COMFACT

Comfact Timestamping

Policy and practice statement

Version date	**2021-12-07**
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
2021-11-26	First public version of new release of document.	Management Team

COMFACT

Table of contents

1 Scope

In Comfact AB's provides robust trust services and time-stamps is an important function. A time-stamp provides an electronically signed assertion which proves that arbitrary data existed before a specific time, and that it has not been manipulated or altered since. Comfact Time-stamping service (hereinafter "Comfact Timestamp") is fully compliant with the IETF RFC 3161 specifications, as profiled in ETSI EN 319 422, which defines the time-stamp protocol.

The present document specifies policy and security requirements relating to the operation and management practices of Comfact's issuing of time-stamps. It aims to meet the general requirements of the international community to provide trust and confidence in electronic transactions, including, amongst others, applicable requirements for Trust Service Providers.

Comfact Timestamp issues timestamp tokens in accordance with ETSI EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

Comfact Timestamp provides time-stamps for digitally signed and unsigned documents.

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 Time-Stamps
ETSI EN 319 422	Electronic Signatures and Infrastructures (ESI); Time-stamping Protocol and Time-stamp 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 Time-stamp 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

P&PS	Policy and Practice Statement (This document)
TSA	Time-Stamping Authority
TSP	Trust Service Provider
TST	Time-stamp token
TSU	Time-Stamping 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 Time-stamping	Trust service provided by Comfact AB for issuing time-stamps
Comfact Timestamping	This document
Coordinated Universal Time	Time scale based on the second as defined in Recommendation ITU-R
Relying party	Recipient of a time-stamp who relies on that time-stamp
Subscriber	Legal or natural person to whom a time-stamp token is issued to and who is bound to subscriber obligations included in a Comfact Service Agreement
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 time-stamp to a particular community and/or class of application with common security requirements
Time-stamp token	Indicates that a datum existed at a particular point in time establishing evidence that the datum existed before that time.
Time-Stamping Authority	TSP providing time-stamping services using one or more time-stamping units
Time-stamping service	Trust service for issuing time-stamps
Time-Stamping Unit	Set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time
Trust service	Electronic service that enhances trust and confidence in electronic transactions

Trust Service Provider	Entity which provides one or more trust services
TSA Disclosure statement	Set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to subscribers and relying parties, for example to meet regulatory requirements
TSA practice statement	Statement of the practices that a TSA employs in issuing time-stamp
TSA system	Composition of IT products and components organized to support the provision of time-stamping 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

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 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 service

Comfact Timestamp service include the following components:

- **Time-stamping Provision**: The technical components that issues the time-stamp tokens, henceforth referred to as TSTs.
- **Time-stamping management**: The service component that monitors and controls the time-stamping operation to ensure that the service provided is as specified in Comfact CPS and Comfact Timestamp P&PS, including ensuring that the clock used for time-stamping is correctly synchronized with the UTC time source.

4.3 Time-stamping Authority (TSA)

A Trust Service Provider (TSP) providing time-stamping services is called the Time-Stamping Authority (TSA). Comfact Timestamp takes the overall responsibility for the provision of the time-stamping services as identified in section 4.2.

Comfact Timestamp has the overall responsibility for the operation of one or more Time-Stamping Units (TSUs), which creates and signs TSTs on behalf of the TSA. Each TSU has its own private key assigned to it. Below is a summary of the current Comfact TSUs and their issuers:

TSU Subject	TSU Issuer	Trust Anchor
CN = Comfact Time Stamping Authority C = SE O = Comfact AB OI = 5563426666	CN = Comfact Seal CA G1 OU = Certificate Services OI = 5563426666 O = Comfact AB C = SE	CN = Comfact Root CA G1 OU = Certificate Services O = Comfact AB C = SE

4.4 Time-Stamping Authority parties

4.4.1 Subscriber

A subscriber to Comfact Timestamp is an entity, natural or legal person, that holds a service agreement (CSA) with Comfact AB, and have agreed to its terms and conditions. When the subscriber is a legal person, it is responsible for the activities of their associated end-users and Relying Parties, and are expected to inform them of appropriate usage of Comfact Timestamp services according to the agreed terms and conditions.

When the subscriber is a natural person, that end-user will be held directly responsible if its obligations are not correctly fulfilled according to the service agreement (CSA) with Comfact AB.

4.4.2 TSA relying parties

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

4.5 Time-stamp policy and TSA practice statement

Comfact Timestamp Policy (TSP) and Comfact Timestamp Practice (PS) Statement have been merged into this one document. Comfact Timestamp P&PS specifies a time-stamp policy and practice statement to meet the requirements for trusted time-stamping services, and is based on the P&PS as specified in ETSI EN 319 421, and is applied to Comfact Timestamp issuing TSTs.

This document, Comfact Timestamp P&PS, is a public document and available in the Comfact Repository.

5 Time-stamp policies and general requirements

5.1 General

Comfact Timestamp issues the TSTs in accordance with ETSI EN 319 421 and the current Time-Stamping Policy. The TSTs are issued with an accuracy of ±1 second of the UTC, or better, and contains an identifier to the applicable policy (see section 5.2). Comfact Timestamp TSUs meet the technical specifications of ETSI EN 319 422 and RFC 3161.

5.2 Identification

The object-identifier (OID) of the Comfact Time-Stamping Policy specified for this document is:

1.2.752.253.8.2

By including this OID in the generated time-stamps, Comfact Timestamp claims conformance to this Time-Stamping policy, as defined in this document, as well as ETSI BTSP best practices policy for time-stamps (OID 0.4.0.2023.1.1).

5.3 User community and applicability

5.3.1 Best practices time-stamp policy

The closed community of Comfact Timestamp only includes Subscribers and their Relying Parties. Comfact AB does not provide public time-stamp services.

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

6 Policies and practices

6.1 Risk assessment

Comfact AB is certified according to ISO 27001 and performs risk assessments on a regular basis to ensure the quality and reliability of its time-stamping services.

Comfact AB's risk assessment identifies, analyses and evaluates trust service risks regularly, and takes into account both business and technical issues. Based on this, appropriate risk treatment measures are selected accordingly.

6.2 Trust Service Practice Statement

At Comfact AB, information security is of the highest importance. In accordance with Comfact ABs ISO 27001 certification, a variety of security controls have been implemented to ensure the quality and reliability of the time-stamping services operation. This work is continually ongoing in order to remain updated and effective against new threats.

Similarly, this document, Comfact Timestamp Authority P&PS, is regularly reviewed and maintained. Actual and planned changes to this document will be announced in Comfact Repository.

The security controls are documented in accordance with ISO 27001, and are independently reviewed by an external certified auditor.

6.2.1 Time-stamp format

The issued TSTs by Comfact Timestamp are compliant with RFC 3161. The service issues the time-stamps with the signature algorithm RSA with PKCS#1 version 1.5, and accepts the SHA2 256/384/512-bit digest algorithm. The RSA key length is 2048 bit.

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 the hosting environment, providing PCI DSS compliant time conformance. The time included in the time-stamp is that of the processing by the TSU and not the time of submission or acceptance.

The time server synchronizes all systems either NTP- or SNTP-compatible and uses a built-in GPS radio clock as its reference time source. A highly stable and precise oscillator is capable of bridging interferences or a temporary loss of reception.

The time synchronization data is reliably signed and secured by symmetric keys and the NTP autokey procedures. This protects against manipulated time and man-in-the-middle attacks and allows for NTP packet verification when received.

6.2.3 Limitations of the service

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 service Comfact Timestamp 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 Time-stamping service

6.2.4 Obligations of the subscribers

Please see "Terms and conditions" in Comfact Timestamp service contract for detailed information. Before placing any reliance on a time-stamp issued by Comfact Timestamp, the subscriber must verify that the TST has been signed correctly, and that the private key is not revoked.

6.2.5 Obligations of relying parties

Please see "Terms and conditions" in Comfact Timestamp service contract for detailed information. Before placing any reliance on a time-stamp issued by Comfact Timestamp, the relying party must verify that the TST has been signed correctly, and that the private key is not revoked.

6.2.6 Time-stamp verification

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

- ***Verification of Response and TST*** – The ASN.1 structure of the time-stamp response and TST is first checked. Followed by the time-stamp response's status code, and mandatory attributes such as e.g., the certificate identifier of the TSA certificate.
- ***Verification of time-stamp issuer*** – The integrity of the time-stamp issuers certificate is checked. This includes controlling if the certificate is recognized by Comfact TSU and CA, and if that same certificate is correctly referenced to in the TST.
- ***Verification of the time-stamp revocation status*** – CRL distribution points are included in the certificate used to sign the time-stamp, and available to verify the current revocation status of the certificate used in the time-stamp.
- ***Verification of the integrity of the time-stamp*** – 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, ETSI EN 301 549
- IETF RFC 3161

6.2.8 Service availability

Comfact AB has implemented the following measures to provide high availability of the service:

- Redundant IT environments and systems to avoid single point of failures
- Redundant internet connection to avoid loss of service due to network failures
- Use of uninterruptable power sources (UPS)

Comfact AB makes no express or implied representations or warranties relating to the availability or accuracy of Comfact Timestamp and an annual availability of 100% cannot be guaranteed. Comfact AB bears no specific liability for damage to Subscribers and Relying Parties in relationship to valid TST relied upon in accordance with specific national laws and service agreements entered into.

6.3 Terms and conditions

Comfact AB publishes its terms and conditions in Comfact Repository.

6.3.1 Trust service applied

Terms and conditions for using Comfact Timestamp service are available to all subscribers and relying parties, and available in Comfact Repository.

These terms and conditions apply to the service Comfact Timestamp 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 come to the knowledge of the subscriber. The expected life-time 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 time-stamps and of any other relevant conditions.

6.3.4 Relying party information

The TST in e.g., included in a PDF document, can be verified by opening the document in software such as Adobe which automatically checks any included trust service tokens. It is also possible for a subscriber or relying part to verify the trust service token with any ETSI compliant validation service.

6.3.5 TSP event logs

Events of time-stamping actions are by default retained for 10 years. If defined otherwise and requested differently by a Subscriber this is configured accordingly in the CSA.

6.3.6 Limitation of liability

Comfact does not in any event include damage for loss of profit or any other indirect damage or loss of data, except such loss of data caused by Comfact's negligence to fulfill its obligations in this document "Comfact Timestamping". No Party is liable for the other Party's liability towards a third party. The limitation of liability in this clause does not apply in the event of personal injury or in the event of intent or gross negligence. A Party shall, in order to keep its right to compensation, make claims for damages to the other Party within two (2) months from the time of damage.

Comfact AB may not be held liable for any damage suffered by relying parties where the subscriber or relying party breaches its duties according to this Policy. Comfact AB may also not be held liable for any damage resulting from breach of its obligations as a result of force majeure.

6.3.7 Applicable legal system

This document shall be construed in accordance with and be governed by the laws of Sweden. Any dispute, controversy or claim arising out of or in connection with this document, or the breach, termination or invalidity thereof, 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 the breach, termination or invalidity thereof, 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 included Comfact AB in yearly ISO 27001 review by an accredited evaluator. This review includes all Comfact services as stated in the ISO certificate: "Development, operation and support of trust services. All in accordance with statement of applicability established 2019-01-09.

6.3.10 Contact information

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

6.4 Information security policy

Comfact AB including its service Comfact Timestamp, 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, as such, reviewed on a regular basis, and subjected to external audits. The Comfact Management approves any changes in the information security policy.

All Comfact employees must adhere to this policy and its security concepts.

The current information security policy (ISP) is available in the Comfact Repository.

6.5 TSA obligations

6.5.1 General

The present document places the following obligations on the Subscriber:

- The subscriber is obligated to verify that the TST has been correctly signed with the corresponding key of the TSU certificate, and ensure that the private key used to sign the TST has not been revoked
- Subscribers must use secure cryptographic functions for time-stamping requests
- Subscribers must inform its end users (including any relevant Relying Parties) about Comfact AB P&PS and CP/CPS
- Subscriber obligations are also defined in Comfact Timestamp service contract

6.5.2 TSA obligations towards subscribers

The present document places no specific obligations on the Subscriber beyond any TSA specific requirements stated in Comfact Timestamp service contract, or otherwise stated under section "Terms and Conditions" in the present document.

6.6 Information for relying parties

The present document places the following obligations on Relying Parties:

- Relying Parties are obligated to verify that the TST has been correctly signed with the corresponding key of the TSU certificate, and ensure that the private key used to sign the TST has not been revoked
- Relying Parties should take into account any limitations on usage of the time-stamp indicated by this P&PS and any other precautions prescribed in agreements or elsewhere

7 TSA management and operations

7.1 Introduction

Comfact AB has implemented an information security management system in accordance with ISO 27001, to maintain and ensure the information security of its trust services.

7.2 Internal organization

Comfact ABs 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 available to customers with a service agreement including terms and conditions.

Third-party agreements and relationships, including subcontractor's, outsourcing and similar, are documented as according to ISO 27001. Furthermore, business continuity plans can be found as outlined in section 7.13. Comfact AB is a legal entity according to Swedish national law.

7.3 Personnel security

Personnel controls are outlined in the relevant information security policy which is communicated with all employees impacted by it. However, considering the classified nature of the information security policy, only the following excerpts are elaborated on.

7.3.1 Qualifications, experience, and clearance requirements

All employees holding a trusted role at Comfact shall sign a confidentiality (non-disclosure) agreement. Personnel that hold or is employed for a trusted role shall possess qualification, expert knowledge and experience obtained through training and/or attained from practice for the particular role. Upon applying for a trusted role, the person must present proof of the requisite qualifications and experiences needed to perform the tasks. Note that the assignment of a trusted role falls upon Management Team.

The job description of trusted roles (both temporary and permanent) and their responsibilities are clearly defined in which must first be accepted and signed by the person being assigned a trusted role. The job description includes the required skills and experiences, but also specific functions on segregation of duties and policies on least privilege, access levels, procedure on background screening, as well as training and awareness.

7.3.2 Background check procedures

Prior to being employed under 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 of criminal records, and
- Check of credit and financial records.

Background interviews are reviewed by human resources (HR) and security personnel, who will 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) maybe lead to cancellation of employment offers, termination of existing trusted roles or employment.

7.3.3 Training requirements

Upon employment, Comfact provides all personnel with training that cover 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 responsibilities and duties the person is expected to perform, and personnel is expected to keep up to date with industry-relevant best practice by attending e.g., conferences and seminar on work related topics and practices. Information on security updates, relevant threats, and vulnerabilities are discussed and reviewed on a biweekly basis, and security updates on training and practices at least every year (12 months).

7.3.4 Retaining frequency and requirements

Retraining is frequented to the extent that ensures personnel maintains proficiency to perform 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 this CPS, 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 whilst pending management review.

7.3.7 Independent contractor requirements

Independent contractors may, in certain circumstances, be used to fill trusted positions, abiding the same criteria and security requirements as would any other employee holding a trusted role.

Independent contractor or consultant that have yet to complete 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 as trusted. 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 within 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 Time-stamps

All personnel in trusted roles must be free from conflict of interest that might bias or prejudice the impartiality of Comfact Timestamping operations.

Trusted personnel define separation of trusted roles and access to information and application system functions. Note that all trusted personnel shall be identified and authenticated before access and use to critical applications related to Comfact Timestamping Services. These roles include:

- **Security Officers**: Overall responsibility for planning and overseeing implementation and governance of security practices. This includes planning and reviewing logical, physical, and administrative security controls as well as review logs and archives for incidents, anomalies, attempted compromise, 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 maintain 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, polices, and procedures.
- **HSM Administrator**: Authorized to install, configure, and maintain the hardware security modules, e.g., securely setup or dispose of HSMs, and perform backups of private keys.
- **Systems Developer**: Authorized to develop, configure, and maintain Comfact Timestamping Service's custom software and applications.
- **Secret Share Holder**: Responsible to ensure 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

The number of persons required to carry out manual, sensitive tasks are at least two (2) people. All participants shall hold a trusted role as defined in section 7.3.9, where at least one shall be an administrator. The objective is to limit the possibility of malicious activities being carried out by one actor.

The following activities are examples which shall only be allowed with multiple-person control (n-out-of-m):

- Access to the hosting area of the Comfact Timestamping Services, where HSM containing private keys as well as servers with CA system and related material are stored and operate
- Changes to the HSM, e.g., creating, removing, activation, or backing up of private keys
- Access to backups of private keys

The following activities are examples which shall only be allowed after a person has been successfully identified with strong authentication or multi-person control (n-out-of-m):

- Access to and administration of application servers of Comfact Timestamping Services
- Access to and administration of Comfact Certificate Services PKI repository
- Access to and administration of databases related to Comfact Timestamping services

7.3.11 Staff training

Upon employment, Comfact provides all personnel with training that cover 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 responsibilities and duties the person is expected to perform, and personnel is expected to keep up to date with industry-relevant best practice by attending e.g.,

conferences and seminar on work related topics and practices. Information on security updates, relevant threats, and vulnerabilities are discussed and reviewed on a biweekly basis, and security updates on training and practices at least every year (12 months).

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 the Management Team. The trusted role will be suspended whilst pending management review.

7.4 Asset management

According to operations and measures implemented in accordance with Comfact ISO 27001 ISMS, all relevant systems are identified and classified in an asset registry for the protection of those assets, consistent with the risk analysis. Furthermore, information handling follows an established information classification scheme, regulating how information and data is handled at rest and in transit. This includes clear procedures for, e.g., how sensitive information or data must be securely stored, deleted, and disposed of.

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.

Various different security layers are in place to maintain high security of physical, logical, and administrative access and operation. In particular:

- Firewalls, configured to protect unauthorized access, including access by subscribers and third parties. The firewall is also configured to prevent all protocols and accesses not required for the operation of the TSP or similar services provided by Comfact AB.
- All system accounts and operations are administered by Comfact AB Administrators, which also administrates and audits the system. This includes management and removal of system access in a timely manner.
- User accounts are controlled and limited to their trusted roles. This includes segregation of duties, such as separation of security administration and operation functions. For example, system utility programs are restricted and controlled.
- Event logs are maintained in order for relevant analysis and monitoring, and to enforce accountability for a user's activities on a system.
- According to defined information classification scheme, sensitive data is protected from re-used storage objects, such as deleted files.
- Physical access to Comfact AB and its IT environments is controlled through an access control system including white-listing, smart cards and security escort. Intrusion detection systems, as well as video surveillance systems are installed as well.
- Comfact ABs systems are constantly monitoring and logging events, including successful and failed authentications and similar events.

7.6 Cryptographic controls

7.6.1 General

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

7.6.2 TSU key generation

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

Comfact TSU uses RSA key pairs, with a length of 2048 bits, dedicated solely for signing TSTs. All keys used for Comfact Timestamp related purposes are generated in a FIPS 140-2, level 3 hardware security module (HSM).

7.6.3 TSU private key protection

To maintain high confidentiality and reliably of cryptographic keys, cryptographic keys included in Comfact Timestamping and similar services are generated and used solely within a HSM certified to FIPS 140-2 level 3.

Private keys can be backed up, but only in encrypted form and stored on specialized hardware, i.e., cryptographic smart cards, and 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 isolated by trusted roles within Comfact AB, and ensures 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 Comfact Repository
- Comfact TSU does not issue time-stamps before the signature verification (public) key is loaded into the TSU or its cryptographic device. When the public key is loaded in the TSU, the TSA verifies that the certificate was signed by a trusted certificate authority
- Comfact TSU certificates are not 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 Comfact repository.

7.6.5 Rekeying TSU’s key

Each Comfact TSU certificate lifetime has been chosen based on considerations of its algorithm and key length security. The keys of the TSU have a maximum operating life of 2 years, half of that of its issuer. The issuer is however renewed after half its lifetime, to ensure it can rekey and issue new TSU signing certificates and CRLs throughout its full lifecycle. TSU private signing keys are thus replaced before the end of their validity period. The TSU rejects any attempt to issue time-stamps once a private key has expired.

7.6.6 Life cycle management of signing cryptographic hardware

The following particular requirements apply for Comfact Timestamp:

- Comfact AB have procedures and instructions in place to ensure that any time-stamp signing cryptographic hardware are not tampered with during shipment or storage
- Installation, activation and duplication of TSU's signing keys are performed only by M of N authorized personnel with trusted roles, requiring at least dual control in a physically secured environment
- Private keys are erased from usage and modules upon device retirement, in accordance with manufacturer's instructions

7.6.7 End of TSU key life cycle

TSU private keys are replaced upon their expiration. After expiration, TSU private signing keys, or any key part, including any copies are securely erased in a way the private keys cannot be retrieved.

7.7 Time-stamping

7.7.1 Time-stamp issuance

Comfact Timestamp follows the IETF RFC 3161 specification, as profiled in ETSI EN 319 422, to issue time-stamps. TSTs issued by a Comfact TSU carries the object identifier (OID) of the present P&PS. The service URL and correlating credentials are specified in the Subscriber's contract agreement.

Version	Version 1
Policy	OID 0.4.0.2023.1.1 (ETSI EN 319 421)
messageImprint	Structure that contains the hash of the dated document and the hash algorithm used and sent by the client. The value is exactly equal to that of received in the request.
serialNumber	Unique serial number of the generated time-stamp
genTime	Time stamp assigned by Comfact Timestamping Service
accuracy	Indicates the precision of the time provided.
ordering	FALSE
nonce	Random integern 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

Comfact TSU issues the time-stamps using the signature algorithm RSA with PKCS#1 version 1.5, and accepts usage of SHA2 256/384/512-bit digest algorithm. The RSA key length is 2048 bit.

Comfact Timestamp logs all issued TSTs and their unique serial numbers in accordance with RFC 3161 requirements. Therefore, Comfact Timestamp can 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 ±1 second of UTC, or better, by calibration with multiple independent time sources. These include e.g., Meinberg LANTIME M300/GPS and local NTP servers with external time authorities. No time-stamps will be issued if the time has drifted outside of the declared accuracy.

7.8 Physical and environmental security

7.8.1 Physical production area

Comfact Timestamp is located in a highly secure physical environment. The physical protection includes both logical and physical access controls to both systems and hardware. The physical location is independently monitored by a third-party, as well as surveillance equipment maintained by Comfact AB in the security area. Each person requesting entry to the facility has to register and identify themselves, checked against a white-list, time marked for entrance and exit, and during the

stay be accompanied by a security escort. Finally, Comfact AB equipment is locked in a separate high security area within the IT environment, where only a limited trusted role has access to.

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 disaster, 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 to, and connected to, production is 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 systems security. Controls incorporated by Comfact AB includes:

- Version control is applied for any changes made, and mandatory code review procedure follows
- TSP, and similar systems, are protected against malicious and unauthorized software
- Systems developed and designed by Comfact AB is thoroughly tested, and discussed by experienced systems developers, following a secure development lifecycle
- Policy for defining accepted procedures and guidelines has been implemented throughout the company, in relation to ISO 27001
- Mandatory authentication at operating system level and application
- Possibility of being audited in terms of security
- Segregation of duties, in accordance with employees' roles
- Procedures for how to exchange and store sensitive information, including databases
- Key restoration procedures, should a hardware security module malfunction
- Means of monitoring and reporting incidents

7.10 Network security

Comfact AB trusted services and workstations are connected to a segregated LAN, with controlled access, and divided into zones based on risk assessments considering their sensitive nature. All systems related to PKI, with exception of the public repository, are kept in a high security zone only available to trusted roles. Connections between zones are limited to "need to know" basis, and established only through secured channels, and provide identification. Therefore, access from the internet is not available for high security systems, and other systems are protected by a firewall. Network configurations and design has been examined by an independent external third-party.

The external network connection to the internet is redundant to ensure high availability. Similarly, a geographically separate environment mirroring the primary site is also available.

7.11 Incident management

System activities, access, logs and users of the systems, including requests, are monitored. In particular, anomalies and abnormal system activities that indicate potential security violations, including intrusion into Comfact Timestamp's network or systems, have measures to be detected and reported as alarms to the system owner. Similarly, Comfact Timestamp monitors the start-up and shutdown of the logging functions, as well as the availability and utilization of required services within the network. This also includes regularly review audit logs to identify evidence of malicious activities. Monitoring activities take into account of the sensitivity of any information collected or analyzed.

Detected incidents are acted upon in a timely and coordinated manner, in order to respond as quickly as possible and thus limit the impact of the incident and breaches of security. The follow-up on each alarm or detected incident is done Comfact Systems Administrator group. The conducted follow-up also ensure that relevant incidents are reported in line with Comfact Timestamp's procedures. This includes notifying appropriate parties (such as the national supervisory body, and/or affected natural or legal person) in line with the applicable regulatory rules, within 24 hours of identified breaches considered to have 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 a period of 48 hours after its discovery. This work is aligned with the risk analysis as conducted in accordance with ISO 27001.

7.12 Collection of evidence

In order to analyze and mitigate vulnerabilities in the systems, as well as providing evidence in any legal proceedings, records are kept accessible for an appropriate period of time (necessary for providing legal evidence, as notified in Comfact Timestamp terms and conditions) after the activities of Comfact Timestamp have ceased. This is for the purpose of ensuring continuity of Comfact services.

The confidentiality and integrity of current and archived records are maintained. Records concerning operation of services are, in particular, kept confidentially archived in accordance with described business practices. However, records concerning the operation of services are made available, if necessary, to provide evidence of the correct operation of the service for the purpose of legal proceedings.

In particular, records concerning Comfact Timestamp's environment, key management and clock synchronization are monitored and logged. This includes records concerning all events related to the life-cycle of the TSU keys and certificates. But also records concerning all events relating to synchronization of the TSU's clock to UTC (such as normal re-calibration or synchronization of clocks used in time-stamping) and detection of loss of synchronization.

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 Timestamp abides by the Business Continuity plans as outlined and certified under ISO 27001. This means that Comfact Timestamp has a defined and maintained continuity plan to enact in case of a disaster, e.g., compromise (or suspected compromise) of a private signing key, loss of calibration of a TSU clock, or compromise of other credentials of the TSA. Operations are restored within the delay established in the continuity plan, while having mitigated or remedied the disaster.

Should any disaster occur, or suspected to have occurred, Comfact Timestamp 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 recover fully from the compromise.

Examples of steps, if necessary, include:

- Notify the security manager to coordinate further measures to be taken
- Start 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 which can be used to identify the timestamps which may have been affected, unless this breach the privacy of the TSAs 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. In particular, this means continued maintenance of information required to verify the validity and correctness that Comfact Timestamp provided, will be transferred to a trusted, reliable party for a reasonable period of time. This includes public keys and CRLs.

In particular, before Comfact Timestamp terminates its services, all subscribers and other entities with which Comfact Timestamp has agreements or other form of established relations with, such as relying parties and national supervisory bodies, shall be informed. Similarly, each of these entities, including sub-contractors, authorization shall be terminated so as unable to act on behalf of Comfact Timestamp in carrying out any functions relating to the process of 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 fulfil these minimum requirements, in the case Comfact becomes bankrupt of for other reasons is unable to cover the cost by itself.

7.15 Compliance

Comfact Timestamp ensures compliance with applicable laws and standards. Specifically, it is compliant to:

- 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

-@-