MICROSEC

# e-Szignó Certification Authority

# eIDAS conform
# Certificate for Website Authentication
# Disclosure Statement

**ver. 2.4**

**Date of effect: 30/09/2017**

| | |
|---|---|
| OID | 1.3.6.1.4.1.21528.2.1.1.197.2.4 |
| Version | 2.4 |
| First version date of effect | 01/07/2016 |
| Security classification | PUBLIC |
| Approved by | Gergely Vanczák |
| Date of approval | 31/08/2017 |
| Date of effect | 30/09/2017 |

Microsec Micro Software Engineering & Consulting Private Company Limited by Shares
Hungary, H-1031 Budapest, Záhony u. 7. D

| Version | Description | Effect date | Author(s) |
|---|---|---|---|
| 2.0 | New policies according to the RFC 3647 and the eIDAS requirements. | 01/07/2016 | Csilla Endrődi, Szabóné Sándor Szőke, Dr. Kornél Réti |
| 2.1 | Changes according to the NMHH comments. | 05/09/2016 | Melinda Szomolya, Sándor Szőke, Dr. |
| 2.2 | Changes according to the auditor comments. | 30/10/2016 | Sándor Szőke, Dr. |
| 2.3 | Changes according to the NMHH comments. | 30/04/2017 | Sándor Szőke, Dr. |
| 2.4 | Yearly revision. | 30/09/2017 | Sándor Szőke, Dr. |

# Table of Contents

**1 Introduction** **6**
1.1 Document Name and Identification . . . . . 6
1.1.1 Certificate Policies . . . . . 6
1.2 Geographical Scope . . . . . 7
1.3 The Trust Service Provider . . . . . 8
1.3.1 Data of the Provider . . . . . 8
1.3.2 Contact information of the customer service . . . . . 9
1.4 Certificate Types . . . . . 9
1.5 Certificate Usage . . . . . 10
1.5.1 Appropriate Certificate Uses . . . . . 10
1.5.2 Prohibited Certificate Uses . . . . . 10
1.6 Supervisory body . . . . . 10

**2 Identification and Authentication** **10**
2.1 Initial Identity Validation . . . . . 10
2.1.1 Method to Prove Possession of Private Key . . . . . 10
2.1.2 Authentication of an Organization Identity . . . . . 11
2.1.3 Authentication of an Individual Identity or e Domain . . . . . 13
2.1.4 Non-Verified Subscriber Information . . . . . 15
2.1.5 Validation of Authority . . . . . 15
2.1.6 Criteria for Interoperation . . . . . 16
2.2 Privacy policy . . . . . 16

**3 The Requirements for Certificates** **16**
3.1 Key Pair and Certificate Usage . . . . . 16
3.1.1 Subscriber Private Key and Certificate Usage . . . . . 16
3.1.2 Relying Party Public Key and Certificate Usage . . . . . 17
3.2 Certificate Revocation and Suspension . . . . . 17
3.2.1 Who Can Request Revocation . . . . . 18
3.2.2 Procedure for Revocation Request . . . . . 18
3.2.3 End-User Certificates . . . . . 19

**4 Compliance Audit and Other Assessments** **20**

**5 Other Business and Legal Matters** **21**
5.1 Representations and Warranties . . . . . 21
5.1.1 Subscriber Representations and Warranties . . . . . 21
5.1.2 Relying Party Representations and Warranties . . . . . 23

5.2 Limitations of Liability . . . . . 24
5.3 Dispute Resolution Provisions . . . . . 25
5.4 Governing Law . . . . . 25

**A REFERENCES** **26**

# 1 Introduction

This document is the *Disclosure Statement* concerning the issuance of certificate for website authentication service of e-Szignó Certification 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 Certification Authority |
| Document name | eIDAS conform<br>Certificate for Website Authentication<br>Disclosure Statement |
| Document version | 2.4 |
| Date of effect | 30/09/2017 |

The listing 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* refers to that *Certificate Policy* based on which they were issued.

The *Certification Authority* issues *Certificate*s according to the following *Certificate Policies* based on the present *Disclosure Statement*:

| OID | DENOMINATION | SHORT NAME |
|---|---|---|
| 1.3.6.1.4.1.21528.2.1.1.159.2.4 | belonging to the III. certificate class, for website authentication certificates, prohibiting the use of pseudonyms. | HWxxN |
| 1.3.6.1.4.1.21528.2.1.1.161.2.4 | belonging to the II. certificate class, for website authentication certificates, prohibiting the use of pseudonyms. | KWxxN |
| 1.3.6.1.4.1.21528.2.1.1.162.2.4 | Issued during automatic issuance, controlling website authentication certificate issuance, Certificate Policy prohibiting the use of pseudonyms. | AWxxN |

The detailed requirements of the listed *Certificate Policy*(s) can be found in " e-Szignó Certification Authority – eIDAS conform Non Qualified Certificate for Website Authentication Certificate Policies ver.2.4." [8]

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] |
|---|---|---|---|---|
| HWxxN | (x) | X | X* | X** |
| KWxxN | (x) | X | X* | X** |
| AWxxN | (x) | X | X* | X** |

* if the name of the *Organization* is indicated in the *Certificate*

** if the name of the natural person is indicated in the *Certificate*

## 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: | 1031 Budapest, Záhony street 7. D. building |
| 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/pki-services/certificate-policies-general-terms-and-conditions.html`

The access of the price list:

- `https://e-szigno.hu/hitelesites-szolgaltatas/arlista/`

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 Certification Authority |
| Customer service: | 1031 Budapest, Záhony street 7.,<br>Graphisoft Park, D building |
| 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 |
| E-mail address of the customer service: | `info@e-szigno.hu` |
| Service related information access: | `https://www.e-szigno.hu` |
| Place for registering complaints: | Microsec zrt.<br>1031 Budapest, Záhony str. 7.,<br>Graphisoft Park, D building |
| Relevant Consumer Protection Inspectorate: | Budapest Capital Authority for Consumer Protection<br>1052 Budapest, Városház str. 7.<br>1364 Budapest, Pf. 144. |
| Relevant Arbitration Board: | Arbitration Board of Budapest<br>1016 Budapest, Krisztina krt. 99. III. em. 310.<br>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 Certification 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 Certification 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 *Certificate* requester owns and has it under his control 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 *Certificate* of the *Subject* – typically on *Hardware Security Module* in case of *Certificate Policies* requiring such – , then it does not have to specially verify that the *Subject* owns the private pair of the public key to be verified.

If the *Subject* 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 confirms, that the owner of the private key asked for the *Certificate* indeed.

### 2.1.2 Authentication of an Organization Identity

**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* ;

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 and registered office 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 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];

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

- 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 in authentic databases.

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:

- 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* can 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 the certificate, 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.

**Authentication of domain identity**

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 about the eligibility of the *Subject* to use the domain name or IP address. During the inspection a confirmation shall be obtained from authentic records or from a reliable third party, that the *Subject* is entitled to use the domain name or IP address, or the *Subject* 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 joker "*" character is indicated in the *Certificate* (wildcard certificate), the *Certification Authority* ensures that, the *Applicant* is the legal user of the

[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*.

full domain namespace. The *Certification Authority* does not issue a *Certificate*, in which the joker "*" character stands at the place of the highest domain name that can be registered, that is located directly on the left side of the public domain endings (for example: "*.com", "*.co.uk").

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.

### 2.1.3 Authentication of an Individual Identity or e Domain

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

1. During personal identification.

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

   - the natural person shall appear in person at the *Registration Authority* to perform the personal identification;
   - 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. 85.§ (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. 85.§ (4) [4];
     – in case of identifying natural persons abroad none on the basis of the above documents the *Certification Authority* applies identity verification in accordance with Eüt. 82. (5) [4] only in the case of identifying European citizens. In such case, accepts a personal identity card with a photo issued by the European country of nationality accepted as a trusted document for identity verification.
   - the natural person shall verify the accuracy of the data for the registration and identity verification with a statement signed with a handwritten signature;
   - the natural person's address shall be checked against a residence card suitable for identification;
   - the *Certification Authority* verifies, whether any alteration or counterfeiting happened to the presented identity cards.

   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;
   - the *Applicant* sends a copy of one of its official identity cards suitable for identity verification to the *Certification Authority*.
   - The *Certification Authority* performs data reconciliation with public registers in case of certificates belonging to the II. certification class.

- 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.

When the *Certification Authority* verifies the identity of foreign citizens it performs data reconciliation with the proper records of the country, if such records are available. Additional steps are necessary for verifying the foreign document with appropriate confidence, as well as to access the foreign register. In respect of data verification, the *Certification Authority* accepts:

- certificate issued by the embassy or consulate of the foreign country in Hungary, that the organization exists and the given information are correct;
- certificate issued by a Hungarian embassy or consulate in a foreign country, that the organization exists and the provided information is correct.

The *Certification Authority* can 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. Remotely using an electronic identification device, with respect to that the physical presence of a natural person or a representative entitled to represent the legal person before issuing qualified certificates has been guaranteed, and which complies with the substantial or high security levels defined in Article 8 of eIDAS regulation [1].

   The *Certification Authority* will introduce this identity verification solution after starting the central identification service in Hungary and getting the process approved by the auditor.

   In these cases:

   - In addition, during identification besides subject's name an identification number or other data accepted on a national level that enables that natural persons can be distinguishable from others of the same name shall be supplied.

3. By identification traced back to an electronic signature certificate. 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 definit identification of the natural person.
- The authenticity and confidentiality of the *Certificate Application* shall be verified on the whole certification chain.
- The *Certification Authority* may accept only those electronic signatures, which are based on a *Certificate* issued by a Trust Service Provider which is listed on the Trusted List of one of the EU member states and was valid at the time of the signature creation.

4. By using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.

   The *Certification Authority* will introduce this remote identity verification solution after getting the process approved by the auditor.

   In this case the *Certification Authority* processes the identity verification the same way as in case of the personal identification. The only difference is that the face to face identification is replaced by a remote validation process which ensures that

   - the identity of the natural person can be securely verified;
   - the identity of the natural person and the official proof of identity card used for the verification can be connected with high relaibility by using biometrical identification data;
   - the natural person can be connected to the received *Certificate Application*.

The *Certification Authority* uses the data reconciled during a previous 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 accuracy of the data to be in the *Certificate* and the identity of the person submitting the application shall also be checked.

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 was verified by the *Certification Authority* or on the authenticity of which the *Applicant* made a statement with recognition of their criminal liability.

### 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 *Organization* administrator appointed by an authorized person to represent the *Organization*,

An organization administrator is a person who is eligible to act during the application and revocation of the *Certificate*s issued to the *Organization* .

The organization 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 (manually or qualified electronically) signed by the representative of the *Organization*, which is verified by the registration associate of the *Certification Authority* when received. Appointing an organization administrator is not mandatory, and multiple organization administrators can be appointed too. If there is no appointed organization 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.

### 2.2 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/letoltesek/dokumentumok-es-szabalyzatok/` ), 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;
- 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:

- Before the arriving of the revocation request to the *Certification Authority*, the *Applicant*, and the *Subscriber* is responsible for the damages arising.
- After that moment when, the *Certification Authority* accepts the revocation notification, the *Certification Authority* is responsible for the damages arising. The *Certification Authority* forthwith publishes the changed revocation state of the *Certificate* after accepting the request.
- If the *Certification Authority* has already published the invalid revocation state 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 initiated by:

- the *Subscriber*;
- the *Applicant*;
- in case of *Organizational Certificate*, the *Organization*'s authorized representative;
- the contact person specified in the service agreement;
- the *Certification Authority*.

### 3.2.2 Procedure for Revocation Request

The *Certification Authority* ensures the following possibilities to submit a revocation request:

- on paper signed manually at the customer service of the *Certification Authority* during office hours in person;
- 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 (see section **??**.);
- signed manually, sent by post to the customer service.
- through the website of the *Certification Authority* 24 hours a day. The IT system of the *Certification Authority* shall process immediately the applications submitted through its website, the site shall inform the application submitter about the results of the evaluation.
- through a telephone hotline of the *Certification Authority* 24 hours a day until 2018-01-31. The administrator of the *Certification Authority* shall review the applications received on the *Certification Authority* hotline telephone within the duration of the call, and he shall notify the applicant about his decision.
- by sending a fixed-format SMS text message from 2018-01-01.

  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.

  The below data must be provided in the request sent in the text message:

  – the last three digits of the *Subject*'s 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.

The *Certification Authority* verifies the authenticity of the request, and the submitter's eligibility during the evaluation of the request.

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

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

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* asks for 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.

The revocation request contains the data to identify the *Certificate*.

The requester has to provide particularly the following information:

- the exact denomination of the *Subject*;
- the *Certificate*'s unique identifier;
- identification data of the *Client*.

In case of a successful revocation the *Certification Authority* notifies the *Subject* and the *Subscriber* about the fact by e-mail.

### 3.2.3 End-User Certificates

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

- at most 3 years from issuance;
- shall not exceed the amount of time to which the used cryptographic algorithms are safely usable according to the algorithmic decree of the National Media and Infocommunications Authority;
- shall not exceed the validity period of the *Certificate* issuer provider *Certificate* validity period.

Within the framework of certificate renewal a new *Certificate* may be issued for the end-user 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 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [5]
- ETSI EN 319 411-1 V1.1.1 (2016-02); 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* uses the following cryptographic modules for the certification of the *Certificate*s, and for the provider private key storage:

- nCipher nShield F3 PCI nC4032P-150, firmware verzió: 2.18.15-3;
- nCipher nShield F3 PCI nC4032P-150, firmware verzió: 2.22.6-3;
- nCipher nShield F3 PCI nC4033P-500, firmware verzió: 2.33.60-3;
- nCipher nShield F3 PCI nC4033P-500, firmware verzió: 2.38.7-3;
- nCipher nShield F3 PCIe nC4433E-500, firmware verzió: 2.61.2-3.

The above devices have FIPS 140-2 [7] Level 3 certification.

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 and the standard policy conditions and other documents forming an integral part with it, as well as the relevant *Certificate Policy*s.

#### *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 certificates, in writing, and *Subscriber*s have the right to request the suspension and revocation of such certificates.
- *Subscriber*s have the right to request the revocation of certificates.
- *Subscriber*s are entitled to appoint an organisational administrator.

#### *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 suspension or revocation of the *Certificate* and
  - terminate the usage of 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 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 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 suspend, and 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*;
- for the issuance of a *Website Authentication Certificate* the *Applicant* is bound to hand over the declaration of consent of the given domain owner to the *Certification Authority*;
- acknowledge that the *Certification Authority* has the right to suspend, and 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 suspension or 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 the *Certificate* revocation status 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 *Certificate Policy* and the *Certification Practice Statement*.

## 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:

- *Certification Practice Statement*: 10 years after the repeal;
- All electronic and / or paper-based information relating to Certificates for at least:
  - 10 years after the validity expiration of the Certificate;

### 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 100 000 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 V2.2.0 (2017-08); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[6] ETSI EN 319 411-1 V1.2.0 (2017-08); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

[7] FIPS PUB 140-2 (2001 May 25): Security Requirements for Cryptographic Modules.

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