COMFACT

Comfact Timestamping

Practice statement

Version date	**2025-01-24**
Classification	**Unclassified**
OID	**1.2.752.253.8.1**

Revision history of this document

This document is valid from the date of its publication in Comfact Repository until a new version of the document is made available in the Comfact Repository with a new version date.

Version date	Description	Approval by
2025-01-24	Major update, changes made to the practices and details concerning Comfact AB's timestamping service.	Management Team
2021-11-26	First public version of new release of document.	Management Team

Table of contents

1 Scope

The Comfact Timestamp Service plays a crucial role in Comfact AB's trust services. A timestamp provides an electronically signed assertion that proves arbitrary data existed before a specific time and has not been manipulated or altered since. The Comfact Timestamp Service is fully compliant with the IETF RFC 3161 specifications, as outlined in ETSI EN 319 422, which defines the timestamp protocol.

This document specifies the Timestamping Practice Statement, including security requirements related to the operation and management of the Comfact Timestamp Service's issuance of timestamps. The Comfact Timestamp Practice Statement follows the policy defined in ETSI EN 319 421, "Policy and Security Requirements for Trust Service Providers issuing Timestamps."

2 References

The following documents contain provisions relevant to this document:

Reference	Description
eIDAS EU 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
ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI EN 319 421	Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Timestamps
ETSI EN 319 422	Electronic Signatures and Infrastructures (ESI); Timestamping Protocol and Timestamp Token Profiles
ETSI TS 119 312	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
RFC 3161	Internet X.509 Public Key Infrastructure Timestamp Protocol

3 Abbreviations, Definitions and Terminology

3.1 Abbreviations

The following abbreviations are relevant in this document:

Abbreviation	Description
CA	Certification Authority
CSA	Comfact Service Agreement
OID	Object Identifier
PS	Practice Statement (This document)
TSA	Timestamp Authority

TSP	Trust Service Provider
TST	Timestamp Token
TSU	Timestamp Unit
UTC	Coordinated Universal Time
ISMS	Information Security Management System

3.2 Definitions

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

Term	Definition
Comfact Repository	Documents are currently available at request to: info@comfact.com or at https://www.comfact.se/en-us/Resources/Repository
Comfact Service Agreement	Agreement between Comfact and a subscriber or customer on the conditions to use the service.
Comfact Timestamping Practice Statement	This document.
Comfact Timestamping	Comfact Timestamping service as described in this document.
Coordinated Universal Time	Time scale based on the second as defined in Recommendation ITU-R.
Relying party	Recipient of a timestamp who relies on that timestamp.
Subscriber	Legal or natural person to whom a timestamp token is issued to and who is bound to subscriber obligations included in a Comfact Service Agreement.
Timestamp	Data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time.
Timestamp policy	A set of rules that indicates the applicability of a timestamp to a particular community and/or class of application with common security requirements.
Timestamp token	Indicates that a specific piece of arbitrary data existed at a particular point in time.
Timestamping Authority	Timestamping Authority provides timestamping services using one or more timestamping units.
Timestamping service	Trust service for issuing timestamps.
Timestamping unit	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 Provider	Entity which provides one or more trust services.

TSA Disclosure statement	Statements about TSA policies and practices that need emphasis or disclosure to subscribers and relying parties, especially to meet regulatory requirements.
TSA practice statement	Statement of the practices that a TSA employs in issuing timestamp.
TSA system	Composition of IT products and components organized to support the provision of timestamping services.

3.3 Modal Verbs Terminology

In the present document "shall", "shall not", "should", "should not", "may", "need not", "will", "will not", "can" and "cannot" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

4 General Concepts

4.1 General Policy Requirements Concepts

This document references ETSI EN 319 401 for generic policy requirements. These requirements are based on the use of public key cryptography, public key certificates, and reliable time sources. Subscribers and relying parties are expected to consult the TSA's practice statement for detailed information on how this timestamp policy is implemented by the specific TSA (e.g., protocols used in providing this service).

4.2 Timestamping Service

Comfact is a Trust Service Provider as described in ETSI EN 319 401, providing digital signatures, certificates, and timestamps. The Comfact Timestamp service includes the following components:

- **Timestamping Provision**: The technical components that issue the timestamp tokens, referred to as TSTs.
- **Timestamping Management**: The service component that monitors and controls the timestamping operation to ensure the service provided meets the specifications in this document and the Comfact CPS, including ensuring the clock used for timestamping is correctly synchronized with the UTC time source.

4.3 Timestamping Authority (TSA)

A A Trust Service Provider (TSP) providing timestamping services is called the Timestamping Authority (TSA). Comfact Timestamp is responsible for providing these services, as identified in section 4.2, and oversees the operation of one or more Timestamping Units (TSUs), which create and sign Timestamp tokens (TSTs) using their own private keys. Comfact Timestamp Services may delegate or subcontract the generation of timestamps, but Comfact AB always maintains overall responsibility and ensures compliance with policy requirements.

4.4 Timestamping Authority Parties

4.4.1 Subscriber

A subscriber to Comfact Timestamp can be the subject of a certificate issued by Comfact Certificate Services or an entity (natural or legal person) with a service agreement (CSA) with Comfact AB. Legal person subscribers are responsible for their end-users and Relying Parties, ensuring they use Comfact Timestamping Services appropriately. Natural person subscribers are directly responsible for fulfilling their obligations under the CSA with Comfact AB.

4.4.2 TSA Relying Parties

Relying Party is an entity or individual that relies on a TST generated by Comfact Timestamp under the Comfact Timestamp policy [ETSI EN 319 421]. A Relying Party may or may not also be a Subscriber.

4.5 Timestamp Policy and TSA Practice Statement

The Comfact Timestamping Services Practice Statement outlined in this document specifies how the requirements for trusted timestamping services, as specified in ETSI EN 319 421, are met. This document, the Comfact Timestamping Practice Statement, is a public document available in the Comfact Repository.

5 Timestamp Policies and General Requirements

5.1 General Requirements

Comfact Timestamp issues TSTs in accordance with ETSI EN 319 421 as specified in this document. The TSTs are issued with an accuracy of ±1 second of UTC, or better, and contain an identifier to the applicable practice statement (see section 5.2). Comfact Timestamp TSUs meet the technical specifications of ETSI EN 319 422 and RFC 3161.

5.2 Policy Name and Identification

The object identifier (OID) of the Comfact Timestamping Practice Statement specified for this document is: 1.2.752.253.8.2. By including this OID in the generated timestamps, the timestamp claims conformance to this Timestamping Practice as defined in this document, as well as the ETSI Best Practices Time-Stamp Policy (BTSP) (OID 0.4.0.2023.1.1).

5.3 User Community and Applicability

5.3.1 Best Practices Timestamp Policy

The closed community of Comfact Timestamp includes only Subscribers and their Relying Parties. Comfact AB does not provide public timestamp services. This policy is aimed at meeting the requirements for long-term validity timestamps (e.g., as defined in ETSI EN 319 122) but is generally applicable to any use requiring equivalent quality.

6 Policies and Practices

6.1 Risk Assessment

Comfact AB's ISMS is based on ISO 27001, where risk management is a central part. As such, risk assessments are performed regularly to ensure the quality and reliability of its timestamping services. Comfact AB's risk assessment identifies, analyzes, and evaluates trust service risks regularly, considering both business and technical issues. Based on the assessments, appropriate risk treatment measures are selected accordingly. Residual risks are regularly reviewed and revised.

6.2 Trust Service Practice Statement

At Comfact AB, information security is of the highest importance. In accordance with Comfact AB's ISO 27001 certification, a variety of security controls have been implemented to ensure the quality and reliability of the timestamping services operation. This work is continually ongoing to remain updated and effective against new threats. Similarly, this document, the Comfact Timestamp Authority PS, is regularly reviewed and maintained. Actual and planned changes to this document will be announced in the Comfact Repository. The security controls are documented in accordance with ISO 27001 and are independently reviewed by an external certified auditor.

6.2.1 Timestamp Format

The TSTs issued by Comfact Timestamp conform with RFC 3161. Services compliant with this document issue timestamps using signatures based on either ECDSA, RSA with PKCS#1 version 1.5, or RSASSA-PSS. The hashing algorithms SHA2 256/384/512-bit are allowed to represent the data being timestamped. For additional information about the key size of the signature, please see Comfact CPS.

6.2.2 Time Accuracy

The TSTs are issued with an accuracy of ±1 second of UTC, or better. The time source is provided by Netnod's (funded by the Swedish Post and Telecom Authority) Internet time servers (Stratum-1) and traceable to within 250 nanoseconds of official Swedish time UTC(SP). The time included in the timestamp is that of the processing by the TSU and not the time of submission or acceptance. The time source is distributed in redundant pairs throughout Sweden to ensure redundancy. Each site has redundant servers, two cesium clocks, and two FPGA boards providing an extremely fast hardware implementation of NTP.

6.2.3 Limitations of Use

Comfact Timestamp may be used in relation to any legal transaction, without limitation, when the entity is an approved subscriber or relying party, unless otherwise specified in the service agreement. Comfact AB assumes no financial responsibility for improper use of the Comfact Timestamp service or issued TST. In no event will Comfact AB be liable for any loss of profit or data and any other damages. Comfact AB does not provide a public Timestamping service.

6.2.4 Obligations of the Subscribers

Please see "Terms and Conditions" in the Comfact Timestamp service contract for detailed information. Before placing any reliance on a timestamp issued by Comfact Timestamp, the subscriber must verify that the TST has been signed correctly and that the private key is not revoked. The subscriber should also inform its end-users (including any relevant Relying Parties) about the policies and practices outlined in this document.

6.2.5 Obligations of Relying Parties

Please see "Terms and Conditions" in the Comfact Timestamp service contract for detailed information. Before placing any reliance on a timestamp issued by Comfact Timestamp, the relying party must verify that the TST has been signed correctly and that the private key is not revoked. The relying party should also take into account any limitations on the usage of the TST and timestamping service as indicated in this document.

6.2.6 Timestamp Verification

All the information necessary to validate a signed TST (e.g., certificates and CRLs) can be found in the Comfact Repository. The timestamp verification shall include the following steps:

- **Verification of Response and TST** – The ASN.1 structure of the timestamp response and TST is first checked for conformance with RFC 3161, followed by the timestamp response's status code and mandatory attributes such as the certificate identifier of the TSA certificate.
- **Verification of Timestamp Issuer** – The integrity of the timestamp issuer's certificate is checked. This includes verifying if the certificate is recognized by Comfact TSU and CA, and if that same certificate is correctly referenced in the TST.
- **Verification of the Timestamp Revocation Status** – CRL distribution points are included in the certificate used to sign the timestamp and are available to verify the current revocation status of the certificate used in the timestamp.
- **Verification of the Integrity of the Timestamp** – Lastly, the integrity of the signature itself is verified by checking if the message-digest attribute value matches the expected value.

6.2.7 Applicable Law

Comfact Timestamp ensures compliance with applicable Swedish and European Union law at all times and also ensures compliance with:

- EU Regulation No 910/2014 – eIDAS
- EU Regulation No 2016/679 – GDPR
- EU Directive No 2016/2102 – The accessibility of the websites
- Web Content Accessibility Guidelines (WCAG) 2.1
- ETSI EN 319 401, ETSI EN 319 421, ETSI EN 319 422
- IETF RFC 3161

6.2.8 Service Availability

Comfact AB has implemented redundant IT environments to avoid a single point of failure. Comfact AB makes no express or implied representations or warranties regarding the availability or accuracy of Comfact Timestamp, and cannot guarantee 100% annual availability. Comfact AB bears no specific liability for any damage to Subscribers and Relying Parties in relation to valid TSTs relied upon in accordance with specific national laws and service agreement.

6.3 Terms and Conditions

6.3.1 Trust Service Applied

Terms and conditions for using the Comfact Timestamp service are available to all subscribers and relying parties and are available in the Comfact Repository. These terms and conditions apply to the Comfact Timestamp service, which is a trust service. The service applies this document “Comfact Timestamping”.

6.3.2 Limitation on Use

The use of the service is limited to subscribers that have a valid CSA and do not violate any applicable law. Use of the service is limited to activities that do not violate any applicable law. The subscriber shall notify Comfact AB without any delay of any breach of security or loss of integrity that comes to the knowledge of the subscriber. The expected lifetime of a TST is defined in the CSA.

6.3.3 Subscriber Obligations

Subscribers are obliged to use the Comfact Timestamp service according to the agreed CSA. Subscribers are obliged to inform Relying Parties about their obligations, the correct use of the issued timestamps, and any other relevant conditions.

6.3.4 Relying Party Information

The TST, when included in a document (e.g., a PDF), can be verified by opening the document in software such as Adobe, which automatically checks any included trust service tokens. Subscribers or relying parties can also verify the trust service token with any ETSI-compliant validation service.

6.3.5 TSP Event Logs Retention

Events of timestamping actions are retained for 10 years by default. If otherwise defined and requested by a Subscriber, this can be configured accordingly in the CSA.

6.3.6 Limitation of Liability

Comfact does not cover damages for loss of profit or any other indirect damage or loss of data, except for data loss caused by Comfact’s negligence in fulfilling its obligations as outlined in this document, “Comfact Timestamping”. Comfact AB is not liable for any damage suffered by relying parties if the subscriber or relying party breaches its duties according to this Policy. Comfact AB is also not liable for any damage resulting from a breach of its obligations due to force majeure.

6.3.7 Applicable Legal System

This document shall be construed in accordance with and governed by the laws of Sweden. Any dispute, controversy, or claim arising out of or in connection with this document, or its breach, termination, or invalidity, shall be settled in public court.

6.3.8 Complaints and Dispute Settlement

Any dispute, controversy, or claim arising out of or in connection with this document, or its breach, termination, or invalidity, shall be settled in a public court in Gothenburg, Sweden.

6.3.9 Assessment of the Trust Service Policy

Assessment of the trust service policy compliance is part of an internal, yearly review.

6.3.10 Contact Information

Contact information
Comfact AB Stora Badhusgatan 18 SE-411 21 Gothenburg, Sweden +46 (0)31 13 53 15 info@comfact.com

6.3.11 Availability

The availability of the Timestamping services provided by Comfact AB is generally outlined in section 6.2.8, and may be further detailed in the service agreement for the specific Subscriber.

6.4 Information Security Policy

Comfact AB has implemented an information security policy in accordance with ISO 27001. The policy is approved by Comfact Management and has been effectively implemented throughout the company. The policy is reviewed regularly and subjected to external audits. Any changes to the information security policy must be vetted and approved by Comfact Management.

6.4.1 General

No stipulation.

6.4.2 TSA Obligations Towards Subscribers

The document places no specific obligations on the Subscriber beyond any TSA-specific requirements stated in the Comfact Timestamp service agreement and under section 6.3.

6.5 Information for Relying Parties

Information and obligations for relying parties are outlined in section 6.2.5.

7 TSA Management and Operation

7.1 Introduction

Comfact AB has implemented an information security management system aligned with ISO 27001 to maintain and ensure the information security of its trust services. The provision of a timestamp in response to a request is at the discretion of Comfact AB and depends on the service level agreement with the subscriber.

7.2 Internal Organization

Comfact AB's organizational structure, policies, procedures, and security controls are applicable to Comfact Timestamp services. All practices applied by Comfact AB, including Comfact Timestamp, are non-discriminatory. The service is accessible to all applicants whose activities fall within its declared field of operation, who agree to abide by their obligations as specified in Comfact's terms and conditions, and who hold a service agreement with Comfact AB. Third-party agreements and relationships, including subcontractors, outsourcing, and similar, are documented according to ISO 27001. Furthermore, business continuity plans are outlined in section 7.13. Comfact AB is a legal entity according to Swedish national law and has a commercially reasonable level of liability insurance coverage to support its business practices. Disputes received from customers or other relying parties about the provisioning of the services or arising from this document that cannot be resolved shall be finally settled in a Swedish court.

7.3 Personnel Security

Personnel controls are outlined in the relevant information security policy, which is communicated to all employees impacted by it.

7.3.1 Qualifications, Experience, and Clearance Requirements

All employees holding a trusted role at Comfact shall sign a confidentiality (non-disclosure) agreement. Personnel employed for a trusted role shall possess the necessary qualifications, expert knowledge, and experience obtained through training and/or practice for the particular role. Upon applying for a trusted role, the person must present proof of the requisite qualifications and experience needed to perform the tasks. The assignment of a trusted role falls upon the Management Team. The job description of trusted roles (both temporary and permanent) and their responsibilities are clearly defined and must be accepted and signed by the person being assigned the trusted role. The job description includes the required skills and experience, specific functions on segregation of duties, policies on least privilege, access levels, procedures on background screening, as well as training and awareness.

7.3.2 Background Check Procedures

Prior to being employed in a trusted role, Comfact conducts a background interview. The background interview can be repeated for personnel holding a trusted role. The background interview includes the following:

- Check previous employment and other professional references,
- Check criminal records, and
- Check credit and financial records.

Background interviews are reviewed by human resources (HR) and security personnel, who determine the appropriateness of the employment. Background interviews containing undesirable reports (e.g., certain criminal records, indications of financial problems, and unfavorable or misrepresented references) may lead to the cancellation of employment offers, termination of existing trusted roles, or employment. This thorough review process ensures that only qualified and trustworthy individuals are employed in trusted roles.

7.3.3 Training Requirements

Upon employment, Comfact provides all personnel with training that covers awareness and skills on the following topics:

- Security policies and procedures, and data protection rules.
- Incident handling, disaster recovery, business continuity procedures.
- Basic Public Key Infrastructure (PKI).
- Basic security threat identification, e.g., phishing and social engineering.
- For managerial personnel and personnel with security responsibilities, basic risk assessment sufficient to carry out management functions.

In addition, training is given for the responsibilities and duties the person is expected to perform, and personnel are expected to keep up to date with industry-relevant best practices by attending conferences and seminars on work-related topics and practices. Information on security updates, relevant threats, and vulnerabilities are discussed and reviewed biweekly, and security updates on training and practices are conducted at least every year (12 months).

7.3.4 Retaining Frequency and Requirements

Retraining is conducted as frequently as necessary to ensure personnel maintain proficiency in performing their job duties and responsibilities.

7.3.5 Job Rotation Frequency and Sequence

No stipulation.

7.3.6 Sanctions for Unauthorized Actions

Failure to comply with the practices outlined in this document and security policies by any personnel holding a trusted role will result in appropriate disciplinary and administrative actions by HR. The trusted role will be suspended pending management review.

7.3.7 Independent Contractor Requirements

Independent contractors may, in certain circumstances, be used to fill trusted positions, abiding by the same criteria and security requirements as any other employee holding a trusted role. Independent contractors or consultants who have not yet completed the background check may only enter Comfact secure facilities if escorted and directly supervised by personnel already holding a trusted role.

7.3.8 Documentation Supplied to Personnel

Personnel involved in any capacity with Comfact Timestamping Services operations shall be made aware of the requirements, as well as any other relevant documentation, such as policies, practices, processes, and procedures, needed to maintain the integrity of Comfact Timestamping Services and perform their duties satisfactorily.

7.3.9 Trust Roles

Personnel (e.g., employees, consultants, and contractors) that manage Comfact infrastructure shall be considered trusted. However, people who obtain a role managing Comfact infrastructure must undergo and meet the required security screening. Ceased, terminated, or modified roles are updated or removed in a reasonably timely manner. Trusted personnel include those roles that have access to secure facilities, control authentication, and/or oversee cryptographic operations that may affect:

- Manage Subscriber requests and information.
- Review and conclude applications.
- Review and conclude revocation.
- Processing, rejection, and issuance of Timestamps.

All personnel in trusted roles must be free from conflicts of interest that might bias or prejudice the impartiality of Comfact Timestamping operations. Trusted personnel define the separation of trusted roles and access to information and application system functions. All trusted personnel shall be identified and authenticated before accessing and using critical applications related to Comfact Timestamping Services. These roles include:

- **Security Officers**: Overall responsibility for planning and overseeing the implementation and governance of security practices. This includes planning and reviewing logical, physical, and administrative security controls, as well as reviewing logs and archives for incidents, anomalies, attempted compromises, and so on.
- **System Administrators**: Authorized to install, configure, and maintain Comfact Timestamping Services systems.

- **System Operators**: Responsible for operating Comfact Timestamping Services systems and hardware on a day-to-day basis, including servers, network configuration of firewalls and routers, and maintaining systems updated, patched, and backed up for stability and recoverability.
- **System Auditor**: Responsible for accessing archives and audit logs of Comfact Timestamping Services systems, e.g., to control and review system operation, assess past or present anomalies, and suggest enhancements in controls, policies, and procedures.
- **HSM Administrator**: Authorized to install, configure, and maintain the hardware security modules, e.g., securely setting up or disposing of HSMs, and performing backups of private keys.
- **Systems Developer**: Authorized to develop, configure, and maintain Comfact Timestamping Service's custom software and applications.
- **Secret Share Holder**: Responsible for ensuring the confidentiality, integrity, and availability of a secret assigned (e.g., part of an m-or-of-n secret to enable a certain private CA key).

Further details of trusted roles within Comfact are specified in a classified document, and shall therefore not be detailed publicly.

7.3.10 Segregation of Duties

Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of Comfact AB's assets. At least two people are required to carry out manual, sensitive tasks. All participants must hold a trusted role as defined in section 7.3.9, with at least one being an administrator. The objective is to limit the possibility of malicious activities being carried out by a single actor.

7.3.11 Staff Training

Comfact provides all personnel with training on topics such as:

- Security policies, procedures, and data protection rules.
- Incident handling, disaster recovery, business continuity procedures.
- Basic Public Key Infrastructure (PKI).
- Basic security threat identification, e.g., phishing and social engineering.
- For managerial personnel and personnel with security responsibilities, basic risk assessment sufficient to carry out management functions.

In addition, training is provided for the specific responsibilities and duties the person is expected to perform. Personnel are expected to stay up to date with industry-relevant best practices by attending conferences and seminars on work-related topics. Information on security updates, relevant threats, and vulnerabilities is discussed and reviewed biweekly, with security updates on training and practices conducted at least annually.

7.3.12 Penalties for Unauthorized Actions

Failure to comply with this document, security policies, and practices by any personnel holding a trusted role will result in appropriate disciplinary and administrative actions by HR. The trusted role will be suspended pending management review.

7.4 Asset Management

In accordance with Comfact's ISO 27001 based ISMS, all relevant systems are identified and classified in an asset registry to protect those assets, consistent with the risk analysis. Information handling follows an established information classification scheme, regulating how information and data are handled at rest and in transit. This includes clear procedures for securely storing, deleting, and disposing of sensitive information or data.

7.5 Access Control

Comfact AB maintains appropriate physical, logical, and administrative access controls for information, systems, facilities, and hardware. System access is limited to authorized individuals only. Operators, administrators, and system auditors' access is administered by applying the principle of "least privilege" when configuring access privileges in accordance with Comfact AB's access control policy. All access (physical and logical) is audited, and personnel are accountable for their own activities. Additionally, the removal and suspension of user accounts shall be administered in a timely manner.

7.6 Cryptographic Controls

7.6.1 General

Comfact Timestamping Services use hardware security modules (HSMs), certified to FIPS 140-2 level 3, to protect all private keys hosted and retained by Comfact.

7.6.2 TSU Key Generation

Comfact's key generation practices for private key pairs are described in Comfact CPS and are applicable to this document. For example, the key size used for the generated key pairs follows the documented practices in Comfact CPS. Keys used in Comfact Timestamping services are generated under M of N requirements, with at least dual control by authorized personnel. The authorized personnel for this task are limited to Comfact AB Administrators.

7.6.3 TSU Private Key Protection

To maintain the high confidentiality and reliability of cryptographic keys, cryptographic operations and keys used in Comfact Timestamping and similar services are solely kept within an HSM certified to FIPS 140-2 level 3. Private keys can be backed up, but only in encrypted form and stored on specialized hardware, such as cryptographic smart cards. They can only be restored by applying the M of N requirement, as the backed-up key is always split in a shared secret scheme. Each part of the backed-up key is held in isolation by trusted roles within Comfact AB, ensuring at least dual control in a physically secured environment.

7.6.4 TSU Public Key Certificate

Comfact Timestamping ensures the integrity and authenticity of the TSU signature verification (public) keys with the following steps:

- TSU signature verification (public) keys are made available to Relying Parties in a public key certificate (X.509 v3). The certificates are published in the Comfact Repository.
- Comfact TSU does not issue timestamps before the signature verification (public) key is loaded into the TSU or its cryptographic device. When the public key is loaded into the TSU, the TSA verifies that the certificate was signed by a trusted certificate authority.
- Checking that Comfact TSU certificates have not been renewed.
- Validation information regarding the TSU certificates is updated periodically and is available through their CRL distribution points.

Additional information is provided in "Comfact CPS" in the Comfact Repository.

7.6.5 Rekeying TSU's Key

Each Comfact TSU certificate's lifetime has been chosen based on considerations of its algorithm and key length security, the details of which can be found in Comfact CPS along with routines for handling key compromise and revocation. The TSU rejects any attempt to issue timestamps once a private key has expired or been revoked. This ensures the integrity and security of the timestamping process, maintaining trust in the service.

7.6.6 Life Cycle Management of Signing Cryptographic Hardware

The following particular requirements apply to Comfact Timestamp:

- Comfact AB has procedures and instructions in place to control if any cryptographic hardware has been tampered with during shipment or storage.
- Installation, activation, and duplication of TSU's signing keys are performed using an M of N rule requiring at least dual control and authorized personnel with trusted roles.
- Private keys are erased from usage and the hardware security modules upon device retirement, in accordance with the manufacturer's instructions.

7.6.7 End of TSU Key Life Cycle

TSU private keys are replaced upon their expiration. The lifetime of the TSU key is defined in Comfact CPS along with procedures for how a new key is put in place when a TSU key expires. After expiration, TSU private keys, including any backups, are securely erased.

7.7 Timestamping

7.7.1 Timestamp Issuance

Comfact Timestamp follows the IETF RFC 3161 specification, as profiled in ETSI EN 319 422, to issue timestamps. TSTs issued by a Comfact TSU carry the object identifier (OID) of the present PS. The service URL and correlating credentials are specified in the Subscriber's contract agreement. The response format follows the requirements outlined in IETF RFC 3161, section 2.4.2, and applies the required fields and values as specified by ETSI EN 319 422.

Version	Version 1
Policy	OID 0.4.0.2023.1.1 (ETSI EN 319 421)
messageImprint	A structure that contains the hash of the date and algorithm used. The value is exactly equal to that of received in the request.
serialNumber	Unique serial number of the generated timestamp.
genTime	Time stamp assigned by Comfact Timestamping Service.
accuracy	Indicates the precision of the time provided.
ordering	FALSE
nonce	Random integer used to connect the request with the response and present if it appeared in the request.
tsa	TSA identifier of Comfact Timestamping Services.
extension	Not used.

In addition, the SignedData structure (in which the TSTInfo structure is encapsulated) contains the certificate identifier of the TSU certificate (as an ESSCertIDv2), included as a signerInfo attribute inside a SigningCertificateV2 attribute, as specified in IETF RFC 5816, section 2.2.1. Comfact TSU can be configured to use one of the following signature algorithms: RSA with PKCS#1 v1.5, RSA with PKCS#1 v2.1 (RSASSA-PSS), or ECDSA. The accepted digest algorithms are SHA-2 256/384/512-bit. Comfact Timestamp logs all issued TSTs and their unique serial numbers, in accordance with RFC 3161 requirements, and can therefore prove the existence of a TST at the request of a Relying Party.

7.7.2 Clock Synchronization with UTC

Comfact Timestamp provides time with an accuracy of ±1 second of UTC, or better, by continuous calibration with multiple independent, external time sources to protect against changes to the clock.

7.8 Physical and Environmental Security

7.8.1 Physical Production Area

Comfact Timestamp is located in a highly secure physical environment. The physical location is independently monitored by a third party, as well as surveillance equipment maintained by Comfact AB in the security area. Comfact's equipment resides behind a series of entry points and alarms, each requiring some form of authentication (e.g., multifactor and/or physical keys). Comfact AB equipment is locked in a separate rack, access to which is limited to authorized, trusted Comfact roles. Each entry and exit to the physically secured area is logged, and non-authorized persons are always accompanied by an authorized person while in the secure area. The physical security is protected against various types of threats and is geographically separate from Comfact AB office spaces. Protection includes measures against physical access such as breaking and entering, natural disasters, fire, and power failure.

7.8.2 Physical Development Area

The systems and software development area are protected by physical access controls, alarms, and surveillance systems. Systems used for and connected to production are protected from unauthorized access, only allowed by trusted roles, and protected from unauthorized network access.

7.9 Operation Security

The following requirements refer to the security controls related to computers and applications to ensure high system security. Controls incorporated by Comfact AB include:

- Version control for any changes made and mandatory code review procedures.
- Protection of TSP and similar systems against malicious and unauthorized software.
- Thorough testing and review of systems developed and designed by Comfact AB by experienced systems developers, following a secure development lifecycle.
- Implementation of policies defining accepted procedures and guidelines throughout the company that align with ISO 27001.
- Mandatory authentication at the operating system level and application.
- Segregation of duties in accordance with employees' roles.
- Procedures for exchanging and storing sensitive information, including databases.
- Continuous assessment and application of security patches.
- Key restoration procedures in case of hardware security module malfunction.
- Monitoring of hardware capacity (e.g., server disk space, RAM, and CPU usage) to ensure adequate processing power and storage.
- Procedures for monitoring, reporting, and recovering from incidents and disasters.

7.10 Network Security

Comfact AB's networks employ protective controls such as firewalls (with a deny-all baseline) and intrusion detection and protection systems. Trusted services and workstations are connected to a segmented LAN with controlled access, divided into zones based on risk assessments. For example, all systems related to PKI, except for the public repository, are kept in a high-security zone only available to trusted roles. Connections between zones are limited to a "need-to-know" basis and established only through secured channels, such as VPN, by authorized people with trusted roles. Inbound access from the internet is not allowed for high-security systems. Network configurations and design have been examined by an independent external third party. Internal vulnerability scans are performed regularly, and the results are assessed as part of the continuous risk management process. The external network connection to the internet is redundant to ensure high availability. Similarly, a separate environment mirroring the primary site is available for redundancy.

7.11 Incident Management

System activities, access, logs, and users of the systems, including requests, are monitored. Anomalies and abnormal system activities that indicate potential security violations, including intrusion into Comfact Timestamp's network or systems, are detected and reported as alarms to the system owner. Comfact Timestamp also monitors the start-up and shutdown of logging functions, as well as the availability and utilization of required services within the network. This includes regularly reviewing audit logs to identify evidence of malicious activities. Monitoring activities take into account the sensitivity of any information collected or analyzed. Detected incidents are acted upon in a timely and coordinated manner to respond quickly and limit the impact of the incident and breaches of security. Follow-up on each alarm or detected incident is done by the Comfact Systems Administrator group. The follow-up ensures that relevant incidents are reported, if appropriate, to external parties (such as Data Controllers, the national supervisory body, and/or affected natural or legal persons) in line with applicable regulatory rules, within 24 hours of identified breaches considered to have a significant impact on Comfact Timestamp. Any identified vulnerability considered critical, and which has not previously been addressed by Comfact Systems Administrators, shall be addressed within 48 hours of its discovery. This work is aligned with the risk analysis conducted in accordance with ISO 27001.

7.12 Collection of Evidence

To analyze and mitigate vulnerabilities in the systems, as well as provide evidence in any legal proceedings, records are kept accessible for an appropriate period (necessary for providing legal evidence, as notified in Comfact Timestamp terms and conditions) after the activities of Comfact Timestamp have ceased. This ensures the continuity of Comfact services. The confidentiality and integrity of current and archived records are maintained. Records concerning the operation of services are kept confidentially. However, records concerning the operation of services are made available, if necessary, to provide evidence of the correct operation of the service for legal proceedings. In particular, records concerning Comfact Timestamp's environment and key management are monitored and logged. This includes records concerning all events related to the life cycle of the TSU keys and certificates. Records are stored and maintained on dedicated, isolated systems in parallel storage to make them more difficult to delete, destroy, or otherwise tamper with.

7.13 Business Continuity Management

Comfact AB has defined and maintained incident response and business continuity plans to enact in case of an incident or disaster, such as the compromise (or suspected compromise) of a private signing key, loss of calibration of a TSU clock, or compromise of other TSA credentials. Operations are restored within the delay established in the continuity plan, while mitigating or remedying the disaster. Should any incident or disaster occur, or be suspected to have occurred, Comfact makes available to all subscribers and relying parties a description of the compromise that occurred. Meanwhile, no timestamps will be issued until steps are taken to fully recover from the compromise. Steps, if necessary, include:

- Notifying the security manager to coordinate further measures.
- Starting a security audit of the remaining keys (integrity checks, log analysis, etc.).
- Notify the incident to subscribers and/or relying parties.

In case of a major compromise or loss of calibration, Comfact Timestamp will make available to all subscribers and relying parties' information that can be used to identify the timestamps that may have been affected, unless this breaches the privacy of the TSA's users or the security of the TSA services.

7.14 TSA Termination and Termination Plans

In the event of business or operation termination, potential disruption to subscribers and relying parties shall be minimized. This means continued maintenance of information required to verify the validity and correctness of Comfact Timestamp, which will be transferred to a trusted, reliable party for a reasonable period. This includes public keys and CRLs. More details on the general termination plan are outlined in Comfact CPS, which is also applicable in this context. Before Comfact Timestamp terminates its services, all subscribers and other entities with which Comfact Timestamp has agreements or established relations, such as relying parties and national supervisory bodies, shall be informed.

Similarly, each of these entities, including subcontractors, will have their authorization terminated so they cannot act on behalf of Comfact Timestamp in issuing timestamps. Furthermore, Comfact shall revoke the TSU's certificate and then destroy the TSA's private keys, including backup copies. In the event of business or operation termination, Comfact has arranged to cover the cost to fulfill these minimum requirements. If Comfact becomes bankrupt or is otherwise unable to cover the cost, Comfact will cover the minimum requirements as far as possible within the constraints of applicable bankruptcy legislation.

7.15 Compliance

Comfact Timestamp ensures compliance with applicable laws and standards. In addition, the following specific requirements apply:

- EU Regulation No 910/2014 – eIDAS
- EU Regulation No 2016/679 – GDPR
- EU Directive No 2016/2102 – The accessibility of the websites
- Web Content Accessibility Guidelines (WCAG) 2.1
- ETSI EN 319 401, ETSI EN 319 421, ETSI EN 319 422, ETSI EN 301 549
- IETF RFC 3161

-@-