certificate Policy considers all applicable requirements originating from {Sz20} Mozilla CP.

1.3 PKI participants

1.3.1. Certificate authorities

The Certificate Authority is a central organization of the Service Provider, which consists of certification centres (CA), the central resources of the IT-System supporting the services, the surrounding safe physical environment and the operation staff providing the services.

The Service Provider currently does not cooperate with external organizations in providing the Services.

Root certificate centre

Using its RSA 4096 bit key and the SHA256 algorithm, the Service Provider's root certificate centre issues certificates to productive authentication centres. Main data of the root certificate centre are the following:

Subject: CN= Főtanúsítványkiadó - Kormányzati Hitelesítés Szolgáltató, O= NISZ Nemzeti Infokommunikációs Szolgáltató Zrt, L=Budapest, C=HU

Issuer: CN= Főtanúsítványkiadó - Kormányzati Hitelesítés Szolgáltató, O= NISZ Nemzeti Infokommunikációs Szolgáltató Zrt, L=Budapest, C=HU

SHA1 image file of the root certificate:
FF:B7:E0:8F:66:E1:D0:C2:58:2F:02:45:C4:97:02:92:A4:6E:88:03
SHA256 image file of the root certificate:
C2:15:73:09:D9:AE:E1:7B:F3:4F:4D:F5:E8:8D:BA:EB:A5:7E:03:61:EB:81:4C:BC:23:9F:4D:54:D3:29:A3:8D

Availability of the root certificate:
http://qca.hiteles.gov.hu/cer/GOVCA-ROOT.cer

Productive certificate centre

Using its 2048 bit key and the SHA256 algorithm, the Service Provider's productive certificate centre issues end certificates to Subscribers. Main data of the productive certificate centre are the following:

Subject: CN= SSL Titkosító Tanúsítványkiadó 2014 - GOV CA, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

Issuer: CN= Főtanúsítványkiadó - Kormányzati Hitelesítés Szolgáltató, O= NISZ Nemzeti Infokommunikációs Szolgáltató Zrt, L=Budapest, C=HU

Availability: http://ngca.hiteles.gov.hu/cer/GOVCA-NQ-SSL.cer

1.3.2. Registration authorities

The Service Provider operates a Client Relations Office and a Registration Agency within its own organization.

The Client Relations Office keeps in contact with the clients, records the data of the Subscribers and certificates, checks the identity of the Subscribers and subjects of certificates, prepares Subscriber certificate requests, distributes the completed certificates and ensures that the provisions of the contract are performed.

The Registration Agency provides the technical registration of Subscribers and Subjects of certificates, the administration related to revocation and suspension of certificates and other identification, certificate management and administration tasks.

The Service Provider currently does not cooperate with an external registration agency in providing Services.

1.3.3 Subscribers and Subjects

The Subscriber is a legal entity or organization without legal personality listed in public registers in contract with the Service Provider which orders the Services, typically the issue of a certificate, from the Service Provider for the designated Subjects of certificate.

Subject of the certificate:

- An IT device (web-server) operated by or on behalf of the Subscriber, who is entitled to use its domain name.

1.3.3.1 The Subscriber's Contact Person

During signing the Service Contract, the Subscriber can designate a contact person, who is entitled or authorized by the authorized representative (e.g. signatory) of the Subscriber to act on behalf of the Subscriber's organization in matters related to certificates, and this person can also have signatory right in specified cases. The Service Provider accepts the signature of that person in matters related to certificates, especially in the certificate request process or the certificate revocation process and the requests related thereto. If no contact person is designated, the Service Provider will only accept the signature of an authorized representative in matters related to certificates. In case of website authentication certificates, it is compulsory to designate a Contact Person.

Hereinafter, the Subscriber's Contact Person shall mean the person specified above.

1.3.4. Relying parties

Relying Party: a natural person or legal entity, who or which proceeds based on the website authentication certificate when controlling whether or not there is a real and legitimate organization behind the website.

1.3.5 Other participants

Supervisory Body

The Supervisory Body supervises the Service Provider and the confidential services provided by it, checks the legal compliance of the services. Among others, it follows the development of technological and cryptographic algorithms related to the certificate services, keeps a record of the secure cryptographic algorithms that confidential Service Providers may use in providing their services as well as the requirements for the application of those with specified parameters, and may issue legally binding and executable resolutions for the suspension or revocation of certificates issued within the framework of confidential services.

1.4 Certificate usage

In accordance with Point 38 of Article 3 of {J1} eIDAS, the certificate issued under the scope of this BR-WOT is a non-qualified website authentication certificate, which allows authentication of the website and allocates the website to the legal person for which the certificate was issued.

Under the scope of this BR-WOT, the Service Provider will issue certificates only for domain names which are registered in Hungary by a Hungarian DNS registrar. The issued certificate shall not contain IP address (including internal IP addresses or internal domain names).

Test Certificates

The Service Provider issues test certificates both to test its own system and allow third parties to test the Services. The Service Provider assumes no liability for issuing, using test certificates and the availability of services related thereto.

The Service Provider does not issue a test certificate in the hierarchy of root authentication center providing the live service (neither for domain verification purposes). The test certificates are issued in the hierarchy of the test root authentication centre created specifically for this purpose.

The test certificates are marked in a way that the certificate policy object identifier indicated in the certificate is: 0.2.216.1.200.1100.100.42.3.999.

The test certificates and the website authentication based on those have no legal effects.

1.4.1 Appropriate certificate uses

The issued certificate and the private key belonging to the certificate can only be used for authentication of websites.

In addition to the above, the issued certificates and the related key pairs can be used only for purposes specified in the {D1} General Terms and Conditions and under the terms specified in the {D2} Service Contract.

1.4.2 Prohibited certificate uses

The certificate shall not be used for authenticating other certificates or the provision of any confidential services not agreed upon with the Service Provider.

1.5. Policy administration

1.5.1 Organization administering the document

The Service Provider operates a Certification Policy and Regulation Group within its organization, which shall be liable for the maintenance of this Certification Practice Statement, among others.

1.5.2 Contact person

Data of the Service Provider

Trade register number	01-10-041633
Registered site:	1081 Budapest, Csokonai u.3.
Mailing address:	1389 Budapest, Pf.: 133.
Phone:	+36 1 459-4200
Fax:	+36 1 303-1000
Homepage address:	www.nisz.hu
Data Protection and Security Policy:	Available at http://hiteles.gov.hu/szabalyzatok , in the "*Information on data management for governmental authentication services*" menu.

Client Relations Office

In order to secure client relations, the Service Provider operates a Client Relations Office, which also acts the department competent for the Services, accessible in their opening hours by the clients in person or by phone. The Service Provider publishes the opening hours on the homepage for the Services.

Adress:	1097 Budapest, Vaskapu u.30/b
Phone	+36 1 795-7200
Email	info@hiteles.gov.hu
Homepage for the Service	http://hiteles.gov.hu

The handover of the issued certificates and the related personal identification is also provided by the Customer Relations Office at another location next to the above address: 1054 Budapest, Kálmán Imre utca 2-4. (NISZ Point).

HelpDesk phone line

The Service Provider provides a non-stop (7x24 hours) Help Desk service for receiving requests for certificate revocation as well as reports regarding certificate-related problems (unauthorized use, misuse, etc.) and technical problems of the system used for providing the Services.

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

Competent Consumer Protection Authority

Budapest Government Office, Consumer Protection Department

Address	1052 Budapest, Városház u.7
Phone	+36 1 450-2598
Email	fogyved_kmf_budapest@bfkh.gov.hu

Competent Conciliator

Budapest Conciliator Body

Address:	1016 Budapest, Krisztina krt. 99 Mailing
address:	1253 Budapest, Pf.:20.
Phone:	+36 1 488 2131
Email:	bekelteto.testulet@bkik.hu

1.5.3 Person determining CPS suitability for the policy

The Service Provider verifies if the form and contents of the Certificate Policy and Certification Practice Statement comply with the requirements stated in the applicable laws, regulations and

technical standards, and the results of the verification are considered in th form of change requests.

The change requests are collected by the Certification Policy and Regulation Group, which performs the modifications and submits the changed document for review and approval.

1.5.4 CPS approval procedures

The Service Provider's virtual organization and the leader liable for the Services are responsible and competent to control and approve the document.

Prior to approval, the Service Provider checks whether the Certification Practice Statement matches the Certificate Policy.

The Supervisory Body also checks whether the Certification Practice Statement is in compliance with the applicable laws.

The approved Certification Practice Statement is authenticated with the Service Provider's electronic stamp or the electronic signature of the leader liable for the Services.

The approved Certification Practice Statement is put into force by the leader liable for the Services. The effective date is included in the cover page of the document.

A new version of the Certification Practice Statement is always published with a new version number on the Service Provider's website.

The new version is mandatory for all Subscribers and the changes thereof are recommended to be considered by all Relying Parties using certificates issued under previous versions of the Certification Practice Statement.

1.6 Definitions and acronyms

1.6.1 Definitions

The definitions of terms used in this policy are identical to the definitions described in the laws applicable to the Services (Chapter 1.6.3.1).

The definitions of additional terms are described in Chapter 1.6.1 of the BR-WOT policy.

1.6.2 Acronyms

CA	Certification Authority
CAA	Certification Authority Authorization
CRL	Certificate Revocation List
DNS	Domain Name Service
OCSP	Online Certificate Status Protocol
OVCP	Organizational Validation Certificate Policy
PKI	Public Key Infrastructure
RA	Registration Authority
UTC	Coordinated Universal Time

1.6.3 References

1.6.3.1 References to laws

{J1} 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 and repealing Directive 1999/93/EC (hereinafter: eIDAS)

{J2} Act CCXXII of 2015 on the General Rules for Electronic Administration and Trust Services (hereinafter: E-administration Act)

{J3} Act LXVI of 1992 on Keeping Records on the Personal Data and Address of Citizens (hereinafter: Nytv.)

{J4} Act No. CXXX of 2016 on Civil Procedure (hereinafter: Pp.)

{J5} Act V of 2013 on the Civil Code (hereinafter: Ptk.)

{J6} Decree 24/2017 (VI.30) of Internal Ministry on detailed requirements of trusted services and its service providers

{J7} Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter GDPR)

1.6.3.2 Standards and technical specifications

{Sz1} RFC 3647 Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework

{Sz2} EN 319 401 General policy requirements for Trust Service Providers

{Sz3} EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

{Sz4} EN 319 412-1 Certificate Profiles; Part 1: Overview and common data structures

{Sz5} EN 319 412-2 Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

{Sz6} EN 319 412-3 Certificate Profiles; Part 3: Certificate profile for certificates issues to legal persons

{Sz7} EN 319 412-4 Certificate Profiles; Part 4: Certificate profile for web site certificates

{Sz8} EN 319 412-5 Certificate Profiles; Part 5: QCStatements

{Sz9} RFC 5280 Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile

{Sz10} ITU-T X.520 Information technology - Open Systems Interconnection -The Directory: Selected attribute types

{Sz11} RFC 4514 Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names

{Sz12} ITU-T X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate framework

{Sz13} RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

{Sz14} MSZ/ISO/IEC 15408 ISO/IEC 15408 (parts 1 to 3): Information technology – Security techniques – Evaluation criteria for IT security

{Sz15} ISO/IEC 19790 ISO/IEC 19790:2012: Information technology – Security techniques – Security requirements for cryptographic modules

{Sz16} FIPS 140-2 FIPS PUB 140-2 (2001): Security Requirements for Cryptographic Modules

{Sz17} WebTrust CA Trust Service Principles and Criteria for Certification Authorities, Version 2.2, 1 May 2019, (effective date: 1 June 2019)

{Sz18} WebTrust SSL WebTrust for Certification Authorities – SSL Baseline Requirements Audit Criteria, V2.4.1

{Sz19} Microsoft Root program Microsoft Trusted Root Certificate: Program Requirements

{Sz20} Mozilla CP Mozilla Root Store Policy, Version 2.6.1

{Sz21} BRG CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates

{Sz22} BRG Network Security CA/Browser Forum Network and Certificate System Security Requirements, V1.2

{Sz23} RFC 6844 DNS Certification Authority Authorization (CAA) Resource Record

1.6.3.3 Referred documents

{D1} ÁSZF-GOVCA General Terms and Conditions for NISZ Ltd.'s governmental authentication services

{D2} SZSZ Service Contract

{D3} NISZ Ltd.'s Organizational and Operation Regulation

{D4} NISZ Ltd.'s Data Protection and Security policy

{D5} NISZ Ltd.'s IT Security Policy to PKI Services

{D6} NISZ Ltd.'s Security Regulation to PKI Services

{D7} NISZ Ltd.'s Contingency Plan for PKI Services

{D8} Certificate profiles for NISZ Ltd.'s trust services in accordance with eIDAS regulation

{D9} Certificate order and registration form

{D10} Certificate revocation form

2 PUBLICATION AND AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The Service Provider ensures that the end-user and Service Provider certificates issued by it, the certificates' terms of use, the information about the revocation status of the certificates and the Service Provider's any other announcements of public interest are at the disposal of the Subscribers, the Relying Parties seven days a week, 24 hours a day. The Service Provider makes the information available every day in a year, 24 hours a day with 99% availability in a way that no service failure shall exceed 24 hours.

The Service Provider does not publish documentations containing sensitive and/or confidential information, which include security measures, procedural rules and internal security regulations.

2.2 Publication of certification information

The Service Provider publishes the Service Provider certificates and regulations pertaining to end-user and Service Provider certificates on its website (https://hiteles.gov.hu).

The Service Provider only publishes an end-user certificate in its repository publicly available on its website when the Subscriber has approved publication of the certificate.

The Service Provider also provides the revocation status of end-user and Service Provider certificates in the form of CRL and OCSP. For more details about the publication of the revocation status information, see Chapter 4.10.

2.3 Time or frequency of publication

The Service Provider publishes the Service Provider certificates within 24 hours prior to those going live.

The Service Provider publishes the end-user certificates within 24 hours after the publicly available repository, provided that the Subscriber approves it.

In case the regulations applicable to the certificates are changed, the Service Provider publishes the changed regulations at least 30 days before the changes take effect.

The Service Provider refreshes the CRL at least every 24 hours, therefore the term between two CRL issues does not exceed 24 hours. If the status of a certificate changes, the Service Provider generates and publishes a new CRL immediately but within 7 hours.

Within the framework of its OCSP service, the Service Provider generates and returns a new response to every OCSP query.

2.4 Access controls on repositories

The Service Provider provides unlimited read-only access to the Service Provider certificates and regulations applicable to end-user and Service Provider certificates as well as revocation information of the certificates.

With respect to end-user certificates, it provides the opportunity to search in the public Repository based on data stored in the repository.

The Service Provider takes security measures and applies procedures to protect the information against unauthorized change, deletion, damage and loss.

With respect to the issued certificates, only those regulations which are electronically signed or stamped shall be deemed authentic. Printed versions of the documents should never be deemed as official copies or authentic copies.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

The names in the certificate are entered in accordance with standard {Sz10} ITU-T X.520. In addition to that:

The contents of the Certificate Subject field conforms to:

- the regulations specified in Chapter 4.2.1 of standard {Sz6} EN 319 412-3.

The contents of the Certificate Issuer field conforms to the following:

- the regulations specified in Chapter 4.2.3.1 of standard {Sz5} EN 319 412-2.

3.1.2 Need for names to be meaningful

The meaning of name attributes in the certificate is identical to those defined in {Sz10} ITU-T X.520.

In addition to that, the qualification and certification rules specified in the following sub-chapters apply to the name attributes in the `Subject` field of certificate types specified in Chapter 1.4.

The Service Provider reserves its right to reject pseudonyms or other data which may affront some individuals or groups (e.g. affront against good taste, modesty, ethnic affiliation).

3.1.2.1 Qualification and certification rules pertaining to the subject of the certificate

name attribute	description	certification / verification method

`commonName`
`(OID: 2.5.4.3)`
 	
`(OID: 2.5.4.3)`
	Domain name requested for the web-server. Shall not contain IP address, nether internal domain, nor underline ("_").
	Compulsory.
		Included in Chapter 3.1.2.2.

`serialNumber` `(OID: 2.5.4.5)`	Individual identifier automatically created by the Service Provider's client identification system assigned to the Subscriber and/or the Subject. Compulsory on every certificate.	
`countryName` `(OID: 2.5.4.6)`	Code of the country where the organization is seated. Compulsory.	Verified and certified data based on an official document of the organization (e.g. deed of
`localityName` `(OID: 2.5.4.7)`	Name of locality where the organization is seated. Compulsory.	Verified and certified data based on an official document of the organization (e.g. deed of
`organizationName` `(OID: 2.5.4.10)`	Official (full or brief) name of the organization. Compulsory.	Verified and certified data based on an official document of the organization (e.g. deed of
`organizationalUnitName` `(OID: 2.5.4.11)`	Organizational unit within the organization. Optional, indicated on the certificate when requested by the Subscriber.	This data is certified with a written statement of the Subscriber's Contact Person on the {D9} form.
`organizationIdentifier` `(OID: 2.5.4.97)`	Registered identifier (tax number) of the organization. Compulsory.	Verified and certified data based on an official document of the organization (e.g. deed of foundation, trade register extract).

3.1.2.2 Method for certifying domain names

The Service Provider checks whether the domain name belongs to, is possessed by and can be legally used by the Subscriber. The Service Provider will issue certificates only for domain names which are registered in Hungary by a Hungarian DNS registrar.

The Subscriber shall show the following for each domain name to be entered into `Subject`/ `CommonName` field or `subjectAlternativeName` extension of the certificate:

- an official statement issued by the DNS registrator declaring that the domain is owned by the Subscriber's organization; or
- a proxy issued by the owner of the domain declaring that the Subscriber is entitled to submit request for certificate and receive the certificate (in this case, the official statement issued by the DNS registrator with respect to the owner of the domain shall also be attached).

The Service Provider verifies domain names as follows:

- makes sure whether the statement issued by the DNS registrator is true and valid;
    - using the contact details (email address) specified on the DNS registrator's public website, the Service Provider directly contacts the registrator and checks whether the given domain name is owned by the organization to which the statement was issued;
- in case of application by proxy, the Service Provider, in addition to the verification described above, directly contacts the owner of the domain name (via phone or email) and asks it to confirm that the owner of the domain name issued a proxy to the agent for requesting certificate and acting in the relevant matters;
- The Service Provider contacts the technical or administrative person registered for the given domain name in the Whois database via the given email address and asks for confirmation to start the request for certificate directly or through an agent;
    - The Service Provider sends an e-mail to e-mail addresses belonging to the given domain and having prefixes 'admin', 'administrator', 'webmaster', 'hostmaster', 'postmaster '. Asks the recipient in email to send a reply message within 10 days. If all the e-mail addresses reply that the corresponding e-mail address does not exist, then the it refuses to issue of certificate for the given domain. If no reply is sent within 10 days, then the Service Provider may refuse to issue the certificate.
    - During the email exchange the Service Provider applies the so-called "random number-based method", the essence of which is that the e-mail sent must contain a random number value of at least 14 characters and the confirmation reply must contain the same random number value
- Having reviewed the submitted applications, the Service Provider is entitled to qualify certain applications as High-Risk Application. In the case of such High-Risk Applications, the Service Provider may take additional steps to control these applications: the Service Provider's client manager or an employee of the Client Relations Office visits the applicant and takes a site inspection to control the authenticity of the applicant's data, and records the results of the verification (by preparing a memo and having it kept my the Client Relations Office);
- In addition to the above, the Service Provider may perform further verifications.

The Service Provider records and keeps the sent and received emails and phone call details (name, phone number, time, result).

In case of domain names containing a "*" character (Wildcard certificate), the Service Provider makes sure that the Subscriber is the entitled user of the entire domain name range.

The Service Provider refuses a domain name where the "*" character is in the place of the highest level registrable domain name, i.e. directly left to the public domain ending (e.g. „*.hu", „*.com", „*.co.uk").

The Service Provider refuses a domain name which is registered as a gTLD (generic TopLevelDomain, e.g.: .info domain) by ICANN (Internet Corporation for Assigned Names and Numbers) organization.

3.1.3 Anonymity or pseudonymity of subscribers

Anonymity of the Subscribers and the use of pseudonym is not permitted for the certificate type specified in Chapter 1.4.

3.1.4 Rules for interpreting various name forms

The ASN.1 syntax of `Distinguished Names` in the certificate shall conform to [Sz9} RFC 5280, and the rules of displaying are specified in {Sz11} RFC 4514.

3.1.5 Uniqueness of Names

The Service Provider provides distinguishing name of the subject of the certificate by inserting a unique string automatically generated by its client relations system into the `Subject`/ `serialNumber` field of the certificate.

3.1.6 Recognition, authentication and role of trademarks

By the fact of registration the Subscriber represents that names, trade names, trade marks and other data in the certificate do not violate third party rights.

If the Subscriber requests the indication of trademarks, brand names or other name that a third party may have any right to in the website authentication certificate, then the Service Provider may only accept the request if the Subscriber submits an authentic confirmation, and the Service Provider has personally controlled the compliance of the confirmation and the data thereof.

The Service Provider does not guarantee for Subscribers that their trademarks will be stated in the certificate.

3.2 Initial identity validation

In accordance with the applicable laws, the Service Provider verifies and certifies the identity of the Subscriber's organization and the representation right of the authorized representative (e.g. signatory) as well as the personal identity of the Subscriber's Contact Person.

In accordance with Article 24 of {J1} eIDAS, the Service Provider, in line with the national laws, checks directly or via a third party the identity and unique characteristics of the natural person or legal entity, if applicable, to which the certificate is issued:

a) through personal presence of the natural person or authorized representative of the legal entity; or
b) with the certificate of qualified electronic signature or qualified electronic stamp issued in line with point a).

In case of point a), the Service Provider performs the identification of the Subscriber's Contact Person based on the given person's personal identity card.

In case of point b), the Service Provider can only perform the identification based on a certificate qualified by the Service Provider.

For certifying the organizational identity, a suitable official document (e.g. extract from trade register dated earlier than 30 days before, deed of foundation) and a specimen signature shall be submitted to the Service Provider and the original documents shall be shown.

In addition to the above, the Service Provider verifies if the data provided by the Subscriber and its Contact Person on the {D9} Certificate Order and Registration Form match the data listed in the public register.

3.2.1 Method to prove possession of private key

The Service Provider makes sure that the Subject possesses the private key belonging to the certificate. For this, the Service Provides verifies the digital signature on the PKCS#10 certification request.

3.2.2 Authentication of organization identity

Prior to issuing the certificate, the Service Provider verifies and certifies the full name and unique identifier (tax number or trade register number) and address details of the Subscriber's organization. The validity and effectiveness of the data are verified in a public register or, when no such public register is available, based on the official document requested for the application (e.g. extract from trade register dated earlier than 30 days before, deed of foundation).

Before the certificate is issued, the Service Provider verifies the existence of the authorized representative's rights, based on the applicable law, a public register, deed of foundation or, when these are not available, a proxy.

The Service Provider saves the results of the verification in its records.

3.2.3 Authentication of individual identity

The Subscriber's Contact Person, as a natural person, certifies the validity of data recorded on the {D9} certificate order and registration form, serving as the basis for the verification of registration and personal identity.

The Service Provider checks the personal identity of the contact person through its official personal identity card, and also checks the validity of the card and the correctness of data in the card in the relevant public register.

3.2.4 Non-verified subscriber information

The Service Provider verifies and certifies every data to be entered into the distinguished name of the certificate subject (`Subject`) field. The method of verification and certification is described in Chapter 3.1.2.1.

The Service Provider checks every domain name data to be indicated in the certificate, as described in Chapter 3.1.2.2.

With respect to data to be included in other fields and extensions of the certificate, the Subscriber's contact person made a written statement about their validity by completing and signing the {D9} certificate order and registration form.

3.2.5 Validation of authority

The Service Provider checks whether the {D9} certificate order and registration form is signed by the authorized person (Subscriber's Contact Person).

In accordance with the procedure described in Chapter 3.1.2.2, the Service Provider checks and certifies that the Subscriber is entitled to use each and every domain name to be listed in the certificate.

3.2.6 Criteria for interoperation

The Service Provider does not cooperate with other confidential service providers during provision of the Services.

3.3 Identification and authentication for re-key requests

Re-key is a process when a new public key is authenticated for the same data and with the same term as those listed in the original certificate.

The Service Provider does not provide re-key.

In order to change the key of the certificate, the Subscriber shall request a new certificate, procedure of which is described in Chapter 4.1.

3.3.1 Identification and authentication for routine re-key

No requirements.

3.3.2 Identification and authentication for re-key after revocation

No requirements.

3.4 Identification and authentication for revocation request

Request for revocation can be submitted to the Service Provider personally in the Client Relations Office or on paper (with the original signature of the Subscriber's authorized representative or the Subscriber's contact person).

In case the Subscriber's Contact Person has a valid business certificate issued by the Service Provider, the Service Provider also accepts the request for revocation in electronic format digitally signed by the Subscriber's Contact Person (sent to the email address of the Client Relations Office).

Request for revocation can be submitted seven days a week, 24 hours a day via telephone by calling the HelpDesk phone line. In case of request for revocation submitted via the HelpDesk phone line, the caller shall tell his/her personal data (in order to identify the Subscriber's Contact Person), the serial number or type of the certificate to be revoked, the month of issue and the revocation password in order to prove his/her authorization.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1. Who may submit Requests for Certificates?

Request for certificate may be submitted by the Subscriber's authorized Contact Person to the Service Provider.

4.1.2 Enrollment process and responsibilities

The process of requesting for a certificate is as follows:

1) Before the Service Provider and the Subscriber sign a Service Contract for provision of the Services, the Service Provider informs the Subscriber of the following:

   a) the usage of the certificate and the relevant legal requirements;

   b) the measures to be taken related to the usage of the private key, security measures to protect the private key;

   c) the responsibilities and obligations of the Subscriber and the

   Subject;

   d) the possibility of revocation of the certificate;

   e) the circumstances under which the certificate was issued;

   f) the validity of the certificate, the expiration of its validity;

   g) objective, timely, geographical or other restrictions relevant to the certificate; i) the

   Service Provider's public key;

   h) the availability and contents of the Certification Practice Statement.

2) Preparation of signing the contract
   a) the Service Provider sends the necessary information and forms to the Subscriber in email (e.g. {D9}, or Proxy for Contact Person)

   b) the Subscriber may complete and sign the forms and send them to the Service Provider along with the necessary attachments, but this may also happen after the Service Contract is signed

   c) the Service Provider prepares and sends the draft contract to the Subscriber

3) Signing of the Service Contract
   a) the Service Provider and the Subscriber sign the contract;

   b) the Subscriber designates a contact person, who is authorized to proceed in matters related to certificates: The Subscriber issues a proxy for the contact person, which contains personal data of the contact persons and the number of the contact person's personal identity card. The Subscriber then officially signs the proxy.

4) The Subscriber's Contact Person completes and signs a {D9} Certificate order and registration form for each certificate:
   a) the form may be submitted on paper signed by the Subscriber's Contact Person personally in the Client Relations Office or sent in mail to the Service Provider. The Subscriber's Contact Person may also send a signed and scanned copy of the forms in email to the Service Provider in the contract preparation phase. In this case, the original hard copies are handed over to the Service Provider at a later time (prior to handing over the certificates, at the latest).

b) if the Subscriber's Contact Person already has a business certificate issued by the Service Provider, then the forms can also be submitted in electronic format to the Client Relations Office, authorized with the electronic signature of the Subscriber's Contact Person;

c) by completing and signing the form, the Subscriber or the Subscriber's Contact Person:

- declares that the data on the form are true and valid;
- declares to accept the {D1} General Terms and Conditions and the Certification Practice Statement;
- approves that his/her personal data are managed by the Service Provider;
- approves that the Service Provider publishes the issued certificate in its public repository.

5) the Service Provider's Client Relations Office checks the completed registration form and the attachments and, when necessary, requests for the supplementation of missing documents.

6) In case of successful application, the Client Relations Office performs organizational identification as well as checking and certifying domain names (as described in Chapter 3.2), and proceeds to create and process the request for certificate.

The Parties' liabilities related to the application process are described in Chapter 9.6 and its sub-chapters.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Before accepting the request for certificate, the Service Provider identifies and authenticates the Subscriber's Contact Person and the subject of the certificate (domain) using the completed {D9} Certificate order and registration form and its attachments (e.g. extract from trade register, deed of foundation, specimen signature).

In accordance with the procedure described in Chapter 3.1.2.2, the Service Provider checks and certifies that the Subscriber is entitled to use each and every domain name to be listed in the certificate.

The Service Provider checks the DNS Certification Authority Authorization (CAA) entry whether the domain owner specified the authentication service providers that can issue certificate for the given domain. The Service Provider refuses to issue the certificate if the domain owner designated the authentication service provider, and that is different from the Service Provider. The Service Provider logs and preserves the result of CAA record inquiry.

If the domain owner sets a restriction on the service providers in the CAA record and also wants to authorize the Service Provider to issue a certificate, the following information shall be indicated in the "issue" or "issuewild" field of the CAA record: hiteles.gov.hu

4.2.2 Approval or rejection of certificate applications

The Service Provider accepts the request for certificate if every data entered into the distinguishing name of the certificate's subject (`Subject`) was successfully verified and certified.

The Service Provider refuses to accept the request for

certificate: • in case the form is completed

deficiently or improperly;

- if the authorization cannot be certified for a domain name;

- if the Service Provider finds that the requested certificate cannot be issued due to an applicable legal provision;
- if there is any doubt about the documents belonging to a certain person or about their originality, authenticity or validity;
- if there is any doubt about the originality, authenticity or validity of documents shown for certifying the organizational identity, the right for representation or belonging to the organization.
- if it is not authorized to issue the certificate based on the restriction specified in the CAA record

4.2.3 Time to process certificate applications

After the submission of a request for certificate, the Service Provider processes the request for certificate within the term specified in the Service Contract, or when no such term exists, within 15 calendar days specified in the {D1} General Terms and Conditions.

4.3. Certificate issuance

4.3.1 CA actions during certificate issuance

The Client Relations Office forwards the application based on the accepted request for certificate to the Registration Agency.

The Registration Agency:

- checks the readability and processibility of the request for certificate of PKCS#10 format, the digital signature placed on that, the strength of the keys, and whether the length and algorithm of the key pair is suitable (Chapter 6.1.5 and 6.1.6);
- initiates the creation of the certificate in the IT system supporting the Services;
- notifies the Client Relations Office of the completion of the certificate.

4.3.2. Notification to subscriber by the CA of issuance of certificate

The Client Relations Office notifies the Subscriber's Contact Person in email or by telephone about the completion of the certificate and agree on the way and time of delivering the certificate.

The certificate may be delivered at the Subscriber's site (on-site delivery) or in the Client Relations Office.

During delivery, the Subscriber's Contact Person receives:

- a copy of the {D9} Certificate order and registration form signed by the Service Provider's client relation officer;
- the envelope containing the revocation password;
- the certificate (in .cer file format) on a CD.

The delivery is recorded on an "Acknowledgement of Receipt and Acceptance of the Certificate", which is signed by the Subscriber's Contact Person, acknowledging the receipt and acceptance of the certificate as well as the receipt of the related envelope and devices detailed above. The employee of the Client Relations Office certifies that he/she verified and identity of the receiving person and confirmed the authority for receipt. The Service Provider logs the time of delivery.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The “Acknowledgement of Receipt and Acceptance of the Certificate” form referred to in Chapter 4.3.2 contains the data of the issued certificates and the data included in the certificate.

Based on that, the person receiving the certificate (the Subscriber’s Contact Person) verifies and acknowledges by signature that the data included in the certificate match the data in the {D9} Certificate order and registration form, and accepts the issued certificate. In addition to that, the Subscriber is responsible for checking the data included in the certificate prior to the first use of the private key related to the certificate, and in case of deviation, take immediate measures to revoke the certificate.

If the data in the issued certificate are invalid or do not match the data in the {D9} Certificate order and registration form, then the certificate is not issued and the Service Provider revokes the certificate.

If the certificate is not received within 30 days from the day the Client Relations Office sends the notice, then the Service Provider revokes the certificate.

4.4.2 Publication of the certificate by the CA

In case of written consent by the Subscriber, the Service Provider publishes the issued certificates in the Repository publicly available in the website of Services.

4.4.3. Notification of certificate issuance by the CA to other entities

No requirements.

4.5 Key pair and certificate usage

4.5.1. Subscriber private key and certificate usage

The Subscriber can only use the certificate and the related private key after checking the correctness of the data included in the certificate.

The Subscriber can use the certificate and the private key only for the purposes and in the ways described in Chapter 1.4.1.

While using the certificate and the private key, the Subscriber shall meet its obligations specified in Chapter 9.6.3, with special regards to protecting the activation data (if there is one) related to the private key (PIN code) from unauthorized access.

4.5.2 Relying party public key and certificate usage

During a web-server authentication based on a certificate issued under the scope of this Certificate Policy, the Relying Party shall proceed with due care and diligence, during which it is recommended to comply with the following recommendations:

- it shall perform the verification of the certificate with a reliable application that conforms to the laws listed in Chapter 1.6.3.1 of this Certification Practice Statement and that can support and properly implement the technical standards specified in Chapter 1.6.3.2;
- it shall use the application mentioned above in a reliable environment free from viruses, and the application shall be configured properly;
- it shall perform the generation and validation of the certification path described in Chapter 6 of {Sz9} RFC 5280 as well as the revocation verification with respect to the certificate, and accept the certificate only when these verifications have positive results;

- it shall consider every restriction described in the certificate or the regulations referred to by the certificate.

The Service Provider is not liable for damages caused by the Relying Party's failure to proceed according to the recommendations described above.

4.6 Certificate renewal

Renewal of a certificate is a process whereby the Subject's unchanged key is certified for the unchanged data included in the original certificate for a new term.

The Service Provider does not provide certificate renewal services.

If the certificate expires but there is further need for the service, then the Subscriber shall request a new certificate. The relevant procedure is described in Chapter 4.1. The Service Provider sends a notice to the Subscriber's email address specified in the {D9} Certificate order and registration form 30 days before the certificate expires.

4.6.1 Circumstance for certificate renewal

No requirements.

4.6.2 Who may request renewal

No requirements.

4.6.3 Processing certificate renewal requests

No requirements.

4.6.4. Notification of new certificate issuance to subscriber

No requirements.

4.6.5 Conduct constituting acceptance of a renewal certificate

No requirements.

4.6.6 Publication of the renewal certificate by the CA

No requirements.

4.6.7. Notification of certificate issuance by the CA to other entities

No requirements.

4.7 Certificate re-key

Re-key is a process when a new public key is authenticated for the same data and with the same term as those listed in the original certificate.

The Service Provider does not provide re-key.

In order to change the key of the certificate, the Subscriber shall request a new certificate, procedure of which is described in Chapter 4.1.

4.7.1 Circumstance for certificate re-key

No requirements.

4.7.2 Who may request certification of a new public key
No requirements.

4.7.3 Processing certificate re-keying requests
No requirements.

4.7.4 Notification of new certificate issuance to subscriber
No requirements.

4.7.5 Conduct constituting acceptance of a re-keyed certificate
No requirements.

4.7.6 Publication of the re-keyed certificate by the CA
No requirements.

4.7.7. Notification of certificate issuance by the CA to other entities
No requirements.

4.8 Certificate modification

Modification of certificate is a process whereby a new certificate with changed data (e.g. name, department) is issued for the public key certified with the original certificate.

The Service Provider does not provide certificate modification services.

In case the data included in the certificate change, the Subscriber shall request a new certificate and take measures to revoke the existing certificate.

4.8.1 Circumstance for certificate modification
No requirements.

4.8.2 Who may request certificate modification
No requirements.

4.8.3 Processing certificate modification requests
No requirements.

4.8.4 Notification of new certificate issuance to subscriber
No requirements.

4.8.5 Conduct constituting acceptance of modified certificate
No requirements.

4.8.6 Publication of the modified certificate by the CA
No requirements.

4.8.7 Notification of certificate issuance by the CA to other entities

No requirements.

4.9 Certificate revocation and suspension

Revocation of certificate means that validity of the certificate terminates before the expiration time. Revocation is a final and irrevocable status.

A revoked certificate may not be used.

The use of the private key belonging to the revoked certificate must be terminated immediately. The Subscriber shall be liable for damages occurred in the time until the request for revocation arrives at the Service Provider. The Service Provider shall be liable for damages occurred in the period from the acceptance of the request for revocation until its publication. The above shall not apply to provably fraudulent requests for revocation, in which case the Service Provider shall not be liable for the damages occurred. The Relying Party shall be liable for damages occurred after the revocation is published.

It is recommended that the Relying Parties verify revocation status of the certificate before accepting the web-server authentication based on the certificate.

4.9.1 Circumstances for revocation

The Service Provider revokes the certificate, if:

a. this is requested by the Subscriber or the Subscriber's Contact Person;
    - it is suspected that the private key related to the certificate has been compromised;
    - any data is changed or for other reasons
b. the Subscriber notifies the Service Provider that the original application was not rightful and may not be made rightful retrospectively
c. the Service Provider learns (based on well-founded information) that the private key is compromised or the length of the key or the cryptographic algorithm becomes obsolete
d. the Service Provider becomes aware that the verification of a domain included in the certificate was not performed properly (reliably)
e. the Service Provider learns (based on well-founded information) that the certificate is abused, or the certificate was used unlawfully or it was not used properly
f. the Service Provider learns that the Subscriber failed to meet the provisions of this statement, the ÁSZF-GOVCA or the Service Contract.
g. the Service Provider learns that the Subscriber is no longer authorized to use the domain name included in the issued certificate (e.g. due to a court prohibited the use of the domain, or the owner did not extend its domain registration)
h. the Service Provider learns that the Wildcard certificate is used for fraudulent authentication
i. the Service Provider learns that the data included in the certificate are changed
j. the Service Provider learns that the a given certificate has been issued not in compliance with the requirements of this Certification Practice Statement or the related BR-WOT Certificate Policy
k. the Service Provider learns about any abnormality in relation to the Services, e.g. it finds that any data included in the certificate is misleading or inaccurate, or the data included in the certificate are invalid, and do not conform to the Certificate Policy
l. the Service Provider terminates its activities, or the Service Provider is no longer authorized or permitted to issue certificates
m. the technical parameters (e.g. certain algorithms or key sizes) pose unacceptable risk to the Relying Parties or the Software Developers, or if the algorithm and parameter of the key related to the subscriber certificate or used by the Service Provider is not strong enough for the entire validity period of the certificate belonging to the key.
n. a Certificate Problem has been reported, which was investigated and revocation of the certificate was decided
o. the Supervisory Body orders revocation in its legally binding and executable resolution;

p. the revocation is necessary by law;
q. the certificate is not received within 30 days from the day the Client Relations Office sends the notice;
r. if the Service Provider becomes aware that there is a proven method by which the private key can be cracked or easily calculated from the public key, or the method of generating the secret key was incorrect
s. if the Service Provider's present Certification Practice Statement or the related BR-WOT Certificate Policy requires so, in addition to what is specified above.

4.9.1.1 Reporting of certificate problems

Any reports regarding the unauthorized use or misuse of website authentication certificates (Certificate Problems Reports) can be submitted seven days a week, 24 hours a day on the Help Desk phone line or personally (on workdays in working hours) to the Client Relations Office. Once a Certificate Problem Report is filed, the Service Provider immediately begins investigation of the complaint/remark by forwarding it to a designated circle of persons (leader generally responsible for the service, the Service Manager and the Security Officer) via e-mail and also notifies them via phone. The designate circle of persons is available 7x24 according to a determined schedule, and makes decision within 24 hours about revocation or other necessary action (depending on the person who reported the problem, the nature of the problem, the number of notifications and the parties affected) in line with the relevant laws.

4.9.2 Who can request revocation

In cases specified in Chapter 4.9.1, revocation may be initiated by:

- The Subscriber or the Subscriber's Contact Person;
- The Service Provider (including cases when the certificate is to be revoked due to the resolution of the Supervisory Body or a legal requirement).

4.9.3 Procedure for revocation request

Request for revocation can be submitted personally or via postal mail to the Service Provider's Client Relations Office, using the completed and signed Revocation Request form {D10}, or by phone calling the HelpDesk phone line.

The following data are required in order to fulfil a request for revocation:

- serial number of the certificate or other such data which serve to clearly identify the certificate in the Service Provider's system;
- identification data of the party requesting the revocation;
- the reason of or circumstances leading to revocation.
- password for revocation (in case of requests submitted by phone)

The Service Provider identifies the person requesting revocation as described in Chapter 3.4, and decides whether it is entitled to request for revocation.

After the identification-authentication of the requesting party, if the reasons for revocation are solid, the data correspond, and the requesting party is entitled to initiate the revocation of the certificate, the Service Provider immediately revokes the certificate. Otherwise it rejects the request for revocation.

The Service Provider notifies the Subscriber about revocation of the certificate or refusal of the request for revocation in email.

If the algorithm or parameter of the key used by the Service Provider is not strong enough for the entire validity period of the certificate belonging to the key, the Service Provider takes measures to revoke the affected certificates in due time, and notifies the Subscriber or the Subscriber's Contact Person and the Relying Parties about the time of revocation beforehand.

The Service Provider ensures not to revoke a certificate retrospectively.

If a certificate has been revoked, then the Service Provider never validates it again.

The Service Provider does not provide an opportunity for the applicant to request the revocation of the certificate at a specified future date.

4.9.4 Revocation request grace period

The Service Provider does not apply grace time when performing requests for revocation.

4.9.5 Time within which CA must process the revocation request

In case of successful verification, the Service Provider processes the request for revocation within 24 (twenty-four) hours of submission and sets the certificate status to revoked, then makes it public.
In the case of a revocation request sent by post (including point 4.9.1 b), the twenty-four hour period begins when the postal item arrives at the Service Provider (more precisely at the Customer Relations Office) and the Customer Relations Office staff is convinced of the applicant's entitlement. The latter date will be recorded by the Customer Relation Officer on the {D10} Revoction Request.

In case a Certificate Problem is reported (Chapter 4.9.1.1), the Service Provider decides about revocation in 24 hours, and in case of revocation, immediately sets the certificate status to revoked.
In addition to the above, certificates must be revoked within 24 hours in the following cases: Chapter 4.9.1 (c) and (d) and 4.9.1 (q).
The Service Provider shall revoke the certificates within 5 days in the following cases: e), f), g), h), i), j) k), l), m), r) and s) listed in Chapter 4.9.1 of this Regulation.

4.9.6 Revocation checking requirement for relying parties

It is recommended that the Relying Parties verify the revocation status of every element of the certificate and the related certificate chain based on the downloaded CRL or requested OCSP response available at the contact details described in the certificate or specified in Chapter 4.10.1.

4.9.7 CRL issuance frequency

The CRL of Subscriber certificates shall be updated with the following frequency: At least one CRL every 24 hours. The CRL contains the time of the next update (in the `nextUpdate` field). The Service Provider publishes a new CRL immediately (within 1 hour) following the revocation of a certificate. Upon every CRL updating, the Service Provider deletes from the CRL those certificates validity of which has expired at the time the CRL is updated.

The CRL of Service Provider certificates shall be updated with the following frequency: At least one CRL every 30 days. The CRL contains the time of the next update (in the `nextUpdate` field). Upon every CRL updating, the Service Provider deletes from the CRL those certificates validity of which has expired at the time the CRL is updated.

4.9.8 Maximum latency for CRLs

The Service Provider publishes the CRL immediately after its generation but within 1 hour, at the latest.

4.9.9 Online revocation/status checking availability

The Service Provider also provides OCSP services for end-user and Service Provider certificates at its contact details, with functions and availability stated in Chapter 4.10.

4.9.10 On-line revocation checking requirements

It is recommended that the Relying Parties use the OCSP services primarily for determining the revocation status of certificates, since in the scope of this service the Service Provider supplies revocation status information also for expired certificates.

4.9.11 Other forms of revocation advertisements available

The Service Provider published the revocation status also in the Repository publicly available on its website. This information cannot be used for the verification of web-server identity. This warning is also indicated in the public repository.

4.9.12 Special requirements re key compromise

In the event the Service Provider's private key is compromised, the Service Provider publishes information about the event on its website and notifies the Subscribers via email.

In case the private key of the productive authentication centre is compromised, the Service Provider is able to revoke all affected end-user certificates, issue and publish the affected CRL in 24 hours and revoke the given Service Provider certificate and issue and publish the affected CRL in 12 hours.

4.9.13 Circumstances for suspension

The Service Provider does not provide suspension service for the website authentication certificates.

4.9.14 Who can request suspension

No requirements.

4.9.15 Procedure for suspension request

No requirements.

4.9.16 Limits on suspension period

No requirements.

4.10 Certificate status services

4.10.1 Operational characteristics

The Service Provider provides the revocation information relevant to end-user and Service Provider certificates both in the form of CRL and OCSP.

CRL

The CRL issued by the Service Provider complies with the standard {Sz9} RFC 5280.
The Service Provider uses the same Service Provider's private key which was used for signing the certificate in question.

The CRL shall state a time for next scheduled issue (nextUpdate). In case of the final CRL (the last CRL issued by the given CA) the nextUpdate field should be set to "99991231235959Z" conform RFC 5280 {Sz9}. The Service Provider must ensure that a new CRL is issued before the date indicated in the nextUpdate field.

The CRL includes every revoked certificate validity of which has not expired at the time the CRL is issued.

The Service Provider shall issue a final CRL, when ending the operation of a given CA:

- due to key changeover (Chapter 5.6); or
- due to Service Provider's private key is compromised (Chapter 7.5.3); or
- in case the Services Provider terminates its Certification Service (Chapter 5.8)

The Service Provider may issue the final CRL only after all certificates issued by the CA have expired or have been revoked. The Service Provider (or, in the event of termination of the Certification Service, the trust service provider receiving the service, see Chapter 5.8) must ensure the availability of the final CRL for 10 years after the issuance of the final CRL.

Availability of CRL for end-user certificates:	http://nqca.hiteles.gov.hu/crl/GOVCA-NQ-SSL.crl
Availability of CRL for Service Provider's certificates:	http://qca.hiteles.gov.hu/crl/GOVCA-ROOT.crl

OCSP

The OCSP service provided by the Service Provider complies with the standard {Sz13} RFC 6960.

The Service Provider includes the optional `nextUpdate` field in the OCSP responses. The time in that field may not exceed `thisUpdate`+ 24 hours.

The Service Provider operates the OCSP service in accordance with the "Authorized Responder" principle described in Chapter 2.2 of {Sz13} RFC 6960.

Within the framework of the OCSP service, a positive response (containing a "good" status) can only be replied in case of a certificate that has been issued by the given certificate authority (that is, the certificate is in the certificate store fo the given CA) and if the certificate is not revoked.

A new certificate, valid for 24 hours, is issued for the OCSP responder minimum every 4 hours and maximum every 21 hours to ensure that the certificate signing the OCSP response does not need to be verified; to indicate this, the `id-pkix-ocsp-nocheck` extension is included in the OCSP responder certificate.

Within the framework of the OCSP service, the Service Provider makes the revocation information available for 10 years after the expiration of the certificate, during the operation of the given CA. When a CA is terminating its operation, the Service Provider must issue a final CRL and at the same time reconfigure the operation of the OCSP responder so that each OCSP request is served with a "final" OCSP response in which the `nextUpdate` field contains "99991231235959Z" according to RFC 5280 {Sz9} and the date in the `archiveCutOff` extension coincide with the start date of the validity of the Service Provider's certificate.

Availability of OCSP service for end-user certificates:	http://nqocsp.hiteles.gov.hu/ocsp-ssl
Availability of OCSP service for Service Provider's certificates:	http://qocsp.hiteles.gov.hu/ocsp-root

4.10.2 Service availability

The CRL or OCSP service is available every day in a year, 24 hours a day with 99% availability in a way that no service failure shall exceed 24 hours.
The Service Provider shall provide a response time of 10 seconds or better for both the CRL and the OCSP service, in the case of normal operation.

4.10.3 Optional features

No requirements.

4.11 End of subscription

The Subscriber's contractual relationship terminates when the validity of the certificate expires or if the certificate is revoked prior to expiry at the request of the Subscriber or for any other reason.

4.12 Key escrow and recovery

The Service Provider does not provide key escrow services.

4.12.1 Key escrow and recovery policy and practices

No requirements.

4.12.2 Session key encapsulation and recovery policy and practices

No requirements.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

During the provision of the Services, the Service Provider applies physical, procedural and staff security measures complying with the guiding standards, and the administrative and the governing procedures related to their execution.

Upon developing the system, the Service Provider has performed a risk analysis in order to measure its business risks and to determine the necessary security requirements and operation procedures; it ensures that the risks are reviewed quarterly or when necessary. The Service Provider maintains the IT security infrastructure in order to ensure security management within its organization. Any changes that affect the security level shall be approved by the Service Provider's management.

The security management rules are determined in the Service Provider's security policy {D5}. For reasons of security this policy is confidential. In respect of the Service Provider's systems supporting the service the security regulation for PKI services {D6} shall apply. This regulation contains the tasks in respect of security management grouped by organizational units and by positions, so i.a. the listed confidential positions, the appointment conditions, and the criteria of incompatibility.

The Service Provider established and constantly maintains the security controls and operation procedures of devices, systems and IT assets providing the Services. The Service Provider's internal and external audits verify these procedures, the related documents and the compliance with provisions of the documents regarding the services at regular intervals.

The above procedures are provided by a reliable and professional operating staff employed by the Service Provider.

The Service Provider ensures that all its assets and information are protected on an appropriate level. The Service Provider keeps an inventory of all its IT assets and shall classify and evaluate their security requirements in compliance with the performed risk analysis.

The Service Provider locates its IT systems, equipment and devices involved in the creation of certificates, management of revocation information in its central machine room representing the highest level of protection.

5.1 Physical controls

5.1.1 Site location and construction

The Service Provider locates and operates its IT systems involved in the provision of the Services in an object having the highest level of physical and logical protection. When locating and developing the site, cross-linked protection solutions are applied that can eliminate unauthorized access and protect the IT systems and the confidential information stored by the Service Provider.

5.1.2 Physical access

The Service Provider protects its IT systems involved in the provision of the Services from unauthorized physical access to prevent the devices from tampering.

For this purpose, the Service Provider ensures the following:

- every entry to the machine room is logged;

- only authorized employees fulfilling a confidential position can enter the machine room after identification;
- person without individual authorization may stay in the machine room only in justified and approved cases, for the necessary period of time, under constant supervision of a person having suitable authorization;
- activation data of the devices (passwords, PIN codes, etc.) shall not be stored in an open format even in the machine room;
- in the presence of an unauthorized person:
    - data storage media containing confidential information shall be kept closed;
    - logged in terminals shall be supervised;
    - no work processes can be performed which may result in disclosing confidential information;
- when leaving the machine room, the following shall be checked:
    - every device and equipment is in safe operating status;
    - every terminal is logged out;
    - physical data storage media are properly locked;
    - systems and equipment providing physical protection work properly.

5.1.3 Power and air conditioning

The Service Provider uses an uninterruptible power supply in the machine room, which:

- has adequate performance to supply power to IT and auxiliary devices working in the machine room;
- protects IT equipment from voltage fluctuation, power failures and other interferences of the external grid;
- in case of lasting power failure, an own power generating device provides power supply for an undetermined period of time (if refilled with fuel).

The Service Provider installs an air-condition system in the machine room, which has the following features:

- the oxygen necessary for the safe working of operators is provided;
- the air humidity shall not exceed the level required by IT systems;
- cooling is provided to maintain the necessary operating temperature and prevent devices and equipment from overheating.

5.1.4 Water exposures

The Service Provider protects the machine room from leakage, water ingress and flood using a moisture detector and alarm system.

5.1.5 Fire prevention and protection

The Service Provider installs smoke and fire detectors in the machine room, which automatically alarm the competent staff. The required type and number of fire extinguishers are placed in every room in a well visible location. An automatic fire extinguishing system is installed in the machine room, which is not hazardous to human health and does not damage IT devices.

5.1.6 Media storage

The Service Provider protects all of its data storage media from unauthorized access, loss or accidental damage typically by locking it in a safe.

5.1.7 Waste disposal

The Service Provider ensures disposal of its unnecessary devices and data storage media in accordance with the environmental regulations. The unnecessary devices and data storage media are rendered unusable or irrevocably deleted using widely accepted methods, under the personal supervision of a designated employee.

5.1.8 Off-site backup

The Service Provider keeps backup copies (from which the entire service can be restored in the event of a failure) at a location having suitable physical and operating protection, different from the site of operation. The safe transportation of backup data between the locations is ensured.

The backup or restoration activities are performed by a system administrator fulfilling a confidential position.

5.2 Procedural controls

The Service Provider ensures that its IT systems are operated safely, in accordance with regulations and by minimal risk of defects. The Service Provider's staff performs the tasks in accordance with a procedure that is in line with the relevant laws, standards and internal security regulations.

The procedural rules are included in the following policies:

- {D3} the Service Provider's Organizational and Operation Regulation which determines the Service Provider's organization structure, and within that each scope of activities and the tasks, liabilities and competences,
- this Certification Practice Statement, which controls the relations between the Service Provider and the PKI community (Subscribers, Subjects, Relying Parties);
- {D6} Security Regulation to PKI Services, which contains in detail the security rules related to data and IT systems and to the personal and physical environment.

5.2.1 Trusted roles

The Service Provider has identified the following confidential positions which the security of the Services depend on:

a) leader generally liable for the Service Provider's IT system;

b) Security Officer: person generally responsible for the security of the Service;

c) System Administrator: person performing the installation, configuration and maintenance of the IT system;

d) System Operator: person responsible for non-stop operation, saves and restoration of the IT system;

e) independent System Controller: person responsible for verifying the service provider's logged or archived files, the control of compliance with the control measures performed by the service provider in order to secure a formal operation;

f) Registration Officer: person responsible for approving the creation, issue and revocation of end certificates, proper performance of life-cycle management activities and administration tasks;

The tasks and responsibilities of the confidential positions are described in the Service Provider's internal, not public policy. Persons in a confidential position are employed by the Service Provider.

Employees are appointed to confidential positions by the top management of the Service Provider. Every confidential position is fulfilled at least by two persons.

In addition to confidential positions, the Service Provider also specifies confidential duties to ensure that tasks necessary for the provision of Services are performed efficiently. Persons fulfilling confidential duties are employed by the Service Provider.

The Service Provider keeps a record of the persons fulfilling confidential positions and duties. The Service Provider reports all changes related to the confidential positions to the Supervisory Body before the changes are implemented.

5.2.2 Number of persons required per task

The Service Provider's security regulations state that the following operations can only be performed in a protected environment, in the simultaneous presence of at least two employees fulfilling confidential position, without the presence of unauthorized persons:

- creation of Service Provider key pair;
- saving and restoration of the Service Provider's private key;
- activation of the Service Provider's private key;
- destruction of the Service Provider's private key

5.2.3 Identification and authentication for each role

Staff members fulfilling confidential positions are identified and certified using strong PKI procedures (e.g. by certificates stored on tokens and entering the activation PIN code) before having access to critical IT system involved in the provision of Services.

5.2.4 Roles requiring separation of duties

The Service Provider ensures the following with respect to confidential positions:

a) the security officer cannot perform the tasks of the independent system controller, the system administrator and the leader generally responsible for the IT system;

a) the independent system controller cannot perform the tasks of the leader generally responsible for the IT system, the person responsible for the registration and the system administrator;

c) every effort shall be taken to separate confidential positions.

5.3 Personnel controls

The Service Provider ensures that its staff regulations and exercises regarding employment of staff members increase and support the reliability of the Service Provider's operation.

The Service Provider holds a staff with enough members with education, qualification, professional skills and experience sufficient to the dimensions and quantity of tasks in order to provide the services.

The Service Provider's every employee in a confidential position is free of any such colliding interests that might have an effect on the reliability and security of the Services.

The employees dispose over job descriptions determined based on the principles of divided tasks and minimum authorization.

5.3.1 Qualifications, experience, and clearance requirements

The Service Provider ensures that a confidential position can only be fulfilled by persons whose uninfluencedness and skills can be certified with a certificate of good conduct, professional experience and qualification.

The leader generally responsible for the Service Provider's IT system has a specific higher education degree and at least three years of experience in the field of IT security. Specialized higher education degree shall mean mathematician or physicist university degree or a college or university degree in a scientific engineering field.

In case of Security Officers and System Auditors, a specialized secondary or higher education, by secondary education at least three years, by education of higher level at least one year of professional experience in respect of IT security is required.

With regards to Registration Officer, specialized secondary education and at least one year of professional experience in respect of IT security is required.

For the system operator and system administrator position, specialized secondary education and at least one year of professional experience in respect of IT security is required.

The specialized qualifications expected in the confidential positions are described in the Service Provider's internal, not public policy.

5.3.2 Background check procedures

The Service Provider can only employ persons in leading positions and confidential positions or roles, who:

- have clean record and are not under legal proceedings that may affect their criminal record (the clean record shall be certified with a certificate of good conduct issued within the last three months);
- are not under the effect of being banned from exercising confidential service provision activities.

The Service Provider checks the relevant information included in the curriculum vitae submitted in the application procedure.

Before a confidential position listed in Chapter 5.2.1 is fulfilled, a security vetting of the highest level (national security vetting, as specified in Act CXXV of 1995 on the National Security Services) is performed. In the rest of the confidential positions, the Service Provider performs an advanced security vetting before employing the person in question. Both the highest level and the advanced security vetting are subject to the affected person's consent. No person may hold a confidential position by which the security control has ascertained any risk.

When appointed to a confidential position, the affected person:

- takes over a precise job description from the line manager or the Human Resources organization of the Service Provider,
- shall sign a Confidentiality Statement, which contains three years of confidentiality obligation from the date of leaving the employer;
- receives the necessary training in order to become aware of his scope of tasks and liabilities and to be able to improve their skills.

When leaving the employer:

- At the same time with the decision on secession, the leaving person's physical and logical logon and access rights are terminated immediately. Thereafter the leaving person may only enter the zones related to the Services accompanied by the IT security manager.
- Its device used for identification and authentication shall be taken back and it shall be destroyed in a documented way. The related certificates shall be revoked.

5.3.3 Training requirements

The Service Provider only employs persons in a confidential position or role who have acquired the following to the extent necessary in the given position:

- the PKI theory;
- characteristics and handling of the Service Provider's IT system;
- special knowledge necessary for fulfilling the given role;
- processes and procedures specified in the Service Provider's public and internal regulations;
- legal consequences of each activity;
- the applicable security rules.

Only employees who successfully pass the training can obtain access rights to the Service Provider's live IT systems.

5.3.4 Retraining frequency and requirements

The Service Provider ensures that its employees keep their knowledge up to date, and, when necessary, provide training or refreshing training to its employees.

The Service Provider repeats the training or elements thereof to the affected persons after every considerable change.

In case of considerable changes are e.g. the modification of the organizational security policy, change in the hardware or software system (upgrade) and modifications regarding key management and security management, all employees are trained to the required depth and receive the necessary documentations.

In case of minor changes, the employees receive a written notice before the changes take effect.

The Service Provider provides a training at least once a year about the newly revealed vulnerabilities and current IT security practices relevant to the field of the employee.

5.3.5 Job rotation frequency and sequence

No requirements.

5.3.6 Sanctions for unauthorized actions

The Service Provider controls in the labor contract to be signed with the workers the accountability of the worker in cases of neglects, accidental or intentional damages caused by the worker.

5.3.7 Independent contractor requirements

The Service Provider can only use one of its employees to fulfill a confidential position.

The Service Provider signs a service contract or a written agreement with the supplier for the performance of other tasks. The contracting party signs a confidentiality statement, whereby it agrees not to disclose business secrets and confidential information learned in the course of working to unauthorized parties and not to use such information in any other ways. The statement also specifies the sanctions to be applied in case of breach.

5.3.8 Documentation supplied to personnel

The Service Provider continuously makes the necessary documents and regulations available for the staff.
All employees fulfilling confidential positions receive the following written documents:

- individual job description;
- the Service Provider's organizational and security policies;
- training materials for regular or extraordinary trainings.

5.4 Audit logging procedures

5.4.1 Types of events recorded

The Service Provider logs every event related to its IT system and the provision of Services. The logged file covers the entire service provision process and enables the reconstruction of every Service-related event to the extent of understanding the real situations.

Events related to the IT system are especially the following: system startup and shutdown, change of security profile, system crash and hardware errors, firewall activity, attempts of access, Service Provider key management events, time synchronization events, start and stop of the logging function, change of logging parameters, errors in relation to the storage of log data, damage of integrity of the log data.

Events related to the provision of Services are especially the following:

- every event related to the life-cycle of Service Provider certificates;
- every event related to the life-cycle of the Service Provider certificates, including events resulting from the submission and processing of certificates, submission of request for revocation and the activities resulting therefrom.

The logged data file contains the date and exact time of the logged event, the data necessary for monitoring or reconstructing the event, the name or identifier of the user or other person causing the event.

5.4.2 Frequency of processing log

The Service Provider periodically verifies and assesses log files.

System controllers process the events related to the provision of Services on a monthly basis.

Log files of the IT system events are processed by the system controllers on a regular basis, with the frequency specified in the security policy.

5.4.3 Retention period for audit log

The Service Provider archives log files and securely keeps them for the term specified in Chapter 5.5.2. Until this time, the Service Provider ensures readability of the archived files as well as the necessary hardware and software tools.

5.4.4. Protection of audit log

The Service Provider stores log files and archives in a physically protected environment. The log files are time stamped and the archived log files are provided with an electronic signature or stamp containing a time stamp.

The Service Provider ensures that log files and archived log files can only accessed by authorized persons.

5.4.5 Audit log backup procedures

The Service Provider makes regular backups of the log files. The procedures and rules regarding the creation of backups are described in the Service Provider's internal policy.

5.4.6 Audit collection system (internal vs. external)

Log entries are collected by means of an internal component. The collection of log entries begins upon system start-up and continuously works until system shut-down, and ensures the integrity and availability (and, when necessary, confidentiality) of the collected entries.

In case of malfunction of the collection of log entries, the Service Provider suspends the operation of the affected area until the malfunction is corrected.

5.4.7 Notification to event-causing subject

The Service Provider does not necessarily notify subjects (persons, organizations) triggering extraordinary events. When necessary, the Service Provider may involve the subject triggering the event in the investigation of the event. In such cases, the affected Subscriber shall cooperate with the Service Provider in order to reveal the event.

5.4.8 Vulnerability assessments

The Service Provider performs, at regular intervals specified in the applicable standards ({Sz2} and {Sz22}), vulnerability and intrusion tests based on the assessment of log files and other information, which can help mapping potential internal and external threats, which may result in unauthorized access or impact the process of issuing a certificate, lead to the modification, change, damage or loss of data to be recorded in the certificate.

In relation to the vulnerability test, the Service Provider makes a risk analysis to assess the probability of threats and the expected damage of occurrence. It examines whether the applied processes, IT systems, protective measures can suitably withstand the threat.

The Service Provider repeats the intrusion test:

- in one week at the request of the CA/Browser forum;
- upon every significant change of the system or a network component; • at least once every quarter.

The Service Provider repeats the vulnerability test:

- after every significant infrastructural change or version update;
- at least once a year.

Following the assessment, the Service Provider takes the necessary measures to prevent the revealed vulnerability from being utilized.

The Service Provider continuously monitors the newly revealed critical vulnerabilities and takes the necessary counter-measures possibly in 48 hours. In case of vulnerabilities that may effect the qualitiy of the Certification Service, the Service Provider either prepares an action plan, and implements it in order to prevent the vulnerability from being utilized or reduce its effects to the minimum, or must document the factual basis that the particular vulnerability does not require countermeasures.

5.5 Records archival

5.5.1 Types of records archived

The Service Provider ensures that every information is stored that is necessary to prove the validity of a website authentication certificate and supports the proper operation of the Service Provider and its systems.

For this purpose, at least the following data shall be stored electronically or on paper:

- all data and documents related to the request for certificates and registration, specifically the Service Contract, the statements signed by the Subscriber and acknowledgements of receipt;
- all information related to the certificates for their entire life-cycle;

- all issued versions of the Certificate Policy and the Certification Practice Statement;
- all issued versions of the General Terms and Conditions;
- contracts relevant to the operation of the Service Provider
- all log files.

5.5.2 Retention period for archive

The Service Provider preserves the archives specified in Chapter 5.5.1 for 10 years following the expiry of the certificate (in case of certificate-related data) and until the legally binding close of legal disputes related to the certificate, or for 10 years after the lapse or termination of a contract or regulation.

5.5.3 Protection of archive

The Service Provider provides physical protection and takes security precautions which maintain integrity, credibility, availability and accessibility of the arhives. The Service Provider uses at least an electronic signature or stamp of advanced security and a qualified time stamp for the protection of electronic archives.

5.5.4 Archive backup procedures

The Service Provider preserves and keeps paper-based documents and electronic files in the document directory, and stores electronic files in multiple copies in physically separated locations.

The Service Provider protects electronic archives from being obsolete within the preservation term.

5.5.5 Requirements for time-stamping of records

There is a time mark in every log entry which includes the system time synchronized with sources specified in Chapter 6.8 having an accuracy of under one second.

The electronic signature or stamp of electronic archives contains a qualified time stamp.

During preservation of the archives, the Service Provider maintains authenticity of electronic signatures, stamps and time stamps, when necessary (e.g. in case of algorithm change).

5.5.6 Archive collection system (internal or external)

The log files and other electronic data are collected in the Service Provider’s protected IT system. When moving out of the protected IT system, the data are authenticated with an electronic signature or stamp containing a qualified time stamp.

The Service Provider locates paper-based documents in its document director for preservation.

5.5.7 Procedures to obtain and verify archive information

The Service Provider protects the archives from unauthorized access. The Service Provider controls the authorization and logs every access.

In cooperation with the Client Relations Office, the Service Provider supplies information to the Subscribers about their personal data stored.

In authority or legal proceedings described in Chapter 9.4.6, the Service Provider provides access to the data stored in the archives to the necessary extent.

5.6 Key changeover

The Service Provider ensures that authentication centres have the necessary valid key and certificate at all times.

Before expiration of the Service Provider certificate belonging to the key pair used for signing end-user certificates, the Service Provider issues (and publishes, as described in Chapter 2.3) a new Service Provider certificate in due course to ensure that the confidential Service operates without failure, considering the expiration of the issued end-user certificates.

If a new Service Provider's key pair and certificate needs to be generated, the Service Provider does it in such a way that the transition causes minimum inconvenience for the Subscribers and the Relying Parties:

- following the transition of keys, the issued certificates are only signed using the new Service Provider key;
- it preserves the public key and the Service Provider certificate of the old Service Provider key pair for two years following the expiration of the last issued certificate or ten years from the transition of keys, whichever is longer.

At least 30 days before the planned transition of keys, the Service Provider notifies the Supervisory Body and discusses the necessary tasks.

5.7 Compromise and disaster recovery

The Service Provider takes every necessary measure to reduce damages caused by an extraordinary operating situation and failure of the services to the minimum and to restore the Services within the shortest possible time. In extraordinary operation situations the measures aiming at the restoration of reliable operation of revocations lists shall have precedence over the restoration of any other service or activities.

In case the failure of the revocation directory, the repository and the revocation management service exceeds 24 hours, the Service Provider immediately notifies the Supervisory Body.

In case of other incidents (if the given incident significantly affects the service or the personal data stored therein), the Service Provider shall notify the Relying Parties within 24 hours of the occurrence, and the reports the incident to the Supervisory Body.

Based on the assessment of the incident occurred, the Service Provider takes the necessary modification and corrective measures to prevent the incident from occurring again.

5.7.1 Incident and compromise handling procedures

The Service Provider has a business contingency plan {D7}. For reasons of security this document is confidential.

In extraordinary operating situations, the Service Provider documents the events, their circumstances and the troubleshooting measures.

In extraordinary operating situations, the Service Provider implements its procedures specified in the business contingency plan to ensure that operation is resumed within the term specified in the business contingency plan.

The duration of restoration is determined by the severity of the event, i.e. the classification into severity class described in the business contingency plan.

The Service Provider has established and maintains a backup CA system, which can ensure availability of the repository and public regulations as well as full-scope operation of the revocation management services and the publication of CRLs in extraordinary operating situations.

In case the duration of the extraordinary operating situation exceeds the specified deadline, the Service Provider immediately notifies the Supervisory Body about occurrence of the event, its

impact, expected duration, the taken and planned troubleshooting measures as well as the termination of the extraordinary operating situations.

In extraordinary operating situations, the Service Provider publishes the relevant information on its website within the shortest possible time, and possibly notifies the affected person in an email.

In case of incidents affecting security or integrity (provided that it has negative effects on the Subscribers using the Services), the Service Provider notifies the affected Subscribers without reasonable delay.

If the Service Provider's root authentication certificate is removed from the trusted repository of an internet browser or other widely known commercial software application, then the Service Provider terminates the issue of website authentication certificates that are affected by that event.

In cases specified in Chapter 5.4 of the {Sz18} WebTrust SSL 2 guideline, the Service Provider revokes its intermediate Service Provider certificate within seven days.

5.7.2 Computing resources, software, and/or data are corrupted

The Service Provider operates a secure system which ensures the operation and accessibility to the services also in case of any system failure by using redundant technical solutions, security backups and procedures. The detailed requirements and actions are described in the business contingency plan and the Service Provider's internal policies.

5.7.3 Entity private key compromise procedures

The Service Provider has an action plan in case the Service Provider's private key is compromised, which is described in the business contingency plan. According to this plan, the Service Provides takes the following main steps:

- revokes all affected certificates;
- a final CRL must be issued (see Chapter 4.10.1)
- stops using the affected private key;
- creates new Service Provider key pairs and certificates;
- notifies the Supervisory Body;
- takes measures to notify every Relying Party.

5.7.4 Business continuity capabilities after a disaster

The Service Provider has a backup location and IT system as well as a detailed relocation procedure.

The difference between serious malfunction and disaster is i.a. that in case of disaster it is probably not only the IT system but also its physical environment is partially or wholly destroyed. In the latter case, an emergency team takes measures to relocate to the backup location in accordance with the business contingency plan, and restore the IT system to the necessary extent using the backups previously placed in the backup location.

5.8 CA or RA termination

The Service Provider has the following plan for the termination of the certification service:

- Initiates negotiations in due course with other confidential service providers about handing over and taking over the obligations related to the Services - with special regards to the preservation of data specified in Chapter 5.5.1 for the term specified in Chapter 5.5.2.
- The Service Provider endeavors to minimize the disturbances impacting the user community caused by the termination of providing the Services. It particularly ensures that the certificate management services and the publication services are provided constantly.

- At least 60 days before termination:
  - it notifies the Supervisory Body and informs members of the user community on its website;
  - terminates all authorizations of the contracted sub-contractors acting on its behalf, terminates the contracts concluded with them, and withdraws their competence;
  - ceases to create and issue certificates;
  - signs an agreement with a reliable parts (confidential service provider) about handing over and taking over the obligations related to the Services, and sends a copy of this agreement to the Supervisory Body;
- At least 20 days before termination:
  - it revokes all end-user certificates and issues a final CRL;
  - ceases to provide revocation management services.
  - revokes the affected Service Provider certificates and issues a final CRL;
  - destroys Service Provider private keys and their backups in a way that they cannot be used anymore;
  - ceases to publish certificate and revocation status information (both the CRL publication and the OCSP service), and ensures that revocation information are available at the service provider that took over the Services;
- On the day of termination:
  - The Service Provider makes a full-scope archive of the data in its IT system, provided with time stamp and electronic signature or stamp.

  The Service Provider protects the archived data from unauthorized access and ensures that the contents of the archives cannot be accessed by unauthorized persons. Through the signed contract, the Service Provider ensures the data are accessible and interpretable to authorized persons within the term of storage.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 Service Provider key pair generation

The Service Provider generates the key pairs used for signing certificates and revocation lists on its own in a physically protected environment, in a designated HSM module, in the simultaneous presence of at least two persons in confidential positions, excluding the presence of unauthorized persons. When generating the key pair of the root authentication centre, an external auditor is also present, or the event is video recorded. The procedure is performed according to the key generation scenario and drawn up in minutes, which is certified by the Security Officer with its signature, and, in case of generating the key pair of the root authentication centre, an external audit report is also prepared. The cryptographic module conforms to the requirements set forth in Chapter 6.2.1, and the signature creation data (private keys) remain in the cryptographic module for their entire life-cycle.

The Service Provider creates key pairs used for signing OCSP responses in a physically protected environment, and the private keys remain in this physically protected environment during their entire life-cycle.

6.1.1.2 Subscriber key pair generation

The Subscriber shall provide for generating the subscriber's key pair for the requested certificate, in accordance to the followings:

- the Subject shall generate the key pair in accordance with the criteria relevant to the SHA256withRSA2048 algorithm suit applied and the key length specified in Chapter 6.1.5 and 6.1.6 in a supervised and secure environment.
- the Subject shall ensure protection of the private key and the activation data.

6.1.2 Private key delivery to subscriber

Based on this policy, the Subscriber shall provide for the subscriber's key pair generation, therefor the private key does not need to be delivered to the Subject, because the key is in the Subject's possession.

6.1.3 Public key delivery to certificate issuer

The Subscriber delivers the public key to the Service Provider in a request for certificate in PKCS#10 format, authenticated with a digital signature generated with the private key belonging to the public key. The Service Provider makes sure that the Subject possesses the private key by verifying the digital signature on the request for certificate. In addition, the Subscriber fills in a paper based request as attachment to the PKCS#10 format certificate request, using the broadsheet of the Services Provider, and sends it to the Service Provider.

6.1.4 CA public key delivery to relying parties

The Service Provider publishes its public keys in the Service Provider certificate, as described in Chapter 2.2. The availability of the Service Provider certificate is included in the `AuthorityInformationAccess` extension of the given certificate.

The Service Provider publishes its public keys for the Subjects in form of a certificate chain related to the Subscriber's certificate.

It is recommended for the Relying Parties to perform generation of certificate path and implementation, as described in Chapter 6 of {Sz9} RFC 5280, before using the public key in question.

6.1.5. Key Sizes

In compliance with the applicable resolution of the Supervisory Body, the Service Provider uses standard algorithms, parameters and key lengths during provision of the Services both with respect to the Service Provider's and the end-user's certificates.

Algorithm and key length of key pairs used in Service Provider's certificates:

"Főtanúsítványkiadó - Kormányzati Hitelesítés Szolgáltató"Provider"	SHA256withRSA	4096 bit
„SSL Titkosító Tanúsítványkiadó 2014 - GOV CA"	SHA256withRSA	2048 bit
OCSP responder	SHA256withRSA	2048 bit

Algorithm and key size of key pairs of the Subjects: SHA256withRSA, 2048 bit.

The Service Provider observes the technical development and has the algorithm changed or the key size enlarged if required.
If the algorithm or any parameter of the key pairs used by the Subscribers or the Service Provider is not strong enough for the entire validity period of the related certificate, the Service Provider shall notify the Subscribers and the Relying parties, and order the revocation of the affected certificates.

6.1.6 Public key parameters generation and quality checking

The Service Provider's key pairs are generated in a protected environment (pursuant to Chapter 6.1.1.1) in a certified HSM module, in the simultaneous presence of at least two persons fulfilling confidential positions, excluding the presence of unauthorized persons. When generating Service Provider's key pairs, the Service Provider also adheres to the requirements described in the HSM module certification report.

With respect to the Subscriber's key pairs, the Service Provider checks if the algorithm, parameters and key length of the public key provided by the Subscriber are SHA256swithRSA2048 and meet the criteria specified in the relevant resolution of the Supervisory Body, and the key strength complies to the relevant specifications ({Sz21} point 6.1.1.3).

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Service Provider's private keys are solely used to sign certificates, revocations lists. OCSP responder's private keys are solely used to sign OCSP responses.

The private key related to the end-user certificates issued for the Subjects can exclusively be used for website authentication.

The Service Provider indicates the purpose of the key usage in the `KeyUsage` and `ExtendedKeyUsage` extensions of the certificate in accordance with standard {Sz12} ITU-T X.509 v3.

	extension		extension	
	critical?	**KeyUsage**	**critical?**	**ExtendedKeyUsage**
CA's certificate	yes	keyCertSign cRLSign	-	-
OCSP responder's certificate	yes	contentCommitment[1]	no	OCSPSigning
Subject's certificate	yes	digitalSignature keyEncipherment keyAgreement	no	serverAuth

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

The Service Provider applies a cryptographic module for the generation, storage and usage of the Service Provider's private keys, which

- is a trusted system, assessment of which has been done at level 4 or higher assessment warranty level according to MSZ/ISO/IEC 15408 {Sz14} or equivalent security criteria; or
- conforms to the criteria of ISO/IEC 19790 {Sz15}; or
- conforms to FIPS 140-2 {Sz16} level 3 or higher criteria.

6.2.2 Private key (n out of m) multi-person control

The Service Provider uses multi-person control ("n out of m") in the authentication centres for the activation of key management functions of the root authentication centre.

6.2.3 Private key escrow

The Service Provider does not deposit private keys of the authentication centres.

The Service Provider does not provide private key escrow services to Subscribers.

6.2.4 Private key backup

The private keys of the Service Provider's authentication centres are saved for security reasons. Backup is created by special hardware and software elements, and stored in an encrypted form. In extraordinary operating situations, the Service Provider may restore the private keys of the authentication centres from the encrypted backup, under similar strict physical, security precautions and procedural rules as applied during the generation of the original key pair.

The Service Provider does not backup and store the Subjects' private keys in any form.

6.2.5 Private key archival

The private keys of the Service Provider's authentication centres are saved for security reasons. The backup file shall be created by special hardware and software elements, and stored in an

[1] In previous version of X.509 and RFC 5280 standard: nonRepudiation

encrypted form, with suitable security precautions and procedural rules, which guarantee the integrity and confidentiality of the private key. The saved copies are preserved in encrypted format, in a physically secure environment.

The Service Provider does not backup and store the Subjects' private keys in any form.

6.2.6 Private key transfer into or from a cryptographic module

The private keys of the authentication centres are stored in the HSM module (described on Chapter 6.2.1) for their entire life-cycle.

If the Subscriber would like to store the key pair in a cryptographic module, then the Subscriber shall ensure import of the key pair into the module, inclusive to delete irreversibly all other copies of the private key.

6.2.7 Private key storage on cryptographic module

The private keys of the authentication centres are stored in the HSM module (described on Chapter 6.2.1) for their entire life-cycle. During storing of the keys, the Service Provider adheres to the requirements described in the HSM module certification report.

6.2.8. Method of activating private key

The Service Provider activates the private keys of authentication centres as described in the HSM module manufacturer's documentation.

6.2.9 Method of deactivating private key

The Service Provider ensures that the activated HSM module is protected from unauthorized access. The HSM module can only be used for authentication of the issued certificates, revocation lists and, optionally, OCSP responses. The private key is removed from the HSM module when the operation of the authentication centre terminates.

6.2.10. Method of destroying private key

The Service Provider irrevocably destroys the private key of the authentication centres when they are not needed anymore, or when the related certificate is expired or revoked. The private key and all activation data are destroyed in a way that no parts of the private key can be derived or extrapolated after destroying.

6.2.11 Cryptographic Module Rating

Included in Chapter 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The certificate contains the data used for web-server identification (public key). The Service Provider archives every certificate is issues, and preserves them for 10 years from their expiry or until the definitive settlement of any legal dispute related to the certificate. For security reasons, archives are made in two copies (using a redundant system). The Service Provider may also fulfil its preservation obligation by employing a qualified archiving service provider.

6.3.2 Certificate operational periods and key pair usage periods

The term of usage of the key pair is identical to the term of validity of the certificate that certifies its authenticity:

"Főtanúsítványkiadó - Kormányzati Hitelesítés Szolgáltató"	20 years
"SSL Titkosító Tanúsítványkiadó 2014 - GOV CA"	10 years
OCSP responder for Services Provider's certificates	maximum 30 days
OCSP responder (for end user certificates)	maximum 1 day
Website authentication certificate	maximum 2 years

The Service Provider ensures that the expiration date of the subscriber certificate is in all cases earlier than the expiration date of the Service Provider certificate used for the issuance by performing the key migration described in Chapter 5.6 in a timely manner.

6.4 Activation data

6.4.1 Activation data generation and installation

The Subscriber provides for generating the activation data of the Subject's private key, in a physically protected environment, using a random number generator of good quality, under secure circumstances.

6.4.2 Activation data protection

The Subscriber and the Subject ensure the exclusive possession and protection of the activation data.

6.4.3 Other aspects of activation data

No requirements.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The Service Provider determines the IT security technical requirements in accordance with the IT security technical requirements pertaining to confidential services issuing public key certificates set forth in standards {Sz2} EN 319 401 and {Sz3} EN 319 411-1, which are particularly the following:

#	reference	description
1.	EN 319 401 REQ-7.4-01 REQ-7.4-02 REQ-7.4-03	The Service Provider's systems can only be accessed by authorized persons. The Service Provider's internal network shall be protected with firewalls from unauthorized access, including the access of Subscribers and third parties. The firewalls shall prohibit every protocol and access that is not necessary for the operation.
2.	EN 319 401 REQ-7.4-1	Sensitive data shall be protected against being accessed by unauthorized parties through reused storage objects (e.g. deleted files).

3.	EN 319 411-1 GEN-6.5.5-02 GEN-6.5.5-03	During creation of a certificate, local network components (e.g. router) shall be kept in a physically and logically secure environment, and their configuration shall be regularly checked for compliance woth the requirements.
4.	EN 319 411-1 GEN-6.5.5-03	Multi-factor identification shall be applied for identifying every person and process that may directly result in the creation of certificate.
5.	EN 319 411-1 GEN-6.5.5-05	Applications managing certificate directories shall perform access control in every case that may result in addition, deletion of a certificate or modification of the related information.
6.	EN 319 411-1 GEN-6.5.5-06	Applications managing revocation status shall perform access control in every case that may result in modification of the revocation status information.
7.	EN 319 411-1 GEN-6.5.5-07	The Service Provider shall continuously monitor its resources and have an alarm system so that the Service Provider can detect unauthorized and/or abnormal access attempts, and can take counter-measures in due course.

6.5.2 Computer security rating

The Service Provider performs security evaluation of the IT systems in accordance with the provisions of Act L of 2013 on the Electronic Information Security.

6.6 Life cycle technical controls

6.6.1. System development controls

The Service Provider ensures that in every system development project performed by it or on behalf of it the security requirements are already considered in the planning phase and in the phase of determining the requirements, in order to implement the security into the IT systems.

System development rules on IT lifecycle are stated in the Service Provider's company level information security regulation; such rules determine precisely the tasks of design, preparation, project, operation, management and feedback as well as revocation/reconstruction cycle periods and the applied methodologies. The company level information security regulation considers the requirements specified in Chapter 6.5.6 of standard {Sz2} EN 319 411-1.

6.6.2. Security management controls

The Service Provider uses devices and procedures that guarantee the security of configuration settings of trusted IT systems, the operating system settings and network configuration settings used to provide the Services, and allow the control of integrity and proper operation of the applied security mechanisms.

The security management rules are determined in detail by the Security Regulation to PKI Services {D5} and the security policy {D6}.

6.6.3 Life cycle security controls

At regular intervals, the Service Provider checks the security of configuration settings of trusted IT systems, the operating system settings and network configuration settings used to provide the Services, and the control of integrity and proper operation of the applied security mechanisms.

type of security check	performed by	frequency

operative	IT Infrastructure	system operators	daily
	applications and logs used for the provision of services	system controllers	daily
internal control	IT Infrastructure	security officer	annually
	applications and logs used for the provision of services	security officer	annually
external control	IT Infrastructure	external auditor	annually
	applications and logs used for the provision of services	external auditor	annually

6.7 Network security controls

The network security measures are taken in accordance with the criteria specified in the Service Provider's {D6} security regulations, with consideration to the criterial described in Chapter 6.5.7 of standard {Sz2} EN 319 411-1.

6.8 Time-stamping

The Service Provider synchronizes the trusted systems used for the provision of the Services with trusted time sources (NTP) to the UTC at least once every 24 hours.

The Service Provider operates special technical appliances with high precision for determining the reliable time; these appliances are GPS based, and from time to time make the necessary synchronization to the UTC reference time sources, which have accuracy less than a hundredth second.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate Profile

The certificates issued by the Service Provider shall confirm to standards {Sz9} RFC 5280, {Sz4} EN 319 412-1, {Sz5} EN 319-412-2, {Sz6} EN 319 412-3, {Sz7} EN 319-412-4, {Sz8} EN 319-412-5 and the {Sz21} BRG recommendation.

In accordance with Chapter 4.2.3 of the standard {Sz8} EN 319-412-5, the Service Provider indicates the certificate type in the `QcStatements`/ `QcType`field, as follows:

certificate type	Contents of QcStatements / QcType field
website authentication certificate	`id-etsi-qct-web` (0.4.0.1862.1.6.3)

The Service Provider generates the serial number of certificates (`serialNumber`) from a random number containing at least 64 bits, higher than zero, generated by the CSPRNG random number generator.

Detailed description of the certificate profile is included in document {D8}, which the Service Provider makes available for the Relying Parties upon request.

7.1.1 Version number(s)

Version of certificates: V3.

7.1.2. Certificate extensions

The extensions applied in the certificates shall follow the requirements of standards {Sz9} RFC 5280, {Sz4} EN 319 412-1, {Sz5} EN 319-412-2, {Sz6} EN 319 412-3, {Sz7} EN 319-412-4, {Sz8} EN 319-412-5 in every aspect.

7.1.3 Algorithm object identifiers

The following algorithm identifiers are applied for signing the certificates:

`SHA256WithRSAEncryption {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}`

7.1.4 Name forms

The description of name formats and its interpretation is included in Chapter 3.1.

7.1.5 Name constraints

The Service Provider does not specify name constraints (`NameConstraints`) in the certificates.

7.1.6 Certificate policy object identifier

The Service Provider indicates the object ID of the Certificate Policy in the certificates.

7.1.7 Usage of Policy Constraints extension

The Service Provider does not specify policy constraints (`NameConstraints`) in the certificates.

7.1.8 Policy qualifiers syntax and semantics

The policy qualifiers (`PolicyQualifiers`) and text (`UserNotice`) included in the certificate indicate the applicability of the certificate.

7.1.9 Processing semantics for the critical Certificate Policies extension

The certificate policies (`CertificatePolicies`) extension is not marked as critical.

7.2 CRL profile

The revocation lists issued by the Service Provider comply with the {Sz9} RFC 5280 technical standard.

7.2.1 Version number(s)

Version of the revocation lists: V2.

7.2.2 CRL and CRL entry extensions

The revocation list contains the following extensions with “not critical” marking:

`CRLNumber`	strictly increasing Ref. Number of the revocation list
`AuthorityKeyIdentifier`	CA key identifier of the issuer

In addition to the above, the revocation list may also contain other standard extension, but these extensions may not be marked as “critical”.

Because the Service Provider does not provide revocation information in the form of a CRL for expired certificates, the CRL never includes the `ExpiredCertsOnCRL` extension.

7.3 OCSP profile

The OCSP service provided by the Service Provider comply with the {Sz13} RFC 6960 technical standard.

7.3.1 Version number(s)

Version of the OCSP responses: V1.

7.3.2. OCSP Extensions

The OCSP response contains the following extensions with “not critical” marking:

`Nonce`	random number in the OCSP request for preventing replay attacks (only when this is included in the request and the OCSP response is not a “final” OCSP response according to Chapter 4.10.1)

`ArchiveCutoff`	the time until the Service Provider provides the revocation status following the expiry of the certificate

In addition to the above, the OCSP response may also contain other standard extension, but these extensions may not be marked as “critical”.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

This Certification Practice Statement contains all the criteria to be met during the provision of the Services related to publicly issued, non-qualified website authentication certificates, which are specifically determined by the following standards:

- EN 319 401: General policy requirements for Trust Service Providers {Sz2}
- EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates {Sz3}
- EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures {Sz4}
- EN 319 412-2: Certificate Profiles; Part 2: Certificate profiles for certificates issued to natural persons {Sz5}
- EN 319 412-3: Certificate Profiles; Part 3: Certificate profiles for certificates issued to legal persons {Sz6}
- EN 319 412-4: Certificate Profiles; Part 4: Certificate profiles for web site certificates {Sz7}
- EN 319 412-5: Certificate Profiles; Part 5: QcStatements {Sz8}

8.1. Frequency or circumstances of assessment

The Service Provider performs external and internal audits in order to make sure that its Service-related processes, devices, staff and environment adhere to the applicable laws and standard requirements at all times. The Service Provider's affected organizations and staff shall cooperate with the auditor appointed by the Service Provider and to ensure the conditions for the control.

The conformance of the Service Provider's regulations is controlled by the Certification Policy and Regulation Group of the Service Provider. In order to verify the conformity of the services, the Service Provider performs internal audits.

The Supervisory Body also reviews the Service Provider's public policies during registration and upon modification of the policies, and in case of conformance, it publishes the mandatory policies to be submitted. The Supervisory Body may perform regular on-site inspections to verify the Service Provider's operation.

The Service Provider has a quality assurance system and IT security control system, which are verified by an independent external system controller for proper operation.

The Service Provider performs external and internal reviews (to be performed by its own controlling organization) at regular intervals specified in the security policy of PKI services, but at least once a year.

8.2 Identity/qualifications of assessor

The Service Provider employs an expert or organization providing expertise services, which are independent from the Service Provider and from the audited system, field, and can guarantee expertise in the field of PKI and IT security as well as technical, technological, legal, procedural skills and auditing methodologies relevant to those areas.

The internal audits relevant to the Service Provider's activities and IT security are performed by the Service Provider's internal organization, involving the security officers working for that organization.

8.3 Assessor's relationship to assessed entity

The organization, its employees and the external system auditor providing external audits shall be totally independent from the Service Provider.

8.4 Topics covered by assessment

The audit covers the following fields:

- regulations and documents;
- control and verification requirements;
- personal security requirements;
- requirements related to the management of the Service Provider's key pair;
- operational and access security;
- physical and environmental security;
- provision of non-stop service;
- data security and archiving.

During audit, it is examined whether the Service Provider and the Services provided by it comply with:

- the applicable laws and standards;
- the Certificate Policy and the Certification Practice Statement.

8.5 Actions taken as a result of deficiency

The Service Provider prepares an action plan for managing deficiencies and bad practices revealed by operational checks, internal and external audits and expert's analyses. The deficiencies are immediately rectified and the actions are documented and verified.

The Service Provider shall eliminate any defects revealed during the on-site inspections by the Supervisory Body within the term agreed with the authorities, in accordance with the applicable laws and with consideration to the information and recommendations given by the authorities.

8.6 Communication of results

Persons performing internal and external audits and expert's analyses may only provide information about the Service Provider's activities to their client. The results of the audit and control are confidential trade secrets of the Service Provider; therefore these shall be managed in accordance with the company's data protection provisions. The Service Provider is not obliged to disclose specific defect.

In case of web-trust audit, the Service Provider publishes the audit report or an extract of it.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

The Service Provider may announce the service fees on the homepage for services, or may send a price information material to the parties interested. The Service Provider is entitled to unilaterally determine and change the fees.

The respective service fees for the Subscriber are stated in the Service Contract.

9.1.1 Certificate issuance or renewal fees

The Service Provider charges the Subscriber with a one-time or annual fee, which includes:

a. the fee for issuing certificates;

b. the fee for publishing it in the Repository (if the Subscriber consents to the publication of the certificate)

c. the fee for revocation of the certificate (if applicable) d. and the archiving fee for

expired certificates.

9.1.2 Certificate access fees

The Service Provider shall not charge any fees for providing access to the Service Provider's certificates and the Subscriber's certificates published in the public repository.

9.1.3 Revocation or status information access fees

The Service Provider shall not charge any fees for providing certificate revocation status information (CRL and OCSP).

9.1.4. Fees for Other Services

No requirements.

9.1.5 Refund policy

The Subscriber is entitled to the reimbursement of the fee of issued certificates in the following cases:

a. any data of the issued certificate is defect by fault of the Service Provider;
b. the issued certificate, private key and activation data do not cohere;
c. the issued PKCS#12 format keystore storing the private key and the activation code do not match;
d. the Service Provider fails to meet any of its obligations during the management of the Subscriber's certificate.

The claim for reimbursement shall be submitted in written form by the Subscriber to the Service Provider within 30 calendar days from the issue of the certificate at the Client Relations Office. The Service Provider shall judge the request in 15 calendar days.

In case the reimbursement request is accepted, the Service Provider revokes the certificate, and:

- issues a new certificate for the Subscriber, or

- re-transfers the fee within 20 calendar days to the bank account designated by the Subscriber.

After 30 calendar days following the issue of the certificate the Subscriber is entitled to any reimbursement of the fee solely in case of the proven breach of the agreement or of the obligations by the Service Provider.

The Service Provider is not obliged to reimburse invoiced fees for any other of its provided activities.

9.2. Financial responsibility

The General Terms and Provisions (ÁSZF-PKI) determines the extent of the Service Provider's financial liability and their limits.

9.2.1 Insurance coverage

The Service Provider possesses a liability insurance, which shall cover certificate-related damages caused out of the scope of the contract and the damaged caused by the breach of the contract, and which provides coverage for all damaged parties up to the limit specified in the liability insurance, in accordance with the provisions of the {D1} General Terms and Conditions.

The liability insurance also covers the following:

- costs described in Article 89 of the E-administration Act arisen for the Supervisory Body due to the failure of its obligations specified in Article 88 of the E-administration Act;
- costs of the compliance-assessment organization employed by the Supervisory Body in accordance with Paragraph (4) c) of Article 17 of {J1} eIDAS, provided that this is considered by the Supervisory Body as a procedural cost.

The liability limit specified in the insurance contract is HUF 3,000,000 or occasionally a higher amount.

9.2.2 Other assets

No requirements.

9.2.3 Insurance or warranty coverage for end-entities

No requirements.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

The Service Provider treats every data and information confidential that is not listed in Chapter 9.3.2.

9.3.2 Information not within the scope of confidential information

The following information are not deemed confidential:

- Service Provider certificates and the data included therein;
- The certificate and the data included therein, subject to the consent of the Subscriber;
- revocation information related to certificates;
- public information, policies and other documents published on the Service Provider's website;
- any data that is available from public data sources.

9.3.3 Responsibility to protect confidential information

The Service Provider provides access to confidential information only to persons and organizations having relevant authority. The protection of confidential information is ensured by providing suitable training to the staff and signing agreements with the employees and contractual partners.

9.4. Privacy of personal information

9.4.1 Privacy plan

The Service Provider has a corporate-level data protection policy ({D4}) and data protection guidelines relative to the Services, which are public documents and available on the Service Provider's website. These documents are in line with the relevant international and national laws.

9.4.2 Information treated as private

The Service Provider collects personal data directly only from the Subscriber and its Contact Person with their express written consent, and only to the extent necessary for issuing the certificate, providing information and determining personal identity.

The Service Provider deems the Subscriber's Contact Person's personal data as confidential data

9.4.2 Information not deemed private

The status information (for all certificates) shall not be treated confidentially. The status information shall include the reason and time of the certificate revocation (if any).

9.4.4 Responsibility to protect private information

The Service Provider ensures that the protection of personal data, its operation and regulations comply with the provisions of the {J7} GDPR.

9.4.5 Notice and consent to use private information

By filling out and signing the registration form, the Subscriber's Contact Person shall consent that the Service Provider will register, manage and store the data necessary for issuing the certificate, as well as the publication of the issued certificate.

By signing the Service Contract, the Subscriber shall consent that the Service Provider will register, manage and store the data necessary for issuing the certificate and signing the contract.

9.4.6 Disclosure pursuant to judicial or administrative process

In order to investigate or prevent crimes and for reasons of national security the Service Provider shall disclose confidential information specified in the relevant law − in case the conditions set forth in the relevant law are met − to the detective authority and the national security services without delay and subject to no additional conditions. The Service Provider records the fact of data provision, but does not notify the affected Subscriber thereof.

During a civil trial or non-trial legal procedure affecting the certificate's validity − in case the identity of the Requesting Party has been duly proven − the Service Provider disclose confidential information to the adverse party or its representative or the Court. The Service Provider records the fact of providing information and notifies the affected Subscriber thereof.

9.4.7 Other information disclosure circumstances

In case the Service Activities or the provision of Services are terminated, the Service Provider forwards the data of Subscribers to a third party, pursuant to the relevant laws.

9.5 Intellectual property rights

The owner of the certificates issued by the Service Provider to its clients and of the related respective asymmetric Key Pair is the Subscriber and its fully entitled user is the Subject without respect to the physical environment where the keys are stored and protected. In cases described in the Service Provider's regulations and terms and conditions, the Service Provider may publish, duplicate and revoke the certificate, or manage it in another way. The Subscriber and/or the Subject is entitled to use the distinguished name and other identifiers included in end-user certificates.

The Service Provider's certificates, the revocation information and the identifiers included in the end-user certificates and generated by the Service Provider are the properties of the Service Provider.

The Service Provider's regulations, contractual terms and conditions and other Service-related documents published on the website of the Services are exclusive properties of the Service Provider. These documents can only be used in relation to the use of the Services; any other uses for commercial or other purposes are strictly prohibited.

9.6 Representations and warranties

9.6.1 CA representations and warranties

The Service Provider is liable for fully meeting all its obligations specified in the Certificate Policy, in this Certification Practice Statement as well as the Service Contract signed with the Subscriber, even when certain tasks related to the provision of Services are performed by other sub-contractors.

The Service Provider is liable for the damages caused by the certificate to third parties not in a contractual relationship with the Service Provider in accordance with Article 6:519 {J5} Civil Code and to the Subscriber being in contractual relationship with the Service Provider in accordance with Article 6:142 of the {J5} Civil Code, if the Service Provider has breached the provisions of the Certificate Policy and this Certification Practice Statement as well as the Service Contract signed with the Subscriber, or the relevant obligations as per the applicable law effective at the time of the event. In case of doubt the Service Provider shall provide evidence that these obligations were met. The Service Provider is liable for the damages caused by other sub-contractor during provision of the Services as if those were caused by the Service Provider.

The Service Provider pays compensation for proven damages within its own competence, with consideration to the restrictions specified in the Service Contract signed with the Subscriber and Chapter 9.8.

The Service Provider shall not be liable for

- the Subjects' activities in relation to the private key;
- the Relying Parties' activities related to the verification and use certificates;
- policies issued by the Relying Parties or others.

The Service Provider's obligations

By issuing a Subscriber certificate under this Certification Practice Statement, the Service Provider, and its other sub-contractors involved in provision of the Services, undertakes to fully comply with the provisions of this statement during provision of the Services. The Service Provider takes all reasonable measures to ensure that the Subscribers and the Subjects proceed according to the requirements of this statement.

9.6.2 RA representations and warranties

Registration activities are performed by the Service Provider's Client Relations Office and Registration Agency. The Client Relations Office and Registration Agency comply with the requirements specified in the relevant laws and Service Provider policies.

The Service Provider shall be liable for the following activities during issuing the certificate:

- Providing full-scope and clear information to the Subscriber about what is specified in Point 1) of Chapter 4.1.2;
- identification of the Subject of the certificate;
  - authentication of the identity of organization using the procedure described in Chapter 3.2.2;
  - verification that each domain name to be listed in the certificate is used legally using the procedure described in Chapter 3.1.2.2;
- identification of the Subscriber's Contact Person, determination of his/her authorization to proceed;
- checking every data to be entered into the distinguishing name of the certificate's Subject (`Subject`) in public registers, where possible;
- verification of data entered into other fields and extensions of the certificate;
- recording data necessary for registration and issuing of the certificate in the designated IT system;
- generation of certificate using the data specified in the recorded request to the key pair provided by the Subscriber.

9.6.3 Subscriber representations and warranties

The Subscriber's rights The Subscriber is entitled to:

- use the Services in accordance with this Certification Practice Statement, the Service Contract and annex {D1} General Terms and Conditions;
- designate a contact person;
- request a certificate for the Subjects designated by him/her;
- request for the revocation of the certificates.

The Subscriber's liability

The Subscriber's liabilities are specified in the Service Contract and in annex {D1} General Terms and Conditions.

The Subscriber's obligations

While using the Services (including the subscriber's key pair generation, request and usage of certificates), the Subscriber shall proceed in accordance with the Service Provider's policies and the contractual terms and conditions. The Subscriber's obligations are specified in this Certification Practice Statement, in the Service Contract and in {D1} General Terms and Conditions.

The Subject's rights

The Subject is entitled to:

- use the issued certificate and the related private key for the purposes described in Chapter 1.4.1 and in the way described in this policy;
- request for the revocation of the certificate
- use other services related to the certificate, as described in this Certification Practice Statement.

With respect to the website authentication certificate, certain rights of the Subject may reasonably be exercised by the Subscriber or its Contact Person.

The Subject's liability

The Subject is liable for:

- the actuality, validity and accuracy of its data provided during registration;
- checking the data entered into the certificate;
- reporting any changes to its data without delay;
- secure management of the private key and the activation data;
- proper use of the certificate and the private key in accordance with the regulations;
- notifying and fully informing the Service Provider without delay in case of disputes;
- generally for meeting the requirements set forth in this policy.

With respect to the website authentication certificate, the Subject's liabilities apply to the Subscriber or its Contact Person.

The Subject's obligations

The Subject shall:

- read and understand this Certification Practice Statement prior to using the Services;
- provide complete and accurate data requested by the Service Provider and necessary for using the Services;
- use the Services for the purposes allowed or not prohibited by law, in line with the regulations of this policy and the referred documents;
- in case of data change (especially when the given data are included in the certificate) immediately send a written notification to the Service Provider, initiate revocation of the certificate and stop using the certificate;
- ensure that no unauthorized persons can access to the data and tools necessary for using the Services (especially the activation data);
- initiate revocation of the certificate without delay in the event the private key belonging to the certificate or the activation data are disclosed to unauthorized parties or lost, damaged, destroyed, and immediately cease to use the certificate and the related private key;
- respond to the Service Provider's query within the period determined by the Service Provider, in suspicion of key compromising or illegal use;
- acknowledge that the Subscriber is entitled to request for the revocation of the certificate;
- acknowledge that the Service Provider issues the certificate in the way and following the verification steps described in this policy.
- acknowledge that the Service Provider is entitled to revoke the certificate under circumstances described in Chapter 4.9.1;
- permanently stop using the private key and the related certificate when he/she learns of the compromising of an authentication centre of the Service Provider involved in the issue of the certificate;
- send a written notification to the Service Provider without delay when a legal dispute is arisen in relation to the certificate or the use thereof.

With respect to the website authentication certificate, the Subject's obligations apply to the Subscriber or its Contact Person.

9.6.4. Relying party representations and warranties

The Relying Parties may decide on accepting and the way of using certain certificates to their own consideration and/or according to their policies. When assessing the validity of the certificate, the Relying Party shall proceed with due diligence, and therefore it is strongly recommended to:

- comply with the requirements and provisions of the Certification Practice Statement;
- use trusted IT environment and applications;
- consider all limitations pertaining to the use of the certificate listed in the certificate or the Certification Practice Statement;
- act diligently when checking the certificate.

The Service Provider excludes liability (Chapter 9.8) if the Relying Party fails to proceed with caution or due diligence upon accepting the certificate or the web-server authenticity based thereon.

9.6.5. Representations and warranties of other participants

No reqiurements.

9.7 Disclaimers of warranties

The Service Provider excludes its liability if:

- the Relying Party fails to proceed with caution during checking and using the certificates, i.e. does not proceed pursuant to this Certification Practice Statement or the applicable laws;
- policies issued by the Relying Parties or others are not in compliance with tihs Certification Practice Statement;
- it cannot fulfil its information or other communicational obligations due to the operating error of the internet or any part thereof;
- the notification email address entered by the Subscriber's Contact Person has changed or has been deleted in the meantime, and therefore the Service Provider cannot notify them;
- the Subscriber fails to meet its obligations prescribed in the Certification Practice Statement;
- the Subject fails to meet its obligations prescribed in the Certification Practice Statement;
- the damage is caused by the error or weakness of cryptographic algorithms provided by the Supervisory Body in its effective resolution to the Service Provider;

9.8 Limitation of liability

The Service Provider limits its liability for compensation:

- in total, for all certificates and damages.

The Service Provider shall not be liable for occurred damages if during the control and use of the certificates or time-stamps the Relying Party did not proceed in accordance with applicable laws and competent technical standards or if it did not proceed with care and diligence.

The limits of the Service Provider's financial liabilities are specified in the Service Contract and in annex {D1} General Terms and Conditions. If the total amount of the well-founded claim for compensation submitted by several beneficiaries exceeds this limit, then each claim is paid in proportion to the rate of total claim and the insurance limit.

9.9 Indemnities

In addition to what is described in Chapter 9.8 of this statement, more details about claims for compensation are found in the Service Contract and {D1} General Terms and Conditions.

9.10 Term and termination

9.10.1 Term

Timely effect

A version of the Certification Practice Statement shall be effective from its effective date indicated on the front page and shall exist for an indefinite period of time. The effect of this statement terminates when a new version of the Certification Practice Statement takes effect or upon termination of the Services.

Objective force

The scope of this Certification Practice Statement covers the provision and use of the Services.

Personal force

The personal force of this Certification Practice Statement covers the Service Provider's staff involved in the provision of the Services, the Subscriber's Contact Persons and the persons liable for the use of certain certificates within the Subscriber's organization.

9.10.2. Termination

The Certification Practice Statement shall be regarded as terminated when the Service Provider terminates its service activities.

9.10.3 Effect of termination and survival

The provisions that remain effective also after termination, if any, are determined in the {D1} General Terms and Conditions and the Service Contract.

9.11 Individual notices and communications with participants

In cases where this Certification Practice Statement does not prescribe communication between the parties or its legally binding way, the Service Provider shall be notified in writing or in email, authenticated by the Subscriber's Contact Person's hand signature or electronic signature, sent to the contact details of the Client Relations Office. Electronic notifications can only be deemed as received after the Service Provider sends a confirmation thereof. The Service Provider sends response to queries within 30 days in an electronically signed or stamped reply message.

9.12 Amendments

9.12.1 Procedure for amendment

This Certification Practice Statement shall be modified in accordance with the rules described in Chapter 0 and 1.5.4. The modification of the Certification Practice Statement is indicated by the change of version.

9.12.2 Notification mechanism and period

In case of material or significant change of the Services, the Service Provider publishes a notification on its website (and may also send an information email to the Subscriber) in due time before the changes take effect so that the Relying Parties can prepare for the changes.

9.12.3 Circumstances under which OID must be changed

When a new version of the Certification Practice Statement is issued, the part of OID relevant to the version number will also change.

9.13 Dispute resolution provisions

In case of any disputes the Subscriber shall immediately notify and fully inform the Service Provider on every aspect of the matter before taking legal actions.

Complaints may be submitted in written form or personally to the contact details of the Client Relations Office. The Service Provider investigates every claim within 30 days from filing and notifies the plaintiff about the result of such investigation in a written form.

The procedure to be followed in case of legal disputes is stated in the {D1} General Terms and Conditions.

If any disputes arise, the Subscriber is entitled to contact a conciliator body before court proceedings, if the Subscriber is deemed a consumer according to the relevant laws. The name and contact details of the competent conciliator body is stated in Chapter 1.5.2 of this statement.

9.14 Governing Law

The Hungarian law shall apply for the Service Provider's agreements ant regulations and their fulfilment, ant these are to be interpreted in accordance with the Hungarian Law.

9.15 Compliance with applicable law

The Service Provider operates in accordance with the respective EU and Hungarian laws.

9.16 Miscellaneous provisions

No requirements.

9.16.1 Entire agreement

No requirements.

9.16.2 Assignment

No requirements.

9.16.3 Severability

If a provision of this Certification Practice Statement becomes invalid for any reasons, then the rest of the provisions will remain intact and in effect.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

The Service Provider may claim for compensation and the payment of attorney's fees to compensate for the damages, losses and costs caused by its partners. If the Service Provider fails to exercise its claim for compensation in a certain case, it does not mean that the Service Provider will waive its claim for compensation in other breach of this Certification Practice Statement in the future.

9.16.5 Force Majeure

Force Majeure: Events that occur independently from the will, acts and person of the Service Provider, and inevitable events that are out of the Service Provider's control (e.g. strike, war, civil uprising, natural disaster, inevitable physical or legal barriers arising by any of the Parties or other inevitable state of emergency) shall be regarded as force majeure, which hinders or renders it impossible to meet the obligations specified in this Certification Practice Statement provided that such circumstances arise after this Certification Practice Statement takes effect, or took effect beforehand, but their consequences affecting the performance of this Certification Practice Statement could not be foreseen at the given time.

The Service Provider shall not be liable for damages caused by force majeure.

9.17 Other provisions

The Service Provider makes the Services and the end-user products applied during the Services available for people with disabilities, when possible.