Policy and Practice Statement

DigiSign Time-Stamping Authority

Qualified Electronic Time-Stamps

compliant with eIDAS Regulation and national legislation

Category:	**Public Document**	Language:	**English**
Written by:	**Policies and Procedures Management Body**		
Verified by:	**Internal Auditor**	Edition:	**2**
Approved by:	**General Manager**	Version:	**3**

OID: **1.3.6.1.4.1.34285.3.1.1.1.1.1.0**

1.3.6.1.4.1.34285.3.1.1.2.3.1.0

DIGISIGN S.A.

74B Nicolae G. Caranfil street, 1st District

014146, Bucharest, Romania

+4 031 620 20 00

+4 031 620 20 80

office@digisign.ro

www.digisign.ro

Document history

Edition	Version	Description	Date	Author
1	0	First release: Policy and Practice Statement for DigiSign Time Stamping Authority, compliant with eIDAS Regulation and national legislation	May 15, 2017	Policies and Procedures Management Body
1	1	Updates as per the recommendations resulted after the audit	June 15, 2017	Policies and Procedures Management Body
1	2	Updating contact information	December 03, 2018	Policies and Procedures Management Body
1	3	Minor updates	July 28, 2020	Policies and Procedures Management Body
2	0	Minor updates	June 25, 2021	Policies and Procedures Management Body
2	1	Minor updates	December 22, 2022	Policies and Procedures Management Body
2	2	Minor updates	October 23, 2024	Policies and Procedures Management Body
2	3	Address update	Decembrie 21, 2024	Policies and Procedures Management Body

Contents

Introduction

DIGISIGN S.A. (hereinafter DigiSign) operates a Public Key Infrastructure (hereinafter PKI) in order to provide trust services qualified electronic signatures, qualified electronic seals and qualified electronic time-stamps. DigiSign PKI is currently using several Root Certification Authorities which have intermediate Certificate Authorities, dedicated to a class or type of service it provides. Within a Certification Authority, there are several certificate profiles used in order to issue a specific type of certificate.

As a Certification Authority (hereinafter CA), DigiSign issues high quality and highly trusted digital certificates to entities including private and public companies and individuals, in accordance with the rules, principles and practices outlined in DigiSign CA Certification Practice Statement (hereinafter CA CPS). In its role as a CA, DigiSign performs functions associated with public-key operations that include receiving requests, issuing, revoking, suspending and renewing digital certificates, as well as maintenance, issuance and publication of Certificate Revocation Lists (hereinafter CRLs) and Online Certificate Status Protocol (hereinafter OCSP), for users within DigiSign PKI.

As a Time Stamping Authority (hereinafter TSA), DigiSign issues high quality and highly trusted time stamps in order to support electronic signatures and application requiring to prove that a datum existed in a specific form before a specific time.

DigiSign is a leading Qualified Trust Service Provider (hereinafter QTSP) which successfully provides trust services such as Qualified Electronic Signatures, Qualified Electronic Seals and Qualified Electronic Time Stamps, and acts as a Trusted Third Party (hereinafter TTP) when it comes to the creation and validation of those services.

1. Scope

DigiSign TSA Policy and DigiSign TSA Practice Statement have been merged into this document which represents a public statement of the policies and practices followed by DigiSign as a Qualified Trust Service Provider, in order to successfully issue, validate and generally administrate time stamps, and is therefore names DigiSign TSA Policy and Practice Statement (hereinafter TSA PPS).

This TSA PPS contains an overview of the polices, practices and procedures that DigiSign employs for its operation as a Time Stamp Authority, in order to issue Qualified Time Stamps (hereinafter QTS), complying with Regulation EU no. 910/2014, by implementing the requirements laid out in ETSI EN 319 421 – Policy and Security Requirements for Trust Service Providers issuing Time Stamps" standard.

This document does not specify the protocols used in order to access DigiSign Time Stamping Authority, how the requirements identified herein can be assessed by an independent entity, the requirements for making such information available to those independent entities or the requirements that must be met by those independent entities.
The TSA PPS is reviewed at least once a year.

2. References

2.1. Normative references

- Regulation EU no. 910/2014 of the European Parliament and of the Council of 22 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

- Regulation EU no. 765/2008
- Romanian Law no. 451/2004 concerning the time stamps
- ETSI EN 319 421 – Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing Time Stamps
- ETSI EN 319 422 - Electronic Signatures and Infrastructures (ESI); Time-stamping protocols and time-stamp token profiles;
- ETSI EN 319 402 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- IETF RFC 3161 – Internet X.509 Public Key Infrastructure Time-Stamp Protocol
- DigiSign CA Certification Practice Statement (hereinafter CA CPS)

2.2. Informative references

- ITU-R TF. 460-6 (2002) – Standard-frequency and time-signal emissions
- IETF RFC 5905 – Network Time Protocol Version 4: Protocol and Algorithm Specifications
- ISO/IEC 19790:2012 – Information technology; Security techniques; Security requirements for cryptographic modules
- ISO/IEC 15408 (part 1 to 3) – Information technology; Security techniques; Evaluation criteria for IT security
- FIPS PUB 140-2 (2001) – Security requirements for cryptographic modules

3. Definitions and abbreviations

3.1. Definitions

- **Coordinated Universal Time**: Time scale based on the second as defined in Recommendation ITU-R TF.460-6. For all practical purposes, UTC is equivalent to the solar time average in the prime meridian (0°). More specifically, UTC is a compromise between the highly stable atomic time (Temps Atomique International - TAI) and the solar time derived from the irregular Earth rotation. The UTC is the principal standard of the hour by which the world regulates clocks and the time.
- **Datum**: The data that has been time-stamped.
- **Network Time Protocol**: is a networking protocol for clock synchronization of computer systems over network packet routing with variable latency. The standard for reference is the IETF RFC 1305 (Network Time Protocol (NTP v3)).
- **Relying Party**: The recipient of a time-stamp who relies on that time-stamp.
- **Time-Stamping Authority**: The authority managed by a TSP which provides time-stamping services using one or more time-stamping protocols.
- **Subscriber**: A legal or a natural person to whom a time-stamp is beeing issued to.
- **Time-Stamp**: Data in electronic form which binds other electronic data to a specific time, providing evidence that these data existed at that particular moment in time.
- **Time-Stamp Policy**: A set of rules that indicate the applicability of a time-stamp to a community and/or class of application with common security requirements.
- **Time-Stamping Unit**: The set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time.
- **Trust Service Provider**: The entity which provides one or more trust services.
- **TSA Disclosure Statement**: A set of public statements concerning the policies and practices of a TSA which particularly requires emphasis in the disclosure to Subscribers and Relying Parties, for example to meet regulatory requirements.
- **TSA Practice Statement**: A public statement of the practices that a TSA employs in issuing a time-stamp.

- **TSA System**: A set of IT products and components employed to provide support to the provision of time-stamping services.
- **UTC (k)**: A time scale given by the laboratory „k" and which has a close relaton to the UTC, with the goal to reach ± 100 ns.

3.2. Abbreviations

For the purposes of this document, the following abbreviations apply:

ADR	The Authority for the Digitalization of Romania
BIPM	Bureau International des Poids et Mesures
BTSP	Best practices Time-Stamp Policy
CA	Certification Authority
CAB	Conformity Assessment Body
CAR	Conformity Assessment Report
CRL	Certificate Revocation List
DN	Distinguished Name
ETSI	European Telecommunications Standards Institute
GMT	Greenwich Mean Time
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IERS	International Earth Rotation and Reference System Service
IT	Information Technology
PKI	Public Key Infrastructures
SB	Supervisory Body
TAI	International Atomic Time
TCP	Transmission Control Protocol
TSA	Time-Stamping Authority
QTSP	Qualified Trust Service Provider
TST	Time-Stamp Token
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time

4. General concepts

The present documents reference DigiSign CA Certification Practice Statement for the generic policy requirements common to all trust services provided by DigiSign as a Qualified Trust Service Provider.

The policy requirements laid out in the CA CPS and this document are based upon the use of public key cryptography, public key certificates and reliable time sources.

All interested parties, such as Subscribers and Relying Parties, are expected to consult this document in order to obtain details of precisely how DigiSign provides the time-stamping service, and thus to establish the trustworthiness of this service.

4.1. Time Stamping Services (TSS)

The provision of time-stamping services is broken down in the present document into the following component services, for the purposes of classifying requirements:

- Time-Stamping provision: The service component that issues the TSTs;

- Time-Stamping management: The service component that monitors and controls the operation of the time-stamping services, including synchronization with the reference UTC time source, to ensure that the service provided is as specified in this TSA PPS.

DigiSign TSA adheres to the standards and regulations described in Chapter 2 – References of this document, in order to keep trustworthiness of the time-stamping services for Subscribers and Relying Parties.

4.2. Time Stamping Authority (TSA)

DigiSign as a Qualified Trust Service Provider manages a Time-Stamping Authority as part of its Public Key Infrastructure in order to provide to the public time-stamping services. The TSA within DigiSign domain has the overall responsibility for the provision of the time-stamping services, and thus the TSA has the responsibility for the operation of one or more TSUs which creates and signs TSTs on behalf of the TSA. DigiSign TSA may make use of other parties in order to provide parts of the time-stamping services, but the TSA always maintains overall responsibility and ensures that the policy requirements laid out in this document are met.

DigiSign TSA is audited at least every 24 months by a Conformity Assessment Body as defined in point 13 of Article 2 of Regulation EU no. 765/2008. The CAB audits DigiSign TSA and issues a Conformity Assessment Report which DigiSign submits to the Romanian Supervisory Body in order to obtain the qualified status. Upon obtaining the qualified status for the time-stamping services, DigiSign shall duly inform the SB of any change in the provision of this service.

As stated above, DigiSign TSA is identified in the TSU certificate and DigiSign TSA may operate one or more TSUs. Each TSU has a different pair of keys, but the key usage is set to ***digital signature*** and the extended key usage is set to ***timestamping*** only. The validity of the TSU certificate is 12 years. DigiSign TSA is providing only time-stamping services. Within DigiSign domain and under this PPS, no TSU certificate will be used to sign End-Users certificates or other type of certificates.

Below is a table which contains a summary of the current DigiSign TSUs and their issurs:

DigiSign TSU	TSU DN	TSU Issuer	Trusted List
DigiSign Time-Stamping Authority	CN = DigiSign Time Stamping Authority SERIALNUMBER = 200506245DT47 OU = Autoritate de Marcare Temporala - Time Stamping Authority O = DigiSign S.A. L = BUCURESTI C = RO	CN = DigiSign Qualified CA Class 3 2017 OU = DigiSign Certification Services 2.5.4.97 = VATRO-17544945 O = DigiSign S.A. C = RO	EUTL

4.3. TSA Policy and Practices (TSA PPS)

DigiSign Time-Stamp Policy („what is adhered to") and DigiSign TSA Practice Statement („how it is adhered to") have been merged into this one document called DigiSign TSA PPS. This document

specifies a time-stamp policy and practice statement to meet general requirements for trusted time-stamping services as defined by the standards described in Chapter 2 – References of this document.

All DigiSign policies and practice statements, as well as disclosure statements, are under the control of DigiSign CPS Management Body which makes available to the public all documents related to the provision of DigiSign's services at the following address:
www.digisign.ro

This document establishes the general rules concerning the operation of DigiSign TSA. Additional internal and confidential documents define exactly how DigiSign meets the techincal, organizational and procedural requirements identified in relevant standards. Those documents shall not be provided to the public due to their importance regarding the security of DigiSign's operations.

This document is managed by DigiSign through its CPS Management Body. The rules described in Chapter 1.4 – CPS Management of DigiSign CA CPS apply to the TSA PPS as well.

For any additional details regarding the provision of time-stamping services by DigiSign, all interested parties can address DigiSign CPS Management Body at:

DIGISIGN S.A.	
Address:	74B Nicolae G. Caranfil street, 1st District, 014146, Bucharest, Romania
Phone:	+4 031 620 20 00
Fax:	+4 031 620 20 80
E-mail:	office@digisign.ro
Website:	www.digisign.ro

4.4. Subscribers and Relying Parties

Subscribers and Relying Parties are one of the main actors in DigiSign's PKI, as for them the time-stamping services are indented.

4.4.1. Subscribers

The Subscribers are entities that hold a Time-Stamping Service Agreement with DigiSign and they can be either an individual user, either an organization comprising one or several individual users.

If the Subscriber is an individual user (End-User), she/he shall be held directly responsible of its obligations when those are not correctly fulfilled.

If the Subscriber is an organization which comprises one or several individual users, some of the obligations that apply to that organization must apply as well to the individual users. In any case, the organization shall be held responsible for the correct fulfilment of the obligations of its individual users and therefore the organization is expected to suitably inform its individual users about the correct form of use of time-stamps issued by DigiSign TSA and the conditions of the TSA PPS.

4.4.2. Relying Parties

A Relying Party is an entity which acts in reliance of a TST generated under DigiSign TSA PPS and may or may not also be a Subscriber. The RP is fully responsible for the decision of trust or not a time-stamp

and thus has the obligation to identify and be aware of the conditions under which that time-stamp has been issued.

5. Time-Stamp Policies

5.1. Overview

DigiSign TSA issues TSTs in accordance with the requirements of ETSI EN 319 421 standard and the provisions of this document. The TSTs issued by TSUs within DigiSign TSA, have an accuracy of 1 second of UTC or better.

DigiSign TSA issues time-stamps using private keys that are reserved specifically for this purpose. The time-stamps can be requested using the HTTP(S) protocol, as described in RFC 3161.

5.2. Identification

The identifier of this TSA PPS under which DigiSign issues TSTs is: 1.3.6.1.4.1.34285.3.2.4.256.2.1.3.n[1]. By including this OID in all time-stamps generated by DigiSign TSA, DigiSign claims conformance to this time-stamp policy.

5.3. User community and applicaibility

This policy is aimed at meeting the requirements of time-stamp for long term validity (e.g. as defined in ETSI EN 319 122), but it is generally applicable to any use which has a requirement for equivalent quality. This policy may be used for public time-stamping services or timestamping services used within a closed community.

DigiSign time-stamps may be applied through any application which has capabilities of incorporating a time-stamp.

5.4. Conformance

DigiSign references the policy identifier described in section 5.2. of this document in all time-stamps to indicate conformance with this policy. DigiSign TSA is subject to period independent internal and external reviews in order to demonstrate that DigiSign TSA meets its obligations and has implemented appropriate controls as described in this document.

6. Policies and Practices

6.1. Risk assessment

DigiSign TSA performs risk assessments on a regular basis to ensure the quality and reliability of the time-stamping services. Security controls are defined in a security framework of the time-stamping services and they are subject to control at least once at 12 months in order to ensure their efficiency.

6.2. Trust Service Practice Statement

[1] 1 – ISO; 3 – Identified Organization; 6 – DoD; 1 – Internet; 4 – Private; 1 – Enterprise; 34285 – DigiSign's IANA assigned number; n - MMYYYY

Quality assurance is one of the most important values that a Trust Service Provider must have, precisely because they have to ensure the trustworthiness of their system. Therefore, DigiSign has implemented a variety of security controls to ensure quality, performance and operation os the time-stamping service it provides.

All security controls implemented by DigiSign TSA has been documented and are subject to regularly revisions by an independent trustworthy entity, capable to verify the adherence of the security controls.

Additionally, in order to ensure the compliance with ETSI EN 319 421 standard, the following measures, described in this chapter, have been implemented by DigiSign TSA.

6.2.1. Time-Stamp format

DigiSign TSA issues TSTs compliant with RFC 3161 specifications. The time-stamping service uses the RSA algorithm with SHA-256 hash function and a key length of 2048 when generates TSTs.

6.2.2. Time accuracy

DigiSign TSA issues TSTs with an accuracy of 1 second of UTC or better. The time source is provided by ADR's IT system which provides the Romanian official time source, in accordance with Romanian legal framework.

6.2.3. Limitations of the service

As long as the Subscriber has a Time-Stamping Service Agreement concluded with DigiSign TSA, then the time-stamp service provided by DigiSign TSA may be used in relation to any legal transaction, without limitation, unless otherwise specified in the agreement.

Within the limit set by the Romanian Law, defined by th Certificate Policy User Notice and except for fraud or willful misconduct, in no event DigiSign will be liable for:

- any loss of profit or data;
- any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license and performance or non-performance of certificates or electronic signatures;
- any other damages.

DigiSign assumes no financial responsibility for improperly used of time-stamps. No Subscriber or Relying Party which uses time-stamping services provided by DigiSign TSA shall invoke the not-knowing of the conditions of this document.

DigiSign shall cover the damages it might cause due time-stamp services for those who build their moral on the legal effects of the qualified electronic certificates up to the amount of 100 RON for every risk insured. The insured risk represents every damage caused even if there are more such damages following the TSP not fulfilling of the liabilities mentioned by Romanian applicable law.

6.2.4. Subscribers obligations

Refer to *Terms and conditions* at www.digisign.ro.

6.2.5. Relying Parties obligations

Refer to *Terms and conditions* at www.digisign.ro.

6.2.6. Time-Stamp verification

In order to verify a time-stamp issued by DigiSign TSA, the following task have to be successfully completed:

I. Time-Stamp issuer verification

The issuer of a time-stamp is a TSA that has to use appropriate electronic certificates for issuing that time-stamp. The public keys of the stamping certificates are included in the TSU and CA certificates and are published to enable the verification that the time-stamp has been signed correctly by the TSA. The certificates of TSUs within DigiSign domain are available for verification at: www.digisign.ro.

II. Time-Stamp revocation status verification

DigiSign makes available to the interested parties an OCSP service to verify the revocation status of the certificates used by the TSU to sign the time-stamp. The address for accessing the OCSP responder service is included in the certificate of the TSU, used to sign the time-stamp.

III. Time-Stamp integrity verification

In order to verify the integrity of a time-stamp, one has to verify the time-stamp cryptographic integrity, for example if the ASN.1 structure is correct and the datum belongs to the application. This information can be verified through DigiSign TSA web service provided free of charge by DigiSign.

6.2.7. Applicable law

DigiSign provides qualified time-stamping services in accordance with the European and Romanian applicable law, in force. This version of TSA PPS is governed by the following two laws:

- Regulation EU 910/2014 (eIDAS) of the European Parliament and of the Council of 22 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC and
- Romanian Law no. 451/2004 concerning the time stamps.

6.2.8. Service availability

DigiSign TSA has implemented the following measures to ensure availability of the service:

- redundant setup of IT Systems to avoid single point of failures,
- redundant high speed internet connections to avoid loss of service,
- use of uninterruptable power supplies and electric generator.

Although these measures ensure service availability of the DigiSign TSA, it cannot be guaranteed an annual availability of 100%. DIGISIGN TSA aims to provide an availability of the service of 99% per year.

6.3. Terms and conditions

In order to use the time-stamping services provided by DigiSign TSA, the Subscribers and the Relying Parties have to comply with the *Terms and Conditions*, available at www.digisign.ro, which contains information about the limitation of the service, the parties obligations, limitations of liability, as well

as information for Relying Parties. The *Terms and Conditions* are completed by the stipulations of this document.

6.3.1. Implementation of the trust service policy

This document stipulates the requirements concerning the applicable trust service policy as for Chapter 5 – Time-Stamp Policies.

6.3.2. Retention time of logs

As a QTSP, DigiSign stores the event logs in files on the system disk until they reach the maximum allowed capacity. After exceeding the allocated space, the event logs are stored in archives, being available offline. Archived logs are stored for at least 10 years.

6.4. Information of security policy

For the Time-Stamping Authority, DigiSign has implemented an Information Security Policy throughout the company. All employees must adhere to the regulations stated in this policy and the derived security concepts. The Information Security Policy is reviewed on a regular basis and especially when significant changes occur. DigiSign Management approves, if the case, the changes in this policy.

6.5. Obligations

As a QTSP, DigiSign operates a Time-Stamping Authority and assumes the responsibility that the requirements of this document, as well as the provisions of eIDAS and Law no. 451/2004, are implemented as applicable to the selected trusted time-stamp policy.

DigiSign acts as a party to the mutual agreements and obligations between the TSA, Subscribers and Relying Parties. The present TSA PPS and DigiSign CA CPS are integral parts of the Service Agreements concluded between DIGISIGN S.A. and the Subscribers.

6.5.1. TSA obligations

DigiSign TSA undertakes the following obligations:

- To operate in accordance with this document, the CA CPS and other relevant operational policies and procedures,
- To ensure that TSUs maintain a minimum UTC time accuracy of ± 1 second,
- To undergo internal and external reviews in order to assure compliance with relevant legislation and internal policies and procedures,
- To provide high availability access to DigiSign TSA systems, except in the case of planned technical interruptions, loss of time synchronization and causes which excludes the liability.

The conformance with the requirements stated in this document are ensured by DigiSign TSA. An independent Conformity Assessment Body verifies the efficiency of the procedures.

Moreover, DigiSign guarantees that:

- Its commercial activity is provided on the basis of reliable equipment and software,
- The activities and services provided are legally compliant and, in particular, they do not violate intellectual property, licenses and other related rights,
- The services provided are conformant with generally accepted norms,

- The TSTs issued by DigiSign TSA do not contain false data or mistakes,
- That shall maintain a competent and experienced team that can ensure the continuity of the time-stamping services,
- It will ensure on a permanent basis the physical and logical security, as well as the integrity of the materials, software's and databases required for the correct functioning of the TSA, as described in this document,
- It will monitor and control the TSA infrastructure, in order to prevent or limit any disturbance or unavailability of the TSA resulting from deliberate attacks,
- It will take all measures required according to generally accepted norms to secure its services,
- It will make available a backup infrastructure that can be used in case of service interruption of the main infrastructure.

6.5.2. TSA Subscribers' obligations

The Subscribers' obligations regarding the use of DigiSign Time-Stamping Services are described in *Terms and Conditions for Time-Stamping Services* at www.digisign.ro, and they refer to:

- The Subscriber is obligated to verify the signature of the TST and to make sure that the private key used to sign the TST has not been revoked,
- The Subscriber is obligated to use secure cryptographic functions for time-stamping requests,
- The Subscriber is obligated to inform its End-Users (e.g. Relying Parties) about the correct used of time-stamps stated in the TSA PPS.

6.5.3. TSA Relying Parties' obligations

The Relying Parties obligations are defined in the Terms and Conditions for Time-Stamping Services at www.digisign.ro. Before placing any reliance on a time-stamp issued by DigiSign TSA, the Relying Parties must:

- Verify that the TST has been correctly signed with the corresponding key of the TSU certificate and to make sure that the private key used to sign the TST has not been revoked,
- Take necessary measures to ensure the validity of the TST beyond the life-time of the TSU certificates within DigiSign domain,
- Consider any limitations on the usage of the TST indicated by the time-stamp policy,
- Consider any other precautions defined in agreements or other relevant documents.

As the main obligation of a Relying Party is to verify the TST and the electronic signature that comes with it, such verification comprises:

- Verification wheather the signature on the TST is valid,
- Verification of the TSU certificate used to sign the TST, as follows:
  - Verification of the trusted path to the trusted root certificate and for each of the certificate in the chain (including the TSU certificate itself),
  - Verification whether the certificate is not expired at the moment of signing,
  - Verification whether the certificate was not revoked or suspended at the moment of signing – this verification, preferentially, shall be done by OCSP request via the link referenced in the AIA of the time-stamp certificate or, alternatively, by CRL lookup with appropriate software, accessing DigiSign's Public Registry or any other validation method proposed by DigiSign.

The Relying Party should only rely on a TST where the TSU certificate has expired when a non-repudiable proof exists (e.g. another TST) that guarantees that the TST did exist before the expiration of the certificate and that the TST has not changed since. This is specifically of importance when the

cryptographic functions or the TSU certificate key length are not considered secure anymore at the time the party intends to rely on the TST.

Note that DigiSign has a number of different TSU Certificates, signed by different DigiSign CAs. It is important that the Relying Parties refer to the repository of this certificates in order to determine the relevant TSU as this may also impact reliance.

6.6. Liability

DigiSign undertakes to operate the TSA in accordance with the provisions of TSA PPS, CA CPS and the terms of agreements with Subscribers. DigiSign declines any responsibility with regard to the usage that is made with the TSTs it delivers and signs.

DigiSign bears specific liability for damage to Subscribers and Relying Parties in relationship to the valid Qualified Electronic Certificates relied upon, in accordance with specific national laws and regulations.

The liability of DigiSign towards the Subscriber is stipulated in the agreements signed with them. DigiSign is not liable for the mistakes in the verification of the validity of time-stamps or for the wrong conclusions conditioned by omissions or for the consequences of such wrong conclusions. DigiSign shall assume no liability for the loss of value of the validity confirmation proof due to force majeure.

7. TSA Management and Operations

This chapter describes the controls implemented by DigiSign TSA in order to provide trusted non-repudiation services like Qualified Time-Stamps Tokens (QTSTs).

7.1. Introduction

DigiSign has implemented an Information Security Management System to maintain the security of the time-stamping services it provides.

The provision of a TST in response to a request, is at the discretion of DigiSign TSA, depending on the Subscriber's agreement.

7.2. Internal organization

DigiSign's organizational structure, policies, procedures and controls are applicable to DigiSign TSA, being described in CA CPS.

The organizational procedures comply with the rules and regulations defined in section 2.1. – Normative references of this document.

7.3. Trusted personnel

The practices defined in section 5.2. – Procedural controls and section 5.3. – Personnel controls of DigiSign CA CPS are applicable.

As for the personnel managing the CAs within DigiSign domain, the persons managing DigiSign TSA are trustworthy and free of conflict of interests that might prejudice the impartiality of the TSA operations.

7.4. Asset management

The practices identified in section 5.1. – Physical security controls of DigiSign CA CPS are applicable.

All systems (software and hardware) used by the time-stamping service, are clearly identified, categorized and filed in an asset management database according to the Classification, Labeling and Information Management Procedure. All media is handled securely and the data from disposed media is securely deleted, either by an electronic erase of data or by physically destroying the disposed media.

7.5. Access control

The practices defined in section 5.2. – Procedural controls and section 5.1. – Physical security controls of DigiSign CA CPS are applicable.

Different security layers in relation to physical and logical access ensure a secure operation of the time-stamping service (e.g. firewalls, secured physical environment etc). In case a person which carries out operations for the time-stamping services, changes the role or leaves the organization, all the security tokens from that person are withdrawn immediately.

7.6. Cryptographic controls

This chapter defines the rules under which DigiSign TSA generates and manages the cryptographic key pair of a TSU, as well as associated technical requirements.

7.6.1. TSU key generation

The key pair generation of a TSU is a critic process given that the way how a key pair is generated is essential to the safety of the entire PKI system. DigiSign TSA ensures that any TSU cryptographic key is generated under controlled circumstances and in accordance with the industry's best practices for key lifecycle, key length and algorithms.

DigiSign generates the pair of cryptographic keys used in its TSA services under M out of N control by authorized personnel in a physically secured environment, within a Hardware Security Module (HSM) that is certified as being compliant with FIPS 140-2 Level 2, 3 standard or with ISO 15408 Common Criteria EAL 4, 5 standards.

Thus, the pair of keys is generated and exists throughout the entire lifetime in a physically and electromagnetically protected environment. The private key is permanently kept in an encrypted format on the HSM device and never leaves the device in an unencrypted format.

All actions taken when the key pair is generated are recorded, dated and signed by each person present during the ceremony. Records are kept for audit reasons or for regular system verifications.

After the key pair is generated and the private key is activated in the HSM, it can be used in cryptographic operations until its validity period expires or until it is compromised.

The TSUs within DigiSign domain uses RSA key pairs with a length of 2048-bit and the private key is only used for signing TSTs.

7.6.2. TSU private key protection

The practices of TSU key protection, storage, backup and recovery, described in section 6.2. – Private key protection and cryptographic module engineering controls of DigiSign CA CPS are applicable.

The TSU private key shall be backed up and stored for the unlikely event of key loss due to unexpected power interruption or hardware failure. A key backup shall be obtained during the Key Generation Ceremony. The backup of the private key is kept in secret and its integrity and authenticity is preserved in a safe box.

7.6.3. TSU public key

DigiSign TSA guarantees the integrity and authenticity of the TSU signature verification keys, as follows:

- TSU public key is available to Subscribers and Relying Parties at www.digisign.ro,
- TSU does not issue a time-stamp before it verifies the certificate chain,
- Each TSU has its one private key,
- The period of validity of a TSU certificate is being updated periodically and the CRLs or OCSP services are available with the references located in the certificates.

DigiSign TSA issues Qualified Time-Stamps as per eIDAS Regulation and the TSU certificate is issued by DigiSign Qualified CA Class 3 2017 under ETSI EN 319 411-2 certificate policy.

7.6.4. TSU rekey

The lifetime of the TSU certificates is no longer than the period of time that the chosen algorithm and key length are recognized as being fit for the purpose.

Only one certificate is issued to any specific TSU key. TSU certificates are not renewed.

7.6.5. End of TSU key life cycle

DigiSign TSA ensures that TSU private signing keys are not used beyond the end of their life cycle. In particular, operational and technical procedures are in place to ensure that a new key is put in place when a TSU's key usage period expires, and that TSU private keys or any part, including any copies are destroyed such that the private key cannot be retrieved. The TST generation system shall reject any attempt to issue a TST if the signing private key is expired or if the signing private key usage period is expired.

7.6.6. Life cycle management of cryptographic module

DigiSign has in place procedures to ensure that hardware security modules intended for non-repudiation services are not tampered with in shipment or storage. Acceptance testing is performed to verify that cryptographic hardware is performing correctly. Installation and activation is performed only by M of N authorized personnel in trusted roles, and the devices operate in a physically secured environment. Private keys are erased from modules when they are removed from service in according with the manufacturer's instructions. Additional information is provided in section 6.6. – Life cycle technical controls of DigiSign CA CPS.

7.6.7. Root Certificate Authority

DigiSign TSA is being operated by DigiSign's own Public Key Infrastructure, consisting of several Root Certification Authorities and an OCSP responder service.

The ROOT CA's are operated offline, all the aspects related to the physical and technical security are detailed in DigiSign CA CPS, published at www.digisign.ro.

7.7. Time-Stamping

7.7.1. Time-Stamp issuer

DigiSign TSA has technical prescriptions in place to ensure that TSTs are issued securely and include the correct time. In line with the requirements referenced in section 2 of this document, each TST includes:

- a representation (e.g. hash value) of the datum being time-stamped as provided by the requestor;
- a unique serial number that can be used to both order TSTs and to identify specific TSTs;
- an identifier for the time-stamp policy;
- the time calibrated to within 1 second of UTC, traceable to a UTC(k) source;
- an electronic signature generated using a key used exclusively for time-stamping;
- an identifier for the TSA and the TSU.

7.7.2. Clock synchronization with UTC

DigiSign TSA ensures that its clock is synchronized with UTC within an accuracy of 1 second or better, using the NTP protocol.

DigiSign TSA monitors its clock synchronization and ensures that, if the time indicated in a TST drifts or jumps out of synchronization with the UTC, this is detected. In case the TSA clock drifts out of accuracy, no time-stamp shall be issued until the clock is synchronized.

Specifically, the following topics are covered:

- Continuous calibration of the TSU clock
- Monitoring of the accuracy of the TSU clock
- Thread analysis against attacks on time-signals
- Behavior while skipping/adding leap seconds
- Behavior while drifting larger that 1s from the UTC

7.8. Physical and environmental security

The practices identified in chapter 5 and 6 of DigiSign CA CPS applies.

Computer systems, terminals and information resources of DigiSign operators are placed in a dedicated area, physically protected against unauthorized access, destruction or disruption of activity. These locations are monitored. Each input and output are recorded in the event log (system logs); the stability of the power sources and temperature are also monitored and controlled.

7.9. Security of operations

The technical requirements presented in this chapter refer to the security controls specific to computers and applications, used within DigiSign domain. Security measures were taken at all levels, starting at the physical level and all the way through the application level.

The controls that belong to the DigiSign TSA have the following security measures:

- mandatory authentication at the operating system level and applications
- discretionary access control,
- possibility of being audited in terms of security,
- the computer is accessible only to authorized personnel with trusted roles in DigiSign,
- segregation of duties, according to their role within the system,
- identification and authentication of roles and personnel performing these roles,
- preventing reuse of an object by another process after it is issued by the authorized,
- cryptographic protection of exchanges of information and protection of databases,
- log archiving operations performed on a computer and data necessary audit,
- a secure path that allows the identification and authentication of roles and personnel
- performing these roles,
- key restoration methods (only in the case of hardware security modules), the application
- and the operating system,
- means monitoring and alerting in case of unauthorized access to computing resources.

The practices identified in chapter 5 and 6 of DigiSign CA CPS also applies.

7.10. Network security

Trusted servers and work stations belonging to DigiSign are connected through a LAN, divided in more subnetworks, with controlled access. Access from the Internet to any segment, is protected by an intelligent firewall. Security checks are developed based on firewall and traffic filters applied at the level of routers and proxy. Events (logs) are registered in the system journals and allow the surveillance of the right use of services provided by DigiSign.

7.11. Incident management

The practices defined in section 5.6.1. Incident and compromise handling procedures of DigiSign CA CPS applies.

7.12. Collection of evidence

At the time a security incident becomes detected, it might be not obvious, if that security incident is subject of further investigations. Therefore, it is important, that any proof, the status of IT system or information is securely saved before they become unusable or destroyed.

The TSP records are kept accessible for an appropriate period, including after the activities of the TSP have ceased. All the relevant information concerning data issued and received by the TSP are guarded to provide evidence in legal proceedings and to ensure continuity of the service. Especially:

- The confidentiality and integrity of current and archived records concerning operation of services is maintained.
- Records concerning the management of services are confidential and filed in accordance with described business practices.
- Records concerning the management of services, if necessary, are made available for the purposes of providing evidence of the correct operation of the services for legal proceedings.

- The TSP registers in the precise moment, the significant environmental events, key management and clock synchronization. The time used to record events, as required in the audit log, is synchronized with the UTC continuously.
- Records concerning services are held for a period after the expiration of the validity of the signing keys or of any service token to provide trust for the necessary legal evidence in accordance to the present document.
- The events are logged in a way that they cannot be deleted or destroyed (except if they can be reliably transferred to long-term media).

7.13. Business continuity management

Backups of the databases of all issued TSTs by DigiSign TSA are kept in an off-site storage. If the TSU private key is compromised or suspected to be compromised, DigiSign TSA shall inform Subscribers and Relying Parties and shall stop using the compromised key. In case of revocation of the TSU certificate, the necessary actions shall be performed in accordance to the Recovery Plan.

In case of loss of clock synchronization, DigiSign TSA suspends its operations to prevent further damage. The Recovery Plan is activated to restore the synchronization and service.

The time-stamping service itself is in a physical secured environment that minimizes the risk of natural disasters (e.g. fire).

The private keys of the TSU are stored in a cryptographic security module.

In case private keys become compromised, the archive of saved time-stamps helps differentiate between correct and false time-stamps in an audit trail.

The HSM is isolated from the public network and, if necessary, the following measures shall be taken:

- Notify the Security Manager for him to coordinate the measures to be taken.
- Start a security audit of the remaining private keys (integrity checks, log file analysis).
- Notify the incident to relying parties.
- In case of natural disasters (e.g. fire, earthquake, storm), if it causes a loss of the facility, the time-stamping service could become suspended until the disaster recovery facility is activated.

7.14. TSA termination and termination plans

The practices identified in section 5.7. – CA or RA termination of DigiSign CA CPS also applies. Additionally:

- In the event the DigiSign TSA terminates its operations for any reason whatsoever, it shall notify the national Supervisory Body prior to termination.
- A timely notice shall be provided to all Subscribers and Relying Parties to minimize any disruptions that are caused because of the termination of the services.
- Furthermore, in collaboration with the Supervisory Body, the DigiSign shall coordinate the necessary measures that ensure retention of all the relevant archived records prior to termination of the service.
- Moreover, DigiSign shall maintain an up-to-date termination plan and before it terminates the time-stamping services, the following procedures will be applied:
  a. DigiSign shall inform the all Subscribers and other entities with whom it has agreements or other form of established relations,
  b. DigiSign shall terminate the authorization of all subcontractors to act on its behalf in carrying out any functions relating to the process of issuing TSTs,

c. DigiSign shall transfer to a reliable entity, for a reasonable time, its obligations of maintaining all necessary information to provide evidence of its operations, unless it can be demonstrated that DigiSign is not the owner of such information,
d. DigiSign TSA private keys, including backup copies, shall be destroyed or withdrawn from use, in a way that the private keys cannot be retrieved,
e. DigiSign TSA shall take the necessary steps to have the TSU certificates revoked,
f. When possible, DigiSign shall use a system that allows the transfer of the services provided to its client to another Qualified Trust Service Provider.

- Also, DigiSign has an arrangement to cover the costs to fulfil these minimum requirements in case it becomes bankrupt or for other reasons by which DigiSign is unable to cover the costs by itself, to the possible extent, within the constraints of the applicable legislation regarding bankruptcy.
- DigiSign shall maintain or transfer to a reliable entity its obligations of making its public key or TSTs available to Relying Parties for a reasonable time.

7.15. Compliance

DigiSign TSA ensures the compliance of the Time-Stamping Services it provides with the applicable legislation in force. Specifically, DigiSign TSA issues Qualified Time-Stamps as per:

- EU Regulation no. 910/2014 (eIDAS)
- Applicable national legislation

Validation of the compliance with the requirements laid out in those two regulations is performed during the conformity assessment, once at 24 months.