MICROSEC

e-Szignó Certificate Authority

eIDAS conform
Certificate for Website Authentication
Disclosure Statement

ver. 2.17

Date of effect: 28/10/2020

OID	1.3.6.1.4.1.21528.2.1.1.197.2.17
Version	2.17
First version date of effect	01/07/2016
Security classification	PUBLIC
Approved by	Gergely Vanczák
Date of approval	22/10/2020
Date of effect	28/10/2020

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	01/07/2016	New policies according to the RFC 3647 and the eIDAS requirements.
2.1	05/09/2016	Changes according to the NMHH comments.
2.2	30/10/2016	Changes according to the auditor comments.
2.3	30/04/2017	Changes according to the NMHH comments.
2.4	30/09/2017	Yearly revision.
2.6	24/03/2018	Global revision. Changes in the domain validation methods. Introducing identity validation by state notaries. Smaller improvements.
2.7	15/09/2018	Yearly revision.
2.8	14/12/2018	Changes based on the suggestions of the auditor.
2.9	24/04/2019	Changes in the domain validation requirements. Smaller improvements. Changes in the CABF BR.
2.10	25/06/2019	Smaller improvements.
2.11	25/09/2019	Yearly revision.
2.12	12/12/2019	Changes based on the suggestions of the auditor.
2.13	05/03/2020	Effect. Identity validation rules. Certificate modification. HSM requirements. Smaller improvements of wording.
2.14	26/05/2020	Adding more information for revocation in chapter 3.2. | Smaller improvements.
2.16	14/08/2020	Remove OCSP Signing EKU from ICA certificates. | Certificate lifetime is 398 days. | Smaller improvements.
2.17	28/10/2020	New domain validation possibility. | Improvements according to the auditor's and the supervisory body's findings. | Smaller improvements.

Table of Contents

1 Introduction

This document is the *Disclosure Statement* concerning the issuance of certificate for website authentication service of e-Szignó Certificate Authority operated by Microsec Micro Software Engineering & Consulting Private Company Limited by Shares (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 imposed by eIDAS regulation [1], the service provided in accordance with these regulations is a trust service according to the regulation.

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

1.1 Document Name and Identification

Issuer	e-Szignó Certificate Authority
Document name	eIDAS conform Certificate for Website Authentication Disclosure Statement
Document version	2.17
Date of effect	28/10/2020

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
1.3.6.1.4.1.21528.2.1.1.159.2.17	belonging to the III. certification class, for website authentication certificates, prohibiting the use of pseudonyms.	HWJSN
1.3.6.1.4.1.21528.2.1.1.161.2.17	belonging to the II. certification class, for website authentication certificates, prohibiting the use of pseudonyms.	KWJSN, KWTSN

1.3.6.1.4.1.21528.2.1.1.162.2.17	Issued during automatic issuance, controlling website authentication certificate issuance, Certificate Policy prohibiting the use of pseudonyms.	AWxSN

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

The detailed requirements of the listed *Certificate Policy*(s) can be found in " e-Szignó Certificate Authority – eIDAS conform Non Qualified Certificate for Website Authentication Certificate Policies ver.2.17." [11]

Among the present *Certificate Policies*:

- each *Certificate Policy* complies with the [LCP] *Certificate Policy* defined in the ETSI EN 319 411-1 [6] standard;
- each *Certificate Policy* complies with the [DVCP] *Certificate Policy* defined in the ETSI EN 319 411-1 [6] standard;
- each *Certificate Policy* complies with the [OVCP] *Certificate Policy* defined in the ETSI EN 319 411-1 [6] standard, if the organization name is indicated in the *Certificate*;
- each *Certificate Policy* complies with the [IVCP] *Certificate Policy* defined in the ETSI EN 319 411-1 [6] standard, if the natural person's is indicated in the *Certificate*;

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.

	[LCP]	[DVCP]	[OVCP]	[IVCP]
HWJSN	(x)		X	
KWJSN	(x)		X	
KWTSN	(x)			X
AWxSN	(x)	X		

1.2 Geographical Scope

The present *Disclosure Statement* includes specific requirements for services primarily provided for Hungarian *Client*s, operating by the Hungarian law in Hungary in Hungarian language. The *Certification Authority* can extend the geographical scope of the service, in this case, it shall use not less stringent requirements than those applicable to Hungarian conditions.

1.3 The Trust Service Provider

1.3.1 Data of the 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`

The access of the *Certificate Policy*, the *Certification Practice Statement* and the Privacy Policy:

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

The access of the price list:

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

Refund:

The termination of the service agreement does not affect the fees paid by the *Subscriber*.

The *Certification Authority* does not issue refunds on fees that have already been paid, unless the service agreement expires due to the *Certification Authority*'s fault, or if the *Certification Authority* explicitly allows for this – for example in case of several packages.

The access of the Hungarian national trust list:

- 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/`

The access of the service agreement:

The *Certification Authority* sends the service agreement to be concluded with the *Client*ss to the notification e-mail address of the *Applicant* given during initial registration.

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 certificate for website authentication 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*.
- *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*. In case of a *Website Authentication Certificate* the webserver domain name or IP address is indicated at the name of the *Subject*, so every *Website Authentication Certificate* is a *Certificate for Automatism*.

- Pseudonymous *Certificate* means a *Certificate* wherein not the official 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. *Website Authentication Certificate* can never be pseudonymous.
- 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 website authentication.

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 website authentication is prohibited.

1.6 Supervisory body

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 below link:

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

2 Identification and Authentication

2.1 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 refuse the issuance of the required *Certificate* at its sole discretion, without any apparent justification.

2.1.1 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 *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*.

2.1.2 Authentication of an Organization Identity or a Domain

3.2.2.1 Authentication of 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* (including the *Website Authentication Certificate*s requested by the *Organization* ;

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,

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];
- 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* [2];
- the *Organization* existence, name and the legal status verification document [3].

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

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.

[1] Section 2.1.5. contains the details regarding the verification of the authorizations and privileges.

[2] In case of Court of Registration registered firms the above documents can be acquired by the *Certification Authority*.

[3] In case of Court of Registration registered firms the above documents can be acquired by the *Certification Authority*.

3.2.2.2 Validation of Domain Authorization or Control

At least one domain name or IP address shall be in the *Website Authentication Certificate*s.

Before the issuance of *Website Authentication Certificate*s the *Certification Authority* ensures about the genuineness of the domain name or IP address to be indicated in the *Certificate*, and the *Applicant* shall demonstrate in practice that he has control over the given domain name or IP address.

If more than one domain name or IP address is indicated in the *Certificate*, the aforementioned verification shall be carried out in each case.

If a domain name containing a wildcard "*" character is indicated in the *Certificate* (wildcard certificate), the *Certification Authority* ensures that, the *Applicant* is the authorized user of the entire domain namespace covered by the wildcard domain name. The *Certification Authority* does not issue a *Certificate*, in which the domain name space to be covered by the wildcard domain name is a registered gTLD or ccTLD (for example: "*.com", "*.co.uk"), or a subdomain under these TLDs under which public domain name registration is directly possible. The *Certification Authority* checks the public domain names open for direct registration in the "ICANN DOMAINS" section of "Public Suffix List" (`https://publicsuffix.org/list/public_suffix_list.dat`).

The *Certification Authority* issues *Certificate*s for public domain names and IP addresses used on the Internet, not for domain names and IP addresses reserved for internal use.

The *Certification Authority* issues *Certificate*s only for those top level domains which can be found on the actual IANA Root Zone Database.

The *Certification Authority* supports the usage of the Internationalized Domain Names according to the IDNA2003 [7] requirements.

The *Certification Authority* doesn't issue *Certificate* for the ".onion" pseudo top level domain.

The *Certification Authority* shall confirm that prior to issuance, the CA has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below in line with the requirements of the latest version of the CA/Browser Forum Baseline Requirements.

3.2.2.2.1 Validating the Applicant as a Domain Contact (BR 3.2.2.4.1)

This validation method is not used.

3.2.2.2.2 Email to Domain Contact (BR 3.2.2.4.2)

Confirming the *Applicant*'s control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The *Certification Authority* sends the Random Value to an email address identified as a Domain Contact.

Each email may be used for identification of multiple Domain Names.

The *Certification Authority* may send the email identified under this section to more than one recipient provided that every recipient is identified by the Domain Name Registrar as representing the Domain Name Registrant for every FQDN being verified using the email.

The Random Value is unique in each email.

The *Certification Authority* may resend the email in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged. The Random Value remains valid for use in a confirming response for 30 days from its creation.

3.2.2.2.3 Phone Contact with Domain Contact (BR 3.2.2.4.3)

This validation method is not used.

3.2.2.2.4 Constructed Email to Domain Contact (BR 3.2.2.4.4)

Confirming the *Applicant*'s control over the FQDN by

- sending an email to one or more addresses created by using
  - "admin",
  - "administrator",
  - "webmaster",
  - "hostmaster" or
  - "postmaster"

  as the local part, followed by the atsign ("@"), followed by an Authorization Domain Name,
- including a Random Value in the email, and
- receiving a confirming response utilizing the Random Value.

Each email may confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed.

The Random Value is unique in each email.

The email may be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient shall remain unchanged.

The Random Value remains valid for use in a confirming response for 30 days from its creation.

3.2.2.2.5 Domain Authorization Document (BR 3.2.2.4.5)

This validation method is not used.

3.2.2.2.6 Agreed-Upon Change to Website (BR 3.2.2.4.6)

Confirming the *Applicant*'s control over the FQDN by confirming the following under the "/.well-known/pki-validation"
directory, on the Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port.

1. The presence of a unique Required Website Content including a Random Value contained in the content of a file. The entire Required Website Content shall not appear in the request used to retrieve the file or web page.

The *Certification Authority* provides a Required Website Content unique to the certificate request and uses the Required Website Content only for 30 days.

The *Certification Authority* uses this domain validation method only till the 31st of May 2020.

3.2.2.2.7 DNS Change (BR 3.2.2.4.7)

Confirming the *Applicant*'s control over the FQDN by confirming the presence of a Request Token containing a Random Value in a DNS TXT record for an Authorization Domain Name.

The *Certification Authority* provides unique Request Token for each *Certificate Application* which is valid only for 30 days.

Once the FQDN has been validated using this method, the *Certification Authority* may also issue *Certificate*s for other FQDNs that end with all the labels of the validated FQDN.

This method is suitable for validating Wildcard Domain Names.

3.2.2.2.8 IP Address (BR 3.2.2.4.8)

This validation method is not used.

3.2.2.2.9 Test Certificate (BR 3.2.2.4.9)

This validation method is not used.

3.2.2.2.10 TLS Using a Random Number (BR 3.2.2.4.10)

This validation method is not used.

3.2.2.2.11 Any Other Method (BR 3.2.2.4.11)

This validation method is not used.

3.2.2.2.12 Validating Applicant as a Domain Contact (BR 3.2.2.4.12)

This validation method is not used.

3.2.2.2.13 Email to DNS CAA Contact (BR 3.2.2.4.13)

Confirming the *Applicant*'s control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value.

The Random Value is sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set is found using the search algorithm defined in IETF RFC 6844 [10] Section 4, as amended by Errata 5065 (Appendix A).

The CAA Email Contact value shall be given in the CAA contactemail property which has the email address as its parameter. The email address shall be given in the format defined by the rfc 6532 [9] section 3.2 with no additional padding or structure.

Example:

$ORIGIN example.com

CAA 0 contactemail "domainowner@example.com"

Each email may confirm control of multiple FQDNs, provided that each email address is a DNS CAA Email Contact for each Authorization Domain Name being validated. The same email may be sent to multiple recipients as long as all recipients are DNS CAA Email Contacts for each Authorization Domain Name being validated. The email may be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) shall remain unchanged.

The Random Value is unique in each email. The Random Value remains valid for use in a confirming response for 30 days from its creation.

Once the FQDN has been validated using this method, the *Certification Authority* may also issue *Certificate*s for other FQDNs that end with all the labels of the validated FQDN.

This method is suitable for validating Wildcard Domain Names.

3.2.2.2.14 Email to DNS TXT Contact (BR 3.2.2.4.14)

Confirming the *Applicant*'s control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value.

The Random Value is sent to a DNS TXT Record Email Contact for the Authorization Domain Name selected to validate the FQDN.

The DNS TXT record shall be placed on the "_validation-contactemail" subdomain of the domain being validated. The entire RDATA value of this TXT record shall be a valid email address as defined in RFC 6532 [9] section 3.2, with no additional padding or structure, or it cannot be used.

Each email may confirm control of multiple FQDNs, provided that each email address is DNS TXT Record Email Contact for each Authorization Domain Name being validated. The same email may be sent to multiple recipients as long as all recipients are DNS TXT Record Email Contacts for each Authorization Domain Name being validated. The email may be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) shall remain unchanged.

The Random Value is unique in each email. The Random Value remains valid for use in a confirming response for 30 days from its creation.

Once the FQDN has been validated using this method, the *Certification Authority* may also issue *Certificate*s for other FQDNs that end with all the labels of the validated FQDN.

This method is suitable for validating Wildcard Domain Names.

3.2.2.2.15 Phone Contact with Domain Contact (BR 3.2.2.4.15)

Confirming the *Applicant*'s control over the FQDN by calling the Domain Contact's phone number and obtain a confirming response to validate the ADN.

Each phone call may confirm control of multiple ADNs provided that the same Domain Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN. In the event that someone other than a Domain Contact is reached, the *Certification Authority* may request to be transferred to the Domain Contact.

In the event of reaching voicemail, the *Certification Authority* may leave the Random Value and the ADN(s) being validated. The Random Value must be returned to the *Certification Authority* to approve the request. The Random Value remains valid for use in a confirming response for 30 days from its creation.

Once the FQDN has been validated using this method, the *Certification Authority* may also issue *Certificate*s for other FQDNs that end with all the labels of the validated FQDN.

This method is suitable for validating Wildcard Domain Names.

3.2.2.2.16 Phone Contact with DNS TXT Record Phone Contact (BR 3.2.2.4.16)

Confirming the *Applicant*'s control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtain a confirming response to validate the ADN.

The DNS TXT record shall be placed on the "_validation-contactphone" subdomain of the domain being validated. The entire RDATA value of this TXT record shall be a valid Global Number as defined in RFC 3966 [8] section 5.1.4, or it cannot be used.

Each phone call may confirm control of multiple ADNs provided that the same DNS TXT Record Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN. The *Certification Authority* may not knowingly be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation.

In the event of reaching voicemail, the *Certification Authority* may leave the Random Value and the ADN(s) being validated. The Random Value must be returned to the *Certification Authority* to approve the request. The Random Value remains valid for use in a confirming response for 30 days from its creation.

Once the FQDN has been validated using this method, the *Certification Authority* may also issue *Certificate*s for other FQDNs that end with all the labels of the validated FQDN.

This method is suitable for validating Wildcard Domain Names.

3.2.2.2.17 Phone Contact with DNS CAA Phone Contact (BR 3.2.2.4.17)

Confirming the *Applicant*'s control over the FQDN by calling the DNS CAA Phone Contact's phone number and obtain a confirming response to validate the ADN.

Each phone call may confirm control of multiple ADNs provided that the same DNS CAA Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN.

The relevant CAA Resource Record Set shall be found using the search algorithm defined in RFC 6844 [10] Section 4, as amended by Errata 5065 (Appendix A). The phone number shall be in the CAA contactphone property as its parameter. The entire parameter value shall be a valid Global Number as defined in RFC 3966 [8] section 5.1.4, or it cannot be used. Global Numbers shall have a preceding + and a country code and may contain visual separators.

The following is an example where the holder of the domain specified the contact property using a phone number.

$ORIGIN example.com.

CAA 0 contactphone "+36 (1) 123-4567"

The *Certification Authority* may not knowingly be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation.

In the event of reaching voicemail, the *Certification Authority* may leave the Random Value and the ADN(s) being validated. The Random Value shall be returned to the *Certification Authority* to approve the request. The Random Value remains valid for use in a confirming response for 30 days from its creation.

Once the FQDN has been validated using this method, the *Certification Authority* may also issue *Certificate*s for other FQDNs that end with all the labels of the validated FQDN.

This method is suitable for validating Wildcard Domain Names.

3.2.2.2.18 Agreed-Upon Change to Website v2 (BR 3.2.2.4.18)

Confirming the *Applicant*'s control over the FQDN by verifying that the Request Token including a Random Value is contained in the contents of a file.

- The entire Request Token shall not appear in the request used to retrieve the file, and
- the *Certification Authority* shall receive a successful HTTP response from the request (meaning a 2xx HTTP status code shall be received).

The file containing the Request Token:

- shall be located on the Authorization Domain Name, and
- shall be located under the "/.well-known/pki-validation" directory, and
- shall be retrieved via either the "http" or "https" scheme, and
- shall be accessed over an Authorized Port.

The *Certification Authority* doesn't accept redirects (3xx HTTP status code).

The Random Value included in the Request Token:

- is unique to each *Certificate Application*;
- will remain valid for use in a confirming response for 30 days from its creation.

Once the FQDN has been validated using this method, the *Certification Authority* may also issue *Certificate*s for other FQDNs that end with all the labels of the validated FQDN.

This method is suitable for validating Wildcard Domain Names.

3.2.2.2.19 Agreed-Upon Change to Website - ACME (BR 3.2.2.4.19)

This validation method is not used.

3.2.2.2.20 TLS Using ALPN (BR 3.2.2.4.20)

This validation method is not used.

3.2.2.3 Authentication for an IP Address

This section defines the permitted processes and procedures for validating the *Applicant*'s ownership or control of an IP Address listed in a *Certificate*.

The *Certification Authority* confirms that prior to issuance, the *Certification Authority* validates each IP Address listed in the *Certificate* using at least one of the methods specified in this section.

The *Certification Authority* maintains a record of which IP validation method, including the relevant BR version number, was used to validate every IP Address.

3.2.2.3.1 Agreed-Upon Change to Website (BR 3.2.2.5.1)

Confirming the *Applicant*'s control over the requested IP Address by confirming the presence of a Random Value contained in the content of a file under the "/.well-known/pki-validation" directory on the IP Address that is accessible by the *Certification Authority* via HTTP/HTTPS over an Authorized Port.

The Random Value shall not appear in the request.

The *Certification Authority* shall provide a Random Value unique to the *Certificate Application* and shall not use the Random Value longer than 30 days.

3.2.2.3.2 Email, Fax, SMS, or Postal Mail to IP Address Contact (BR 3.2.2.5.2)

Confirming the *Applicant*'s control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value shall be sent to an email address, fax/SMS number, or postal mail address identified as an IP Address Contact.

Each email, fax, SMS, or postal mail MAY confirm control of multiple IP Addresses.

The *Certification Authority* may send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the IP Address Registration Authority as representing the IP Address Contact for every IP Address being verified using the email, fax, SMS, or postal mail.

The Random Value shall be unique in each email, fax, SMS, or postal mail.

The *Certification Authority* may resend the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

3.2.2.3.3 Reverse Address Lookup (BR 3.2.2.5.3)

Confirming the *Applicant*'s control over the IP Address by obtaining a Domain Name associated with the IP Address through a reverse-IP lookup on the IP Address and then verifying control over the FQDN using a method permitted under section 3.2.2.2. of this document.

3.2.2.3.4 Any Other Method (BR 3.2.2.5.4)

This validation method is not used.

3.2.2.3.5 Phone Contact with IP Address Contact (BR 3.2.2.5.5)

Confirming the *Applicant*'s control over the IP Address by calling the IP Address Contact's phone number and obtaining a response confirming the *Applicant*'s request for validation of the IP Address. The *Certification Authority* shall place the call to a phone number identified by the IP Address Registration Authority as the IP Address Contact. Each phone call shall be made to a single number.

In the event that someone other than an IP Address Contact is reached, the *Certification Authority* may request to be transferred to the IP Address Contact.

In the event of reaching voicemail, the *Certification Authority* may leave the Random Value and the IP Address(es) being validated. The Random Value shall be returned to the *Certification Authority* to approve the request.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

3.2.2.3.6 ACME "http-01" method for IP Addresses (BR 3.2.2.5.6)

This validation method is not used.

3.2.2.3.7 ACME "tls-alpn-01" method for IP Addresses (BR 3.2.2.5.7)

This validation method is not used.

2.1.3 Authentication of an Individual Identity

The identity of the *Website Authentication Certificate* requester natural person shall be verified.

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

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

   In case of *Certificate*s belonging to the III. certification class:

   - 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; ;
- the natural person's address shall be checked against a residence card suitable for identification;
- 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*.

In case of *Certificate*s belonging to the II. certification class:

- there's no need for personal meeting for the identification of the person, in such cases the *Certification Authority* can identify the *Applicant* remotely;
  During remote identification, the *Certification Authority* may ask the natural person to be identified to take a photograph of herself/himself in accordance with the prescribed conditions and send it to the *Certification Authority*.
- the *Applicant* sends a copy of one of its official identity cards suitable for identity validation to the *Certification Authority*.
- the *Applicant* sends the copy of its official identity cards suitable for the validation of its address to the *Certification Authority*.
- the natural person shall verify the accuracy of the data for the registration and identity validation with a statement signed with a handwritten signature;
- The *Certification Authority* performs data reconciliation with authentic public registers in case of certificates belonging to the II. certification class.
- the natural person's address shall be checked against a residence card suitable for identification;
- The *Registration Authority* verifies the authenticity of the presented cards in this case too. Furthermore the *Certification Authority* verifies that the *Certificate Application* was really sent by the identified *Applicant* through a trustable communication channel. Then the *Certification Authority* asks for confirmation from the *Applicant* through such a contact that was not given during the application procedure, but it originates from other sources. There is no need for confirmation through more reliable communication channel, in case of identification performed by an appropriate electronic

identification device or by a *Certificate Application* submitted with an appropriate electronic signature.

- The *Applicant* can prove its identity at its own discretion according to the III. certification class.

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 format with an electronic signature based on a non-pseudonymous *Certificate* with a security classification not lower than the requested *Certificate*.

- The electronically signed *Certificate Application* shall contain the data needed for the unambiguous identification of the natural person.
- The authenticity and confidentiality of the *Certificate Application* shall be verified 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* uses the data reconciled during a previous natural person identification procedure, if the *Applicant* 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.

2.1.4 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*.

2.1.5 Validation of Authority

The identity of the natural person representing the legal person is verified according to the requirements of Section 2.1.3. 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.

2.1.6 Criteria for Interoperation

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

2.1.7 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.

2.2 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*.

3 The Requirements for Certificates

3.1 Key Pair and Certificate Usage

3.1.1 Subscriber Private Key and Certificate Usage

The private key belonging to the *Certificate* shall only be used for website authentication, and any other usage is prohibited.

A private key corresponding to an expired or revoked *Certificate* can not be used.

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.

3.1.2 Relying Party Public Key and Certificate Usage

To retain the level of security guaranteed by the *Certification Authority*, in the course of performing the webserver authentication, 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*;
- the public keys belonging to the *Website Authentication Certificate*s shall only be used for website authentication;
- the verifications related to the *Certificate* should be carried out for the entire certificate chain up to a trusted root or intermediate provider certificate;
- it is recommended to verify that the *Certificate* was issued according to the appropriate Certificate Policy;
- 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.

3.2 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 *Website Authentication Certificate* shall not be suspended.

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

Responsibility regulations related to 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.

3.2.1 Who Can Request Revocation

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

- the *Subscriber*;
- the *Applicant*;
- 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

- 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`

and in section 1.5.2 of the present *Disclosure Statement*.

3.2.2 Procedure for Revocation Request

The *Certification Authority* ensures the following possibilities for the *Client*s 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.

- by sending a fixed-format SMS text message 24 hours a day.

  The *Client*s of the *Certification Authority* may indicate in an SMS text message sent to the *Certification Authority*'s revocation phone number if a private key is possessed by an unauthorized person.

  The *Certification Authority* immediately begins the processing of the revocation requests arriving in text messages. The *Certification Authority*'s system sends an automatically generated reply message to the phone number of the requester about the result of processing and the success of the revocation.

  In the request sent in the text message the following data shall be provided separated by a space character:

  – date of birth of the *Subject* in the "YYYY-MM-DD" format, or the last three digits of the OID as indicated in the *Certificate*,
  – the revocation password of the *Certificate*.

  Example of formally correct revocation request:

  – "2.1.134 pacsirta"

  The *Certification Authority* always declines the revocation request arriving in a text message from a hidden phone number regardless of the content of the message.

  In order to ensure the availability of the revocation service, the *Certification Authority* also maintains telephone numbers operated by two different mobile service providers. If sending an SMS to one phone number fails (no confirmation is received within a few minutes), please try sending the message to the other phone number.

  Phone numbers to receive revocation SMS:

"+36 (20) 263-4943"

"+36 (30) 326-2187"

- 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.

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*;
- 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.

3.2.3 End-User Certificates

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

- is maximum 398 days (≙13 months) 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.

The validity period of the *Certificate*s and private keys may be affected by a new algorithmic decree issuance by the National Media and Infocommunications Authority, according to which the used cryptographic algorithm or key parameter is not safe until the end of the usage period planned at the time of the issuance.

When this occurs the *Certification Authority* revokes the affected *Certificate*s.

4 Compliance Audit and Other Assessments

The *Certification Authority* has its operation periodically examined by independent external auditor. During the audit it is examined that the operation of the *Certification Authority* 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 319 401 V2.2.1 (2018-04); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [5]
- ETSI EN 319 411-1 V1.2.2 (2018-04); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [6]

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* 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 section 5.4 of this document and sections 8. and 9.15 of the *Certification Practice Statement*.

5 Other Business and Legal Matters

5.1 Representations and Warranties

5.1.1 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 this *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 of the *Certificate*,
- promptly cease using the *Certificate* and its associated private key.

The *Subscriber* may install the *Certificate* and its associated private key only on servers that are accessible at the subjectAltName(s) listed in the *Certificate*, and to use the *Certificate* solely in compliance with all applicable laws and solely in accordance with the service agreement and the General Terms and Conditions.

Subscriber Rights

- *Subscriber*s have the right to use the services in accordance with this *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 revocation of such *Certificate*s.
- *Subscriber*s have the right to request the revocation of *Certificate*s.
- *Subscriber*s are entitled to appoint *Organizational Administrator*s.

Applicant Responsibility

The *Applicant* is responsible for:

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

***Applicant* obligations**

The *Applicant* shall:

- read carefully this *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 *Applicant* 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 revocation of the *Certificate* and
  - terminate the usage of the *Certificate*;
- if the *Applicant* becomes aware of the fact that the subject's *Certificate* has been revoked, or that the issuing CA has been compromised, he shall immediately terminate the usage of the private key belonging to the *Certificate*;
- use the service solely for the purposes allowed or not proscribed by legal regulations, according to the cited regulations and documents;
- to install the *Website Authentication Certificate* only to that server which is accessible on the domain name or IP address in the *Certificate*;
- 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 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;
- the *Applicant* shall 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 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 the *Certification Authority* revokes the issued *Certificate* in case it 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 *Applicant* and in this case, the *Applicant* is bound to terminate the usage of the *Certificate*;
- acknowledge that the *Certification Authority* has the right to revoke *Certificate*s if the *Subscriber* fails to pay the fees of the services by the deadline;
- in case of requesting an *Organizational Certificate*, acknowledge that the *Certification Authority* will issue the *Certificate* solely in the case of the consent of the *Represented Organization*;
- in case of requesting an *Organizational Certificate*, acknowledge that the *Represented Organization* has the right to request the revocation of the *Certificate*;
- acknowledge that the *Certification Authority* has the right to revoke *Certificate* if the *Subscriber* violates the service agreement or the *Certification Authority* becomes aware that the *Certificate* was used for an illegal activity.

***Applicant* Rights**

- *Applicant*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*, *Applicant*s are entitled to request the the revocation of their *Certificate*s, according to this *Certification Practice Statement*.

5.1.2 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*.

5.2 Limitations of Liability

Conditions of liability of the *Certification Authority*:

- 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 this *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;
- All electronic and / or paper-based information relating to Certificates for at least:
  - 10 years after the validity expiration of 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 liability insurance according to the legal regulations required in order to ensure reliability.

Limitation of Financial Liability

The *Certification Authority* limits the obligation for compensation related to services, the extent of this limitation is 4.000.000,-HUF per damage event.

If the valid claim of several entitled parties related to a damage event exceeds the limitation defined for a damage event, then the compensation of the claims takes place in a relative ratio to the limitation.

5.3 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.

5.4 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] ETSI EN 319 401 V2.2.1 (2018-04); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[6] ETSI EN 319 411-1 V1.2.2 (2018-04); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

[7] IETF RFC 3490: Internationalizing Domain Names in Applications (IDNA), March 2003.

[8] IETF RFC 3966: The tel URI for Telephone Numbers, December 2004.

[9] IETF RFC 6532: Internationalized Email Headers, February 2012.

[10] IETF RFC 6844: DNS Certification Authority Authorization (CAA) Resource Record, January 2013.

[11] e-Szignó Certification Authority - eIDAS conform Certificate for Website Authentication Certificate Policies.