Signet Time-Stamping Practice Statement

Advania

TABLE OF CONTENTS

Document version history

Version number	Date	Changes
1.0	14.12.2022	First version

1 INTRODUCTION

Advania Iceland ehf. (Advania) is one of the country's largest provider of managed services. Advania provides applications tailored to different business needs. Government agencies along with small and large enterprises in all sectors trust Advania to with managing their IT needs. Advania was formerly known as Skýrr and in 1952 the Icelandic state and the city of Reykjavik founded Skýrr, an IT company whose purpose was to take a leading role in computing and recordkeeping in Iceland. The company was privatized in 1995 and later became the core element in a group of companies – including EJS – that merged under the Skýrr brand and changed its name to Advania Iceland in 2012. Advania Iceland is today one of the largest IT companies in Iceland. The scope of this document is bound to Advania timestamping service (branded as Signet timestamping).

The information Security Management System (ISMS) applies to Advania's Software Solutions and Hosting Operations including Data Center services, Managed Services, Services to Retail systems and ATMs and Repair shop. Advania Time-Stamping and the Signet solution is part of the Software solutions. The implemented and certified scope is according to ISO 27001 and complies with the requirements of Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) and other relevant international standards for Timestamping Authorities. An independent third-party auditor verifies the efficiency of these procedures on a regular basis.

The Advania eIDAS Qualified Timestamping Practice Statement conforms to Policy and Security Requirements for Trust Service Providers issuing Electronic Timestamps (ETSI EN 319 421) and complies with eIDAS Regulation. Advania's TSU will only issue qualified electronic time-stamps.

The Signet Time-Stamping Authority (Signet TSA) uses the public key infrastructure and trusted time sources to provide reliable time-stamps.

2 REFERENCES

[**ref.1**] Regulation (EU) No 910/2014 of 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

[**ref.2**] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"

[**ref.3**] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps"

[**ref.4**] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Timestamping protocol and timestamp token profiles."

[**ref.5**] RFC 3161: "Internet X.509 Public Key Infrastructure Time-stamp Protocol" https://tools.ietf.org/html/rfc3161

[**ref.6**] Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions."

[**ref.7**] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

3 DEFINITIONS, SYMBOLS AND ABBREVIATIONS

3.1 DEFINITIONS

Coordinated Universal Time (UTC)	The time scale based on the second as defined in ITU-R Recommendation TF.460-6 (02/02)
eIDAS Regulation	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.
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
Network Time Protocol (NTP)	Networking protocol to synchronize system clocks among a set of distributed time servers and clients over packet-switched, variable latency data networks as defined in RFC 5905
Qualified Timestamping Service	Timestamping Service issuing qualified electronic timestamp tokens as per Regulation (EU) No 910/2014 [i.2]
Relying Party	Recipient of a timestamp token who relies on that timestamp token.
Subscriber	Legal or natural person to whom a timestamp is issued and who is bound to any subscriber obligations
Time-stamp	Data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time
Time-stamp policy	Named set of rules that indicates the applicability of a timestamp to a particular community and/or class of application with common security requirements
Time-stamping Authority (TSA)	TSP providing timestamping services using one or more timestamping units
Time-stamping Service	Trust service for issuing timestamps
Time-stamping Unit (TSU)	Set of hardware and software which is managed as a unit and has a single timestamp signing key active at a time
Trust service	Electronic service that enhances trust and confidence in electronic transactions
Trust service policy	set of rules that indicates the applicability of a trust service to a particular community and/or class of application with common security requirements
Trust Service Provider (TSP)	Entity which provides one or more trust services
Trust service token	Physical or binary (logical) object generated or issued as a result of the use of a trust service
TSA Practice Statement	Statement of the practices that a TSA employs in issuing timestamps
TSA system	Composition of IT products and components organized to support the provision of timestamping services

3.2 ABBREVIATIONS

CA	Certification Authority
IP	Internet Protocol
GMT	Greenwich Mean Time
IT	Information Technology
TSP	Trust Service Provider
TAI	International Atomic Time
TSA	Time-Stamping Authority
TSP	Trust Service Provider
TSPS	Trust Service Practice Statement
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time

4 GENERAL CONCEPTS

4.1 GENERAL POLICY REQUIREMENTS CONCEPTS

The present document references ETSI EN 319 401 [4] for generic policy requirements common to all classes of trust service provider’s service.

These policy requirements are based upon the use of public key cryptography, public key certificates and reliable time sources.

Subscriber and relying parties are expected to consult the Advania TSA's practice statement to obtain further details of precisely how this time-stamp policy is implemented by the particular TSA (e.g. protocols used in providing this service).

4.2 TIME-STAMPING SERVICES

Advania takes responsibility for the provision of the timestamping services which is broken down into the following component services for the purposes of classifying requirements:

Timestamping Provision: This service component generates timestamps.

Timestamping Management: This service component monitors and controls the operation of the timestamping services to ensure that the service provided is as specified by the TSA. This service component has responsibility for the installation and de-installation of the timestamping provision service. This subdivision of services is only for the purposes of clarifying the requirements specified in this document and places no restrictions on any subdivision of an implementation of timestamping services.

4.3 TIME-STAMPING AUTHORITY (TSA)

A Trust Service Provider (TSP) providing time-stamping services to the public, is called a Time-stamping Authority (TSA).

The TSA has overall responsibility for the provision of the time-stamping services identified in clause 4.2. The TSA has responsibility for the operation of one or more Time Stamping Units (TSUs) which create and sign on behalf of the TSA.

Signet TSA issues only qualified timestamps and is a trust service provider as described in ETSI EN 319 401 [ref.2].

Signet TSA operates one TSU which is identified in the TSU certificate which is exclusively used to sign TST. TSU certificates are available at Signet public website (https://info.signet.is/repository/).

4.4 SUBSCRIBER

A Subscriber is an organization or an individual end-user who holds a subscriber agreement with Signet time-stamping service.

If the subscriber is an organization, it comprises several end-users or an individual end-user and some of the obligations that apply to that organization will have to apply to the end-users as well. The organization is responsible for a correct fulfilment of the obligations from its end-users and inform them.

4.5 TIME-STAMPING POLICY AND TSA PRACTICE STATEMENT

This clause explains the relative roles of timestamp policy and TSA practice statement. It places no restriction on the form of a timestamp policy or practice statement specification.

A timestamp policy is a form of Trust Service Policy as specified in ETSI EN 319 401 [4] applicable to trust service providers issuing timestamps.

TSA Practice Statement is a form of Trust Service Practice Statement as specified in ETSI EN 319 401 [4] applicable to trust service providers issuing timestamps.

This document specifies the time-stamp policy and the practice statement for the Signet TSA.

5 TIME-STAMPING POLICIES

5.1 GENERAL

This document (TSPS) defines the time-stamp policy, supported by public key certificates, with an accuracy of 1 second of UTC or better.

5.2 IDENTIFICATION

The object-identifier (OID) of the baseline Time-Stamping Policy is 0.4.0.2023.1.1:

```
itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) baseline-ts-policy (1)
```

This OID is referenced in every TST issued by Signet TSA.

5.3 USER COMMUNITY AND APPLICABILITY

This policy is aimed at meeting the requirements of time-stamps for long term validity (e.g. as defined in ETSI EN 319 122 [ref.7]) but is generally applicable to any use which has a requirement for equivalent quality.

This policy may be used for public Time-Stamping services or Time-Stamping services used within a closed community.

6 POLICIES AND PRACTICES

6.1 RISK ASSESSMENT

Advania has implemented a certified Information Security Management System according to ISO 27001. Part of the Security Management is the Risk Assessment Process which includes regular risk assessments for the Signet time-stamping service in terms of business continuity and technical issues.

The objective is to identify threats and vulnerabilities and misuse. For each identified risk, a risk analysis is carried out with the use of impact analysis. Likelihood and consequence in terms of confidentiality, integrity, and availability (CIA) is registered. Risk treatment is executed as improvement projects and risk is re-assessed when selected risk treatment options have been implemented. Responsible Directors approve the risk assessment results and residual risk.

The Security Officer is responsible for planning Risk assessment activities at least annually.

6.2 TRUST SERVICE PRACTICE STATEMENT

Advania ensures the quality, performance and operation of the time-stamping service through the implementation of various security policies and controls.

The Security Management system is reviewed yearly by an independent third party (BSI) in relation to ISO27001 certification. The policies, processes and controls are reviewed regularly via internal audits.

The practices and policies are implemented and approved by management and the TSPS is approved by Advania Security Manager.

The TSPS is reviewed annually by the Security Officer and responsible director.

Proposed changes of the Time-stamping service or the context of the practice statement is published and communicated to stakeholders. Stakeholders are TSA subscribers and TSA Signet employees.

If TSPS document is changed, a new version is published immediately at https://info.signet.is/repository/ and notification of changes sent to subscribers of the TS via email.

This document is available on https://info.signet.is/repository/.

Additionally, for compliance to ETSI EN 319 421 the following measures have been implemented:

6.2.1 TIMESTAMP FORMAT

The issued timestamp tokens by Signet are compliant to RFC 3161 time-stamps. The service issues RSA3072 encrypted time-stamps that accept at least one of the following hash algorithms:

- SHA256
- SHA512

6.2.2 ACCURACY OF THE TIME

Time-stamps are issued with an accuracy of one (1) second.

6.2.3 LIMITATIONS OF THE SERVICE

No stipulation.

6.2.4 OBLIGATIONS OF THE SUBSCRIBER

Please see the “Terms and conditions for use of time-stamping service“for detailed information.

6.2.5 OBLIGATIONS OF RELYING PARTIES

Before placing any reliance on a timestamp, a relying party must verify that the timestamp has been correctly signed and that the certificate used to sign the timestamp was valid at the time indicated within the timestamp.

The Relying Party must take into account any limitations on usage of the timestamp indicated by this Practice Statement.

For qualified timestamps, ETSI EN 319 421 states: “The relying party is expected to use a Trusted List to establish whether the timestamp unit and the timestamp are qualified. If the public key of the TSU is listed in the Trusted List and the service it represents is a qualified timestamping service, then the timestamps issued by this TSU can be considered as qualified.”

During the TSU certificate validity period, the status of the certificate can be checked using the relevant OCSP as stated within the AIA extension of the certificate.

Relying parties should rely on DNS services that respect the TTL value of the A record when accessing the timestamp services and certificate status services.

If this verification takes place after the end of the validity period of the certificate, the Relying Party should follow the guidance denoted in Annex D of ETSI EN 319 421.

6.2.6 VERIFICATION OF THE TIMESTAMP

Timestamp verification includes the following:

Verification of the timestamp issuer

A TSA that uses appropriate electronic certificates issues the timestamp. The public keys of the used certificates, including the TSU and CA certificates, are published to enable a verification that the timestamp has been signed correctly by the TSA.

The certificates can be found on the Signet support site: https://info.signet.is/repository/.

Verification of the timestamp revocation status

An OCSP responder service is available to check the revocation status of the used certificates in the timestamp (provided by the issuer of the certificates).

6.2.7 SERVICE AVAILABILITY

Advania has implemented the following measures to ensure availability of the TSU service:

- Redundant setup of IT Systems, including HSM infrastructure, to avoid single points of failure
- Redundant high-speed internet connections to avoid loss of service
- Use of uninterruptable power supplies
- Active incident management system and response plan is in place

Although those measures ensure service availability, Advania does not guarantee an annual availability of 100%. Advania aims to provide 99% service availability per year while reaching an average availability of 99.95% per year excluding scheduled service downtime.

6.3 TERMS AND CONDITIONS

Information regarding limitations of the service, Subscribers' obligations, information for relying parties or limitations of liability can be found within the published documents (https://info.signet.is/repository/), "General terms of subscriber agreement" and "Terms and Conditions for use of Time-Stamping Service".

All subscribers and parties of the trusted service are informed about the terms and conditions before entering into a contractual relationship and acknowledges it with signature in the Subscriber agreement.

Additionally, the following sections apply.

6.3.1 TRUST SERVICE POLICY BEING APPLIED

This document (TSPS) represents the applied trust service policy. See chapter 5 for further information.

6.3.2 PERIOD OF TIME DURING WHICH TSU EVENT LOGS ARE RETAINED

Advania retains any TSU audit logs generated for at least one year. Advania makes these audit logs available to Qualified Auditors upon request. If the system design changes, Advania makes sure that the logs can be retrieved.

6.4 INFORMATION SECURITY POLICY

Advania has implemented an information security policy throughout the company. All employees must adhere to the regulations stated in the policy and derived security concepts. The information security policy is reviewed on a regular basis and when significant changes occur. Advania Security Management Board approves the changes of the information security policy. Any changes that will impact on the level of security provided is approved by the Advania security manager. The information security policy and all updates on it, is communicated to all employees who are impacted by it by automatic notification when a new version is added.

The public security policy is communicated to 3rd party on advania.is here.

6.5 TSA OBLIGATIONS

The conformance with the procedures that are stated in this document is ensured by Advania. An independent conformity assessment body verifies the efficiency of the procedures on a regular basis.

6.5.1 TSA OBLIGATIONS TOWARDS SUBSCRIBER

This document places no specific obligations on the Subscriber beyond any TSA specific requirements stated in clause 6.3 in this document.

6.5.2 TSA OUTSOURCES LIABILITY

No subcontractors work on the trusted services.

6.6 INFORMATION FOR RELYING PARTIES

The obligations of relying parties (see clause 6.3 in this document) are covered in chapter 6 of the "Terms and Conditions for use of Time-Stamping Service" document. In addition, the relying party shall do the following:

a) verify that the time-stamp has been correctly signed and that the private key used to sign the time-stamp has not been compromised until the time of the verification

b) take into account any limitations on the usage of the timestamp indicated by the timestamp policy

c) take into account any other precautions prescribed in agreements or elsewhere

7 TSA MANAGEMENT AND OPERATION

7.1 INTRODUCTION

Advania has an information security system/framework in place which secures the Signet time-stamping service.

7.2 INTERNAL ORGANIZATION

Advania organisational structure, policies, procedures, and controls apply to the Signet time-stamping service. These internal documents are used by independent bodies to confirm compliance of the service against ETSI EN 319 421.

Advania is a legal entity according to Icelandic law and has implemented an information security system which applies to the Time-stamping Service to ensure security and quality of service. Both Advania's software development and systems operations teams are ISO27001 certified for the signing and time-stamping services. Segregation of duties for trusted roles is defined for the operation of the Signet TSA.

Advania has financial resources in accordance with Icelandic law to cover operational liabilities.

Advania employs a sufficient number of personnel relating to the type range and volume of work necessary to provide time-stamping services. The team qualification and experience for the Trust Service personnel's is a BSc or higher degree in computer science, engineering or equivalent with expertise in PKI infrastructure, or more than 3 years of experience in installation, development or operation of software.

7.3 PERSONNEL SECURITY

Advania maintains HR processes fulfilling security best practice and the requirements of relevant standards. That includes hiring, screening, training, contractor management, appraisal, disciplinary process, end of employment and more.

Managerial and operational personnel possess the appropriate skills and knowledge of Time Stamping, digital signatures, and Trust Services as well as security procedures for personnel with security responsibilities, information security and risk assessments. This includes updates on new threats and current security patches at least annually. Continuous security awareness program is in place for all employees, regular monitoring of potential weaknesses and threats are communicated.

Trusted personnel include all employees that are nominated to a trusted role and have access to or control cryptographic operations. Trusted roles include, but are not limited to:

- Security officer
- System administrator
- System operator
- System auditor

The trusted roles and responsibilities are documented, clearly defined, and named by management in documents available to all concerned personnel. Where appropriate, job descriptions are different between general functions and specific functions. Trusted roles are accepted by the management and the person to fulfil the role. All personnel in trusted roles are introduced to the information security policy for the time-stamping service upon nomination to the role.

User accounts are created for personnel in specific roles that need access to the system in question. All users must log in with dedicated account, and administrative commands are only available with explicit permission and auditing of the execution. File system permissions and other features available in the operating system security model are used to prevent any other use. User accounts are locked as soon as possible when the role change dictates.

Advania ensures that all current and recruited employees are trustworthy by regular screening, financial background checks and criminal records. The employment contracts signed by the employees of Advania provide that they will maintain the secrecy of confidential information and are free from conflict of interest that might prejudice in the impartiality of Advania operations. Personnel do not have access to the trusted functions until the necessary checks are completed. Advania´s disciplinary process is activated if personnel violate Advania's policies or procedures.

7.4 ASSET MANAGEMENT

7.4.1 GENERAL REQUIREMENTS

Advania operational unit (RL) maintains an inventory list for all server-based information assets with classifications according to importance. Other information assets are maintained in the Storage of Assets (SOA) document. Both inventories are reviewed on a regular basis.

7.4.2 MEDIA HANDLING

All media is handled securely and according to the classification. All disposal of media or data is done according to a strict data disposal instructions.

7.5 ACCESS CONTROL

Advania has implemented security measures and enforced access control according to the Access Control Policy to avoid unauthorized access and attempts to add, delete or modify information in applications related to the services, including certificates and revocation status information.

The principle of least privileges is in practice and ensured by roles separations. Duties for the trusted roles are segregated and a person can only be assigned to one of the trusted roles at a time. If a person changes a role, the old role is revoked and the new one is assigned.

Dual control is enforced when making configuration changes to the time-stamping service where changes made by the system administrator must be approved by the security officer for them to take effect.

Access rules and users access rights are monitored and audited at least once a year.

Role based access rules are set up and administrated by Advania with enforced dual control to perform administrative commands/actions in the time-stamping service.

User accounts are created for personnel in specific roles that need access to the system in question. Advania personnel are authenticated before using critical applications related to the services. All users must log in with their personal account with electronic certificate used for authenticating users managing the trusted service. All administrative commands are logged.

Only authorized persons have access to the Time-stamping systems and no person in a trusted role has access to the time-stamping systems until all checks and contracts covered in section 7.3 are completed.

Advania has in place a data protection and data disposal policy to ensure proper protection and disposal of sensitive information.

7.6 CRYPTOGRAPHIC CONTROLS

7.6.1 GENERAL

The timestamp certificate which is used within the TSUs is issued by the “fullgilt audkenni“ CA operated by Auðkenni. The “fullgilt audkenni“ CA is issued by the Root CA “Islandsrot” which is operated by the ministry of finance in Iceland. Advania uses a private key to fulfil its service. One key pair (private & public) is used within the TSU to issue the timestamp. The private key is stored within a cryptographic modules.

7.6.2 TSU KEY GENERATION

The generation of the TSU's signing key pair is undertaken in a physically secured environment (as per clause 7.8) by personnel in trusted roles (as per clause 7.3) under at least dual control. The personnel authorized to carry out this function is limited to those required to do so under Advania's practises.

The generation of the TSU's signing key pair is carried out within a cryptographic modules which are Common-Criteria-certified according to EAL 4 in accordance with ISO/IEC 15408. The TSU key pair generation algorithm, the resulting signing key length and signature algorithm used for signing timestamps key is recognized by any national supervisory body. Signet time-stamping service uses RSA key pair with 3072-bit modulus and is only used for signing time-stamps.

For high availability, the TSA signing key is mirrored into two HSMs. Only one time-stamp signing certificate is active at a time.

7.6.3 TSU PRIVATE KEY PROTECTION

The TSU private signing key is held and used within cryptographic modules which are Common-Criteria-certified according to EAL 4 in accordance with ISO/IEC 15408. Each TSU private signing key is always associated with only one TSU certificate at the time. A TSU is connected to two hardware security modules in a high availability. TSU private keys are not backed up.

7.6.4 PUBLIC KEY CERTIFICATE

Advania guarantees the integrity and authenticity of the TSU signature verification (public) keys as follows:

a) TSU signature verification (public) keys are available to relying parties in publicly available certificates. The certificates can be found on the Signet Support Site: https://info.signet.is/repository/.

b) The TSU signature verification (public) key certificate is issued by AUDKENNI a certification authority operating under ETSI EN 319 411-1 [i.10].

c) The TSU does not issue a time-stamp before its signature verification (public key) certificate is loaded into the TSU or its cryptographic device. When obtaining a signature verification (public key) certificate, Advania verifies that this certificate has been correctly signed (including verification of the certificate chain to its trusted certification authority).

7.6.5 Rekeying TSU's key

The lifetime of the TSU's certificate is never longer than the period of time than the algorithm used and key length is recognized as being fit for purpose. Once a year or when significant changes occur, the security officer (trusted role) verifies any cryptographic algorithms used within the TSU against the algorithms recognized. If an algorithm becomes compromised or is not suitable anymore, Advania will replace the private key and get a new certificate issued. Private keys are not rekeyed.

7.6.6 Life Cycle Management of Signing Cryptographic Hardware

All hardware is inspected and secured during the commissioning process to ensure conformity to supply and no evidence of tampering found. All hardware is stored in a physically secured environment.

Installation, activation, and duplication of TSU's signing keys in cryptographic hardware is done only by personnel in trusted roles using at least dual control in a physically secured environment (as per section 7.8).

The TSU private signing keys stored on TSU cryptographic module are erased upon device retirement in a way that it is practically impossible to recover them.

7.6.7 End of TSU Key Life Cycle

The validity of all private keys for the TSU signing certificates is no longer than the end of validity of the associated public key certificate. The TSU private keys have one-year life cycle with grace period of six weeks. At the end of life, a new key is placed within the cryptographic hardware instead of the expired key and the expired key is securely destroyed so it cannot be retrieved or used anymore.

The expiration date for TSU's key is defined in the private key usage period extension of the TSU certificate.

The validity key periods are defined in accordance with clause 7.6.2.

7.7 Time-stamping

7.7.1 Timestamp Issuance

The structure of the time-stamp token complies with the requirements of ETSI EN 319 422 [5].

Signet TSA ensures that time-stamp tokens are issued securely and include the correct date and time. The time values the TSU uses in the time-stamp token is traceable to UTC with direct communications via two sources with GPS satellite.

The time included in the time-stamp is synchronized with UTC [1] within the accuracy defined in section 6.2.2. Time-stamps are not issued if the clock is detected as being out of the stated accuracy.

The time-stamps are signed using a 3072-bit TSA key generated exclusively for this purpose. The time-stamp generation system rejects any attempt to issue a time stamp when the end validity of the TSU private key has been reached.

7.7.2 CLOCK SYNCHRONIZATION WITH UTC

Advania ensures that the time is synchronized by comparing it with multiple independent stratum 1 time sources via internet, with the main source located in Iceland (ht-time01.isnic.is) where a time signal is provided from GNSS**,** for the declared accuracy defined in section 6.2.2 of this document. Time-stamps are not issued if the time used for time-stamps is detected as being out of the stated accuracy. Advania will not start time-stamp issuance again until the time has been restored.

Audit and calibration records of the synchronization are maintained by Advania. Advania has security controls against threats that could result in undetected change to the clock that takes it outside its calibration.

Signet TSA guarantees that the clock synchronisation is maintained when a leap second is scheduled, as notified by the appropriate body. The change to take into account the leap second is carried out during the last minute of the day on which the leap second is scheduled. A record is maintained of the exact time when these changes occur.

7.8 PHYSICAL AND ENVIRONMENTAL SECURITY

Advania maintains physical and environmental security policies for systems used for Time-Stamping services which cover physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking & entering, and disaster recovery. Controls are implemented to avoid loss, damage or compromise of assets and interruption to business activities and theft of information and information processing facilities.

7.8.1 SITE LOCATION AND CONSTRUCTION

Signet Qualified Time-Stamping Services are located within a secure data center. The data center is a purpose-built facility made of concrete and steel construction.

7.8.2 PHYSICAL ACCESS

Signet Qualified Time-Stamping Services operate within a secure data center that provides premise security with biometric scanners and card access systems. A 24/7 Closed Circuit TV (CCTV) monitoring system as well as digital recording is provided. Qualified security guards secure the physical premises and only security-cleared and authorized personnel are allowed into the premises. Every entry to the physically secure area will be subject to independent oversight and non-authorized person is accompanied by an authorized person whilst in the secure area. Every entry and exist is logged.

7.8.3 POWER AND AIR CONDITIONING

Signet Qualified Time-Stamping Services operate within a secure data center that is equipped with redundant power and cooling system. UPS and failover to power generator are in place in the unlikely event of power outage.

7.8.4 WATER EXPOSURES

Signet Qualified Time-Stamping Services are protected against water. It is located above ground and on a higher floor with raised flooring. In addition, a water detection alarm system is in place and on-site data center operations staff are ready to respond to any unlikely water exposure.

7.8.5 FIRE PREVENTION AND PROTECTION

Signet Qualified Timestamping Services operate within a secure data center that is equipped with a fire detection and suppression system.

7.8.6 MEDIA STORAGE

Storage of backup media is off-site, physically secured and protected.

7.8.7 WASTE DISPOSAL

Advania ensures that all media used for the storage of information is declassified or destroyed in a generally accepted manner before being released for disposal.

7.8.8 OFF-SITE BACKUP

Advania performs regular off-site backup of critical data. The backed-up data is stored at a physically secured off-site location.

7.9 OPERATION SECURITY

Advania has place trustworthy systems in a secure and reliable environment for the trusted services.

Advania has implemented ISO27001 security controls to ensure service security, quality, and availability of the trustworthy systems.

Security requirements are defined and documented in the requirements specification and design phase of the trustworthy systems acquisition and the software implementation undertaken by Advania to ensure that security and reliability is built into IT systems.

Change control procedures are applied and documented for releases, modifications, and emergency software fixes of any operational software and to the configuration. The procedures are formal and apply to all changes like incidents mitigation, problem management, request fulfilments. Dual control is implemented in the change management procedures for sensitive actions.

Advania has specified and applied procedures (Emergency Change) for ensuring that security patches are applied within a reasonable time after they become available. An emergency change must be requested or initiated, and the procedure includes risk evaluation. A security patch does not need to be applied if it would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch. The reasons for not applying any security patches are also documented.

All systems and servers for the trusted services are protected against viruses, malicious and unauthorized software.

Media used within Advania systems is securely handled to protect media from damage, theft, unauthorized access, and obsolescence. Media management procedures protect against obsolescence and deterioration of media within the period that records are required to be retained. Data disposal procedures are also in place.

Procedures are established and implemented for all trusted and administrative roles that have an impact on the provisioning of services.

The configuration of the Time-stamping systems is checked at least annually for changes which violate the TSPs security policies.

Capacity is monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

7.10 NETWORK SECURITY

Advania maintains a network policy to describe the policies and principles to be followed when working on Advania‘s network infrastructure. The aim is to ensure the security and stability of the network and to ensure that the documentation regarding it is adequate and always correct

Advania network is segmented into zones considering risk assessment, functional, logical, and physical (including location) relationship between trustworthy systems and services. All Advania critical TSU systems are kept in secured zones and communications between the zones is restricted and the only allowed access through the firewalls is based on the protocols needed for Advania services. The same security controls apply to all the systems in the same zone. Non-required connections and services are explicitly forbidden or deactivated. The rule set is reviewed annually.

Firewalls are in place for enforcing security policies and administrative access is on a dedicated network which is separated from the operational TS network and is not directly accessible from the public internet. Systems used for administration is not used for non-administrative purposes and out of band management network is in place.

Development and test environment are physically separated from the production environment and have different networks.

The front-end systems are in a DMZ protected by a firewall and TLS offload servers. Actual security-critical services and corresponding HSMs run in a secure zone that is separated by dedicated firewall and has no direct Internet access.

Only trusted roles have access to secure zones and high security zones in accordance with section 7.3. (The cabling and active equipment along with their configuration in Advania internal network are protected by physical and organisational measures.) – according to section 7.8

Advania operates multiple data centres in separate sites and with separate duplicated external network connection for redundancy to ensure high level availability of the time-stamping service. Communication between sites is cryptographically secured.

All data centres are on a common internal secure network carrying the DMZ and secure zone. The transfer of Sensitive Information outside Advania internal network is encrypted.

Communication between distinct trustworthy systems can only be established 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. The external network connection to the internet is redundant to ensure availability of the services in case of a single failure.

The security of Advania internal network and external connections is constantly monitored to prevent all access to protocols and services not required for the operation of the time-stamping service.

Advania performs vulnerability scan/assessment monthly on public and private IP addresses. The assessments focus on internal and external threats that could result in unauthorized access, tampering, modification, or alteration.

The Signet time-stamping service undergoes penetration testing annually at the set up and after infrastructure or application upgrades or modifications determined significant by Advania.

Advania records evidence that each vulnerability scan and penetration testing was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

All TSU systems are configured by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the Signet TSU operations.

7.11 INCIDENT MANAGEMENT

Incident management process is in place with the purpose to restore normal service operation as quickly as possible and minimize the adverse impact on the business operations and ensuring that agreed levels of service quality are maintained.

For the most urgent types of incidents, Advania has implemented and maintains a business continuity plan for the time-stamping service to ensure continuity in operations during crisis/critical security events. The business continuity plan for the time-stamping service is reviewed at least annually.

Advania has in place advanced and active monitoring systems on various levels like network, Operating systems, software and service level which takes into account the sensitivity of any information collected or analysed. Monitors notifies abnormal activities or potential breach of security, including intrusion into Advania network which are detected, and reported as alarms. Advania monitors also the start-up and shutdown of the logging functions and the availability and utilization of needed services within Advania network.

Advania has in place tools and processes to regularly and automatically review the audit logs for malicious activities. Personnel in a trusted role (auditor) is responsible to follow up on alerts to ensure that relevant incidents are reported and acted up on.

In case of information security incidents, emergency situations and critical malicious activities, the business continuity plan is activated.

The national supervisory body is informed without undue delay or within 24 hours after discovery of a critical security breach and, where applicable, other relevant bodies as national CERT.

If breach is likely to involve personal data and is likely to result in high risk to the rights and freedoms of the natural or legal person, Advania will notify Data Protection Agency (Persónuvernd) without undue delay, but at least in 72 hours after initial discovery of the personal data breach.

Advania will address any critical vulnerability not previously addressed by Advania, within a period of 48 hours after its discovery; the vulnerability is remediated, or a mitigation plan is created and implemented to reduce the impact of vulnerability, or a decision has been made and documented that remediation is not required.

Following a critical event, the response and plan is evaluated and updated as needed to prevent similar events in the future.

7.12 COLLECTION OF EVIDENCE

Advania records and keeps accessible for 1 year, including after the activities of Advania have ceased, all relevant information concerning data issued and received by Advania, for providing evidence in legal proceedings and only to be disclosed to law enforcement authorities under court order and to persons with the legitimate request and for the purpose of ensuring continuity of the service. In particular:

a) The confidentiality and integrity of current and archived records concerning operation of services is maintained.

b) Records concerning the operation of services are completely and confidentially archived in accordance with disclosed business practices.

c) The precise time of significant Signet TSU environmental, key management and clock synchronization events are recorded. The time used to record events as required in the audit log is synchronized with UTC continuously.

d) The events are logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period that they are required to be held.

e) Accountability of personnel: All activities accomplished by system administrators are logged. System administrators always identify themselves with named accounts, so administration activities can always be mapped to persons.

f) Records concerning all events relating to the life cycle of TSU keys and certificates is logged.

g) Records concerning all events relating to synchronization of a TSU’s clock to UTC is logged including information concerning normal re-calibration of synchronization of clocks used in time-stamping.

h) Records concerning all events relating to detection of loss of synchronization is logged.

7.13 BUSINESS CONTINUITY MANAGEMENT

Advania has defined and maintains a continuity plan to enact in case of a disaster.

In the event of a disaster, including compromise of a private signing key or compromise of some other credential of Advania, operations are restored within the delay established in the continuity plan, having addressed any cause for the disaster which may recur (e.g. a security vulnerability) with appropriate remediation measures.

Advania's disaster recovery plan addresses the compromise of suspected compromise of TSU's private signing keys or loss of calibration of a TSU clock, which may have affected time-stamps which have been issued. If a compromise occurred, Advania makes a description of the compromise available to all subscribers and relying parties and stops issuing time-stamps until steps are taken to recover from the compromise.

If the compromise of the TSA's operation or loss of calibration is major, Advania will make information which can be used to identify the time-stamps which may have been affected available to all subscribers and relying parties. Advania will though not make the information available if it breaches the privacy of the users or the security of the time-stamping services.

7.14 TSA TERMINATION AND TERMINATION PLANS

In the event Advania terminates its time-stamping operations, it will notify the Icelandic supervisory body prior to termination.

Advania will ensure that prompt notification of termination is provided to Subscribers and other relevant stakeholders in Signet time-stamping services.

Further, in collaboration with the supervisory body, Advania will coordinate steps to ensure retention of all relevant archived records prior to termination of the service. In addition, the following applies:

a) Advania maintains an up-to-date termination plan for the time-stamping service.

b) Before Advania terminates its services at least the following procedures will be applied:

1. Advania will inform the following of the termination: the Icelandic supervisory body, all subscribers and other entities which Advania has agreements or other form of established relations. In addition, this information will be made available publicly to other relying parties.

2. Advania will transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of Advania for a reasonable period.

3. Advania private keys will be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved.

4. Where possible, Advania will make arrangement to transfer the provision of trust services for its existing customers to another TSP.

5. Advania will revoke all Signet TSU certificates.

c) Advania has an arrangement to cover the costs to fulfil these minimum requirements in case it becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.

7.15 COMPLIANCE

The time-stamping service is aimed for legal persons in Iceland, individuals and companies on the US sanctions list are not allowed to use the services.

In accordance with the relevant legislation, Advania does its best to guarantee that all potential service users, especially people with disabilities, can access services provided by Advania on an equal basis. Advania accepts that its services imply at least some sort of qualitative capabilities and legal capacity, but nonetheless truly aspires to provide trust services and related technical solutions in a non-discriminating way.

Advania always ensures compliance with applicable law.

Specifically, the Signet TSA is compliant to:

a) REGULATION (EU) No. 910/2014

b) ETSI EN 319 401 & ETSI EN 319 421

c) IETF RFC 3161