e-Szignó Certification Authority

eIDAS conform
Qualified Time Stamping
Disclosure Statement

ver. 2.2

Date of effect: 30/10/2016

OID	1.3.6.1.4.1.21528.2.1.1.99.2.2
Version	2.2
First version date of effect	01/07/2016
Security classification	PUBLIC
Approved by	Gergely Vanczák
Date of approval	30/09/2016
Date of effect	30/10/2016

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 document according to the eIDAS requirements.	01/07/2016	Sándor Szőke, Dr.
2.1	Changes according to the NMHH comments. OID: 1.3.6.1.4.1.21528.2.1.1.69.2.1	05/09/2016	Melinda Szomolya, Sándor Szőke, Dr.
2.2	Changes according to the auditor comments.	30/10/2016	Sándor Szőke, Dr.

Table of Contents

1 Introduction

This document contains the *Disclosure statement* defined by e-Szignó Certification Authority (hereinafter: *Time-Stamping Provider*) operated by Microsec ltd.

The *Disclosure statement* complies with the requirements set by the eIDAS regulation [1], the service provided according to these regulations is an EU qualified trusted service.

The prerequisites for the qualified trusted service provision and the "EU Trust Mark" indication are:

- the service shall be audited by an independent assessment organization authorized to carry out such an assessment, and it shall issue a conformity assessment certificate for the *Time-Stamping Provider*;
- the *Time-Stamping Provider* shall submit the conformity assessment certificate to the National Media and Infocommunications Authority, as it is the official monitoring body;
- the National Media and Infocommunications Authority shall accept the submitted conformity assessment certificate and it shall publish the service in the national trusted list.

1.1 Compliance

The *Time Stamp*s issued according to the present *Disclosure statement* are compliant with the requirements below:

- ETSI EN 319 421 [4]
  BTSP: a best practices policy for time-stamp
  OID: itu-t(0) identified-organization(4) etsi(0)time-stamp-policy(2023)policy-identifiers(1) best-practices-ts-policy (1)

The *Time-Stamping Provider* includes its own OID in the *Time Stamp*s it issues, and it supports the aforementioned ETSI time-stamping policy (i.e. BSTP).

1.2 The Trust Service Provider

1.2.1 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 *Qualified Time-Stamping Policy*, the *Qualified Time-Stamping 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 *Time-Stamping Provider* does not issue refunds on fees that have already been paid, unless the service agreement expires due to the *Time-Stamping Provider*'s fault, or if the *Time-Stamping Provider* 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 access of the service agreement:

The *Time-Stamping Provider* sends the service agreement to be concluded with the *Client*ss to the notification e-mail address of the *Subject* given during initial registration.

1.2.2 Contact information of the customer service

The name of the provider unit:	e-Szignó Certification Authority
Customer service:	1031 Budapest, Záhony street 7., 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. 1031 Budapest, Záhony str. 7., Graphisoft Park, D building
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.

1.3 Time-Stamp Usage

The *Time Stamp* credibly certifies that, the electronic document with the *Time Stamp* already existed in the given state before the time indicated in the *Time Stamp*.

1.4 Policy Administration

1.4.1 Person or Organization Responsible for the Suitability of the Practice Statement for the *Qualified Time-Stamping Policy*

The provider that issued the *Qualified Time-Stamping Practice Statement* is responsible for its conformity with the *Qualified Time-Stamping Policy* referenced in it and for the provision of the service according to the regulations contained therein.

The *Qualified Time-Stamping 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 *Time-Stamping Provider*s applying these policies.

2 The Certificate of the Time-Stamping Unit and Time-Stamping

2.1 The Time-Stamp

The *Time Stamp* issued by the the *Time-Stamping Provider* complies with the IETF RFC 3161 [7] and the ETSI EN 319 422 [5] standards;

Accordingly the characteristics of the *Time Stamp* are:

- it includes the hash sent in the message of the requester.
- it includes the OID of the *Time-Stamping Policy*.
- it has a unique identifier.

2.1.1 The Time-Stamp Request

The *Time-Stamping Provider* supports the *Time Stamp* requests according to the IETF RFC 3161 [7] section 2.4.1. including the usage of the following fields:

- "reqPolicy"
- "nonce"
- "certReq"

The *Time-Stamping Provider* does not support the usage of the field below:

- "extensions"

The *Time-Stamping Provider* accepts the hashing algorithms in the *Time Stamp* requests specified by ETSI TS 119 312 [6] and the current National Media and Infocommunications Authority algorithmic decree. It takes into account when selecting the hashing algorithms the planned usage time of the *Time Stamp* and the expected duration of the hashing method adequacy.

The currently supported hashing algorithms are:

sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha256(1) }
sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha512(3) }

2.1.2 Time-Stamp Response

The *Time-Stamping Provider* supports the *Time Stamp* responses according to IETF RFC 3161 [7] section 2.4.2 with the following extensions:

- "accuracy";
- "nonce".

In case of the inclusion of the "nonce" in the *Time Stamp* request, the *Time Stamp* response includes the same value.

The *Time-Stamping Provider* uses the cryptographic algorithm sets and key lengths for signing the *Time Stamp*s specified by ETSI TS 119 312 [6] and appointed in the current National Media and Infocommunications Authority algorithmic decree. It takes into account the planned usage time of the *Time Stamp* when selecting the cryptographic algorithm sets and key lengths.

The supported cryptographic algorithm set:

sha256WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1)sha256WithRSAEncryption(11) }
sha512WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1)sha512WithRSAEncryption(13) }

The identifier of the supported ETSI Time-Stamping profile (BTSP):
itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) baseline-ts-policy (1).

2.2 Time-Stamp Accuracy

The *Time-Stamping Provider* guarantees that the deviation of the time indicated in the *Time Stamp*s from the UTC time is at most 1 second.

The *Time-Stamping Unit* clock provider systems are in the strictly protected *Data Centre* of the the *Time-Stamping Provider*, which makes the unnoticed modification of the clock impossible.

The *Time-Stamping Provider* constantly monitors its internal time provider systems. If the internal time deviation from the UTC time exceeds 0.1 second, the the *Time-Stamping Provider* suspends the issuance of *Time Stamp*s.

The accuracy of the internal clock of the *Time-Stamping Provider* is examined every year by the security committee of the *Time-Stamping Provider*.

2.3 Time-Stamp Validation

During the verification of the validity of the electronic signature or electronic seal on the *Time Stamp* the *Relying Party* should act as described in the ETSI EN 319 102-1 [3] specification.

During the verification of the *Time Stamp*:

- it shall be verified that the time-stamped document belongs together with the *Time Stamp* and the *Certificate* of the the *Time-Stamping Provider*;
- the signature on the *Time Stamp* shall be verified;
- it shall be verified that the *Time Stamp* meets the specific purpose, among other things that the accuracy, the reliability and the liability of the related Time-Stamping Service Provider is appropriate.

3 Certificate Life-Cycle Operational Requirements

3.1 Key Pair and Certificate Usage

3.1.1 Relying Party Public Key and Certificate Usage

To retain the level of security guaranteed by the *Time-Stamping Provider*, in the course of using the 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 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*.

4 Facility, Management, and Operational Controls

The *Time-Stamping Provider* applies physical, procedural, and personnel security precautions that comply with acknowledged standards, along with the administrative and governance related procedures that enforce these.

The *Time-Stamping Provider* keeps a record of the system units and resources related to the service provision, and conducts a risk assessment on these. It uses protective measures proportional to the risks related to the individual elements.

The *Time-Stamping Provider* monitors the capacity demands and ensures that the adequate processing power and storage are available for the provision of the service.

4.1 Audit Logging Procedures

In order to maintain a secure IT environment the *Time-Stamping Provider* implements and operates an event logger and control system covering its full IT system.

4.1.1 Types of Events Recorded

The *Time-Stamping Provider* logs every security-related event that can provide information on events, changes happened in the IT system or in its physical environment according to the generally accepted information security practice. In case of every log entry, it stores the following data:

- the time of the event;
- the type of the event;
- the success or failure of the implementation;
- the identification of the user or the system who/what triggered the event.

All of the essential event logs are available to the independent system auditors, who examine the compliance of the *Time-Stamping Provider*'s operation.

4.2 Records Archival

4.2.1 Retention Period for Archive

The *Time-Stamping Provider* preserves the archived data for the time periods below:

- *Qualified Time-Stamping Practice Statement*: 10 years after the repeal;
- main data related to the issuance of the *Time Stamp* for at least 10 years after the issuance.

5 Compliance Audit and Other Assessments

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 *Time-Stamping Provider*.

The *Time-Stamping Provider* applies verified and certified elements (electronic signature production IT system elements) in connection with the service.

The *Time-Stamping Provider* uses the following cryptographic modules for the certification of the *Time Stamp*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 [8] Level 3 certification.

The *Time-Stamping Provider* 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 *Time-Stamping Provider* 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 *Time-Stamping Provider* also has its proprietary internal auditing system, which regularly examines compliance with previous audits, and takes the necessary steps in case of deviations.

The *Time-Stamping Provider* 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.

6 Other Business and Legal Matters

6.1 Financial Responsibility

6.1.1 Insurance or Warranty Coverage for End-entities

- The *Time-Stamping Provider* has liability insurance to ensure reliability.
- The liability insurance policy shall cover the following damages caused by the *Time-Stamping Provider* in connection with the provision of services:
  - damages caused by the breach of the service agreement to the trust service *Client*s;

  - damages caused out of contract to the trust service *Client*s or third parties;
  - damages caused to the National Media and Infocommunications Authority by the *Time-Stamping Provider* terminating the provision of the trust service;
  - under the eIDAS Regulation [1] 17. article (4) e) point, the legal costs of conformity assessment bodies to perform a conformity assessment by the request of the National Media and Infocommunications Authority if it enforces the costs as legal costs.

- The liability insurance policy shall cover at least for 3 000 000 Hungarian forints. Coincidental damages occurred for the same reason constitute a single insurance event.
- The liability insurance shall provide coverage for the full damage of the injured party – up to the liability limit – arising in context of the harmful behaviour of the *Time-Stamping Provider* regardless of whether the damage was caused by breach of contract or outside the contract.
- If the valid claim of several entitled parties related to an insurance event exceeds the liability limit defined for an insurance event in the liability insurance, then the compensation of the claims takes place in the proportion of the liability limit to the total sum of the claims.

6.2 Privacy of Personal Information

6.2.1 Privacy Plan

The *Time-Stamping Provider* has a Privacy Policy for data processing that contains detailed requirements for the personal data management. The Privacy Policy for data processing is published on the webpage of the e-Szignó Certification Authority on the following URL: `https://e-szigno.hu/letoltesek/dokumentumok-es-szabalyzatok/`

6.3 Representations and Warranties

6.3.1 CA Representations and Warranties

Certification Authority's Responsibility

The responsibility of the *Time-Stamping Provider* is in the *Qualified Time-Stamping Practice Statement*, the related *Certificate Policies*, and the service agreement with the *Client* and its attachments.

- The *Time-Stamping Provider* assumes responsibility for compliance with the procedures described in *Certificate Policies* it supports;
- The *Time-Stamping Provider* assumes responsibility as its own for the damages caused during the provision of the service by its subcontractors;

- The *Time-Stamping Provider* is liable under the rules of liability for breach of contract in the Civil Code of the Republic of Hungary [2] in relation to the *Client*s which are in a contractual relationship with it.
- The *Time-Stamping Provider* is liable under the rules of causing damage outside of contract in the Civil Code of the Republic of Hungary [2] in relation to third parties (such as the *Relying Party*) that are not in a contractual relationship with it.
- The *Time-Stamping Provider* will pay compensation for damages with the limitations specified in its regulations, and the service contracts concluded with Clients for proven damages that occur in the scope of its responsibility (see the section Limitation of Liability 6.4.).
- If the valid claim of several entitled parties related to an insurance event exceeds the amount defined for an insurance event in the liability insurance for the damages, then the compensation of the claims takes place in a relative ratio to the amount determined in the liability contract.

The *Time-Stamping Provider* is not responsible for the regulations issued by the *Relying Parties* or others.

Certification Authority Obligations

The *Time-Stamping Provider*'s basic obligations is that it shall provide the services in line with the *Qualified Time-Stamping Policy*, this *Qualified Time-Stamping Practice Statement* and other regulations in the public domain, the contractual terms and conditions, furthermore corporate and security related internal regulations. These basic obligations are as follows:

- to establish the legal, regulatory, material, contractual, etc. framework appropriate for the service;
- to provide high standard and secure services in accordance with the applicable regulations;
- to continuously operate and audit organisations associated with the services (certification body, customer service, etc.);
- to abide by the procedures prescribed in the regulations, and to avoid or eliminate any potentially occurring incorrect operation;
- to ensure the Services to every applicant who accepts the terms and conditions specified in the regulations;
- to maintain public and proprietary records, as well as to make them continuously available to anybody over the internet.

6.3.2 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 *Time-Stamping Provider* while using the service .

The obligations of the *Subscriber* are determined by this *Qualified Time-Stamping Practice Statement*, the service agreement and the standard policy conditions and other documents forming an integral part with it, as well as the relevant *Qualified Time-Stamping Policy*s.

Subscriber Rights

- *Subscriber*s have the right to use the services in accordance with this *Qualified Time-Stamping Practice Statement*.

6.3.3 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 *Time Stamp*s. During the verification of the validity for keeping the security level guaranteed by the *Time-Stamping Provider* 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 *Qualified Time-Stamping Policy* and the corresponding *Qualified Time-Stamping Practice Statement*;
- use reliable IT environment and applications;
- verify the the revocation status of the *Certificate* used for signing the *Time Stamp* based on the current CRL or OCSP response;
- take into consideration every restriction in relation to the *Time Stamp* usage which is included in the *Qualified Time-Stamping Policy* and the *Qualified Time-Stamping Practice Statement*.

6.4 Limitations of Liability

The *Time-Stamping Provider* limits the obligation for the loss related to the service, the extent of this limitation is 100 000 HUF per incident.

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

6.5 Dispute Resolution Provisions

The *Time-Stamping Provider* aims for the peaceful and negotiated settlement of the disputes arising from its operation. The settlement follows the principle of gradual approach.

The *Time-Stamping Provider* 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 *Time-Stamping Provider* shall be addressed to the customer care centre office in written form. The *Time-Stamping Provider* 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 *Time-Stamping Provider* is obliged to issue a written response to the submitter within the specified time limit. The *Time-Stamping Provider* may request the provision of information required for giving a response from the submitter. The *Time-Stamping Provider* 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 *Time-Stamping Provider* involved, the submitter may initiate consultation with the *Time-Stamping Provider* 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 *Time-Stamping Provider*'s response, as well as any documents containing other required information shall be sent to them in writing.

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

6.6 Governing Law

The *Time-Stamping Provider* at all times operates in accordance with the Hungarian legislation in force. The Hungarian law is the proper law of the *Time-Stamping Provider* 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 V of 2013. on the Civil Code .

[3] ETSI EN 319 102-1 V1.1.1 (2016-05); Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation.

[4] ETSI EN 319 421 V1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. (Replaces ETSI TS 102 023).

[5] ETSI EN 319 422 V1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles (Replaces ETSI TS 101 861).

[6] ETSI TS 119 312 V1.1.1 (2014-11); Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

[7] IETF RFC 3161: Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP), August 2001.

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