MICROSEC

# e-Szignó Certificate Authority

# eIDAS conform Remote Key Management Service suitable for Creating Qualified Electronic Signatures/Seals Practice Statement

ver. 2.17

Date of effect: 28/10/2020

| | |
|---|---|
| OID | 1.3.6.1.4.1.21528.2.1.1.204.2.17 |
| Version | 2.17 |
| First version date of effect | 26/05/2020 |
| 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 |
|---|---|---|
| 2.14 | 26/05/2020 | New document according to the eIDAS requirements. |
| 2.17 | 28/10/2020 | Improvements according to the auditor's and the supervisory body's findings. \| Smaller improvements. |

# Table of Contents

# 1 Introduction

This document is the *Remote Key Management Practice Statement* concerning the remote key management service of e-Szignó Certificate Authority operated by Microsec ltd. (hereinafter: Microsec or *Remote Key Management Service Provider*).

The *Remote Key Management Service Provider* provides its services for its *Client*s with whom it has contractual relationship.

The present *Remote Key Management Practice Statement* describes the framework of the provision of the aforementioned services and includes the detailed procedures and miscellaneous operating rules.

The *Remote Key Management Practice Statement* complies with the requirements set by the eIDAS Regulation [1], the Remote Key Management Service provided according to these regulations is an EU Trust Service. The Remote Key Management Service is provided as an independent service component by Microsec as a Qualified Trust Service Provider. The Remote Key Management Service component is connected to other services of the *Remote Key Management Service Provider* which are needed for the *Client*:

- the *Client* need to have a *Certificate* containing the public key pair of the private key which is managed in the Remote Key Management Service
- the *Client* need to have a mobile device which is suitable to run the PassByME mobile authentication application provided by Microsec.

Within the framework of the Remote Key Management Service, the *Remote Key Management Service Provider* manages the private keys of the *Client*s under sufficiently secure conditions, which are under the sole control of the *Client*s during the whole life cycle.

The *Remote Key Management Service Provider* ensures the necessary technical and procedural conditions in order that the *Client*s could carry out remote key operations with their private keys stored at the *Remote Key Management Service Provider*.

By using the Remote Key Management Service, *Client*s may also create qualified electronic signatures or seals.

## 1.1 Overview

The aim of the present *Remote Key Management Practice Statement* is to summarize all the information that the *Client*s coming into contact with the *Remote Key Management Service Provider* should know. This aims to foster that its *Client*s and future *Client*s:

- get better acquainted with the details and requirements of the services provided by the *Remote Key Management Service Provider*, and the practical background of the service provision;
- be able to see through the operation of the *Remote Key Management Service Provider*, and thus more easily decide whether the services comply or which type of services meet their individual needs and expectations.

The content and format of the present *Remote Key Management Practice Statement* is based on the requirements of the IETF RFC 3647 [16] framework but does not fully conformant to it. There are sections in IETF RFC 3647 which are meaningful only in a Certification Service but not relevant in case of the Remote Key Management Service. These chapters are totally missing from the present *Remote Key Management Practice Statement*, so the numbering of the existing chapters do not follow the numbering of the IETF RFC 3647. On the other hand some new chapters are added to this *Remote Key Management Practice Statement*, which are specific to the Remote Key Management Service.

Considering the end user activity related to the services used, besides the present *Remote Key Management Practice Statement* further requirements may be found in the General Terms and Conditions and the service agreement concluded with the provider, and other regulation or document independent from the *Remote Key Management Service Provider* as well.

Section 1.5 of this document specifies several terms which are not or not fully used in this sense in other areas. The terms to be used in this sense are indicated by capitalization and italicization throughout this document.

## 1.2 Document Name and Identification

| | |
|---|---|
| Issuer | e-Szignó Certificate Authority |
| Document name | eIDAS conform<br>Remote Key Management Service<br>suitable for Creating Qualified Electronic Signatures/Seals<br>Practice Statement |
| Document version | 2.17 |
| Date of effect | 28/10/2020 |

### 1.2.1 Service policy

This *Remote Key Management Practice Statement* undertakes to comply with the following ETSI TS 119 431-1 [14] trust service policy:

- EU SSASC Policy (EUSCP OID: 0.4.0.19431.1.1.3).

### 1.2.2 Effect

#### Subject Scope

The *Remote Key Management Practice Statement* is related to the provision and usage of the services described in section 1.3.1.

### Temporal Scope

The present version of the *Remote Key Management Practice Statement* is effective from the 28/10/2020 date of effect, until withdrawal. The effect automatically terminates at the cessation of the services or at the issuance of the newer version of the *Remote Key Management Practice Statement*.

### Personal Scope

The effect of the *Remote Key Management Practice Statement* extends each of the participants mentioned in section 1.3.

The *Remote Key Management Service Provider* provides trust services primarily to citizens of the European Union and organizations registered in the European Union, but does not exclude natural or legal persons from other countries as long as they accept the system of rules followed by the *Remote Key Management Service Provider* and the controls necessary to provide the services can be done safely and economically.

### People with disabilities

The *Remote Key Management Service Provider* strives to ensure equal opportunity access to the services provided by the company to the highest possible standards.

In order to establish equal opportunities regarding the service, the *Remote Key Management Service Provider* applies every possible and reasonable measure to make its services available without obstructions to disabled people as well. It is especially important them to ensure that the disabled clients receive services, which are adapted to their special needs, of the same quality as those for the other clients.

The *Remote Key Management Service Provider* cooperates with clients in order to guarantee them an administrative process which is the most suitable for their personal needs within the framework determined by the *Remote Key Management Practice Statement*.

### Geographical Scope

The Remote Key Management Service provided according to the present *Remote Key Management Practice Statement* is available worldwide.

It can be used anywhere where proper internet access is available.

The validity of the electronic signatures and seals created according to the present *Remote Key Management Practice Statement* is independent of the geographical location where the private keys were activated from.

Information on the legal effect of electronic signatures and electronic seals created using the Remote Key Management Service can be found in the relevant Certification Practice Statement of the Certification Service Provider issuing the *Certificate* belonging to the private key.

The Remote Key Management Service provided according to the present *Remote Key Management Practice Statement* can be only used as described in the present document.

## 1.3 PKI Participants

### 1.3.1 Certification Authorities

**Data of the *Remote Key Management Service Provider***

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

**Customer Service Office**

| | |
|---|---|
| The name of the provider unit: | e-Szignó Certificate Authority |
| Customer service: | |
| | Hungary, H-1033 Budapest,<br>Ángel Sanz Briz str. 13.,<br>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.<br>Hungary, H-1033 Budapest,<br>Ángel Sanz Briz str. 13.,<br>Graphisoft Park South Area, Building C |
| 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. |

**Introduction of the *Remote Key Management Service Provider***

Microsec ltd. is an EU qualified trust service provider according to the 910/2014/EU Regulation [1] (hereinafter: eIDAS).

Microsec ltd. (its predecessor) started the provision of its services related to electronic signatures under the effect of Act XXXV. of 2001. [4] (hereinafter: Eat.):

- provides non-qualified electronic signature certification services, time stamping, and placement of signature-creation data on signature creation devices services according to Eat. since May 30, 2002 (registration number: MH 6834 1/2002.);
- provides qualified electronic signature certification services, time stamping, and device services according to Eat. since May 15, 2005;
- provides qualified long term preservation service according to Eat. since February 1, 2007. (reference number of the decision on the registration: HL-3549-2/2007).

On the 1st of July, 2016. the whole system of services related to electronic signatures changed uniformly on a European basis with eIDAS and its complement Act CCXXII of 2015. [7] coming into force.

Microsec provides its non-qualified trust services conformant to eIDAS furthermore started the issuance of eIDAS qualified signing certificates for natural persons from the 1st of July 2016.

Microsec provides the following qualified trust services conformant to eIDAS form the 20th of December 2016:

- qualified certificates for electronic seals
- qualified time stamping
- qualified archiving (preservation of electronic signatures and seals).

Microsec provides the following qualified trust servic conformant to eIDAS form the 2nd of January 2019:

- qualified certificates for website authentication.

**Quality and Information Security**

Microsec highlights the importance of *Client* experience. In order to maintain a high level of services, the *Remote Key Management Service Provider* has been operating a quality control system compliant with the ISO 9001 standard since January 23, 2002. Compliance with the standard has been verified by Lloyd's Register Quality Assurance.

Microsec assigns high priority to the security of the systems it operates, and has therefore been operating an information security management system that is compliant with ISO/IEC 27001 (formerly known as BS 7799) in its main areas of activity since May 19, 2003. Compliance with the standard has been verified by Lloyd's Register Quality Assurance.

The scope of both the quality control system and the information security management system cover the trust services provided by Microsec.

Microsec has two level risk assessment which covers beyond the information technology risks the whole organization including also the business risks. The risk assessment is updated at least yearly. Based on the results of the risk assessment the *Remote Key Management Service Provider*

- sets up new measures to eliminate the vulnerabilities, or/and
- accepts the identified residual risks by stating the reason of the decision.

The *Remote Key Management Service Provider* makes available for all interested parties its Information Security Policy on its web page on the following link:

`https://www.microsec.hu/en/quality-assurance-and-audit`

Any change to the Information Security Policy is communicated to third parties through this web page.

Changes to the information security policy is communicated to third parties, where applicable. This includes subscribers, relying parties, assessment bodies, supervisory or other regulatory bodies.

Due to their confidential nature the *Remote Key Management Service Provider* dosen't disclose its internal Security Rules. The *Remote Key Management Service Provider* informs its subcontractors, contractors and other interested parties concerned of the security rules applicable to them when concluding the contract.

**Business Providing Certification Services**

Operating as an independent business unit within the organization of Microsec, e-Szignó Certificate Authority is responsible for all of the duties regarding the trust services.

**Services**

The *Remote Key Management Service Provider* provides the following trust services defined by the eIDAS Regulation [1] to the *Subscriber* within the framework of the present *Remote Key Management Practice Statement*:

- Remote Key Management Service.

The *Remote Key Management Service Provider* provides its services within the framework of the present *Remote Key Management Practice Statement* as a qualified trust service provider.

### 1.3.2 Subscribers

The *Client*s of the Remote Key Management Services provided by the *Remote Key Management Service Provider*:

- *Subscriber*
  - signs the service agreement with the *Remote Key Management Service Provider*,
  - accepts the General Terms and Conditions,
  - defines the scope of the users,
  - may appoint *Organizational Administrator*s,
  - responsible for the payment of the fees arising from the usage of the service.

- *Signatory*
  - the user of the Remote Key Management Service, who can create electronic signature or electronic seal by using the service.

### 1.3.3 Relying Parties

The *Relying Party* validates and uses the electronic signatures or electronic seals which were created by using the Remote Key Management Service. The *Relying Party* is not in a contractual relationship with the *Remote Key Management Service Provider*. The *Relying Party* typically doesn't know that the electronic signature or electronic seal was created by using the Remote Key Management Service.

### 1.3.4 Other Participants

The independent auditor who makes the conformity assessment audit.

The supervisory authority.

## 1.4 Policy Administration

### 1.4.1 Organization Administering the Document

The data of the organization administering the present *Remote Key Management Practice Statement* can be found in the following table:

| | |
|---|---|
| Organization name | Microsec e-Szignó Certificate Authority |
| Organization address | Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13. |
| Telephone number | +36 1 505-4444 |
| Fax number | +36 1 505-4445 |
| Email address | info@e-szigno.hu |

### 1.4.2 Contact Person

Questions related to the present *Remote Key Management Practice Statement* can be directly put to the following person:

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

### 1.4.3 Person or Organization Responsible for the Suitability of the Practice Statement for the *Trust Service Policy*

Person responsible for compliance with the present *Remote Key Management Practice Statement* and the *Trust Service Policy* referenced therein is:

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

### 1.4.4 Practice Statement Approval Procedures

Preparing, modifying, acceptance and issuance of a new version of the *Remote Key Management Practice Statement* is implemeted according to unified processes as described in detail in section 7.12.1.

## 1.5 Definitions and Acronyms

### 1.5.1 Definitions

| | |
|---|---|
| Data Centre | A facility designed for the placement and operation of computer systems and associated components. These components typically include telecommunications systems and communication connections, redundant power supply, data storage, air conditioning, fire protection and security systems. |
| Trust Service Supervisory Body | "The National Media and Infocommunications Authority, the supervising authority monitoring the *Trust Service*s." *(Act CCXXII. of 2015. [7] 91.§ 1. paragraph)* |
| Trust Service | "Means an electronic service normally provided for remuneration which consists of:<br>• the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or<br>• the creation, verification and validation of *Website Authentication Certificate*; or<br>• the preservation of electronic signatures, seals or certificates related to those services;<br>" *(eIDAS [1] 3. article 16. point)* |
| Trust Service Policy | "A set of rules in which a *Trust Service Provider*, relying party or other person requires conditions for the usage of the *Trust Service* for a community of the relying parties and/or a class of applications with common security requirements." *(Act CCXXII. of 2015. [7] 1. § 8. point)* |

| | |
|---|---|
| Trust Service Provider | "A natural or a legal person who provides one or more *Trust Service*s either as a qualified or as a non-qualified *Trust Service Provider*." *(eIDAS [1] 3. article 19. point)* |
| Electronic Document | "Means any content stored in electronic form, in particular text or sound, visual or audiovisual recording" *(eIDAS [1] 3. article 35. point)* |
| Electronic Time Stamp | "Means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time." *(eIDAS [1] 3. article 33. point)* |
| Subscriber | A person or organization signing the service agreement with the *Remote Key Management Service Provider* in order to use some of its services. |
| Relying Party | Recipient of the electronic document, who acts relying on the electronic signature or seal on the electronic document. |
| Suspension | A temporary pause of the *Certificate*'s validity before the end of the validity period indicated on the *Certificate*. The *Certificate* suspension is not definitive; the suspended *Certificate*'s validity can be restored. |
| Root Certificate | Also known as top level certificate. Self-signed *Certificate*, which is issued by a specific *Certification Unit* for itself, which is signed with its own private key, so it can be verified with its own public key – indicated on the certificate. |
| HSM: Hardware Security Module | A hardware-based secure device that generates, stores and protects cryptographic keys and provides a secure environment for the implementation of cryptographic functions. |
| Certification Authority | A *Trust Service Provider*, who/which identifies the requester within the confines of the certification service, issues *Certificate*s, keeps a record, receives the *Certificate* related data changes, and publishes the regulations belonging to the *Certificate* and the information on the current state (especially on possible revocation) of the *Certificate*. |

| | |
|---|---|
| Certification Unit | A unit of the *Remote Key Management Service Provider*'s system that signs the *Certificate*s. Always just one Certificate-Creation Data (signing key, signature-creation data) belongs to a *Certification Unit*. It is possible that a Certification Authority simultaneously operate several *Certification Unit*s. |
| Compromise | A cryptographic key is considered as compromised, when it can be assumed, that unauthorized person has access to it. |
| Intermediate Certification Unit | A *Certification Unit* whose *Certificate* was issued by another *Certification Unit*. |
| Cryptographic Key | A unique digital data string controlling a cryptographic transformation, the knowledge of which is required for encryption, decryption and the creation and verification of electronic signatures and seals. |
| Key Management | The production of cryptographic keys, their delivery to users or its algorithmic implementation, as well as the registration, storage, archival, revocation and termination of keys which are closely linked to the used security method. |
| Private Key | In the public key infrastructure, the element of an asymmetric cryptographic key pair belonging to the key-pair owner that the<br>*Subject* shall keep strictly secret.<br>During the issuance of *Certificate*s, the *Certification Authority* uses the private keys of the *Certification Unit* for placing an electronic signature or seal on the *Certificate* to protect it. |
| Qualified Trust Service | "A *Trust Service* that meets the applicable requirements laid down in the eIDAS Regulation." *(eIDAS [1] article 3. point 17.)* |
| Qualified Trust Service Provider | "A *Trust Service Provider* who provides one or more *Qualified Trust Service*s and is granted the qualified status by the supervisory body." *(eIDAS [1] article 3. point 20. )* |
| Public Key | In the public key infrastructure, the element of an asymmetric cryptographic key pair belonging to key-pair owner, which should be made public. The disclosure is typically in the form of a *Certificate*, which links the name of the actor with its public key.<br>The authenticity of the *Certificate*s can be verified with the public key of the *Certification Unit*. |

| | |
|---|---|
| Public Key Infrastructure, PKI | An infrastructure based on asymmetric cryptography, including the cryptographic algorithms, keys, certificates, the related standards and legislation, the underlying institutional system, a variety of providers and devices. |
| Extraordinary Operational Situation | An extraordinary situation causing disturbance in the course of the operation of the *Remote Key Management Service Provider*, when the continuation of the normal operation of the *Remote Key Management Service Provider* is not possible either temporarily or permanently. |
| Organization | Legal person. |
| Trust Service Practice Statement | "The statement of the *Trust Service Provider* of the detailed procedures or other operational requirements used in connection with the provision of particular *Trust Service*s." *(Act CCXXII. of 2015. [7] 1. § point 41.)* |
| Service Agreement | "The contract between the *Trust Service Provider* and the *Trust Service* client, which includes the conditions for the provision of the *Trust Service* and for using the services." *(Act CCXXII. of 2015. [7] 1. § point 42.)* |
| Certificate | "The electronic signature certificate, the electronic seal certificate and the *Website Authentication Certificate*, and all those electronic verifications issued within the framework of the *Trust Service* by the service provider, which includes the certificate related verification data and the certificate usage related information, and which as an electronic document is reliably protected against the available counterfeiting technologies at the time of the issuance and during its validity period." *(Act CCXXII. of 2015. [7] 1. § point 44.)* |
| Certificate Application | The data and statements given by the *Applicant* to the *Remote Key Management Service Provider* for *Certificate* issuance, in which the *Applicant* reaffirms the authenticity of data to be indicated on the *Certificate*. |
| Certificate Repository | Data repository containing various *Certificate*s.<br>A Certification Authority has a Certificate Repository in which the issued *Certificate*s are disclosed, but the system containing *Certificate*s available to the application on the computer of the *Relying Party* is also called Certificate Repository. |

| | |
|---|---|
| Remote Key Management Service | A Trust Service in which a service provider manages Customers' private keys under secure conditions, ensures the necessary technical and procedural conditions in order that the Customers could carry out remote key operations with their private keys stored at the service provider, such as creating electronic signatures or electronic seals. |
| Remote Key Management Service Policy | A Trust Service Policy that defines the procedural requirements to be followed by the Remote Key Management Service. |
| Client | The *Subscriber* other denomination. |
| Revocation | The termination of the *Certificate*'s validity before the end of the validity period indicated on the *Certificate* too. The *Certificate* revocation is permanent, the revoked *Certificate* cannot be reinstated any more. |
| Revocation Status Records | The internal records of the suspended and revoked *Certificate*s which includes the fact of the suspension or revocation and the time of the suspension or revocation given in seconds maintained by the *Certification Authority*. |

### 1.5.2 Acronyms

| | |
|---|---|
| eIDAS | electronic Identification, Authentication and Signature |
| EUSCP | EU SSASC Policy |
| LDAP | Lightweight Directory Access Protocol |
| LSCP | Ligthweight SSASC Policy |
| NMHH | National Media and Infocommunications Authority |
| NSCP | Normalized SSASC Policy |
| OCSP | Online Certificate Status Protocol |
| OID | Object Identifier |
| PKI | Public Key Infrastructure |
| SAD | Signature Activation Data |
| SAM | Signature Activation Module |
| SAP | Signature Activation Protocol |
| SCA | Signature Creation Application |
| SCAL | Sole Control Assurance Level |
| SCDev | Signature Creation Device |
| SCP | SSASC Policy |
| SIC | Signer's Interaction Component |
| SSA | Server Signing Application |

| | |
|---|---|
| SSASC | Server Signing Application Service Component |
| SSASP | Server Signing Application Service Provider |
| TSP | Trust Service Provider |
| TW4S | Trustworthy System Supporting Server Signing |

# 2 Publication and Repository Responsibilities

## 2.1 Repositories

The *Remote Key Management Service Provider* discloses the contractual conditions and policies electronically on its website on the following link:

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

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

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

The actual version of policies and contractual conditions is readable in printed form at the customer service of the *Remote Key Management Service Provider*.

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

The *Remote Key Management Service Provider* notifies its *Client*s about the change of the General Terms and Conditions.

## 2.2 Publication of Certification Information

The *Remote Key Management Service Provider* does not publish any information regarding the enduser *Certificate*s belonging to the managed enduser keys. Such publication information can be found in the Certification Practice Statement of the Certificate Authority who issued the given *Certificate*.

## 2.3 Time or Frequency of Publication

### 2.3.1 Frequency of the Publication of Terms and Conditions

The most important terms and conditions for the Remote Key Management Service are contained in the service contract to be signed by the *Client* during the conclusion of the contract, or in the General Terms and Conditions [18] document referenced therein.

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

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

The *Remote Key Management Service Provider* will accept comments connected to the General Terms and Conditions published for 14 days prior to their becoming effective, at the following email address:

`info@e-szigno.hu`

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

The *Remote Key Management Service Provider* will close and publish the version of the General Terms and Conditions as amended with remarks on the 7th day prior to its becoming effective.

### 2.4 Access Controls on Repositories

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

The information disclosed by the *Remote Key Management Service Provider* shall only be amended, deleted or modified by the *Remote Key Management Service Provider*. The *Remote Key Management Service Provider* prevents the unauthorized changes to the information with various protection mechanisms.

## 3 Detailed specification of the Service

### 3.1 General requirements

#### 3.1.1 Signing key generation

The *Remote Key Management Service Provider* uses the following Qualified Electronic Signature Creation Device for managing the enduser private keys:

- Product: Trident version 2.1.3
- Developer: I4P.informatikai Kft. (I4P Ltd.)
- Certifier: OCSI
- Certificate reference: 2/20
- web: `http://www.ocsi.isticom.it/documenti/accertamenti/i4p/ac_rda_eidas_trident_213_v1.0.pdf`

The *Remote Key Management Service Provider* generates all the enduser keys in the above listed Qualified Electronic Signature Creation Device, and manages all the keys in it during the whole life cycle of the keys.

The Qualified Electronic Signature Creation Device is Common Criteria certified on assurace level EAL4+, augmented by AVA_VAN.5 and ALC_FLR.3

The *Remote Key Management Service Provider* uses only the following cryptograhic algorithm supported by the Qualified Electronic Signature Creation Device:

- cryptograhic algorithms: RSA
  - key length: 2048 bit
  - hash algorithm: SHA-256
  - padding algorithm: PKCS#1 ver.1.5
- cryptograhic algorithms: ECC
  - key length: 256 bits
  - hash algorithm: SHA-256
  - curve: ECC NIST P-256

End user and service provider private keys leave *Qualified Electronic Signature Creation Device* for backup purposes only. In any case, backup files are only sent in encrypted form from *Qualified Electronic Signature Creation Device*. The *Remote Key Management Service Provider* uses only AES256 symmetric keys to encrypt private keys.

The deployment of the *Qualified Electronic Signature Creation Device* requires the involvement of at least 2 administrators. The policy of the *Remote Key Management Service Provider* ensures that every admin created on the device is associated with a specific person and that a person can have only one admin account.

The *Remote Key Management Service Provider* always uses algorithms and parameters that meet the current cryptographic requirements.

The *Remote Key Management Service Provider* always checks the validity of the corrseponding *Certificate* before using the private keys, and refuses to use the key for *Certificate* expiring later than the cryptographic algorithm's lifetime.

The expiration date for the current cryptographic algorithm set is December 31, 2022.

The *Remote Key Management Service Provider* does not pre-generate end-user keys. The end-user keys are always generated after the successful authentication of the *Subject* just before the activation of the Remote Key Management Service.

To request the issuance of the first *Certificate* corresponding to the private key, the *Remote Key Management Service Provider* compiles a PKCS#10 request. The request is signed by the private key of the *Subject*. The use of the private key is already required in this case to identify the *Subject* and to get its explicit approval.

Before the issuance of the *Certificate* the *Certification Authority* verifies the correctness of the PKCS#10 request, this ensures control over the key and the correctness of the data in the *Certificate*.

No additional key operation is required for additional *Certificate*s issued for any reason (renewal, modification) belonging to the private key.

### 3.1.2 eID means linking

The *Remote Key Management Service Provider* uses the PassByME electronic user identification system developed and maintained by Microsec to validate the identity of the *Subject*. PassByME is a high-security, mobile-based personal identification system, which makes possible the identification of the users, and the individual validation of their electronic transactions. The operation of the PassByME system is based on the use of authentication and signing certificates which use RSA 2048 keys generated on the mobile device of the *Subject* onboard. All connections in the system are based on mutual PKI-based authentication and all transactions are protected by electronic signatures or seals.

Electronic identifier used in the PassByME system and assigned to the *Subject* is issued through the authentication procedure prior to the issuance of the first *Certificate* belonging to the private key, thus guaranteeing the highly reliable identification of the *Subject* uses Remote Key Management Service according to the eIDAS requirements, and assigning the identification data to the *Subject*.

The electronic identifier does not change when additional *Certificate*s issued for any reason (renewal, modification) belonging to the private key. The identifier is the same during the whole life-time of the private key.

The PassByME system is Common Criteria certified.

The *Certificate* issued by *Certification Authority* always contains the unique identifier (OID) assigned by *Certification Authority* to the *Subject*. During registration with PassByME, Microsec assigns this unique identifier OID value to certificates issued in the PassByME service. When using a key, the *Subject* selects the *Certificate* he wants to use and provides the password - which is valid regardless of the *Certificate* and can be changed by the user at any time - needed to activate the private key. Based on the information provided, the PassByME system identifies the current user and sends a confirmation request message to the registered mobile device of the user. Based on the confirmation, *Remote Key Management Service Provider* activates the appropriate key and performs the requested key operation.

The *Remote Key Management Service Provider* does not use subcontractors to issue an electronic ID.

### 3.1.3 Certificate linking

In case of issuance of a new *Certificate* due to any reason, the *Remote Key Management Service Provider* checks the issued *Certificate*, verifies the correlation between the generated key and the *Certificate* issued and stores the *Certificate*. The *Remote Key Management Service Provider* always assigns the last issued *Certificate* to the key. Before using the key, the *Remote Key Management Service Provider* always makes sure that the *Certificate* that you have selected and stored is matched.

The first use of the private key for *Subject* is to sign the PKCS#10 request. The use of a private key is already required in this case and in all other cases to identify the *Subject* to be approved by him.

### 3.1.4 eID means provision

To create PassByME-based credentials, *Subject* will receive the short live unique credentials for activation during the face-to-face meeting, or using an already existing secure client communication

channel.

### 3.1.5 Signature activation

The *Remote Key Management Service Provider* will only makes possible for the *Subject* to use his/her private key after the *Subject* has been successfully identified and the transaction approved.

The systems and protocols used by the *Remote Key Management Service Provider* provide adequate protection to prevent unauthorized use of the private key.

The *Subject*s and any third parties do not have direct access to the data stored in the systems. The *Subject*s can activate functions only through well-defined protocols. The functions are performed by the *Subject* by using internal systems of the *Remote Key Management Service Provider*.

Systems run by the *Remote Key Management Service Provider* ensure, that the DTBS/R provided under control of the *Subject* is only signed by the signing key belonging to this *Subject* and to the selected *Certificate*.

In order to activate the private key, the *Subject* shall present the key activation password and a unique short validity period password (TOTP).

The *Remote Key Management Service Provider* uses security measures based on risk analysis to protect against activating data threats.

The private key can only be used to sign the signature data (DTBS/R) received in the activation protocol.

The *Remote Key Management Service Provider* always checks the validity of the *Certificate* belonging to the private key before using the private key. The *Remote Key Management Service Provider* doesn't allow the usage of private key belonging to invalid (expired, suspended, or revoked) *Certificate*.

The use of a private key is always needs the identification and approval of the *Subject*.

### 3.1.6 Signing key deletion

The *Remote Key Management Service Provider* will destroy the *Subject* private key if:

- each *Certificate* belonging to the private key expires
- each *Certificate* belonging to the private key is revoked
- the Service Agreement is terminated
- requested by the *Subject*
- the assignment between the private key and the *Subject* is removed.

The *Remote Key Management Service Provider* deletes unnecessary private keys from the active system so that they cannot be restored.

Backups containing deleted private keys will be destroyed by the *Remote Key Management Service Provider* within 30 days.

### 3.1.7 Signing key backup and recovery

Private keys are only present in encrypted form in backup copies. The *Remote Key Management Service Provider* uses cryptographic algorithms that provide adequate protection (AES256). Backup files exist only in the copy required for safe operation.

The *Remote Key Management Service Provider* uses only cryptographic algorithms and parameters to protect backup files that provide adequate protection for the entire planned lifetime of the private key.

End-user and infrastructure private keys can only be saved and restored by staff with special security roles. Provider private keys used to encrypt backups can only be saved with the help of two employees with trusted security roles.

## 3.2 EU specific requirements

### 3.2.1 SSASP as a Qualified TSP

The Remote Key Management Service is provided by Microsec EHSZ, which is a qualified trust service provider under the eIDAS Regulation [1].

### 3.2.2 Policy name and identification

Section 1.2.1 of this *Remote Key Management Practice Statement* declares compliance with the EUSCP trust service policy.

### 3.2.3 General requirements

The Remote Key Management Service complies with the EUSCP trust service policy, which includes compliance with all requirements of the NSCP policy.

Chapter 3.1.1 of this *Remote Key Management Practice Statement* contains information about the Qualified Electronic Signature Creation Device certification used.

### 3.2.4 Signing key generation

The *Remote Key Management Service Provider* always generates the *Subject* private key in Qualified Electronic Signature Creation Device.

The *Remote Key Management Service Provider* always operates the Qualified Electronic Signature Creation Device in accordance with the requirements of the certification documentation.

### 3.2.5 Signature activation

The *Remote Key Management Service Provider* always stores the private key of the *Subject* in Qualified Electronic Signature Creation Device in active state and makes possible the key operations for the *Subject* only in Qualified Electronic Signature Creation Device.

The *Remote Key Management Service Provider* always operates the Qualified Electronic Signature Creation Device in accordance with the requirements of the certification documentation.

The *Remote Key Management Service Provider* provides cryptographic strength mechanisms that protect the authentication factors against compromise by the protocol threats as well as trusted third party impersonation attacks (e.g. key password, TOTP, session tokens, TLS, timestamp, evidences signed by RSA2048 based electronic signatures or seals etc.).

The protocol used by the Remote Key Management Service is protected against replay, bypass and forgery attack between signer and the remote SCDev (TOTP, session tokens, TLS, timestamp, evidences signed by RSA2048 based electronic signatures or seals etc.).

The Qualified Electronic Signature Creation Device used by the *Remote Key Management Service Provider* contains the signature activation module (SAM). The Qualified Electronic Signature Creation Device is tamper protected and Common Criteria certified on EAL4+ level, which proofs the compliance with the requirements of "prEN 419 221-5, v0.15, 29 November 2016".

The protocol used by the Remote Key Management Service assures that the SAD is always reliably protected against duplication or tampering against an attacker with high attack potential (key password, TOTP, session tokens, TLS, timestamp, evidences signed by RSA2048 based electronic signatures or seals etc.).

The protocol used by the Remote Key Management Service assures that the signer can always reliably protect the signing key activation by the SAD against an attacker with high attack potential.

### 3.2.6 Signature activation data management

The SAD is a set of data which consist of

- a given DTBS/R or a set of DTBS/R
- items to identify the authenticated *Subject*
- the activation password of the selected signing key
- time based One Time Password (TOTP)

The SAD is collected (TOTP is generated) in the signer's IT environment by the SIC.

The protocol used by the Remote Key Management Service assures with a high level of confidence by using PKI technology the integrity of the SAD.

The SAD can be computed only after successful two factor authentication of the *Subject*.

The SAP used by the Remote Key Management Service assures with a high level of confidence the protection of integrity and the transfer of the SAD to the SAM.

The creation of the electronic seal or electronic signature is always initiated by a natural person. The collection and generation of the SAD happens under the control of the natural person with a high level of confidence. The SAD is transferred through a protected communication channel to the SAM which ensures the confidentiality of the key password.

The SAP assures that the SAD is always submitted under the sole control of the signer by means that are in possession of the signer.

The *Remote Key Management Service Provider* uses PKI technology to protect the integrity of all the internal messages which assures that the SAD is protected against highly unlikely activites such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential.

# 4 Facility, Management, and Operational Controls

The *Remote Key Management Service 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 *Remote Key Management Service 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 *Remote Key Management Service Provider* monitors the capacity demands and ensures that the adequate processing power and storage are available for the provision of the Remote Key Management Service.

## 4.1 Physical Controls

The *Remote Key Management Service Provider* takes care that physical access to critical services is controlled, and keeps physical risk of the assets related to critical services at a minimum.

The purpose of physical precautions is to prevent illegitimate access, damage, and unauthorized access to the *Remote Key Management Service Provider*'s information, and physical zones.

Services that process critical and sensitive information are implemented at secure locations in the system of the *Remote Key Management Service Provider*.

The provided protection is proportional to the identified threats of the risk analysis that the *Remote Key Management Service Provider* has performed.

In order to provide adequate security:

- The *Remote Key Management Service Provider* implements the strongly protected services in its protected computer room. This computer room has been designed and constructed specifically for this purpose, by its design uniform enforcement of various aspects of protection (the placement and structure of the site, physical access (access control and supervision), power supply, air conditioning, protection against water leakage and flooding, fire prevention and protection, media storage etc.) took place.
- The *Remote Key Management Service Provider* implements every critical service and every necessary tool in a separate security zone. All the devices necessary for this are placed in a protected computer room – forming part of the security zone.

### 4.1.1 Site Location and Construction

The IT system of the *Remote Key Management Service Provider* is located and operated within a properly secured *Data Centre* with physical and logical protection that prevents illegitimate access. Defensive solutions – as for example guarding, security locks, intrusion detection systems, video surveillance system, access control system – are applied over the course of locating and establishing the *Data Centre* that are built on each other and interdependent and together they provide a powerful protection system for the IT systems participating in service provision, and for the preservation of the confidential data stored by the provider.

### 4.1.2 Physical Access

The *Remote Key Management Service Provider* protects devices and equipment that take part in the service provision from unauthorized physical access in order to prevent tampering with the devices.

*Remote Key Management Service Provider* ensures that:

- each entry to the *Data Centre* is registered;
- entry to the *Data Centre* may only happen after the simultaneous identification of two authorized staff members with trusted roles – and at least one of the staff members shall be a system administrator;
- persons without independent authorization can only stay in the *Data Centre* in justified cases, for the time required and accompanied by personnel with appropriate rights;
- the entry logs shall be archived continuously and evaluated weekly.

The activation data (passwords, PIN codes) of the devices shall not be stored openly even in the *Data Centre*.

In the presence of unauthorized persons:

- data media containing sensitive information are physically out of reach;
- the logged-in terminals are not left without supervision;
- no work process is carried out during which confidential information may be revealed.

When leaving the computer room the administrator shall verify that:

- every equipment of the *Data Centre* is in an adequately secure operation state;
- there's no terminal left logged-in;
- physical storage devices are locked properly;
- systems, devices providing physical protection operate properly;
- the alarm system has been activated.

There are appointed responsible people to carry out regular physical security assessments. The results of the examinations are recorded in the appropriate log entries.

### 4.1.3 Power and Air Conditioning

The *Remote Key Management Service Provider* applies an uninterruptible power supply unit in the *Data Centre* that:

- has adequate capacity to ensure power supply for the *Data Centre*'s IT and subsidiary facility systems;

- protects IT equipment from voltage fluctuations in the external network, power outages, spikes and other;
- in case of lasting power outage has its own power generation equipment, which – by allowing refueling – is able to provide the necessary energy for any period of time.

The air of the outer environment shall not get into the *Data Centre* directly. The *Data Centre* air purity is ensured with adequate filter system to detect a variety of contaminants from the air (dust, pollutants, and corrosive materials, toxic or flammable substances). The ventilation system provides the necessary amount of fresh air with adequate filtration for the safe working conditions of the operators.

The humidity is reduced to the level required by the IT systems.

The *Remote Key Management Service Provider* uses cooling systems with proper performance to provide the necessary operating temperature, to prevent overheating of IT devices.

### 4.1.4 Water Exposures

The *Data Centre* of the *Remote Key Management Service Provider* is adequately protected from water intrusion and flooding. The total area of the security zone is free from sanitary facilities, there is not any drain or water pipe close to it. The total area of water security zone is monitored by an intrusion detection system. In the protected computer room security is further increased by the use of a raised floor.

### 4.1.5 Fire Prevention and Protection

In the *Data Centre* of the *Remote Key Management Service Provider*, a fire protection system approved by the competent fire headquarters operates. Smoke and fire detectors automatically alert the fire brigade. Water vapor based, automatic fire extinguishing system has been installed in the computer room, which is not hazardous to human life, and does not damage the IT equipment.

There is the type and quantity of manual fire extinguishers in accordance with the relevant regulations at clearly visible locations in each room.

### 4.1.6 Media Storage

The *Remote Key Management Service Provider* protects its media storages from unauthorized access and accidental damage. All audit and archive data is created in duplicate. The two copies are stored separately from each other physically, at locations in a safe distance from each other. The stored media storages are protected from damaging environmental influences such as low or high temperatures, dirt, moisture, sunlight, strong magnetic fields, strong radiation.

The *Remote Key Management Service Provider* stores the primary media storages in the operational room of the certification organization, a code locked fireproof vault, the secondary copies in a vault in the customer service office.

### 4.1.7 Waste Disposal

The *Remote Key Management Service Provider* ensures the environmental standards compliant disposal of the superfluous assets, and media.

The *Remote Key Management Service Provider* does not use the electronic storage media containing information classified as confidential even for storing data classified as not confidential after deleting their content and devices like that shall not be taken outside of the premises of the *Remote Key Management Service Provider*. The *Remote Key Management Service Provider* physically destroys – according to the rules of disposal – the defective for any other reason unusable, redundant media storages containing confidential classified information:

- chops paper documents up in a shredder machine;
- disassembles the hard drives and smashes the critical components;
- destroys the optical disc with a suitable shredder machine.

### 4.1.8 Off-Site Backup

The *Remote Key Management Service Provider* creates a backup weekly from which the whole service could be restored in case of a fatal error. The backups – at least including the last full backup – are stored at an external location that's physical and operational protection is identical to the primary site. The secure data transmission from the primary to the backup locations is resolved.

Based on the randomly selected backup data a restoration test is made at least yearly. The main circumstances and results of the restoration test is recorded in an audit report.

## 4.2 Procedural Controls

The *Remote Key Management Service Provider* takes care that its systems are operated securely, according to the rules, and with a minimal risk of defects.

Procedural precautions have the objective of supplementing, and at the same time intensifying the effectiveness of physical safeguards, along with those applicable to personnel, by means of appointing and isolating trusted roles, documenting the responsibilities of various roles, as well as specifying the personnel headcounts and exclusion roles necessary for the various tasks, moreover identification and authentication expected in the various roles.

The *Remote Key Management Service Provider*'s internal governance system ensures that its operation complies with legal, as well as its internal regulations. In its system a responsible person shall be clearly assigned for every given system unit and process.

Individuals responsible for a given system element or process are assigned unambiguously to every system element and every process in its system. Development and operations related tasks are sharply segregated in the *Remote Key Management Service Provider*'s system. The auditing activity of the independent system auditor and the *Remote Key Management Service Provider*'s internal auditor ensures the system's appropriate operation.

### 4.2.1 Trusted Roles

The *Remote Key Management Service Provider* creates trusted roles for the performance of its tasks. The rights and functions are be shared among the various trusted roles in such a way that one user alone shall not be able to bypass the security protection measures.

The *Remote Key Management Service Provider* defines the following trusted roles, with the following responsibilities:

**Manager with overall responsibility for the IT system of the *Remote Key Management Service Provide*** The individual responsible for the IT system.

**Security officer:** Senior security associate, the individual with overall responsibility for the security of the service.

**System administrator:** Infrastructure administrator. The individual with the task to install, configure and maintain the systems of the *Remote Key Management Service Provider*. Responsible, for the reliable and continuous operation of the assigned system units, and for monitoring the development of technology, and for the detection and proposing of development solutions of the vulnerabilities of each system component.

**Operator:** System operator, individual performing the IT system's continuous operation, backup and restore.

**Independent system auditor:** Individual who audits the logged, as well as archived dataset of the *Remote Key Management Service Provider*, responsible for verifying the enforcement of control measures the service provider implements in the interest of operation that complies with regulations, moreover for the continuous auditing and monitoring of existing procedures.

For the provision of trusted roles the manager responsible for the security of the *Remote Key Management Service Provider* formally appoints the *Remote Key Management Service Provider*'s employees.

Only those persons may hold a trusted role who are in employment relationship with the *Remote Key Management Service Provider*. Trusted roles shall not be hold in the context of a commission contract.

Up to date records are kept of the trusted roles and in case of any change, the National Media and Infocommunications Authority is notified without delay.

### 4.2.2 Number of Persons Required per Task

The security and operational regulations of the *Remote Key Management Service Provider* define that the following tasks can be only performed in protected environment, with the contemporaneous presence of two employees holding trusted roles:

- the generation of the *Remote Key Management Service Provider*'s own service key pair;
- the backup of the provider's private key;
- the activation of the provider's private key;
- the destruction of the provider's private key.

At least one of the persons performing the procedures listed above shall be a system administrator, and the other person shall not be the independent system auditor.

During the implementation of the operations listed, unauthorized person shall not be present in the room.

### 4.2.3 Identification and Authentication for Each Role

The users managing the IT system of the *Remote Key Management Service Provider* have unique identification data, enabling secure identification and authentication of the users.

The users can only access the IT systems critical from the aspect of the provision of the certification service after identification and authentication.

The identification and authentication data are revoked without delay in case of the cessation of user rights.

Every user of the IT system and every actor in the administrative process is identified individually.

For the verification of the physical access, the *Remote Key Management Service Provider* uses an RFID card based access control system, and for the logical access control, it uses VPN Certificates issued on a Secure Signature-Creation Device. Before successful authorization, not even a single security-critical task can be performed. Every employee of the *Remote Key Management Service Provider* has exactly as many access rights, as it is absolutely necessary for the assigned role.

### 4.2.4 Roles Requiring Separation of Duties

Employees of the *Remote Key Management Service Provider* can hold multiple trusted roles at the same time, but the *Remote Key Management Service Provider* ensures that:

- the security officer and the registration officer shall not hold the independent system auditor role;
- the system administrator shall not hold the security officer and the independent system auditor role;
- the manager with overall responsibility for the IT system shall not hold the security officer and the independent system auditor role.

In addition to the aforementioned, the *Remote Key Management Service Provider* seeks the complete separation of trusted roles.

## 4.3 Personnel Controls

The *Remote Key Management Service Provider* takes care that its personnel policy, and its practices applicable to employing staff members intensify and support the reliability of the *Remote Key Management Service Provider*'s operation. The objective of precautions applicable to personnel is to reduce the risk of human errors, theft, fraud and cases of misuse.

The *Remote Key Management Service Provider* addresses personnel security already during the hiring stage, including the conclusion of contracts, as well as their validation when they are being employed. In the case of all trusted roles, applicants have valid certificate of no criminal record at the time of the application. Every employee in a trusted role and external parties – who get in contact with the *Remote Key Management Service Provider*'s services – shall sign a non-disclosure agreement.

At the same time, the *Remote Key Management Service Provider* ensures for its employees obtaining as well as further developing of common, general know-how along with the specialized professional knowledge necessary for performing the various jobs.

### 4.3.1 Qualifications, Experience, and Clearance Requirements

As a hiring requirement, the *Remote Key Management Service Provider* requires at least intermediate education degree, but the *Remote Key Management Service Provider* continues to takes care that employees receive appropriate training. Immediately after recruitment, the *Remote Key Management Service Provider* grants a training for its new employees, under the course of which they acquire the knowledge necessary to carry out the job. The *Remote Key Management Service Provider* usually supports the professional development of the employees, but it also expects employees to independently develop their skills in their respective fields. Some of the employees of the *Remote Key Management Service Provider* have the role to detect and gather the technical and business innovations and to organize, and share this knowledge with their colleagues.

Trusted roles can be held at the *Remote Key Management Service Provider* only by persons, who have no external influence and possess the necessary expertise validated by the *Remote Key Management Service Provider*. All personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the *Remote Key Management Service Provider*'s operations.

The manager with overall responsibility for the IT system can only be a person who has:

- specialized degree (mathematics, physics college or university degree or a college/university degree acquired at an engineering department belonging to the technical field of science);
- at least three years of expertise in professional working experience related to information security.

### 4.3.2 Background Check Procedures

The *Remote Key Management Service Provider* only hires employees for trusted or leading roles, who

- have a clean record and there's no proceeding in progress against them that may affect the impunity.
- are not subject to professional disqualifications prohibiting to exercise electronic signatures related services.

At the time of the appointment, shall the leading role holder *Remote Key Management Service Provider* employee with a statement, a trusted role holder employee with a certificate of good conduct less than 3 months old justify the clean criminal record.

The *Remote Key Management Service Provider* verifies the authenticity of the relevant information given in the applicant's CV during the hiring process, like previous employment, professional references, most relevant educational qualifications.

### 4.3.3 Training Requirements

The *Remote Key Management Service Provider* trains the newly recruited employees, over the course of which they acquire

- basic PKI knowledge;

- the specifics and the way of handling the *Remote Key Management Service Provider*'s IT system;
- the necessary special knowledge for fulfilling their scope of activities;
- processes and procedures defined in the public and inner regulations of the *Remote Key Management Service Provider*;
- the legal consequences of the individual activities;
- the applicable IT security regulations to the extent necessary to the specific scope of activities;
- the data protection rules.

Only employees having passed the training shall gain access to the he production IT system of the *Remote Key Management Service Provider*.

### 4.3.4 Retraining Frequency and Requirements

The *Remote Key Management Service Provider* ensures that the employees have the necessary knowledge continuously, so if needed, further or repeater type of training is held.

Further training is held if there's a change within the processes or the IT system of the *Remote Key Management Service Provider*.

The training material is updated at least in every 12 months and contains the new threats and actual security practices.

The training is adequately documented, from what the syllabus and the scope of the participator employees can be clearly determined.

### 4.3.5 Job Rotation Frequency and Sequence

The *Remote Key Management Service Provider* does not apply mandatory rotation between individual work schedules.

### 4.3.6 Sanctions for Unauthorized Actions

The *Remote Key Management Service Provider* regulates the prosecution possibilities of the employees in an employment contract in case of failures, errors, accidental or intentional damage. If the employee – due to negligence or intentionally – violates their obligations, sanctions could be taken against him by the *Remote Key Management Service Provider*, which it sets out having regard to the offense and the consequences. The sanctions may include disciplinary proceedings, dismissal, revocation of appointment, criminal liability. Upon appointment every trusted role employee as part of the employment documents:

- gets written information about legal liabilities, rights, certification and management standards for the treatment of personal data,
- gets a job description that includes the concerning security tasks,

- signs a confidentiality agreement in which the related consequences non-compliant with security measures, (criminal sanctions) can be found too.

All of these include the labor legislation or criminal consequences, that sanction the different discipline – job obligations – violation or breaking the law.

### 4.3.7 Independent Contractor Requirements

The *Remote Key Management Service Provider* only assigns trusted roles to its employees.

The *Remote Key Management Service Provider* chooses persons employed with engagement contract or subcontract to perform the other tasks, chosen if possible, from the list of previously qualified suppliers. The *Remote Key Management Service Provider* concludes a written contract before working with suppliers.

Each contracting party – before the start of the active work – signs a confidentiality statement in which he agrees that the business / corporate secrets learned later on will not be covered up to unauthorized persons, and will not be exploited in any other way.The confidentiality statement includes sanctions in case of violation. External employees employed under the contract are expected to have appropriate technical skills, and the *Remote Key Management Service Provider* does not hold any trainings for them.

### 4.3.8 Documentation Supplied to Personnel

The *Remote Key Management Service Provider* continuously provides for the employees the availability of the current documentation and regulations necessary to perform their roles.

Each employee in trusted role receives the following documents in writing:

- the organizational security regulations of the *Remote Key Management Service Provider*,
- the confidentiality agreement to be signed,
- personal job description,
- educational materials on the occasion of the planned or special training for the specific form of education.

All employees are informed in a written notice about any changes in the organizational security regulations.

## 4.4 Audit Logging Procedures

In order to maintain a secure IT environment the *Remote Key Management Service Provider* implements and operates an event logger and control system covering its full IT system.

### 4.4.1 Types of Events Recorded

The *Remote Key Management Service 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 identification of the user or the system who/what triggered the event;
- the success or failure of the audited event.

All new audit record is appended to the audit records. The earlier saved audit records can't be modified or deleted.

All of the essential event logs are available to the independent system auditors, who examine the compliance of the *Remote Key Management Service Provider*'s operation.

The *Remote Key Management Service Provider* logs The following events at minimum:

- INTERNAL CLOCK
  - the synchronization of the internal clock to the UTC time, including the operational re-calibrations too;
  - the loss of synchronization;
- REMOTE KEY MANAGEMENT
  - significant TW4S environmental events;
  - user signing events (e.g. successful signing with a signer's signing key and DTBS/R request management);
  - user authentication during SAP;
  - signer's SAD management by TW4S;

  User signing events SHALL include associate certificate to the signing key.
- LOGGING:
  - the shutdown, restart of the logging system or some of its components;
  - the modification of any parameter of the logging settings, for example the frequency, alert threshold, and the event to be examined;
  - the modification or deletion of the stored logging data;
  - the activities performed because of the logging system's failure.
- SYSTEM LOGINS:
  - successful logins, unsuccessful login attempts for trusted roles;
  - in case of password based authentication:
    - the change of the number of permitted unsuccessful attempts;
    - reaching the limit of the permitted number of the unsuccessful login attempts in case of user login;
    - readmission of the user blocked because of the unsuccessful login attempts;

  - changing the authentication technique ( for example from password based to PKI based).

- KEY MANAGEMENT:
  - all events for the entire life cycle of service keys (key generation, saving, loading, destruction etc.);
  - all user key management event (generating, usage and destruction);
- CERTIFICATE MANAGEMENT:
- DATA FLOWS:
  - any kind of security-critical data manually entered into the system;
  - security-relevant data, messages received by the system;
- Qualified Electronic Signature Creation Device:
  - installing Qualified Electronic Signature Creation Device;
  - removing Qualified Electronic Signature Creation Device;
  - disposing, destructing Qualified Electronic Signature Creation Device;
  - delivering Qualified Electronic Signature Creation Device;
  - clearing (resetting) Qualified Electronic Signature Creation Device;
  - uploading keys, certificates to the Qualified Electronic Signature Creation Device.
- CONFIGURATION CHANGE:
  - hardware;
  - software;
  - operating system;
  - patch;
- PHYSICAL ACCESS, LOCATION SECURITY:
  - person entry to and exit from the security zone holding the system components used for providing the trust service;
  - access to a system component used for providing the trust service;
  - a known or suspected breach of physical security;
  - firewall or router traffic.
- OPERATIONAL ANOMALIES:
  - system crash, hardware failure;
  - software failures;
  - software integrity validation error;
  - incorrect or wrongly addressed messages;

  - network attacks, attack attempts;
  - equipment failure;
  - electric power malfunctions;
  - uninterruptible power supply error;
  - an essential network service access error;
  - violation of the *Remote Key Management Practice Statement*;
  - deletion of the operating system clock.

- OTHER EVENTS:
  - appointment of a person to a security role;
  - operating system installation;
  - PKI application installation;
  - initiation of a system;
  - entry attempt to the PKI application;
  - password modification, setting attempt;
  - saving the inner database, and restore from a backup;
  - file operations ( for example creating, renaming, moving);
  - database access.

### 4.4.2 Frequency of Audit Log Processing

The independent system auditors of the *Remote Key Management Service Provider* evaluates the generated log files every working day.

During the evaluation, the authenticity and integrity of the examined logs is ensured, the error messages in the logs are checked and if needed, document the differences and take measures to eliminate the cause of the deviation.

For the IT system evaluation, the *Remote Key Management Service Provider* uses automated evaluation tools too, that are used to monitor the resulting log entries according to preset criteria and, where necessary, alert the operational staff. The notifications received from the automated evaluation tools are processed and evaluated by the experts of the IT operation within 24 hours.

The fact of the investigation, the results of the investigation and the measures undertaken to avert deficiencies found are properly documented.

### 4.4.3 Retention Period for Audit Log

Before the deletion from the on-line system, the logs are archived and their secure preservation is ensured by the *Remote Key Management Service Provider* for the amount of time defined in Section 4.5.2, but at least 10 years from the date of their creation.

For that time period, the *Remote Key Management Service Provider* ensures the readability of archived data, and maintains the software and hardware tools necessary for that.

### 4.4.4 Protection of Audit Log

The *Remote Key Management Service Provider* protects the created logs for the required preservation time. During the whole preservation time, the following properties of the logs' data is ensured:

- protection against unauthorized disclosure: only authorized persons – primarily the independent system auditors – access the logs;
- availability: authorized persons are granted access to the logs;
- integrity: any data alteration, deletion in the log files and change in the order of the entries, etc. is prevented.

The *Remote Key Management Service Provider* provides the log records with qualified *Time Stamp*s, and they are stored in a way excluding the seamless insertion and deletion of the log entries.

The log files are protected against accidental and malicious damage by backups. In case of log entries containing personal data, the *Remote Key Management Service Provider* makes sure of the confidential storage of the data. Only those individuals are entitled to access to the log entries, who absolutely need it for their work. The *Remote Key Management Service Provider* verifies the accesses in a secure way. The *Remote Key Management Service Provider* preserves the log files in a secure environment. Keeps copies of the files at the second operation site.

### 4.4.5 Audit Log Backup Procedures

Daily log files are created from the continuously generated log entries during the operation in each system.

The daily log files are archived in two copies after the evaluation and stored physically apart from each other, at separate sites for the required time.

The exact process of backups shall be defined in the backup regulations of the *Remote Key Management Service Provider*.

### 4.4.6 Audit Collection System (Internal vs External)

Each application automatically collects and sends the records to the logging system.

The logging functions start automatically at the time of the system launch and they are run continuously during the entire period of system operation.

In case of any anomaly in the automatic examiner and logging systems, the operation of the related areas are suspended by the *Remote Key Management Service Provider* until the incident is resolved.

### 4.4.7 Notification to Event-causing Subject

The persons, organizations and applications that caused the error event are not always notified, but if necessary the *Remote Key Management Service Provider* involves them in the investigation of the event. The Clients affected by triggering the event has the duty to cooperate with the *Remote Key Management Service Provider* to explore the event.

### 4.4.8 Vulnerability Assessments

Besides processing daily the log entries, the experts of the *Remote Key Management Service Provider* monitor the publicly available information about possible vulnerabilities and the new software patches. They analise the information, classify the vulnerability and if necessary inform the management about the result and propose an action plan to increase the security of the system.

Every major event of significant deficiencies detected or in case of external threat within a period of 48 hours after its discovery, but at least once a year the experts of the *Remote Key Management Service Provider* perform a comprehensive vulnerability analysis using a mapping of potential internal and external threats that may result in unauthorized access.

Based on the results of the analysis the *Remote Key Management Service Provider*

- creates and implements a plan to mitigate the vulnerability; or
- documents the factual basis for the decision that the residual risk is accepted and the vulnerability does not require remediation.

At first the new software versions and software patches are installed on the test system of the *Remote Key Management Service Provider* and only after the successfully finished test are installed on the live system which is used to provide the services.

The new software patches are not installed on the live system if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them. The reasons for not applying any security patches are documented.

## 4.5 Records Archival

### 4.5.1 Types of Records Archived

The *Remote Key Management Service Provider* is prepared to the proper secure long-term archiving of electronic and paper documents.

The *Remote Key Management Service Provider* archives the following types of information:

- every document related to the accreditation of the *Remote Key Management Service Provider*;
- all issued versions of the *Remote Key Management Practice Statements*;
- all issued versions of the General Terms and Conditions;
- contracts related to the operation of the *Remote Key Management Service Provider*;
- every electronic and paper based log entry.

### 4.5.2 Retention Period for Archive

The *Remote Key Management Service Provider* preserves the archived data for the time periods below:

- *Remote Key Management 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 other documents to be archived for at least 10 years from the date of their creation.

### 4.5.3 Protection of Archive

The *Remote Key Management Service Provider* stores all archived data in two copies at locations physically apart from each other. Authentic paper or electronic copy is made in accordance with the applicable law from the only authentic paper based copy of the document available.

Each of the two locations fulfils the requirements for archiving security and other requirements.

During the preservation of the archived data, it is ensured that:

- their integrity is preserved;
- they are protected against unauthorized access ;
- they are available;
- they preserve authenticity.

The archived electronic data is provided with at least an advanced electronic signature or seal and a qualified *Time Stamp*.

### 4.5.4 Archive Backup Procedures

The *Remote Key Management Service Provider* makes an authentic electronic copy of the original paper documents in accordance with the relevant legislation. Electronic copies are stored according to the same rules as other protected electronic documents.

After archiving the authentic electronic copies the *Remote Key Management Service Provider* may destroy the original paper documents.

### 4.5.5 Requirements for Time-stamping of Records

Every electronic log entry is provided with a time mark, on which the system provided time is indicated at least to one second precision.

The time value is given by the internal clock of the *Remote Key Management Service Provider* which is synchronized to two separate Stratum-1 UTC time sources:

- one accurate time source uses the satellite-based GPS signal;
- the other accurate time source is based on the longwave time signal service (DCF77).

In order to provide accuracy the *Remote Key Management Service Provider* synchronizes its own internal time with the above Stratum-1 sources within a 0.1 second accuracy, and it performs this synchronization at least 4 times a day.

This way the *Remote Key Management Service Provider* guarantees that the deviation of the time indicated in the time marks from the UTC time base is at most 1 second.

The *Remote Key Management Service Provider* provides the daily log files with a qualified *Time Stamp*.

During the preservation of the archived data, if necessary (for example algorithm change expiration of the original *Time Stamp*) the authenticity of the data is ensured.

### 4.5.6 Archive Collection System (Internal or External)

The log entries are generated in the *Remote Key Management Service Provider*'s protected computer system, and only the log files that are electronically signed and protected with qualified timestamps can leave it.

One original copy of the documents created during the service provision is stored and protected by the *Remote Key Management Service Provider* in an inner data storage operated by it.

### 4.5.7 Procedures to Obtain and Verify Archive Information

The *Remote Key Management Service Provider* creates the log files manually or automatically. In case of an automatic logging system, the certified log files are generated daily.

The archived files are protected from unauthorized access.

Controlled access to the archived data is only available to the eligible persons:

- *Client*s are eligible to see the data stored about them;
- in legal litigation in order to provide evidence the necessary data shall be provided.

## 4.6 Compromise and Disaster Recovery

In case of a disaster, the *Remote Key Management Service Provider* takes all necessary measures in order to minimize the damage resulting from the shortfall of the service, and it restores the services as quickly as possible.

Based on the assessment of the incident that occurred, it takes the necessary amendments, corrective measures to prevent future occurrence of the incident.

Once the problem resolved, the event is reported to the National Media and Infocommunications Authority, as the supervisory authority.

### 4.6.1 Incident and Compromise Handling Procedures

The *Remote Key Management Service Provider* has a business continuity plan.

The *Remote Key Management Service Provider* has increased security tools and systems in order to minimize the software and hardware failures and data corruptions. The recoverability of services is guaranteed by the underpinning contracts and own backup tools of the *Remote Key Management Service Provider*.

The *Remote Key Management Service Provider* constructed its IT system providing the trust services in such a way that in case of the dropout of any one device, it is able to continue the provision of its trust services.

### 4.6.2 Computing Resources, Software, and/or Data are Corrupted

The IT systems of the *Remote Key Management Service Provider* are built of reliable hardware and software components. The critical functions are implemented using redundant system elements so that in the event of an item failure they are able to operate further.

The *Remote Key Management Service Provider* makes a full daily backup of its databases and the generated log events.

The *Remote Key Management Service Provider* makes full system backups as frequently as necessary to be able to restore the full service in case of a disaster.

The business continuity plan of the *Remote Key Management Service Provider* includes accurate requirements for the tasks to be performed in case of critical system component failure.

Once the problem resolved and the integrity restored, the *Remote Key Management Service Provider* restarts its services as soon as possible.

### 4.6.3 Business Continuity Capabilities After a Disaster

The tasks to be performed in case of service failure due to natural or other disaster are defined in the *Remote Key Management Service Provider*'s business continuity plan.

In the event of disaster, the regulations come into force, the damage control and the restoration of the services begins.

The *Remote Key Management Service Provider* is obliged to notify the affected users as quickly as possible in the event of the disaster.

After the restoration of the services, the *Remote Key Management Service Provider* restores its devices damaged during the disaster and the original service security level as quickly as possible

## 4.7 Termination of the Service

In the event of the planned termination of the Remote Key Management Service, the *Remote Key Management Service Provider* notifies the end users and the National Media and Infocommunications Authority at least 60 days prior to the termination of the Remote Key Management Service.

At the same time with the notification about the Remote Key Management Service termination, the *Remote Key Management Service Provider* shuts down the following services:

- signing new subscriber contract,
- key generation,
- re-key.

At the same time of the termination, the *Remote Key Management Service Provider* shuts down the following services:

- remote usage of the user keys,
- technical support.

- information provision.

The *Remote Key Management Service Provider* requests the revocation of the *Certificate*s belonging to the end user keys managed in the Remote Key Management Service from the Certificate Authority immediately after the termination of the Remote Key Management Service. The *Remote Key Management Service Provider* destroys all end-user keys managed in its system, including all backup files created from the keys. The *Remote Key Management Service Provider* takes a record of the destruction of the keys.

Before a planned termination, the *Remote Key Management Service Provider* engages in negotiations about the taking over of its services with other Trust Service Provider whose rating is identical to its own. Under section 7.3 , it will hand over its records, including confidential user data, to such a Trust Service Provider or to the National Media and Infocommunications Authority come what may, along with its other services, depending on the outcome of the negotiations or terminates without handover.

The *Remote Key Management Service Provider* informs the National Media and Infocommunications Authority about the final outcome of the negotiations. The *Remote Key Management Service Provider* is to inform its *Client*s by electronic mail, and *Relying Parties* by means of a publication on its website.

Upon termination the Remote Key Management Service, the *Remote Key Management Service Provider* produces a full scope backup of its data contained in its IT system, protected by a qualified *Time Stamp*.

In order to make the handing over of its data to another Trust Service Provider possible, the *Remote Key Management Service Provider* places data on media and in a format which the new Trust Service Provider can receive or provides the new Trust Service Provider with the opportunity to process data in the original format, and hands over the appropriate tools, documentation and know-how for this. After the termination of the Remote Key Management Service the *Remote Key Management Service Provider* deletes all the private keys and identification data of the *Subscriber*s from its IT systems in an unrecoverable way.

# 5 Technical Security Controls

The *Remote Key Management Service Provider* uses systems consisting of reliable, and safety technically assessed equipment for the provision of its services. The *Remote Key Management Service Provider* manages the provider and enduser cryptographic private keys during their whole life-cycle within a Qualified Electronic Signature Creation Device that has appropriate Certification.

Both the *Remote Key Management Service Provider* and the system supplier and execution contractors have significant experience with deployment of PKI based systems and trust services and they use internationally recognized technology.

The *Remote Key Management Service Provider* continuously monitors the capacity needs, and with setting the trends it estimates the expected future capacity demands. It can arrange if needed an extension of the limited capacity, thereby providing the necessary processing and continuous availability of storage capacities.

## 5.1 Key Pair Generation and Installation

The *Remote Key Management Service Provider* makes sure that the generation and management of all the private keys generated by it – for the *Subject*s or its IT systems – is secure and complies with the regulatory requirements in force and with industry standards.

### 5.1.1 Key Pair Generation

The *Remote Key Management Service Provider* uses key generation algorithms for the key-pair generation, which comply with the requirements set out in the following normatives:

- ETSI TS 119 312 [13];
- the current National Media and Infocommunications Authority algorithmic regulation issued pursuant to the authorization of the year 2015. Act CCXXII [7] 92. § (1) b) .

In case of generating the infrastructure keys used in its own IT systems, the *Remote Key Management Service Provider* ensures that:

- the generation of the *Remote Key Management Service Provider*'s infrastructure key is carried out in a physically protected environment (see section 4.1) by an authorized person in a role of trust (see section 4.2.1), excluding the presence of other unauthorized persons;
- the key generation fully complies with the instructions in the device user documentation.

In case of the generation of the key pair generated for the *Subject*s by the *Remote Key Management Service Provider*, it ensures that:

- Keys are generated in a physically protected environment, either automatically or with the participation of persons with trusted roles only.
- The *Remote Key Management Service Provider* generates the enduser keys on its *Qualified Electronic Signature Creation Device* which makes the disclosure of the private key impossible.
- The *Remote Key Management Service Provider* ensures that the generated key pair is compliant with the requirements defined in Sections 5.1.4 and 5.1.5, and the private key is not one of a known weak key pair.

### 5.1.2 Private Key Delivery to Subscriber

In case of Remote Key Management Service:

- During the whole service, the *Remote Key Management Service Provider* shall store the private keys generated by it for the *Subject*s and the activation data securely to prevent the key disclosure, copy, modification, damage and the usage by unauthorized people.
- The *Remote Key Management Service Provider* shall use an identification procedure that ensures that the private keys can only be used by the *Subject*.

- The *Remote Key Management Service Provider* shall store sufficient evidence of the fact that, the handover of the disposal over the private key to the *Subject* happened at a specific authentic time.
- The *Remote Key Management Service Provider* shall ensure that following the handover of the disposal over the private key only the *Subject* is able to run the identification process necessary for the usage of the private key.

### 5.1.3 Public Key Delivery to Certificate Issuer

The *Remote Key Management Service Provider* shall fulfil the following requirements:

- the public key shall be sent to the Certificate Authority in a manner that it can be unambiguously assigned to the *Subject*;
- the *Certificate Application* process shall prove that the *Subject* really owns the private key corresponding to the public key.

As part of the Remote Key Management Service *Remote Key Management Service Provider* generates the enduser keys and creates a PKCS#10 formatted *Certificate Application* which is signed with the private key belonging to the public key to be indicated in the *Certificate*. The *Certificate Application* is sent to the Certificate Authority. The PKCS#10 formatted *Certificate Application* contains the public key generated for the *Subject* and the *Subject* data to be indicated in the *Certificate*, so both requirements are met.

### 5.1.4 Key Sizes

The *Remote Key Management Service Provider* uses cryptographic algorithms and minimum key sizes, which comply with the requirements set out in the following norms:

- ETSI TS 119 312 [13];
- the current National Media and Infocommunications Authority algorithmic regulation issued pursuant to the authorization of the year 2015. Act CCXXII [7] 92. § (1) b) .

The *Remote Key Management Service Provider* in the Remote Key Management Service supports only the usage of RSA keys with at least 2048 bits length.
The *Remote Key Management Service Provider* supports the following ECC curves:

- ECC NIST P-256 (256 bit)

### 5.1.5 Public Key Parameters Generation and Quality Checking

The *Remote Key Management Service Provider* generates the keys according to the description of the section 5.1.1.

**Verification of Compliance of Parameters**

The compliance of the key generation parameters is verified by the system from two points of view:

- checking the conformity of the random number generation used for the parameters (whether the generation is sufficiently statistically random),
- checking the fulfilment of the requirements for parameters.

Every Qualified Electronic Signature Creation Device used in the system is able to statistically test the uniformity and independence of the bit sequence it generated. The modules enable the invocation of the tests through a standard interface.

### 5.1.6 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The *Remote Key Management Service Provider* may use the enduser private keys only according to the key usage settings included in the corresponding *Certificate*.

## 5.2 Private Key Protection and Cryptographic Module Engineering Controls

The *Remote Key Management Service Provider* ensures the secure management of the private keys held by it and prevents the private key disclosure, copy, deletion, modification and unauthorized usage. The *Remote Key Management Service Provider* may only preserve the private keys as long as the provision of the service definitely requires.

### 5.2.1 Cryptographic Module Standards and Controls

The systems of the *Remote Key Management Service Provider* stores the enduser private keys in such secure hardware devices that are compliant with the following:

- the requirements of CEN 419 241-1 [15], and published on the EU Futurium QSCD list [3].

The *Remote Key Management Service Provider* stores the provider and enduser private keys outside of the Qualified Electronic Signature Creation Device only in encrypted form. Only those algorithms and key parameters are used for encoding wichs fizs to the actual algorithmic decision of the National Media and Infocommunications Authority that was issued according to the year 2015. Act CCXXII [7] 92. § (1) b) and that are expected to be able to withstand the cryptographic attacks during the entire lifetime of the keys.

The *Remote Key Management Service Provider* provider private keys are stored in a physically secure site even in an encrypted form, in the safe of the *Data Centre* , where they are only accessible to authorized people.

In case of the weakening of cryptographic algorithms and key parameters, the *Remote Key Management Service Provider* destroys the coded keys or recodes them again using algorithm and key parameters that ensure higher protection.

### 5.2.2 Private Key (N out of M) Multi-Person Control

The *Remote Key Management Service Provider* implements the "n out of m" at the activation of the private key related key management functions. The parameters are determined so that the simultaneous presence of at least two; trusted role holder employees is needed for the critical operations carried out with its provider private keys.

### 5.2.3 Private Key Escrow

The *Remote Key Management Service Provider* does not escrow its provider or enduser private keys.

### 5.2.4 Private Key Backup

The *Remote Key Management Service Provider* makes security copies of its provider private keys, before putting the provider private key into service and the enduser private keys on daily base as described in section 5.2.1. in a protected environment, in the simultaneous presence of at least two people holding trusted roles, with the exclusion of other people. During the backup, the private key leaves the module in an encrypted form, and this encrypted key can be loaded into another module. Both the backup and the restore can only be performed by protection mechanisms described in section 5.2.2..

The *Remote Key Management Service Provider* stores the backup copy in duplicate, and at least one copy of those is stored at a different place from the service provider location.

The same strict security standards are applied to the management and preservation of backups as for the operation of the production system.

### 5.2.5 Private Key Archival

The *Remote Key Management Service Provider* does not archive its provider private keys and the enduser private keys of the *Client*s.

### 5.2.6 Private Key Transfer Into or From a Cryptographic Module

All of the provider private keys of the *Remote Key Management Service Provider* and the enduser keys managed by the *Remote Key Management Service Provider* are created in a Qualified Electronic Signature Creation Device that meets the requirements.

The private keys do not exist in an open form outside of the Qualified Electronic Signature Creation Device.

The *Remote Key Management Service Provider* only exports the private key from the Qualified Electronic Signature Creation Device for the purpose of making a secure copy.

The export and loading of the provider private keys is performed according to section 5.2.2.

### 5.2.7 Private Key Storage on Cryptographic Module

The *Remote Key Management Service Provider* keeps its private keys used for Remote Key Management Service provision and the enduser keys managed by the *Remote Key Management Service Provider* in Qualified Electronic Signature Creation Devices according to section 5.2.1.

Private keys are stored and used in the Qualified Electronic Signature Creation Device as specified in the certification of the device with full compliance with the related operating instructions.

### 5.2.8 Method of Activating Private Key

The *Remote Key Management Service Provider* keeps its provider private keys in a secure Qualified Electronic Signature Creation Device and complies with its user guide and the requirements outlined in the certification documents. The Qualified Electronic Signature Creation Device can only be activated by the corresponding operator cards and the private keys within the Qualified Electronic Signature Creation Device can not be used before activating the module. The *Remote Key Management Service Provider* keeps the operator cards in a safe environment and those cards can be only reached by entitled employees of the *Remote Key Management Service Provider*.

### 5.2.9 Method of Deactivating Private Key

The private key used by the *Remote Key Management Service Provider*, and managed by the cryptographic devices becomes deactivated if (in a regular or irregular way) the device is removed from active status. This can happen in the following cases:

- the user deactivates the key,
- the power supply of the device is interrupted (switched off or power supply problem),
- the device enters an error state.

The private key deactivated like this can not be used until the module is in active state again.

### 5.2.10 Method of Destroying Private Key

The discarded, expired or compromised *Remote Key Management Service Provider*'s private keys are destroyed in a way that makes further use of the private keys impossible.

The *Remote Key Management Service Provider* destroys the provider private keys stored in the secure Qualified Electronic Signature Creation Device of the according to the procedures, requirements defined in the user guide and in the certification documents of the used Qualified Electronic Signature Creation Device, in the simultaneous presence of two *Remote Key Management Service Provider* employees (an infrastructure administrator and a security officer) with the exclusion of other persons.

The *Remote Key Management Service Provider* destroys each backup copy of the private key in a documented way in such a way that its restoration and usage becomes impossible.

### 5.2.11 Cryptographic Module Rating

According to the requirements of Section 5.2.1 the *Remote Key Management Service Provider* manages the end user private keys in a cryptographic module that

- has an at least EAL-4 level Common Criteria [17] based device certificate attesting compliance with the requirements of the CEN 419 241-1 [15], and published on the EU Futurium QSCD list [3].

## 5.3 Other Aspects of Key Pair Management

### 5.3.1 Certificate Operational Periods and Key Pair Usage Periods

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

If this happens, the *Remote Key Management Service Provider* revokes the related *Certificate*s. The *Remote Key Management Service Provider* destroys the enduser private keys which belong to the revoked *Certificate*s.

## 5.4 Activation Data

### 5.4.1 Activation Data Generation and Installation

The *Remote Key Management Service Provider*'s private keys are protected in accordance with the procedures, requirements defined in the used Qualified Electronic Signature Creation Device user guide and the certification documents.

In case of password based activation data usage, the passwords are sufficiently complex in order to ensure the required level of protection.

### 5.4.2 Activation Data Protection

The employees of the *Remote Key Management Service Provider* manage the private key activation devices and the activation data securely, protect them using technical and organizational measures and passwords are stored in encrypted form only.

### 5.4.3 Other Aspects of Activation Data

No stipulation.

## 5.5 Computer Security Controls

### 5.5.1 Specific Computer Security Technical Requirements

During the configuration and operation of its IT system of the *Remote Key Management Service Provider* ensures the compliance with the following requirements:

- the user identity is verified with two-factor authentication controls by using VPN certificates stored on the card before granting access to the system or the application;
- roles are assigned to users and it ensures that all users only have permissions appropriate for his or her roles;
- a log entry is created for every transaction, and the log entries are archived;
- for the security-critical processes it is ensured that the internal network domains of the *Remote Key Management Service Provider* are sufficiently protected from unauthorized access;
- proper procedures are implemented to ensure service recovery after loss of key or system failure.

### 5.5.2 Computer Security Rating

Microsec highlights the importance of *Client* experience. In order to maintain a high level of services, the *Remote Key Management Service Provider* has been operating a quality control system compliant with the ISO 9001 standard since January 23, 2002. Compliance with the standard has been verified by Lloyd's Register Quality Assurance.

Microsec assigns high priority to the security of the systems it operates, and has therefore been operating an information security management system that is compliant with ISO/IEC 27001 (formerly known as BS 7799) in its main areas of activity since May 19, 2003. Compliance with the standard has been verified by Lloyd's Register Quality Assurance.

The scope of both the quality control system and the information security management system cover the trust services provided by Microsec.

Microsec has two level risk assessment which covers beyond the information technology risks the whole organization including also the business risks. The risk assessment is updated at least yearly. Based on the results of the risk assessment the *Remote Key Management Service Provider*

- sets up new measures to eliminate the vulnerabilities, or/and
- accepts the identified residual risks by stating the reason of the decision.

## 5.6 Life Cycle Technical Controls

### 5.6.1 System Development Controls

The *Remote Key Management Service Provider* only uses applications and devices in its production IT system that are:

- commercial boxed software, designed and developed by a documented design methodology, or;
- custom hardware and software solutions developed by the *Remote Key Management Service Provider* itself during which design structured development methods and controlled development environment were used, or;

- custom hardware and software solutions developed by a reliable party for the *Remote Key Management Service Provider* during which design structured development methods and controlled development environment were used, or;
- open source software which comply with the security requirements and their adequacy is ensured by software verification and structured development and life-cycle management.

Procurement of IT tools is performed in a way that excludes changes to the hardware and software components using reliable, regularly qualified suppliers.

The hardware and software components applied for the provision of services are not used for other purposes by the *Remote Key Management Service Provider*.

The *Remote Key Management Service Provider* prevents the malicious software from entering into the devices used for certification services with appropriate security measures.

The hardware and software components are checked regularly for malicious software prior the first usage, and subsequently.

The *Remote Key Management Service Provider* acts with the same carefulness in case of program update purchases as at the acquisition of the first version.

The *Remote Key Management Service Provider* employs reliable, adequately trained staff over the course of installing software and hardware.

The *Remote Key Management Service Provider* only installs softwares to its service provider IT equipment necessary for the purpose of service provision.

The *Remote Key Management Service Provider* has a version control system where every change of the IT system is documented.

The *Remote Key Management Service Provider* operates automatic monitoring system to record all unauthorized changes, which records all changes in every file and in case of changes in the monitored files it generates a log entry or sends an alert to the system operators.

### 5.6.2 Security Management Controls

The *Remote Key Management Service Provider* implements processes for documenting, operating, verifying, monitoring and maintaining the systems used in the service including their modification and further development. The version control system detects any kind of unauthorized changes, data entry that affects the system, the firewall, the routers, programs and other components used in the service. Installing the program used in the service the *Remote Key Management Service Provider* ensures that the program to be installed is the proper version and that it is free from any unauthorized modification. The *Remote Key Management Service Provider* regularly checks the integrity of the software in its system used in the service.

Each Qualified Electronic Signature Creation Device applied by the *Remote Key Management Service Provider* has been verified, tested and evaluated. The *Remote Key Management Service Provider* verifies the integrity of the modules:

- following the acquisition of the devices during the takeover,
- immediately before the first usage,
- regularly during operation.

The *Remote Key Management Service Provider* deletes the provider keys from the Qualified Electronic Signature Creation Devices permanently or temporarily withdrawn from use.

The *Remote Key Management Service Provider* stores the unused Qualified Electronic Signature Creation Devices at a physically protected location.

### 5.6.3 Life Cycle Security Controls

The *Remote Key Management Service Provider* ensures the protection of the used Qualified Electronic Signature Creation Devices during their whole life cycle.

During the operation of the IT equipment and systems used for the provision of the services, the *Remote Key Management Service Provider* takes into account the security aspects related to the life cycle of the equipment, according to which:

- it uses properly certified Qualified Electronic Signature Creation Devices in its systems;
- ensure, upon receipt of the Qualified Electronic Signature Creation Devices, that the quality control ensures that that the protection of the Qualified Electronic Signature Creation Devices against tampering was ensured during transportation;
- it stores the Qualified Electronic Signature Creation Devices in a safe place, and ensure the protection of the Qualified Electronic Signature Creation Devices against tampering during storage;
- continuously complies with the requirements set out in the Qualified Electronic Signature Creation Device's security target, instructions for use and certification report during operation;
- deletes the private keys stored in their decommissioned Qualified Electronic Signature Creation Devices in such a way that it becomes practically impossible to restore the keys;
- handle and dispose of decommissioned Qualified Electronic Signature Creation Devices in accordance with the requirements of its security target, instructions for use and certification report.

## 5.7 Network Security Controls

The *Remote Key Management Service Provider* keeps its IT system configuration under strict control, and it documents every change including the smallest modification, development, software update too. The *Remote Key Management Service Provider* implements proper procedures for the detection of any hardware or software change, system installation, and maintenance occurred on the IT system. The *Remote Key Management Service Provider* checks the authenticity and integrity of every software component at their first loading.

The *Remote Key Management Service Provider* applies proper network security measures for example:

- divides its IT system into well separated security zones;
- separates dedicated network for administration of IT systems and the *Remote Key Management Service Provider*'s operational network;

- separates the production systems for the TSP services from systems used in development and testing;
- establishes communication between distinct trustworthy systems only through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure;
- operates the IT systems used for the live operational network in secure network zones;
- restricts access and communications between zones to those necessary for the operation of the Remote Key Management Service;
- disables the not used protocols and user accounts;
- disables unused network ports and services ;
- only runs network applications unconditionally necessary for the proper operation of the IT system .
- reviewes the established rule set on a regular basis.

The *Remote Key Management Service Provider* undergoes or performs a vulnerability scan on public and private IP addresses:

- within one week of receiving a request from the CA/Browser Forum;
- after any system or network changes that the CA determines are significant;
- at least every three (3) months.

The *Remote Key Management Service Provider* checks the compliance of the local network components (e.g. routers) configuration with the requirements specified by the *Remote Key Management Service Provider* at least every three months.

The *Remote Key Management Service Provider* orders a penetration test from an external independent expert who has the necessary skills, tools, proficiency and code of ethics to provide a reliable report yearly and in case of a significant change in the IT network.

## 5.8 Time-stamping

For the protection of the integrity of the log files and other electronic files to be archived the *Remote Key Management Service Provider* uses qualified electronic *Time Stamp*s issued by the e-Szignó Certificate Authority.

# 6 Compliance Audit and Other Assessments

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

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

- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [1];
- ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers; [12]
- ETSI EN 319 401 V2.2.1 (2018-04); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [11]
- ETSI TS 119 431-1 V1.1.1 (2018-12) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev [14]

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 *Remote Key Management Service Provider*.

The *Remote Key Management Service Provider* applies verified and certified elements (electronic signature production IT system elements) in connection with the service.

The *Remote Key Management Service Provider* offers the Remote Key Management Service by using the following *Qualified Electronic Signature Creation Device*:

- distributed remote Qualified Signature Creation Device (drQSCD) v1.0
  (Supplier: I4P.informatikai Kft. (I4P Ltd.))

Before using *Qualified Electronic Signature Creation Device*, the *Remote Key Management Service Provider* makes sure that it has a valid device certificate that meets the current requirements.

The *Remote Key Management Service Provider* manages the *Qualified Electronic Signature Creation Device* throughout its life cycle in accordance with the requirements in the appendix to the device certificate.

The *Remote Key Management Service Provider* monitors the certification status of the used *Qualified Electronic Signature Creation Device*s at least until the end of the validity period of the last *Certificate* issued on them and takes appropriate measures in case of modification of this status.

In case of the revocation of the *Qualified Electronic Signature Creation Device*'s device certificate the *Remote Key Management Service Provider* request the revocation all the valid *Certificate*s issued on that *Qualified Electronic Signature Creation Device* in which *Certificate*s the "id-etsi-qcs 4" statement was set.

The actual list of the *Qualified Electronic Signature Creation Device*s used by the *Remote Key Management Service Provider* and the information related to its certification can be found on the web page of the *Remote Key Management Service Provider* on the following link:

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

The informativ full list of the certified *Qualified Electronic Signature Creation Device*s can be found on the web page of the European Commission. [1]

The *Remote Key Management Service 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 *Remote Key Management Service 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 *Remote Key Management Service 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 *Remote Key Management Service 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. (see section: 1.3.1.)

## 6.1 Frequency or Circumstances of Assessment

The *Remote Key Management Service Provider* has the conformance assessment carried out annually on its IT system performing the provision of the Remote Key Management Services .

## 6.2 Identity/Qualifications of Assessor

The *Remote Key Management Service Provider* performs the internal audits with the help of its employees who hold the independent system auditor role.

The eIDAS and ETSI conformity assessment is performed by an organization, which has a qualifying mandate issued by the national accreditation organization of an EU Member State.

## 6.3 Assessor's Relationship to Assessed Entity

External audit is performed by a person who:

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

- is independent from the owners, management and operations of the examined *Remote Key Management Service Provider*;
- is independent from the examined organization, namely neither himself or herself nor his or her immediate relatives have any employment or business relationship with the *Remote Key Management Service Provider*.
- remuneration is not dependent on the findings of the activities carried out during the audit.

## 6.4 Topics Covered by Assessment

The review covers the following areas:

- compliance with the legislation currently in force;
- compliance with technical standards;
- compliance with the Certification Policy and the *Remote Key Management Practice Statement*;
- adequacy of the employed processes;
- documentation;
- physical security;
- adequacy of the personnel;
- IT security;
- compliance with the data protection rules.

## 6.5 Actions Taken as a Result of Deficiency

The independent auditor summarizes the result of the screening in a detailed screening report that covers the tested system components, processes, and contains the evidence used in the screening and the auditor statements. The discrepancies revealed during the examination and the deadlines set for correcting them are recorded in a separate chapter of the report.

The independent auditor may record based on their severity the differences and discrepancies revealed during the examination:

- modification suggestions to be optionally taken into consideration;
- derogations to be averted mandatorily.

The independent auditor shall report the revealed serious derogations without delay to the National Media and Infocommunications Authority that is authorized to take the necessary measures.

The *Remote Key Management Service Provider* shall answer the problems stated by the independent auditor in writing, and to report the measures taken to avert them at the occasion of the next authority review.

The independent auditor shall send the assessment report in each case to the National Media and Infocommunications Authority.

### 6.6 Communication of Results

The *Remote Key Management Service Provider* publishes the summary report of the assessment on its web page on the following url:

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

The *Remote Key Management Service Provider* doesn't publish the detailes of the findings, they are treated as confidential information.

## 7 Other Business and Legal Matters

### 7.1 Fees

The *Remote Key Management Service Provider* publishes fees and prices on its webpage, and makes them available for reading in printed form at its customer service.

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

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

#### 7.1.1 Refund Policy

See section: 7.1.

### 7.2 Financial Responsibility

In order to facilitate trust the *Remote Key Management Service Provider* takes financial responsibility to fulfil all its obligations defined in the present *Remote Key Management Practice Statement*, the related *Trust Service Policy* and the service agreement concluded with the *Client*.

#### 7.2.1 Insurance Coverage

The *Remote Key Management Service Provider* has sufficient financial resources for its responsibilities related to the provision of services and for providing the costs related to its termination.

#### 7.2.2 Insurance or Warranty Coverage for End-entities

- The *Remote Key Management Service Provider* has liability insurance to ensure reliability.
- The liability insurance covers the following damages caused by the *Remote Key Management Service 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 *Remote Key Management Service 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 provides coverage for the full damage of the aggrieved party – up to the liability limit – arising in context of the harmful behaviour of the *Remote Key Management Service 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.

## 7.3 Confidentiality of Business Information

The *Remote Key Management Service Provider* manages clients' data according to legal regulations. The *Remote Key Management Service Provider* has a data processing regulation (see section 7.4), which addresses the processing of personal data in particular.

By signing the service agreement, *Client*s consent to the *Remote Key Management Service Provider* retaining and processing their personal data (in a manner that complies with the data processing regulations). Such consent applies to the forwarding of information specified by law and entered in records to third parties in case the *Remote Key Management Service Provider*'s services go offline; moreover to forwarding such information to the *Remote Key Management Service Provider*'s subcontractors – solely for the purpose of performing tasks associated with providing the service.

The *Remote Key Management Service Provider* uses clients' data solely in connection with the provision of its services. The *Remote Key Management Service Provider* retains data of which it becomes aware in accordance with statutory requirements, and for the stipulated period of time. In the course of retaining data, the *Remote Key Management Service Provider* sees to the intactness, confidentiality, and secure storage of information. It only permits accessing information to individuals whose tasks justify this.

The *Remote Key Management Service Provider* provides for the confidentiality and intactness of information that is not public during the forwarding of *Client*s' data.

### 7.3.1 Scope of Confidential Information

The *Remote Key Management Service Provider* treats as confidential:

- all *Client* data, with the exception of those that qualify as information not considered confidential in section 7.3.2;
- besides the *Client* data:

- transaction related data and log data,
- non-public regulations,
- all data whose public disclosure would have an adverse effect on the security of the service.

### 7.3.2 Information Not Within the Scope of Confidential Information

The *Remote Key Management Service Provider* considers all data public that can be obtained from a public source, or to the disclosure of which the *Subscriber* gave its consent in writing beforehand.

### 7.3.3 Responsibility to Protect Confidential Information

The *Remote Key Management Service Provider* is responsible for the protection of the confidential data it manages.

The *Remote Key Management Service Provider* obliges its employees, subcontractors, affiliated partners to protect all confidential data by signing declaration of confidentiality or by contract.

The *Remote Key Management Service Provider* processes confidential information it comes to possess according to the provisions of Act CXII of 2011. on the Right to Freedom Of Information, and only discloses it to persons/organizations in the following case:

- **Information provision for authorities**

  For the purpose of investigating or preventing acts of crime committed using the trusted services it provides, as well as in the case of national security related interests, the *Remote Key Management Service Provider* – if the statutory criteria applicable to data requests are met – discloses the related identity information and the information verified by the *Remote Key Management Service Provider* according to the section (1) of the Eüt. [7] 90. § to investigating authorities and national security services free of charge.

  The *Remote Key Management Service Provider* records the fact of data transfers, but does not inform involved clients about it.

- **Disclosure upon owner's request**

  Upon a *Client*'s personal request to do so or on the basis of its authorisation granted officially, in writing, the *Remote Key Management Service Provider* reveals confidential user information pertaining to the *Client* to third parties.

## 7.4 Privacy of Personal Information

The *Remote Key Management Service Provider* takes care of the protection of the personal data it manages, the operation and regulations of the *Remote Key Management Service Provider* comply with the requirements of the Act CXII of 2011. on the Right to Freedom Of Information [5] and the 2016/679 EU General Data Protection Regulation [2].

The *Remote Key Management Service Provider*:

- preserves,
- upon expiry of the obligation to retain – unless the *Client* otherwise indicates – deletes from the client database

the registered personal data and information on the *Client* in accordance with the legal requirements.

The *Remote Key Management Service Provider* stores identification data, data about the *Subscriber* associated with contact details and data connected to the provision of the service in its records.

The *Remote Key Management Service Provider* hands over *Client* data to third parties solely in cases where this is stipulated by a legal regulation or if the *Client* has granted its consent to this in writing.

### 7.4.1 Privacy Plan

The *Remote Key Management Service Provider* has a Privacy Policy and a Privacy Notice document, which contain detailed regulations on the handling of personal data.

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

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

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

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

### 7.4.2 Information Treated as Private

The *Remote Key Management Service Provider* protects all personal data related to the data subject or containing conclusions on the data subject that cannot be accessed publicly from public data source.

The *Remote Key Management Service Provider* collects data of the *Subscriber* only with its explicit prior consent and only to that extent which is necessary for the provision of the Remote Key Management Service.

### 7.4.3 Information Not Deemed Private

The *Remote Key Management Service Provider* need not treat as confidential information those personal data that can be accessed from a public source.

### 7.4.4 Responsibility to Protect Private Information

The *Remote Key Management Service Provider* stores securely and protects the personal data it manages. The data is protected by appropriate measures in particular against unauthorized access, alteration, and against disclosure.

The *Remote Key Management Service Provider* is generally responsible to comply with the requirements described in its Privacy policy and its liability extends to activities carried out by the subcontractors too.

### 7.4.5 Notice and Consent to Use Private Information

The *Remote Key Management Service Provider* only uses the personal data of the *Client* to the extent required for Remote Key Management Service provision, to contact the *Client*.

### 7.4.6 Disclosure Pursuant to Judicial or Administrative Process

In cases defined in the relevant legislation the *Remote Key Management Service Provider* may disclose the stored personal data about the *Client* without notifying the *Client*.

### 7.4.7 Other Information Disclosure Circumstances

No stipulation.

## 7.5 Intellectual Property Rights

During its business operation, the *Remote Key Management Service Provider* shall not harm any intellectual property rights of a third person.

The present *Remote Key Management Practice Statement* is the exclusive property of the *Remote Key Management Service Provider*. The *Client*s and other *Relying Parties* are only entitled to use the document according to the requirements of the present *Remote Key Management Practice Statement* and any other use for commercial or other purposes is strictly prohibited.

The present *Remote Key Management Practice Statement* may be freely distributed in unchanged form, in full length and with the indication of origin.

The rules of the application of the software provided for the use of the Remote Key Management Service by the *Remote Key Management Service Provider* is accessible in the description of the software and it is included in the user's guide referenced in the description.

## 7.6 Representations and Warranties

### 7.6.1 CA Representations and Warranties

**Certification Authority's Responsibility**

The responsibility of the *Remote Key Management Service Provider* is in the *Remote Key Management Practice Statement*, the related *Certificate Policies*, and the service agreement with the *Client* and its attachments.

- The *Remote Key Management Service Provider* assumes responsibility for compliance with the procedures described in *Certificate Policies* it supports;
- The *Remote Key Management Service Provider* assumes responsibility as its own for the damages caused during the provision of the Remote Key Management Service by its subcontractors;
- The *Remote Key Management Service Provider* is liable under the rules of liability for breach of contract in the Civil Code of the Republic of Hungary [6] in relation to the *Client*s which are in a contractual relationship with it.

- The *Remote Key Management Service Provider* is liable under the rules of causing damage outside of contract in the Civil Code of the Republic of Hungary [6] in relation to third parties (such as the *Relying Party*) that are not in a contractual relationship with it.
- The *Remote Key Management Service 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 7.8.).
- 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 *Remote Key Management Service Provider* is not responsible:

- for the certificate verification and usage activities of the *Relying Parties*;
- for the regulations issued by the *Relying Parties* or others.

**Certification Authority Obligations**

The *Remote Key Management Service Provider* shall fulfil the requirements defined in section (2) of article 24. of the eIDAS regulation [1].
The *Remote Key Management Service Provider*'s basic obligations is that it shall provide the Remote Key Management Service in line with the *Trust Service Policy*, this *Remote Key Management Practice Statement*, the General 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 ( 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.

### 7.6.2 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 *Remote Key Management Service Provider* while using the Remote Key Management Service .

The obligations of the *Subscriber* are determined by this *Remote Key Management Practice Statement*, the service agreement, the General Terms and Conditions, as well as the relevant *Trust Service Policy*.

***Subscriber* Rights**

- *Subscriber*s have the right to use the services in accordance with this *Remote Key Management Practice Statement*.

### 7.6.3 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 *Certificate* and *Time Stamp*s. During the verification of the validity for keeping the security level guaranteed by the *Remote Key Management Service 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 *Trust Service Policy* and the corresponding *Remote Key Management Practice Statement*;
- use reliable IT environment and applications;
- verify the revocation status of all *Certificate*s based on the current CRL or OCSP response;
- take into consideration every restriction which is included in the *Remote Key Management Practice Statement* and in the corresponding *Trust Service Policy*.

### 7.6.4 Representations and Warranties of Other Participants

No stipulation.

## 7.7 Disclaimers of Warranties

The *Remote Key Management Service Provider* excludes its liability if:

- the *Client*s do not follow the requirements related to the management of the private key and the activation data;
- az *Client*s can't access Remote Key Management Service due to a reason which is out of the responsibility of the *Remote Key Management Service Provider*;
- it is unable to provide information or fulfil communication obligations due to the problems of the Internet, or part of it;

- the damage comes from a vulnerability or error of the cryptographic algorithms accepted by the National Media and Infocommunications Authority algorithmic decree.

## 7.8 Limitations of Liability

The *Remote Key Management Service 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.

## 7.9 Indemnities

### 7.9.1 Indemnification by the *Remote Key Management Service Provider*

The detailed rules of the indemnities of the *Remote Key Management Service Provider* are specified in this regulation (see section: 7.8. ), the service agreement and the contracts concluded with the *Client*s.

### 7.9.2 Indemnification by Subscribers

The *Subscriber* and the Subject are liable for damages to the *Remote Key Management Service Provider* for the loss or damage caused by non-compliance with their obligations and the relevant recommendations.

### 7.9.3 Indemnification by Relying Parties

See section: 7.8.

## 7.10 Term and Termination

### 7.10.1 Term

The effective date of the specific *Remote Key Management Practice Statement* is specified on the cover of the document.

### 7.10.2 Termination

The *Remote Key Management Practice Statement* is valid without a time limit until withdrawal or the issuance of the newer version of the *Remote Key Management Practice Statement*.

### 7.10.3 Effect of Termination and Survival

In case of the withdrawal of the *Remote Key Management Practice Statement* the *Remote Key Management Service Provider* publishes the detailed rules of the withdrawal and the rights and obligations persisting after withdrawal on its webpage.

The *Remote Key Management Service Provider* guarantees that in case of a the *Remote Key Management Practice Statement* withdrawal, requirements for the protection of the confidential data remain in effect.

## 7.11 Individual Notices and Communications with Participants

The *Remote Key Management Service Provider* maintains a customer service in order to contact with its *Client*s.

The *Client*s may make their legal declarations to the *Remote Key Management Service Provider* solely in writing, and in executed form. Executing in representation of an organisation shall only be valid together with certification of such right of representation.

The e-Szignó Certificate Authority informs its *Client*s by means of publication on its webpage or in electronic mail.

## 7.12 Amendments

The *Remote Key Management Service Provider* reserves the right to change the *Remote Key Management Practice Statement* in a controlled way in case of the change of normative rules, security requirements, market conditions or other circumstances.

### 7.12.1 Procedure for Amendment

The *Remote Key Management Service Provider* only discloses those of its procedures in its public domain regulations whose knowledge does not jeopardize the security of the services. The *Remote Key Management Service Provider* has a number of internal security and other regulations, as well as operative level stipulations which it treats in confidence (this certificate practice statement mentions several such). The procedures described in section 6.4. audit these documents as well.

A team responsible for maintaining regulations and documentation operates within the *Remote Key Management Service Provider*'s organization. This team collects change requests, carries out modifications, and meets any internal and external information provision related obligations. The statement is approved by the director of the e-Szignó Certificate Authority.

The team produces internal, non-public working copies of the regulations as it collects changes, and these undergo internal review before being published. The *Remote Key Management Service Provider* strives to only issue new regulations at the least frequent intervals possible.

The *Remote Key Management Service Provider* reviews the *Remote Key Management Practice Statement* annually or in case of exceptional request for change with priority and performs the necessary changes. The document will receive a new version number even after the smallest change and by taking into account the time required by the endorsement process, the planned date of coming into effect will be determined too.

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

The *Remote Key Management Service Provider* will accept remarks connected to new regulations published for 14 days prior to their becoming effective, at the following email address:

`info@e-szigno.hu`

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

The *Remote Key Management Service Provider* will close and publish the version of the regulation as amended with remarks on the 7th day prior to its becoming effective.

### 7.12.2 Notification Mechanism and Period

The *Remote Key Management Service Provider* notifies the *Relying Parties* of new document version issuances as described in Section 7.12.1..

### 7.12.3 Circumstances Under Which OID Must Be Changed

The *Remote Key Management Service Provider* issues a new version number in case of even the smallest change to the *Remote Key Management Practice Statement*, which is part of the document identifier (OID), so any change to the document will result in an OID change, namely two documents – entered into force – with different content cannot have the same OID.

## 7.13 Dispute Resolution Provisions

The *Remote Key Management Service Provider* aims for the peaceful and negotiated settlement of the disputes arising from its operation. The settlement follows the principle of gradual approach.

The *Remote Key Management Service 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 *Remote Key Management Service Provider* shall be addressed to the customer care centre office in written form. The *Remote Key Management Service 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 *Remote Key Management Service Provider* is obliged to issue a written response to the submitter within the specified time limit. The *Remote Key Management Service Provider* may request the provision of information required for giving a response from the submitter. The *Remote Key Management Service 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 *Remote Key Management Service Provider* involved, the submitter may initiate consultation with the *Remote Key Management Service 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 *Remote Key Management Service 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.

## 7.14 Governing Law

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

## 7.15 Compliance with Applicable Law

The applicable regulations:

- 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];
- (Hungarian) Act CXII of 2011 on the Right to Freedom Of Information [5];
- (Hungarian) Act V of 2013. on the Civil Code. [6].
- (Hungarian) Act CCXXII of 2015 on electronic administration and the general rules of trust services [7];
- (Hungarian) Ministry of Interior Decree 24/2016. (VI. 30.) on the requirements for trust service providers and their services [8];
- (Hungarian) Ministry of Interior Decree 25/2016. (VI. 30.) on the administrative service fees paid to the trust service supervisory body and on fee rates [9];
- (Hungarian) Government Decree 470/2017. (XII. 28.) on the announcement according to trust services and on the content of registers maintained by the trust service supervisory body [10];

## 7.16 Miscellaneous Provisions

### 7.16.1 Entire Agreement

No stipulation.

### 7.16.2 Assignment

The providers operating according to this *Remote Key Management Practice Statement* may only assign their rights and obligations to a third party with the prior written consent of *Remote Key Management Service Provider*.

### 7.16.3 Severability

Should some of the provisions of the present *Remote Key Management Practice Statement* become invalid for any reason, the remaining provisions will remain in effect unchanged.

### 7.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

The *Remote Key Management Service Provider* is entitled to claim payment for damages and attorney fees for reimbursement of the damages, losses, expenses caused by its partners. If in a particular case the *Remote Key Management Service Provider* does not exercise its claim for damages that does not mean that in similar cases in the future or in case of violation of other provisions of the present *Remote Key Management Practice Statement*, it would waive the enforcement of claims for damages.

### 7.16.5 Force Majeure

The *Remote Key Management Service Provider* is not responsible for the defective or delayed performance of the requirements set out in the *Trust Service Policy* and the *Remote Key Management Practice Statement* if the reason for failure or delay was a condition that is outside the control of the *Remote Key Management Service Provider*.

## 7.17 Other Provisions

No stipulation.

# 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] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) .

[3] Compilation of Member States notification on SSCDs and QSCDs; `https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-`

[4] (Hungarian) Act XXXV of 2001 on Electronic Signatures (repealed from 1st July 2016.) .

[5] (Hungarian) Act CXII of 2011 on the Right to Freedom Of Information .

[6] (Hungarian) Act V of 2013. on the Civil Code .

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

[8] (Hungarian) Ministry of Interior Decree 24/2016. (VI. 30.) on the requirements for trust service providers and their services .

[9] (Hungarian) Ministry of Interior Decree 25/2016. (VI. 30.) on the administrative service fees paid to the trust service supervisory body and on fee rates .

[10] (Hungarian) Government Decree 470/2017. (XII. 28.) on the announcement according to trust services and on the content of registers maintained by the trust service supervisory body .

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

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

[13] ETSI TS 119 312 V1.3.1 (2019-02); Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

[14] ETSI TS 119 431-1 V1.1.1 (2018-12) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev.

[15] CEN EN 419 241-1:2018 (July 2018); Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements.

[16] IETF RFC 3647: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework, November 2003.

[17] Common Criteria for Information Technology Security Evaluation, Part 1 - 3.

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