MICROSEC

e-Szignó Certificate Authority

eIDAS conform
Qualified Certificate for Electronic Signature
Disclosure Statement

ver. 2.23

Date of effect: 2021-07-31

OID	1.3.6.1.4.1.21528.2.1.1.193.2.23
Version	2.23
First version date of effect	2016-07-01
Security classification	PUBLIC
Approved by	Gergely Vanczák
Date of approval	2021-07-24
Date of effect	2021-07-31

Microsec Micro Software Engineering & Consulting Private Company Limited by Shares
Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13.

Version	Effect date	Description
2.0	2016-07-01	- eIDAS conformity.
2.1	2016-09-05	- Changes according to the NMHH comments.
2.2	2016-10-30	- Changes according to the auditor comments.
2.3	2017-04-30	- Changes according to the NMHH comments.
2.4	2017-09-30	- Yearly revision.
2.6	2018-03-24	- Global revision. - Introducing identity validation by state notaries. - Smaller improvements.
2.7	2018-09-15	- Yearly revision.
2.8	2018-12-14	- Changes based on the suggestions of the auditor.
2.11	2019-09-25	- Yearly revision.
2.12	2019-12-12	- Changes based on the suggestions of the auditor.
2.13	2020-03-05	- Effect. - Identity validation rules. - Certificate modification. - HSM requirements. - Smaller improvements of wording.
2.14	2020-05-11	- Smaller improvements. - Introduction of video-based natural person identification in Section 3.1.3. - Adding more information for revocation in chapter 4.2.
2.15	2020-06-26	- Improvements regarding the Remote Key Management Service. - Removing video-based natural person identification from Section 3.1.3. - Smaller improvements.
2.16	2020-08-14	- Remove OCSP Signing EKU from ICA certificates. - Smaller improvements.
2.17	2020-10-28	- Improvements according to the auditor's and the supervisory body's findings. - Smaller improvements.
2.19	2020-12-15	- Introduction of video-based natural person identification in Section 3.1.3. - More detailed rules for the Certificate renewal initiated by the Service Provider. - Smaller improvements.

Version	Effect date	Description
2.21	2021-03-19	- Adding MD 940 to QSCD list. - Smaller improvements.
2.22	2021-06-30	- Clarifications and additions in accordance with the CPS in Chapters 1 and 2. - Publication of conformity assessment results. - Service fees. - Protection of personal data. - Smaller improvements.
2.23	2021-07-31	- 3 years certificate validity. - Certificate application through Customer portal.

Table of Contents

1 Introduction

This document is the *Disclosure Statement* concerning the issuance of qualified certificate for electronic signature service of e-Szignó Certificate Authority operated by Microsec ltd. (hereinafter: Microsec or *Certification Authority*).

The *Disclosure Statement* contains comprehensive information of the conditions for consumers using the service corresponding to the provisions of the *Certification Practice Statement*, according to the provisions of the decree 24/2016. (VI. 30.) of Ministry of Interiors concerning detailed requirements for trust services and their providers.

The *Disclosure Statement* complies with the requirements set by the eIDAS Regulation [1], the service provided according to these regulations is an EU qualified Trust Service.

The *Certification Authority* announced the provision of the trust service to the National Media and Infocommunications Authority on the 1st of July 2016.

The conformity assessment audit of the qualified trust services was carried out by the independent auditor TÜV Informationstechnik GmbH (hereinafter: TÜViT).

Based on the successful conformity assessment audit the National Media and Infocommunications Authority registered the qualified trust service and published it in the Hungarian Trusted List [10] on the 20th of December 2016.

The conformity assessment of the qualified trust service will be performed by Hunguard Kft (hereinafter Hunguard) as an independent auditor from October 2020.

1.1 Document Name and Identification

Issuer	e-Szignó Certificate Authority
Document name	eIDAS conform Qualified Certificate for Electronic Signature Disclosure Statement
Document version	2.23
Date of effect	2021-07-31

The list and identification information of the *Certificate Policies* that can be used according to the present *Disclosure Statement* can be found in section 1.1.1.

1.1.1 Certificate Policies

All *Certificate*s issued by the *Certification Authority* refer to that *Certificate Policy* on the basis of which they were issued.

In accordance with this *Disclosure Statement* the *Certification Authority* issues *Certificate*s based on the following *Certificate Policies*:

OID	DENOMINATION	SHORT NAME
1.3.6.1.4.1.21528.2.1.1.142.2.23	Qualified, for electronic signature creation and and validation, for natural persons controlling *Certificate*s issued on *Qualified electronic signature creation device* , Certificate Policy prohibiting the use of pseudonyms.	MATBN
1.3.6.1.4.1.21528.2.1.1.143.2.23	Qualified, for electronic signature creation and and validation, for natural persons controlling *Certificate*s issued on *Cryptographic Hardware Device* , Certificate Policy prohibiting the use of pseudonyms.	MATHN
1.3.6.1.4.1.21528.2.1.1.144.2.23	Qualified, for electronic signature creation and and validation, for natural persons controlling *Certificate*s issued by software, Certificate Policy prohibiting the use of pseudonyms.	MATSN

The rules of the formation and interpretation of the *Certificate Policy* short names can be found in the Appendix of this document.

The *Certification Authority* doesn't issue *Certificate*s with pseudonym.

The detailed requirements of the listed *Certificate Policy*(s) can be found in " e-Szignó Certificate Authority – eIDAS conform Qualified Certificate for Electronic Signature Certificate Policies ver.2.23." [11]

Among the present *Certificate Policies*:

- each *Certificate Policy* complies with the [QCP-n] *Certificate Policy* defined in the ETSI EN 319 411-2 [9] standard;
- the [MATBN] *Certificate Policy* complies with the [QCP-n-qscd] *Certificate Policy*.
- the [MATHN] *Certificate Policy* complies with the [NCP+] *Certificate Policy* defined in the ETSI EN 319 411-1 [8] standard.

Compliance with the ETSI Certificate Policies

In cases when an ETSI Certificate Policy is based on another ETSI Certificate Policy and this way contains all the requirements of it, only the Identifier of the Higher Level Certificate Policy is referenced in the issued *Certificate*s.

	[QCP-n]	[QCP-n-qscd]	[NCP+]
MATBN	(x)	X	
MATHN	X		X
MATSN	X		

1.2 Geographical Scope

The *Certification Practice Statement* based on the European Union requirements includes Hungarian specific requirements for services operating under the Hungarian law in Hungary.

The *Certification Authority* may extend the geographical scope of the service, in this case it shall use not less stringent requirements than those applicable in the *Certification Practice Statement*. At services provided to foreign *Client*s, detailed conditions that differ from the *Certification Practice Statement* may be regulated in a specific service agreement.

The service provided according to the *Certification Practice Statement* is available worldwide. The validity of the *Certificate*s, Certificate Revocation Status Lists and OCSP responses issued according to the *Certification Practice Statement* is independent of the geographical location where they were requested from, and where they will be used.

The service provided according to the *Certification Practice Statement* can be only used as described in the *Certification Practice Statement* and in the *Certificate Policy*.

1.3 The Trust Service Provider

1.3.1 Data of the Service Provider

Name:	MICROSEC Micro Software Engineering & Consulting Private Limited Company by Shares
Company registry number:	01-10-047218 Company Registry Court of Budapest
Head office:	Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13.
Telephone number:	(+36-1) 505-4444
Fax number:	(+36-1) 505-4445
Internet address:	`https://www.microsec.hu`, `https://www.e-szigno.hu`

1.3.2 Contact information of the customer service

The name of the provider unit:	e-Szignó Certificate Authority
Customer service:	
	Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13., Graphisoft Park South Area, Building C
Office hours of the customer service:	on workdays between 8:30-16:30 by prior arrangement
Telephone number of the customer service:	(+36-1) 505-4444
Email address of the customer service:	`info@e-szigno.hu`
Send revocation request to:	`revocation@e-szigno.hu`
Service related information access:	`https://www.e-szigno.hu`
Place for registering complaints:	Microsec ltd. Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13., Graphisoft Park South Area, Building C
Relevant Consumer Protection Inspectorate:	Budapest Capital Authority for Consumer Protection 1052 Budapest, Városház str. 7. 1364 Budapest, Pf. 144.
Relevant Arbitration Board:	Arbitration Board of Budapest 1016 Budapest, Krisztina krt. 99. III. em. 310. Mailing address: 1253 Budapest, Pf.: 10.

1.4 Certificate Types

The *Certificate Policies* supported by the *Certification Practice Statement* corresponding to the issuance of qualified certificate for electronic signature service are presented in section 1.2.1 of the *Certification Practice Statement*. The ID of the applied *Certificate Policy* is always indicated in the "Certificate Policies" field of the *Certificate*.

The e-Szignó Certificate Authority provides various certificate types for its *Client*s, which mainly differ concerning their properties and data authentically bound to the *Subject*.

- *Organizational Certificate* means a *Certificate* wherein the *Subject* is an *Organization*, a device under the control of the *Organization* or the *Certificate* attests the relationship of a natural person *Subject* with the *Organization*. In this case, the name of the *Organization* is

indicated in the "O" field of the *Certificate*. This type of a *Certificate* can only be used as specified by the *Organization*.

In case of an *Organizational Certificate* issued to a natural person, further restrictions can be indicated in the "Title" field, related to the usage of the *Certificate*.

- *Certificate for Profession* means a *Certificate* issued to a natural person which is not an *Organizational Certificate* and which contains the title or profession of the *Subject* in the "Title" field.
- *Certificate for Automatism* means a *Certificate* wherein the denomination of the IT device (application, system) is indicated amongst the *Subject* data in the *Certificate*, by the help of the *Subject* uses the *Certificate*.
- Pseudonymous *Certificate* means a *Certificate* wherein not the official – verified by the *Certification Authority* – denomination of the *Subject* is in the *Certificate*. In the pseudonymous *Certificate*s the requested name is indicated in the "Pseudonym" field, and it is stated in the "CN" field that the *Certificate* contains a pseudonym.
- *Certificate*s requiring *Qualified electronic signature creation device* usage: In that case the *Certificate* was issued to a public key for which the corresponding private key was generated on a *Qualified electronic signature creation device* – so it is guaranteed that the private key can not be extracted and copied –, then that information is indicated on the *Certificate* in the "QCStatements" field. Qualified electronic signature can be created only based on a *Certificate* this type.
- Personal *Certificate* means a *Certificate* that does not contain either an "O" or a "Title" field. This type can only be issued to natural persons.

The e-Szignó Certificate Authority issues *Certificate*s for natural persons and legal persons. In case of *Certificate*s issued to legal persons the authorized representative natural person or a trustee authorized by the representative need to act on behalf of the legal person.

1.5 Certificate Usage

1.5.1 Appropriate Certificate Uses

The private keys belonging to the end-user *Certificate*s issued by the *Certification Authority* based on the present service can be only used for electronic signature creation, with the *Certificate*s the *electronic signature creator* can verify the authenticity of the documents signed by him.

The public key in the *Certificate*, the *Certificate* itself, the *Certificate Revocation List*s, the *Time Stamp*s and the online revocation status responses can be used for the electronic signature.

1.5.2 Prohibited Certificate Uses

*Certificate*s issued in accordance with the present *Certificate Policies*, and the private keys belonging to them using for other purposes than the generation and verification of electronic signature is prohibited.

1.6 Policy Administration

1.6.1 Person or Organization Responsible for the Suitability of the Practice Statement for the *Certificate Policy*

Person responsible for compliance with the *Certification Practice Statement* and the *Certificate Policy* referenced therein is:

Responsible person	Head of Process Management Department
Organization name	Microsec ltd.
Organization address	Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13.
Telephone number	+36 1 505-4444
Fax number	+36 1 505-4445
Email address	info@e-szigno.hu

The *Certification Practice Statement*s and the provision of the services are supervised by the National Media and Infocommunications Authority. The National Media and Infocommunications Authority maintains a register on the *Certificate Policies* and on the *Certification Authority*s applying these policies.

The register of the National Media and Infocommunications Authority on trust services is available on the following link:

`http://webpub-ext.nmhh.hu/esign2016/`

2 Publication and Repository Responsibilities

2.1 Repositories

The *Certification Authority* discloses the contractual conditions and policies electronically on its website on the following link:

`https://e-szigno.hu/en/terms-and-information`

The draft version of the new documents to be introduced are disclosed on the website 30 days before coming into force.

The documents in force are available on the site in addition to all previous versions of all documents.

The actual version of policies and contractual conditions is readable in printed form at the customer service of the *Certification Authority*.

After concluding the contract, the *Certification Authority* makes the General Terms and Conditions, the *Disclosure Statement*, the *Certificate Policy* and the *Certification Practice Statement* available to the *Client* in the form of an electronically signed PDF file that can be downloaded from its website. The *Certification Authority* makes the individual Service Agreement available to the *Client* on paper, authenticated with a handwritten signature and seal, or in the form of an electronic document in PDF format with a qualified electronic signature.

The *Certification Authority* notifies its *Client*s about the change of the General Terms and Conditions.

2.2 Publication of Certification Information

The *Certification Authority* publishes on its webpage (`https://www.e-szigno.hu`) and through LDAP protocol (`ldap://ldap.e-szigno.hu`)

- its provider *Certificate*s;
- the end user *Certificate*s.

Service Provider Certificates

With the following methods the *Certification Authority* discloses the *Certificate*s of the time-stamping units, certification units and the online certificate status service units it operates:

- The denomination of the root certification units, and the hash of its root certificates in the *Certification Practice Statement*. The information related to their change of status are available at the website of the *Certification Authority*.
- The status change of *Certificate*s of intermediate (non-root) certification units and the *Time-Stamping Unit*s is disclosed on the *Certificate Revocation List*s, its website and within the confines of the online certificate status response services.
- For the signers of the online certificate status responses the *Certification Authority* – compliant with the best international practice – issues a *Certificate* with extremely short period of validity (for 10 perc) thereby eliminating the need for *Certificate* revocation status verification.

  Each OCSP responder *Certificate* contains an indication ("nocheck"), that indicates that its revocation status doesn't need to be checked.

End-User Certificates

With the following methods the *Certification Authority* discloses status information related to the end-user *Certificate*s which it had issued:

- on *Certificate Revocation List*s,
- within the confines of the online certification status response service.

The end-user *Certificate* revocation status information

is disclosed by the *Certification Authority*, and the *Subject*'s consent is not required for it.

The *Certification Authority* guarantees, that the availability of its system publishing its service *Certificate*s, the *Certificate Repository* and the revocation status information on an annual basis will be at least at least 99.9% per year , while service downtimes may not exceed 3 hours in each case.

2.3 Time or Frequency of Publication

2.3.1 Frequency of the Publication of Terms and Conditions

The most important terms and conditions for the service are contained in the service contract to be signed by the *Client* during the conclusion of the contract, or in the General Terms and Conditions [12] document referenced therein.

The *Certification Authority* reviews the General Terms and Conditions annually or in case of exceptional request for change with priority and performs the necessary changes. The document will receive a new version number even after the smallest change and by taking into account the time required by the endorsement process, the planned date of coming into effect will be determined too.

The accepted document will be published on the webpage of the *Certification Authority* and it will be sent for review to the National Media and Infocommunications Authority 30 days prior to the planned entry into force date.

The *Certification Authority* will accept comments connected to the General Terms and Conditions published for 14 days prior to their becoming effective, at the following email address:

`info@e-szigno.hu`

In case of observations that require substantive changes, the document will be amended.

The *Certification Authority* will close and publish the version of the General Terms and Conditions as amended with remarks on the 7th day prior to its becoming effective.

2.3.2 Frequency of the Certificates Disclosure

The *Certification Authority*, regarding the disclosure of *Certificate*s, follows the practices below:

- the *Certificate*s of the root certification units operated by it are disclosed before commencing the service;
- the *Certificate*s of the intermediate certification units operated by it are disclosed within 5 workdays after issuance;
- the *Certification Authority* discloses the end-user Certificates in its *Certificate Repository* after issuance without delay.

2.3.3 The Changed Revocation Status Publication Frequency

The status information related to the end-user *Certificate*s issued by the *Certification Authority* and the provider *Certificate*s are available immediately within the confines of the online certificate status service.

The information related to the status of the *Certificate*s are disclosed in the Certificate Repository and on the *Certificate Revocation List*s.

2.4 Access Controls on Repositories

The provided information is freely available for anybody for reading purposes according to the specifics of the publication method.

The information disclosed by the *Certification Authority* shall only be amended, deleted or modified by the *Certification Authority*. The *Certification Authority* prevents the unauthorized changes to the information with various protection mechanisms.

3 Identification and Authentication

3.1 Initial Identity Validation

The *Certification Authority* can use any communication channel within the limits provided by law, for the verification of the identity of the person or organization requesting the *Certificate*, and for checking the authenticity of the data provided.

The *Certification Authority* may, in its sole discretion, refuse the issuance of the requested *Certificate* without any specific justification.

3.1.1 Method to Prove Possession of Private Key

Prior to the issuance of a *Certificate* the *Certification Authority* ensures and makes sure that the *Applicant* actually owns or manages the private key belonging to the public key of the *Certificate* .

If the *Certification Authority* generates within its organization the private key belonging to the qualified *Certificate* of the *Subject* – typically on *Qualified electronic signature creation device* or on *Cryptographic Hardware Device* in case of *Certificate Policies* requiring such – , then it does not have to specially verify that the *Applicant* owns the private pair of the public key to be verified.

If the *Applicant* requests the *Certificate* issuance for a key provided by it – typically in case of software certificates –, then the *Certification Authority* accepts the *Certificate Application* in PKCS#10 format, which at the same time verifies, that the holder of the private key did indeed request the *Certificate*.

The *Certification Authority* considers equivalent evidence that the *Subject* submits the *Certificate Application* with the public key to be included in the requested *Certificate* signed with the use of a valid qualified *Certificate* based electronic signature.

If the *Subject* private key is generated and managed by another *Trust Service Provider*, then the *Trust Service Provider* verifies that, the referred *Trust Service Provider* owns the private key, and it is under the sole control of the *Subject*. The *Certification Authority* may accept the authentic statement of the referred *Trust Service Provider* about this. The format of the statement may be electronic. The *Certification Authority* verifies the authenticity of the statement. The verification of the ownership happens with the acceptance of a PKCS#10 formatted *Certificate Application*.

3.1.2 Authentication of an Organization Identity

The identity of the *Organization* is verified in the following cases:

- if the *Subject* of the *Certificate* to be issued is the *Organization*;
- if the *Subject* of the *Certificate* to be issued is the device or system operated by the *Organization*;
- if the *Certificate* is issued to a natural person, but the name of the *Organization* is indicated on the *Certificate* as well.

Prior to the issuance of an *Organizational Certificate* the *Certification Authority* verifies the organizational data authenticity to be included on the *Certificate* based on authentic public registers.

Furthermore it is verified in these cases, that:

- whether the natural person acting on behalf of the *Organization* is entitled to act on behalf of the *Organization*;
- whether the *Organization* consented to the issuance of the *Certificate*.

For performing the verification, the *Client* shall give the following data:

- the official denomination, registered office and legal status of the *Organization*,
- official registration number of the *Organization* (e.g. company registration number, tax identification number), if applicable;
- the name of the organization unit within the *Organization*, if its indication in the *Certificate* is requested,
- in case of an *Organizational Certificate* issuance to a natural person, the role of the *Subject* within the *Organization*, if its indication in the *Certificate* is requested.

The following certificates and evidences have to be attached to the *Certificate Application*:

- the statement with the application submitter's manual signature on that, justifying that the data given for the *Organization* identification is correct and comply with reality;
- a declaration of the the applicant with his signature that there is no trademark amongst the data to be indicated in the *Organization Certificate*, or if included, proof that the *Organization* is entitled to use the trademark;
- a certificate regarding that on behalf of the organization the *Certificate Application* submitter natural person is entitled to submit the application [1];
- in case of an *Organizational Certificate* issuance to a natural person, the certificate regarding that the organization consents to that the name of the organization is indicated on the certificate issued to the natural person [2];
- the specimen signature of the person entitled to represent the *Organization* or other, official document equal to the specimen signature, which contains the name and signature of the persons entitled to represent the *Organization* [3];
- the *Organization* existence, name and the legal status verification document [4].

The *Certification Authority* is bound to verify the validity and authenticity of the presented documents.

[1] Section 3.1.5. contains the details regarding the verification of the authorizations and privileges.
[2] Section 3.1.5. contains the details regarding the verification of the authorizations and privileges.
[3] In case of Court of Registration registered firms the above documents can be acquired by the *Certification Authority*.
[4] In case of Court of Registration registered firms the above documents can be acquired by the *Certification Authority*.

Identity validation of foreign Organizations

The *Certification Authority* does not exclude the verification of *Organization*s registered abroad, as far as the data verification with adequate records of the country or obtaining a certificate issued by a trusted third party is feasible.

In respect of data verification, the *Certification Authority* accepts:

- information obtained directly from the government register of the foreign country by the *Certification Authority* or queried by a third party but authenticated by the primary data provider;
- certificate issued by the embassy or consulate of the foreign country in Hungary, that the organization exists and the given information is correct;
- certificate issued by a Hungarian embassy or consulate in a foreign country, that the organization exists and the given information is correct.

The *Certification Authority* may accept other documents and evidences too, if it makes sure that the level of security is the same as of the above. Obtaining such evidence and submitting it to the *Certification Authority* is the *Client*ś responsibility.

The *Certification Authority* only accepts valid documents, and evidences not older than 3 months.

The *Certification Authority* does not issue the *Certificate* if it considers that based on its internal rules it can not verify with corresponding confidence a certificate issued abroad, a document or the data of the foreign organization.

The *Certification Authority* guarantees by the proper usage of the trusted roles and the internal administrative processes that during the registration and verification process of the personal data at least two employees needed by the proper trusted roles.

3.1.3 Authentication of an Individual Identity

The natural person's identity shall be verified:

- if the *Subject* of the *Certificate* to be issued is a natural person;
- if a natural person is acting on behalf of an *Organization* for *Organizational Certificate* application.

When issuing a qualified *Certificate*, the identity of the natural person shall be verified according to (1) paragraph of Article 24 of the eIDAS regulation [1] by the physical presence or by a method providing equivalent security. The *Certification Authority* uses the identification methods described in the (1) paragraph of article 24. as follows.

The *Certification Authority* verifies the identity of the natural person applying one of the following methods.

1. **During face to face identity validation.**

   - the natural person shall appear in person before the person performing the identity validation, who may be one of the following:
     - officier of the *Registration Authority*,
     - state notary, as a third party in accordance with the Hungarian legislation.

   - the identity of the natural person is verified during personal identification based on a suitable official proof of identity card;

     The identification can be based on the following official documents:
     - in case of natural persons within the scope of Act LXVI. of 1992. (henceforth: Nytv. [2]) official cards appropriate for verifying identity defined in Nytv. in accordance with Eüt. 82.§ (3) [4];
     - in case of natural persons outside the scope of Nytv. [2] on the basis of a travel document defined in the Act on the entry and residence of persons enjoying the right of free movement and residence or the law on entry and residence of third-country nationals [3] in accordance with Eüt. 82.§ (4) [4];
     - in case of identification of natural persons who have none of the documents mentioned above the *Certification Authority* applies personal identity validation in accordance with Eüt. 82.§ (5) [4] only in the case of identifying European citizens. In such case a personal identity card with a photo issued by the European country of natural person's nationality is accepted as a trusted document for identity validation.
   - the natural person shall declare the correctness of the personal identification data used for the identity validation with a written statement signed with a handwritten signature in the presence of the identification person; ;
   - In case of natural persons within the scope of Nytv. [2] the validity of the data on the identity card used for personal identification and the validity of the identity card is validated by the *Registration Authority* by using an authentic public register. In case of any other natural persons the *Certification Authority* doesn't validate the validity of the data on the identity card used for personal identification and the validity of the identity card by using an authentic public register, if such register is not available, it is not accessible to the *Certification Authority* or the costs of access and control are disproportionately high.
   - The person performing the identity validation verifies, whether any alteration or counterfeiting happened to the presented identity cards.

   During the initial identity validation the *Certification Authority* may accept the identification of a natural person carried out by a state notary as equivalent to the identity validation

made by its own *Registration Authority*, if it can be stated on the basis of the notarial certification clause attached to the *Certificate Application* signed before the notary that the state notary had compared the personal data of the *Applicant* having appeared before the notary with the content of an authentic public registry or other central database.

Further rules for the identity validation of foreign citizens

The *Certification Authority* may accept the identification carried out by a public notary as equivalent to the identity validation made by its own *Registration Authority*, if the public notary registered in such foreign country,

- which concluded an international bilateral treaty with Hungary on the mutual recognition of public deeds or
- which country ratified the "Hague Convention Abolishing the Requirement of Legalisation for Foreign Public Documents" of 5th October 1961. (Apostille)

The document issued by the public notary shall follow the requirements specified in the given agreement.

The *Certification Authority* may accept the *Certificate Application* signed before the notary public if the notarial certification clause shows that

- the notary public has verified the identity of the *Applicant* based on a suitable official document for identity validation (ID card, passport etc.);
- the *Applicant* has signed the *Certificate Application* in the presence of the notary public.

The *Certification Authority* always accepts the original documents when issued in Hungarian or English language. In case of documents issued on any other language the *Certification Authority* may request the official Hungarian translation of the documents translated by the OFFI (Hungarian Office for Translation and Attestation).

The *Certification Authority* may also accept other documents and evidences, if it makes sure that the level of security is the same as of the above. Obtaining such evidence and submitting it to the *Certification Authority* is the *Client*'s responsibility.

The *Certification Authority* only accepts valid documents and evidences not older than 3 months.

The *Certification Authority* does not issue the *Certificate* if it considers that based on its internal rules, that it can not verify with corresponding confidence the certificate, document or the data of the foreign organization.

2. **By identification traced back to a certificate of an electronic signature.**

   In this case:

   - The *Applicant* submits the *Certificate Application* in electronic form with a qualified electronic signature based on a non-pseudonymous qualified *Certificate*.
   - The electronically signed *Certificate Application* shall contain the data needed for the unambiguous identification of the natural person.
   - The *Certification Authority* verifies the authenticity and confidentiality of the *Certificate Application* on the entire certification chain.
   - The *Certification Authority* accepts only those electronic signatures which are based on a *Certificate* issued by a Trust Service Provider according to a Trust Service, which is listed on a national Trusted List published on the EU List of Lists and was valid at the time of the signature creation.
   - The *Certification Authority* may accept only those electronic signatures which are based on such a *Certificate* which was issued in compliance with the paragraph (1) point (a) or (b) of Article 24 of the eIDAS regulation [1].

3. **Using another method of identification approved on national level**

   Based on the 541/2020. (XII. 2.) Government Decree [5], the *Certification Authority* may also verify the identity of the natural person using identification by means of an electronic communication device providing video technology (hereinafter: video technology identification), which is recognized as equivalent to the face to face validation.

   In this case, the *Certification Authority* shall act as prescribed during the personal identification, with the difference that the personal meeting shall be replaced by a video technology based remote identification procedure in which:

   (a) In the case of video technology identification, the *Certification Authority* takes a video image of the *Client* during a live telecommunication connection, then compares the image taken of the *Client* with the photograph in the document used for identification (hereinafter: ID document). Identification is appropriate if it can be clearly established by the *Certification Authority* that the person in the ID document is the same as the *Client* in the video.

   (b) The *Certification Authority* sets out in detail in the "Information on online video identification terms" [13] document the conditions for the use of video technology identification, in particular the minimum requirements for the quality of the video connection. The document will be published on the *Certification Authority*'s website in accordance with the public regulations.

In order to perform a successful video technology identification, it is advisable to provide the following conditions:

- ID document in good condition
- properly lit environment
- quiet, undisturbed environment
- exclusion of the presence of other persons
- IT device with two-way audio and video capability
- camera with min. 2 megapixel video resolution
- stable internet connection at a speed of min 1.5Mbps.

(c) By presenting the *Certification Practice Statement* and the "Information on online video identification terms" [13] document and during the video recording, the *Certification Authority* ensures that the *Client* can get to know the conditions of the video technology identification in detail, and has expressly agreed to comply with them, and acts accordingly.

(d) The *Certification Authority* records and keeps for at least 10 years from the date of recording the entire communication established between the *Certification Authority* and the *Client* during the video technology identification, the detailed information of the *Client* related to video technology identification, and the *Client*'s express consent to this in a retrievable way, on video and audio, on a way that does not degrade the quality of the image and sound recording.

(e) The condition of successful video technology identification is that the image resolution of the electronic communication device enabling video technology identification and the illumination of the image be suitable for recognizing the gender, age and facial features of the *Client*, and the *Client*

- shall look into the camera so that his or her portrait can be recognized, captured and identified on the basis of the portrait shown on the ID document presented by him or her,
- shall communicate in a comprehensible manner the identifier of the document used for video identification,
- present his / her ID document in such a way that the security features and data sets contained therein can be identified, recorded and verified, and
- the data contained in the ID document can be matched with the data available about the *Client* at the *Certification Authority*, and the *Client* can be identified with the image shown on the ID document based on his / her image.

(f) The *Certification Authority* makes sure that the document is suitable for performing video technology identification, so

- the document complies with the requirements of the issuing authority,
- the individual security features, in particular the hologram, the kinegram or other equivalent security features, are recognizable and undamaged, and
- the document ID is the same as the document ID provided by the *Client*, recognizable and undamaged.

(g) During the video technology identification, the *Certification Authority* makes sure that

- the *Client*'s portrait is recognizable and identifiable by the portrait on the document presented by him, and
- the data contained in the document can be logically corresponded to the data available about the *Client* at the *Certification Authority*.

(h) A live telecommunications connection is also eligible if the *Certification Authority* examines the terms by machine or after the termination of the telecommunications connection, but makes sure that the *Client* is in a live connection during the identification.

The *Certification Authority* shall issue the *Certificate* only if the video technology identification fully complies with the above requirements.

The *Certification Authority* uses the data reconciled during a previous natural person identification procedure, if the *Subject* requests new *Certificate* instead of an expired or a revoked one, or if he requests a new *Certificate* besides the existing one during the validity period of the service agreement. The authenticity of the *Certificate Application*, the validity of the data to be icluded in the *Certificate* and the identity of the *Applicant* is validated by the *Certification Authority*.

The *Certification Authority* guarantees by the proper usage of the trusted roles and the internal administrative processes that during the registration and verification process of the personal data at least two employees needed by the proper trusted roles.

3.1.4 Non-Verified Subscriber Information

Only that data can be in the *Certificate* issued by the *Certification Authority* which has been verified by the *Certification Authority*.

3.1.5 Validation of Authority

The identity of the natural person representing the legal person is verified according to the requirements of Section 3.1.3. before issuing an *Organizational Certificate*.

The right of representation of the natural person shall be verified.

Persons entitled to act on behalf of an *Organization*:

- a person authorized to represent the given *Organization*,
- a person who is mandated for that purpose by an authorized person to represent the *Organization*,
- an *Organizational Administrator* appointed by an authorized person to represent the *Organization*.

The *Organizational Administrator* can be appointed during *Certificate Application*, or anytime later with the help of the corresponding form. The identifier information of the designated person(s) shall be given on the form, by which he/she can be identified in later litigation. The form shall be signed (manually or by creating a qualified electronic signature based on a non pseudonymous *Certificate*) by the representative of the *Organization*, which is verified by the registration associate of the *Certification Authority* when received.

Appointing an *Organizational Administrator* is not mandatory, and multiple *Organizational Administrator*s can be appointed too. If there is no appointed *Organizational Administrator*, then the person entitled to represent the *Organization* can perform this task.

3.1.6 Criteria for Interoperation

The *Certification Authority* does not work together with other Certification Authorities during the provision of the service.

3.1.7 Email address validation

For applications submitted on the *Certification Authority*'s web site, the *Certification Authority* validates the *Applicant*'s email address by verifying the email address before completing the *Certificate Application* form. The web page asks for the *Applicant*'s email address before filling in the form and does not allow other details to be filled in. The *Certification Authority* will send a randomly selected URL with a limited period of validity to the email address provided. The *Applicant* can only complete the form by clicking on the unique link provided. Each incoming *Certificate Application* therefore has an email address that is verified during operation.

In the case of a *Certificate Application* submitted otherwise, the *Certification Authority* sends an e-mail with a random number to the e-mail address to be verified, to which the *Applicant* shall respond and confirm the request. The response email shall include the random number sent by the *Certification Authority*. The random number is valid for 30 days.

3.2 Privacy Policy

The *Certification Authority* treats *Client*s' data according to legal regulations. The related Privacy Policy is accessible from the webpage of the *Certification Authority*

(`https://e-szigno.hu/en/all-documents.html`),

and for more information see section 9.3 of the *Certification Practice Statement*.

4 The Requirements for Certificates

4.1 Key Pair and Certificate Usage

4.1.1 Subscriber Private Key and Certificate Usage

The *Subject* shall only use its private key corresponding to the *Certificate* for electronic signature creation, and any other usage (for example, authorization and encryption) is prohibited.

A private key corresponding to an expired, revoked, or suspended *Certificate* shall not be used for electronic signature creation.

The *Subject* is bound to ensure the adequate protection of the private key and the activation data.

The limitations determined in Section 1.5. have to be followed during the usage.

4.1.2 Relying Party Public Key and Certificate Usage

To retain the level of security guaranteed by the *Certification Authority*, in the course of accepting the electronic signature verified, the *Relying Party* is recommended to proceed prudentially particularly regarding to the following:

- the *Relying Party* shall verify the validity and revocation status of the *Certificate*;
- *Certificate*s for electronic signatures and the corresponding public keys shall only be used for electronic signature validation;
- the verifications related to the *Certificate* should be carried out for the entire certificate chain up to a trusted root or intermediate provider certificate;
- when building the certificate chain, accept a Trust Service Provider *Certificate* as a trusted issuer (trust anchor) that
  - is listed in the Hungarian Trusted List [10] as a trust service entitled to issue qualified end-user *Certificate*s, and
  - it is accompanied by a Service Provider *Certificate* that was valid at the time of creating the signature and at the time of issuing the enduser *Certificate* used to create the signature;

- the electronic signature verification shall be performed with a reliable application, which complies with the related technical specifications, can be resiliently configured, and has been set correctly, and it runs within a virus-free environment;
- in case of personal *Certificate*s related to an organization, it is recommended to verify that the title of the Signatory by which it is entitled to sign the document can be identified by the certificate (for example indicated in the Title field);
- it is recommended to verify that the *Certificate* was issued according to the appropriate Certificate Policy;
- when accepting a qualified electronic signature it is recommended to verify that the *Certificate* was issued based on a *Certificate Policy* requiring *Qualified electronic signature creation device*;
- if it is indicated in the *Certificate*, it is recommended to verify the highest value of the obligation undertaken at one time (the Certification Authority is not responsible for the claims arising from electronic documents issued and signed concerning transactions in excess of those limits and for the damage caused this way.);
- the *Relying Party* shall consider any restrictions indicated in the *Certificate* or in the regulations referenced in the *Certificate*.

The *Certification Authority* makes available a service for its *Client*s and *Relying Parties* that they can use to verify the issued *Certificate*s.

4.2 Certificate Revocation and Suspension

The process when the *Certification Authority* terminates the validity of the *Certificate* before expiration is called *Certificate* revocation. The *Certificate* revocation is a permanent and irreversible status change, the revoked certificate will never be valid again.

The process when the *Certification Authority* temporarily ceases the validity of the *Certificate* before expiration is called *Certificate* suspension. The *Certificate* suspension is a temporary state; the suspended *Certificate* can be revoked, or before the end of the validity, with the withdrawal of the suspension it can be made valid again. In case of the withdrawal of suspension the *Certificate* becomes valid retroactively, as if it has not been suspended.

The usage of the private key belonging to the revoked or suspended *Certificate* shall be eliminated or suspended immediately. If possible, the private key belonging to the revoked *Certificate* shall be destroyed immediately after revocation.

Responsibility regulations related to suspension and revocation:

- If the *Certification Authority* has already published the revoked status of the *Certificate*, the *Certification Authority* does not take any responsibility, if the *Relying Party* considers the *Certificate* valid.

4.2.1 Who Can Request Revocation

The revocation of the *Certificate* may be requested by anyone using the web-based revocation service operated by the *Certification Authority* who knows the secret revocation password and the requested identification data.

The revocation of the *Certificate* may be requested in writing by the *Client*s, namely:

- the *Subscriber*;
- the *Subject*;
- in case of *Organizational Certificate*, the *Organization*'s authorized representative;
- the contact person specified in the service agreement; *Organizational Administrator* appointed by the *Subscriber*;

and

- in case of remote key management service the Remote Key Management Service Provider;
- the *Certification Authority*.

Additionally, *Subscriber*s, *Relying Parties*, Application Software Suppliers, and other third parties may submit High Risk Certificate Problem Reports informing the *Certification Authority* of reasonable cause to revoke the *Certificate*, like fraud, misuse or key compromise.

The *Certification Authority* provides clear instructions on how to report suspected Private Key Compromise, *Certificate* misuse, or other types of possible fraud, compromise, misuse, inappropriate conduct, or any other matter related to *Certificate*s on the following website:

`https://e-szigno.hu/en/report-certification-security-events.html`

4.2.2 Procedure for Revocation Request

The *Certification Authority* ensures the following possibilities

to submit a revocation request:

- through the website of the *Certification Authority* 24 hours a day.

  The IT system of the *Certification Authority* processes the applications submitted through its website immediately, the site informs the application submitter about the results of the evaluation.

- in an electronic form with an electronic signature based on the non-pseudonymous *Certificate* with a security classification not lower than the *Certificate* to be revoked
- on paper signed manually at the customer service of the *Certification Authority* during office hours in person, or sent by post.

In case of a Revocation request submitted in writing the *Certification Authority* verifies the authenticity of the request, and the submitter's eligibility during the evaluation of the request.

In case of Revocation request signed with a valid electronic signature, there is no need for further verification of the identity of the applicant and the authenticity of the request.

In case of submitting revocation request on paper, via mail the *Certification Authority* verifies the manual signature on the request.

The reason for revocation shall be stated. If the revocation was requested by the *Client*, and it does not state the reason for revocation, then the *Certification Authority* considers that the reason for revocation is that the *Subject* does not want to use the *Certificate* anymore.

If the *Client* request the revocation due to key compromise, the *Certification Authority* ensures a possibility during the revocation process, to request a new *Certificate* in the framework of *Re-key* to replace the *Certificate* to be revoked.

When the revocation is requested in writing, the *Certification Authority* makes possible to ask the revocation in advance for a later date by giving the requested date of the revocation.

The revocation request shall contain the data to identify the *Certificate*.

The requester shall provide particularly the following information:

- the exact denomination of the *Subject*;
- if the *Certificate* was issued on a *Qualified electronic signature creation device*, the unique identifier of the *Qualified electronic signature creation device*;
- the *Certificate*'s unique identifier;
- the requested date of the revocation, if the revocation shall not happen immediately;
- identification data of the *Client*.

In case of invalid or incomplete revocation request the *Certification Authority* rejects the request. The *Certification Authority* notifies the *Subject* and the *Subscriber* about the fact and reason of the rejection by email.

In case of complete and valid request the *Certification Authority* makes a decision about the acceptence of the request. Depending on the content of the request the *Certification Authority* revokes the *Certificate* immediately or sets up the date of revocation according to the request.

In case of a successful revocation the *Certification Authority* notifies the *Subject* and the *Subscriber* about the revocation by email.

Further information about the suspension and revocation can be found on the home page of the *Certification Authority* on the following link:

`https://e-szigno.hu/en/certificate-suspension-and-revocation.html`

High-Priority Certificate Problem Report

The *Certification Authority* maintains a continuous 24x7 ability to respond internally to a High Priority Certificate Problem Report.

The *Certification Authority* begins investigating the Certificate Problem Report within 24 hours after receiving and decides whether revocation is appropriate based on the following criteria:

- the nature of the alleged problem,
- the consequences of revocation,
- the number of Certificate Problem Reports received about a particular *Certificate* or *Subscriber*,
- the entity making the complaint, and
- relevant legislation.

The *Certification Authority* provides a preliminary report on its findings to both the *Subscriber* and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, the *Certification Authority* works with the *Subscriber* and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the *Certificate* will be revoked, and if so, a date which the *Certification Authority* will revoke the *Certificate*.

The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation shall not exceed the time frame set forth in Section 4.9.5 of the *Certification Practice Statement*.

If necessary, the *Certification Authority* informs the National Media and Infocommunications Authority about the reported problem.

4.2.3 End-User Certificates

The validity period of the end user *Certificate*s issued by the *Certification Authority*

- is maximum

  3 years from issuance;

- shall not exceed the amount of time until which the used cryptographic algorithms can be used safely according to the algorithmic decision of the National Media and Infocommunications Authority;
- shall not exceed the expiration date of the provider *Certificate* that issued the *Certificate*.

During the Certificate renewal the *Certification Authority* may issue the new *Certificate* for the same end-user private key.

Both the service provider and the end-user key validity period is affected, if the National Media and Infocommunications Authority issues a new algorithm decree, according to which the used cryptographic algorithm or key parameter is not secure to the end of the planned usage period.

If this happens, the *Certification Authority* revokes the related *Certificate*s.

5 Compliance Audit and Other Assessments

The operation of the *Certification Authority* is supervised by the National Media and Infocommunications Authority in line with European Union regulations. The National Media and Infocommunications Authority holds site inspections on at least yearly basis at the *Certification Authority* location. Before the site inspection, the *Certification Authority* has a screening of its operations by an external auditor and sends the detailed report of the screening to the National Media and Infocommunications Authority within 3 days from its receipt. During the screening it is to be determined whether the operation of the *Certification Authority* meets the requirements of the eIDAS Regulation [1] and the related Hungarian legislation and the requirements of the applied *Certificate Policy*(s) and the corresponding *Certification Practice Statement*(s).

The subject and methodology of the screening complies with the following normative documents:

- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [1];
- ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers; [7]
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [6]

- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [8]
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates; [9]

The result of the screening is a confidential document accessible only to authorized persons.

The conformity certificate issued in accordance with the conformity assessment report is published on the webpage of the *Certification Authority*.

The *Certification Authority* applies verified and certified elements (electronic signature production IT system elements) in connection with the service.

The *Certification Authority* provides the following *Qualified electronic signature creation device*s for the *Subject*s:

- IDPrime MD 840 (contact mode only) and IDPrime MD 3840 (contact and non-contact mode) smartcard which consist of M7820 A11 security controller, MultiApp v3 Java Card platform and IAS v.4 electronic signature application.
  (Supplier: Gemalto)

- IDPrime MD 940 (contact mode only) and IDPrime MD 3940 (contact and non-contact mode) smartcard which consist of M7892 G12 security controller, MultiApp v4.0.1 Java Card platform and IAS Classic v.4.4.2 electronic signature application with MOC server v1.1.
  (Supplier: Gemalto)

In case of remote key management service:

- Product: Trident version 2.1.3

  (Supplier: I4P.informatikai Kft. (I4P Ltd.))

Devices being phased out

The following *Qualified electronic signature creation device*s will be gradually phased out by the end of 2025 due to the planned change in the usable cryptographic algorithms. The *Certification Authority* doesn't have these devices on stock so there will be no *Certificate* issuance on new *Qualified electronic signature creation device* and there will be no new key generation on these type of devices.

The *Certification Authority* may issue *Certificate*s for the *Qualified electronic signature creation device*s which were issued earlier and are still in use during the normal *Certificate* renewal or modification process.

The *Certification Authority* provides ongoing technical support and the software components required for the operation of the devices.

- Smartcard which consist of ST19WR66I microchip and Touch & Sign2048 V1.00 signature creation application.
  (Supplier: ST Incard)

- MultiApp ID Citizen 72k smartcard which consist of S3CC91C microchip, MultiApp v1.1 Java Card platform and IAS Classic v.3.0 electronic signature application.
  (Supplier: Gemalto)

- IDClassic 340 smartcard which consist of P5CC081V1A microchip, MultiApp ID v2.1 Java Card platform and IAS Classic v.3 electronic signature application (version: MPH117 V2.2 filter).
  (Supplier: Gemalto)

Before using *Qualified electronic signature creation device*, the *Certification Authority* makes sure that it has a valid device certificate that meets the current requirements.

The *Certification Authority* manages the *Qualified electronic signature creation device* throughout its life cycle in accordance with the requirements in the appendix to the device certificate.

The *Certification Authority* monitors the certification status of the used *Qualified electronic signature creation device*s at least until the end of the validity period of the last *Certificate* issued on them and takes appropriate measures in case of modification of this status.

In case of the revocation of the *Qualified electronic signature creation device*'s certificate the *Certification Authority* revokes all the valid *Certificate*s issued on that *Qualified electronic signature creation device* in which *Certificate*s the "id-etsi-qcs 4" statement was set .

The actual list of the *Qualified electronic signature creation device*s used by the *Certification Authority* and the information related to its certification can be found on the web page of the *Certification Authority* on the following link:

`https://e-szigno.hu/en/certification-of-qscd-devices.html`

The informativ full list of the certified *Qualified electronic signature creation device*s can be found on the web page of the European Commission. [5]

[5] `https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds`

The *Certification Authority* has rated every one of the system elements used for providing the services into security classes on the basis of its risk assessment system. The *Certification Authority* keeps records about these system elements and the security ratings associated with them in the scope of its risk management system.

In addition to the external audit, the *Certification Authority* also has its proprietary internal auditing system, which regularly examines compliance with previous audits, and takes the necessary steps in case of deviations.

The *Certification Authority* has an ISO 9001 standard compliant quality management system since 2002, moreover an ISO 27001 (formerly BS 7799) compliant information security management system since 2003, which are continuously audited and reviewed by an external auditing organisation

For more information on the governing law and compliance audits see sections 8. and 9.15 of the *Certification Practice Statement*.

5.1 Communication of Results

The *Certification Authority* publishes the summary report of the assessment on its web page on the following URL:

`https://e-szigno.hu/en/eidas/`

The *Certification Authority* doesn't publish the details of the findings, they are treated as confidential information.

The certificates of the conformity assessment audit can be found on the official site of the auditor [6], and they are published also on the site of the *Certification Authority* on the following link:

`https://e-szigno.hu/eidas/eidas.html`

The availabilities of the Hungarian National Trusted List are:

- human readable PDF format: `http://www.nmhh.hu/tl/pub/HU_TL.pdf`
- machine-processable XML format: `http://www.nmhh.hu/tl/pub/HU_TL.xml`

The register of the National Media and Infocommunications Authority on trust services is available on the following link:

`http://webpub-ext.nmhh.hu/esign2016/`

[6] `https://www.hunguard.hu/en/ugyfeleinknek/tanusitott-termekek-rendszerek/eidas-rendelet-szerinti-bizalmi-szolgaltatas/microsec-zrt/`

6 Other Business and Legal Matters

6.1 Fees

The *Certification Authority* publishes fees and prices on its webpage, and makes them available for reading at its customer service.

Price list availability:

- `https://e-szigno.hu/en/price-list`

The *Certification Authority* may unilaterally change the price list. The *Certification Authority* publishes any modification to the price list 30 days before it comes into force. The changes favorable for the *Client* may come into force with shorter deadline than 30 days. Modifications will not affect the price of services paid in advance.

Provisions associated with the payment and refunding of fees are contained in the service agreement and its annexes – the General Terms and Conditions in particular.

6.1.1 Certificate Access Fees

The *Certification Authority* grants free of charge online access to its *Certificate Repository* for the *Relying Parties*.

6.1.2 Revocation or Status Information Access Fees

The *Certification Authority* provides free of charge online CRL and OCSP service for the *Relying Parties* on the status of all end-user and intermediate *Certificate*s it issued.

6.2 Financial Responsibility

6.2.1 Insurance or Warranty Coverage for End-entities

- The *Certification Authority* has liability insurance to ensure reliability.
- The liability insurance covers the following damages caused by the *Certification Authority* in connection with the provision of services:
  - damages caused by the breach of the service agreement to the trust service *Client*s;
  - damages caused out of contract to the trust service *Client*s or third parties;
  - damages caused to the National Media and Infocommunications Authority by the *Certification Authority* terminating the provision of the trust service;

  - under the eIDAS Regulation [1] 17. article (4) e) point, the legal costs of conformity assessment bodies to perform a conformity assessment by the request of the National Media and Infocommunications Authority if it enforces the costs as legal costs.

- The liability insurance policy shall cover at least for 3.000.000 Hungarian forints. Coincidental damages occurred for the same reason constitute a single insurance event.
- The liability insurance provides coverage for the full damage of the aggrieved party – up to the liability limit – arising in context of the harmful behaviour of the *Certification Authority* regardless of whether the damage was caused by breach of contract or outside the contract.
- If the valid claim of several entitled parties related to an insurance event exceeds the liability limit defined for an insurance event in the liability insurance, then the compensation of the claims takes place in the proportion of the liability limit to the total sum of the claims.

6.3 Privacy of Personal Information

6.3.1 Privacy Plan

The *Certification Authority* has a Privacy Policy and a Privacy Notice document, which contain detailed regulations on the handling of personal data.

The Privacy Policy is published on the webpage of the e-Szignó Certificate Authority on the following URL:

`https://e-szigno.hu/en/all-documents.html`

The Privacy Notice is published on the webpage of the e-Szignó Certificate Authority on the following URL:

`https://e-szigno.hu/en/privacynotice.html`

6.4 Representations and Warranties

6.4.1 Subscriber Representations and Warranties

Subscriber Responsibility

The responsibility of the *Subscriber* is set by the service agreement and its attachments (including the terms and conditions).

Subscriber Obligations

The responsibility of the *Subscriber* is to act in accordance with the contractual terms and regulations of the *Certification Authority* while using the service including requesting and applying the *Certificate*s and private keys.

The obligations of the *Subscriber* are determined by the *Certification Practice Statement*, the service agreement, the General Terms and Conditions, as well as the relevant *Certificate Policy*.

When the *Subscriber* is informed about any actual or suspected misuse or compromise of the private key associated with the public key included in a *Certificate* belonging to the *Subscriber*, the *Subscriber* is obliged to

- promptly report this fact to the *Certification Authority*,
- promptly request the revocation or suspension of the *Certificate*,
- promptly cease using the *Certificate* and its associated private key.

Subscriber **Rights**

- *Subscriber*s have the right to use the services in accordance with the *Certification Practice Statement*.
- *Subscriber*s are entitled to specify which *Subject*s should be allowed to receive *Certificate*s, in writing, and *Subscriber*s have the right to request the suspension and revocation of such *Certificate*s.
- *Subscriber*s have the right to request the suspension and revocation of *Certificate*s.
- *Subscriber*s are entitled to appoint *Organizational Administrator*s.

Subject **Responsibility**

The *Subject* is responsible for:

- the authentication, accuracy and validity of the data provided during registration;
- the verification of the data indicated in the *Certificate*;
- to provide immediate information on the changes of its data;
- using its *Electronic signature creation device*, private key and *Certificate* according the regulations;
- the secure management of its private key and activation code;
- the secure management of the *Electronic signature creation device*
- for the immediate notification and for full information of the *Certification Authority* in cases of dispute;
- to generally comply with its obligations.

***Subject* obligations**

The *Subject* shall:

- read carefully *Certification Practice Statement* before using the service;
- completely provide the data required by the *Certification Authority* necessary for using the service, and to provide truthful data;
- if the *Subject* becomes aware of the fact that the necessary data supplied for using the service – especially data indicated in the certificate – have changed, it is obliged to immediately:
  - notify the *Certification Authority* in writing,
  - request the suspension or revocation of the *Certificate* and
  - terminate the usage of the *Certificate*;
- immediately terminate the usage of the private key belonging to the *Certificate*, if the *Subject* becomes aware of the fact that the subject's *Certificate* has been revoked, or that the issuing CA has been compromised;
- use the service solely for the purposes allowed or not proscribed by legal regulations, according to the cited regulations and documents;
- ensure that no unauthorized individuals have access to data and tools (passwords, secret codes, signature-creation devices) necessary for using the service;
- notify the *Certification Authority* in writing and without delay in case a legal dispute starts in connection with

  any of the electronic signature or the *Certificate*s associated with the service;
- cooperate with the *Certification Authority* in order to validate the data necessary for issuing certificates, and to do everything they can to allow the soonest possible completion of such verification;
- report this fact to the *Certification Authority* promptly and in writing, in case a *Subject*'s private key, *Electronic signature creation device* or the secret codes necessary for activating the device end up in unauthorized hands or are destroyed, and will also be obliged to initiate the revocation and/or suspension of the *Certificate*s and terminating the usage of the *Certificate*;
- answer to the requests of the *Certification Authority* within the period of time determined by the *Certification Authority* in case of key compromise or the suspicion of illegal use arises;

- acknowledge that the *Subscriber*s entitled to request the revocation and/or suspension of the *Certificate*;
- acknowledge that the *Certification Authority* issues *Certificate*s in the manner specified in the *Certification Practice Statement*, upon the completion of the validation steps described therein;
- acknowledge that the *Certification Authority* only displays data that are corresponding to reality in issued *Certificate*s. Accordingly, the *Certification Authority* validates data to be entered in *Certificate*s according to the *Certification Practice Statement*;
- acknowledge that in case of requesting an *Organizational Certificate*, the *Certification Authority* will issue the *Certificate* solely in the case of the consent of the *Represented Organization*;
- acknowledge that in case of requesting an *Organizational Certificate*, the *Represented Organization* has the right to request the revocation of the *Certificate*;
- acknowledge and accept that the *Certification Authority* is entitled to suspend and/or revoke the issued *Certificate* immediately if
  - the *Certification Authority* becomes aware that the data indicated in the *Certificate* do not correspond to the reality or the private key is not in the sole possession or usage of the *Subject* and in this case, the *Subject* is bound to terminate the usage of the *Certificate*;
  - the *Subscriber* violates the terms of service agreement or General Terms and Conditions;
  - the revocation is required by the *Certification Authority*'s *Certificate Policy* or *Certification Practice Statement*;
  - the *Certification Authority* becomes aware that the *Certificate* was used for an illegal activity
  - the *Subscriber* fails to pay the fees of the services by the deadline.

***Subject* Rights**

- *Subject*s have the right to apply for *Certificate*s in accordance with the *Certification Practice Statement*.
- In case this is allowed by the applicable *Certificate Policy*, *Subject*s are entitled to request the suspension and the revocation of their *Certificate*s, according to *Certification Practice Statement*.

6.4.2 Relying Party Representations and Warranties

The *Relying Parties* decide based on their discretion and/or their policies about the way of accepting and using the *Certificate* . During the verification of the validity for keeping the security level guaranteed by the *Certification Authority* it is necessary for the *Relying Party* to act with caution, so it is particularly recommended to:

- comply with the requirements, regulations defined in the present *Certificate Policy* and the corresponding *Certification Practice Statement*;
- use reliable IT environment and applications;
- verify the revocation status of the *Certificate* based on the current CRL or OCSP response;
- take into consideration every restriction in relation to the*Certificate* usage which is included in the *Certificate*, in the *Certification Practice Statement* and in the corresponding *Certificate Policy*.

6.5 Limitations of Liability

- The *Certification Authority* is not responsible for damages that arise from the *Relying Party* failing to proceed as recommended according to effective legal regulations and the *Certification Authority*'s regulations in the course of validating and using certificates, moreover its failing to proceed as may be expected in the situation.
- The *Certification Authority* shall only be liable for contractual and non-contractual damages connected to its services in relation to third parties with respect to provable damages that occur solely on account of the chargeable violation of its obligations.
- The *Certification Authority* is not liable for damages that result from its inability to tend to its information provision and other communication related obligations due to the operational malfunction of the Internet or one of its components because of some kind of external incident beyond its control.
- If The *Certification Authority* engages data comparison with an authentic database before the issuance of the *Subject*'s *Certificate*, it relays on the data received from the authentic database. The *Certification Authority* will not assume any liability for damages arising out of the inaccuracy of information provided by such authentic databases.
- The *Certification Authority* assumes liability solely for providing the services in accordance with the provisions of *Certification Practice Statement*, as well as the documents to which reference is cited herein (Certification Policies, standards, recommendations), moreover with its proprietary internal regulations.

Administrative Processes

The *Certification Authority* logs its activities, protects the intactness and authenticity of log entries, moreover retains (archives) log data over the long term in the interest of allowing for the establishing, documenting, and evidencing of financial accountability, its proprietary liability related to damage it causes, as well as that of damage compensation due to it for damage it suffers.

The *Certification Authority* preserves the archived data for the time periods below:

- the *Certificate Policy* for at least 10 years from the date of repeal;
- *Certification Practice Statement* for at least 10 years from the date of repeal;
- General Terms and Conditions for at least 10 years from the date of repeal;
- in the case of video identification, all communications recorded during the identification for at least 10 years from the date of recording;
- All electronic and / or paper-based information relating to Certificates for at least:
  - 10 years after the validity expiration of the Certificate;
  - until the completion of the dispute concerning the electronic signature generated with the certificate;
- all other documents to be archived for at least 10 years from the date of their creation.

Financial Liability

The *Certification Authority* has appropriate deposit according to the relevant legal requirements for its financial liability and to guarantee costs related to its termination and for reliability.

The *Certification Authority* has liability insurance according to the legal regulations required in order to ensure reliability.

Limitation of Financial Liability

The *Certification Authority* does not limit the highest level of the obligation undertaken at the same time.

In connection with the services provided as a qualified provider, the *Certification Authority* defines tariff plans, which differ from each other in the financial liability of the *Certification Authority* as stated below.

Certificate type	Limitation of the provider liability [M HUF]
basic	0,02

bronze	0,1
silver	5
gold	20
platinum	200

If the valid claim of several entitled parties related to an insurance event exceeds the amount defined for an insurance event in the liability insurance for the damages, then the compensation of the claims takes place in a relative ratio to the amount determined in the liability contract.

6.6 Dispute Resolution Provisions

The *Certification Authority* aims for the peaceful and negotiated settlement of the disputes arising from its operation. The settlement follows the principle of gradual approach.

The *Certification Authority* and the *Client* mutually agree that in the case of any disputed issue or complaint arising whatsoever, they will attempt amicable consultation through negotiation before taking the dispute to legal channels. The initiating party will be obliged to notify every other affected party promptly and to inform them fully concerning all of the case's implications.

The *Client* in case of a deputation is entitled to appeal to the Arbitration Board of Budapest before incidental judicial proceedings.

Questions, objections, and complaints related to the activity of the *Certification Authority* or the use of issued *Certificate*s shall be addressed to the customer care centre office in written form. The *Certification Authority* notifies submitting parties at the address they specify about having received a submission and the time required for investigation, within 3 business days calculated as of receiving a submission. The *Certification Authority* is obliged to issue a written response to the submitter within the specified time limit. The *Certification Authority* may request the provision of information required for giving a response from the submitter. The *Certification Authority* investigates complaints within 30 days, and notifies submitters about the results thereof.

Should a submitter find the response inadequate or if the dispute which had arisen can not be settled based on it without getting the *Certification Authority* involved, the submitter may initiate consultation with the *Certification Authority* and the *Relying Parties*. All participants of such consultation shall be given written notice regarding the date of consultation 10 business days in advance thereof; and the submission, the *Certification Authority*'s response, as well as any documents containing other required information shall be sent to them in writing.

Should consultation fail to achieve a result within 30 business days calculated as of a complaint being submitted, the submitter may file a lawsuit with respect to the issue. The *Relying Parties* shall subject themselves to the sole jurisdiction of the II. and III. District Court of Budapest and/or that of the Municipal Court of Budapest.

6.7 Governing Law

The *Certification Authority* at all times operates in accordance with the Hungarian legislation in force. The Hungarian law is the proper law of the *Certification Authority* contracts, regulations, and their execution, and they are to be construed by the Hungarian law.

A REFERENCES

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

[2] (Hungarian) Act LXVI of 1992 on the registration of citizens' personal data and address .

[3] (Hungarian) Act II of 2007 on the entry and residence of persons enjoying the right of free movement and residence .

[4] (Hungarian) Act CCXXII of 2015 on the general rules of electronic administration and trust services .

[5] (Hungarian) Government Decree 541/2020. (XII. 2.) on Other Methods of Identification Recognized at National Level as Providing Trust Equivalent to Personal Presence in the Case of Trust Services.

[6] ETSI EN 319 401 V2.3.1 (2021-05); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[7] ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers;.

[8] ETSI EN 319 411-1 V1.3.1 (2021-05); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

[9] ETSI EN 319 411-2 v2.3.1 (2021-05); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates;.

[10] Magyarország (Hungary): Trusted List (`http://www.nmhh.hu/tl/pub/HU_TL.pdf`).

[11] e-Szignó Certification Authority - eIDAS conform Qualified Certificate for Electronic Signature Certificate Policies.

[12] e-Szignó Certification Authority - General Terms and Conditions. .

[13] Microsec ltd. - Information on online video identification terms .