IN GROUPE DENMARK PS

TIME STAMP AUTHORITY PS

Document information			
No. of pages : 13	Reference : N/A	Department : eID Application Development	Classification : Public
Creation date : 17/02/2025		Last saved update: February 25	Version : 1.0

Version history			
Version	**Date**	**Author**	**Description of update Updated paragraphs**
1.0	17/02/2025 00:00	KJAERSGAARD, Jan	Initial version
	Cliquez ou appuyez ici pour entrer une date.		
	Cliquez ou appuyez ici pour entrer une date.		
	Cliquez ou appuyez ici pour entrer une date.		
	Cliquez ou appuyez ici pour entrer une date.		
	Cliquez ou appuyez ici pour entrer une date.		

CONTENTS

1 INTRODUCTION

IN Groupe Denmark A/S is a qualified trust service provider under the eIDAS regulation. Its services cover certificate issuance, time-stamp issuance and signature generation.

IN Groupe Denmark A/S is denoted QTSP in this document.

This document is the practice statement for the issuance of time-stamps, which is a qualified service offered by the QTSP.

The QTSP documentation is organised with a generation practice statement document describing how requirements from [EN 319 401] are met, and this document references to the general description for relevant topics.

The service is part of a public key infrastructure, that also includes a certification authority with a remote signing service aimed to create qualified signatures. By adding qualified time-stamps to the electronic signatures, a proof of existence at the time specified in the time-stamp is achieved.

2 DEFINITIONS AND ABBREVIATIONS

Term	Definition
CPS	Certificate Practice Statement
QTSP	Qualified Trust Service Provider
rQSCD PS	Remote Qualified Signature Creation Device Practice Statement
TSA	Time Stamp Authority
TSA PS	Time-Stamping Authority Practise Statement
TSP PS	Trust Service Provider Practice Statement

3 GENERAL CONCEPTS

3.1 Time-stamping services

The time-stamping service (TSS) consists of system, which generates time-stamps. The time-stamps are provided as time-stamp tokens, that is an evidence that a specific piece of data, identified with a digest value, existed at a point in time.

3.2 Time-Stamping Authority

A Trust Service Provider (TSP) providing time-stamps is a called a Time-Stamping Authority (TSA).

IN Groupe Denmark A/S is a Qualified Trust Service Provider (QTSP) acting as a TSA under the [eIDAS] regulation. In this document, we use TSA whenever referring to IN Groupe Denmark A/S as a QTSP providing a qualified time-stamping service.

The TSA has one Time Stamp Unit, which carries out the actual issuance of time stamps.

The TSU is connected to reliable time sources and whenever a request to the service arrives, the TSU signs the digest value in the request as well as the current time and returns that in a time-stamp token. The TSU is identified by its certificate.

3.3 Subscriber

The subscribers of the TSS are signing services operated by IN Groupe Denmark A/S. As such the service is not generally available.

4 INTRODUCTION TO TIME-STAMP POLICIES AND GENERAL REQUIREMENTS

4.1 General Requirement

The IN Groupe TSA implements the BTSP policy specified [EN 319 421] and provides time stamps with an accuracy of 1 second.

4.2 Policy Name and Identification

The TSA issues time-stamp under the BTSP policy form [EN 319 421]. The policy is identified by:

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

It is included in time stamps provided by the TSA.

4.3 User Community and Applicability

4.3.1 Best Practices time-stamp Policy

The TSA provides its services to provide non-repudiation and cater for long term validity of digital signatures. The service is available for signature solutions operated by the IN Groupe QTSP.

5 POLICIES AND PRACTICES

5.1 Risk Assessment

The QTSP performs risk assessments, which is described in [TSP PS].

5.2 Trust Service Practice Statement

The QTSP has a practice statement [TSP PS], which describes how general requirements from [EN 319 401] are met.

This document is the practice statement for the qualified time-stamping services provided by IN Groupe Denmark A/S. It describes how specific requirements related to [EN 319 421] for the policy BTSP are met.

The TSA supports SHA-256 as hash algorithm for digest values provided by the subscriber in the time-stamping request.

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

The TSS are provided for signature services operated by IN Groupe Denmark A/S.

There are no subscriber obligations.

Before a relying party can trust a time-stamp issued by the TSA, it shall establish that:

a) That the signature of time-stamp can be verified
b) That the TSU certificate is available on the list of trusted lists and is valid at the time indicated within the time stamp.
c) That the TSU certificate is issued by IN Groupe DK A/S Root CA.

The QTSPs TSA is conformity assessed under the [eIDAS] regulation and supervised in Denmark. There are no additional Danish laws related to time-stamping, which the TSAs meets.

The time-stamp disclosure agreement is provided in the QTSPs repository.

5.3 Terms and Conditions

The TSA Disclosure agreement constitutes all terms and conditions for use of the TSS.

5.4 Information Security Policy

See [TSP PS] for general considerations relayed to information security policy.

5.5 TSA Obligations

5.5.1 General

The TSA adheres to any additional obligations indicated in the time-stamp either directly or incorporated by reference.

5.5.2 TSA Obligations towards Subscribers

The present document places no specific obligations on the subscriber beyond any TSA specific requirements stated in the TSA Disclosure agreement.

5.6 Information for Relying Parties

The TSA Disclosure Agreement describes information for Relying Parties.

6 TSA MANAGEMENT AND OPERATION

6.1 Internal Organization

See [TSP PS] for general considerations related to internal organization.

6.2 Personnel Security

See [TSP PS] for general considerations related to personnel security.

6.3 Asset Management

See [TSP PS] for general considerations related to asset management.

6.4 Access Control

See [TSP PS] for general considerations related to access control.

6.5 Cryptographic Controls

6.5.1 General

See [TSP PS] for general considerations related to cryptographic controls.

6.5.2 TSU Key Generation

The generation of TSU key pair is carried out in a physically secure environment, involving personnel in trusted roles under dual control.

The TSA authorises sufficient individual according to the TSA practice to carry out his function.

The TSU key pair are generated, protected and used within a cryptographic module, which meets the requirements in [EN 419 221-5].

The TSA only uses algorithms reference in [TS 119 312].

The TSA provides its TSS using several active TSUs each with dedicated cryptographic modules, using the same private key and certificate.

The TSA creates a new TSU with associated key pair before the active TSU certificate expires.

6.5.3 TSU Private Key Protection

The TSU private key is protected in integrity and confidentiality using a cryptographic module, which meets the requirements of in [EN 419 221-5].

The TSU key pair are generated, protected and used within a Cryptographic Module, which meets the requirements in [EN 419 221-5].

TSU private keys are not backed up.

6.5.4 TSU Public Key Certificate

The TSA creates TSU keys pair and issues TSU certificates using scripts and procedures, which ensures the integrity and authenticity of the certificate.

The issuer and subject fields of the certificate are as specified in [Profiles] clearly stating the TSA identifiers. During certificate issuance, the certificate is checked to be according to its specification.

The certificate is made available for relying parties at the TSA repository as well as on the list of trusted list.

A TSU will only issue time stamps when the TSU certificate is configured at the TSU software.

6.5.5 Re-keying TSU's Key

The TSA does not support re-key of TSUs keys. Instead, when a TSU key can no longer be use, the TSA creates a new TSU is created with its ow key pair.

6.5.6 Life Cycle Management of Signing Cryptographic Hardware

See [TSP PS] for general considerations of management of cryptographic modules.

Only personnel in trusted roles, using dual control, can access the physically secured environment and access the cryptographic module for TSU key pair generation, activation and duplication.

TSU private keys are securely erased by the cryptographic module at the module retirement.

6.5.7 End of TSU Key Life Cycle

The TSA has established an expiration date for TSU private keys which is 9 Year, which is one Year less than the validity of the associated public key certificate.

The validity of all QTSP certificates takes recommendations from [TS 119 312] into consideration.

Well before and timely enough, a TSU key private key is to expire, the TSA prepares a new TSU with its own certified key pair. This new TSU and public certificate is to be published in the list of trusted list before the old certificate expires.

Expired TSU private keys are deleted using the cryptographic module where it resides.

6.6 Time-stamping

6.6.1 Time-stamp Issuance

Time-stamps issued by the TSA are described in [Profiles] and they conform to the profile described in [EN 319 422]. They are issued by trustworthy systems, which are only accessed by signature services. The time-stamps are signed by the TSUs and the public certificate is included in the time-stamp to ensure the authenticity and integrity of the token.

The time values used by the TSU in timestamps is linked to one of the UTC(k) laboratories under the Bureau International des Poids et Mesures (BIPM) organization. The time is synchronized with UTC in accordance with an accuracy of less than 1 second.

The TSA monitors if the time maintained by the TSA systems deviates from the sources. In case the deviation is more than the stated accuracy, the issuance of time-stamps is suspended.

Each TSU has a dedicated private key, which is only used for signing timestamp tokens.

The QTSP will create a new TSU before expiry of current TSU private key. The new TSU will replace current TSU, which will be terminated.

6.6.2 Clock Synchronization with UTC

The TSU clock synchronizes with UTC with an accuracy of less than one second and is calibrated to ensure the clock is within the stated accuracy.

The QTSP operates services in an environment which provides physical protection for unauthorized access. The TSU clock is thus protected against changes to the clock which takes it outside of calibration with UTC and stated accuracy.

When the appropriate body announces introduction of a leap second, the TSA follows the UTC process and schedules the leap second correction during the last minute of the day when the leap second occurs. The TSA equipment records when this occurs.

6.7 Physical and Environmental security

See [TSP PS] for general considerations related to physical and environmental security.

6.8 Operation Security

See [TSP PS] for general considerations related to operation security.

6.9 Network Security

See [TSP PS] for general considerations related to network security.

6.10 Incident Management

See [TSP PS] for general considerations related to incident management.

6.11 Collection of evidence

See [TSP PS] for general considerations related to records.

Any action related to the lifecycle of TSU keys and certificates are recorded in the change management system.

The TSA system logs events with synchronisation with the UTC time. If the system detects loss of synchronization, it is logged.

6.12 Business Continuity Management

See [TSP PS] related to business continuity management.

The TSA's disaster recovery plan addresses the unlikely event that TSU private keys may have been compromised, or that the TSU clock has lost its calibration with UTC. In this case, the QTSP will provide relying parties with relevant information on its repository. This includes if relevant information required to identify issued affected timestamp tokens.

Until the system has been fully recovered, the TSA will suspend issuance of timestamps.

6.13 TSA Termination and Termination Plan

See [TSP PS] related to general considerations related termination.

6.14 Compliance

See [TSP PS].

7 ADDITIONAL REQUIREMENTS FOR QUALIFIED ELECTRONIC TIME-STAMPS AS PER REGULATION (EU) NO 910/2014

7.1 TSU Public Key Certificate

IN Groupe Denmark A/S is a QTSP providing several qualified services including qualified certificate issuance and qualified electronic time-stamps. The service for issuance of qualified certificate meets the requirements in [EN 319 411-2].

7.2 TSA Issuing Non-qualified and Qualified Electronic Time-stamps as per regulation (EU) No 910/2014

The TSA only issues time-stamps which are claimed to be qualified electronic time-stamps as per Regulation [eIDAS].

8 REFERENCES

References	
Text reference	**Description**
[eIDAS]	Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.
[EN 319 401]	ETSI EN 319 401, Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[EN 319 421]	ETSI EN 319 421, Electronic Signatures and Trust Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
[TSP PS]	Trust Service Provider Practice Statement, IN Groupe Denmark A/S, 2025.
[Profiles]	Certificate Profiles, IN Groupe Denmark A/S, 2025.
[TS 119 312]	ETSI TS 119 312, Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites
[EN 419 221-5]	CEN EN 419 221-5, CEN TC224 WG17, Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services, 2016.
[EN 319 411-2]	ETSI EN 319 411-2, Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
[EN 319 422]	ETSI EN 319 422, Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.