DIGITALSIGN - CERTIFICADORA DIGITAL, SA.

REMOTE QSCD MANAGEMENT SERVICE POLICY AND PRACTICE STATEMENT

VERSION 1.0 – 15/07/2026

[LANGUAGE: ENGLISH]

VERSION HISTORY

Date	Edition n.º	Content
15/07/2026	1.0	Initial draft Publication as autonomous policy and practice statement for the qualified trust service for the management of remote qualified electronic signature/seal creation devices, pursuant to Regulation (EU) 2024/1183

RELATED DOCUMENTS

Document Details	Author(s)
Certification Practice Statement	DigitalSign

AUTHORIZATIONS

Created by	Approved by
	

LEGAL NOTICE

Any question or request for information regarding the content of this document should be directed to rqms@digitalsign.pt.

CONTENTS

1. INTRODUCTION

1.1. OVERVIEW

The purpose of this document is to define the policy, practices and procedures used to support the provision, by DigitalSign – Certificadora Digital, SA. ("DigitalSign"), of the qualified trust service for the **management of remote qualified electronic signature and seal creation devices**, as defined in Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183 (Articles 29a and 39a).

The service consists of a server signing application and a remote QSCD, jointly referred to in this document — in accordance with ETSI terminology — as the **Server Signing Application Service (SSAS)**. DigitalSign, as the Trust Service Provider operating this service, acts as **Server Signing Application Service Provider (SSASP)**.

This document constitutes both the **SSAS Policy** and the **SSAS Practice Statement**, as permitted by ETSI TS 119 431-1, clauses 4.3.1 and 4.3.2, and should be read in conjunction with the current version of the Certification Practice Statement (CPS) of DigitalSign, available at https://pki.digitalsign.pt. Requirements common to all trust services operated by DigitalSign (derived from ETSI EN 319 401) are implemented as described in the CPS and are incorporated herein by reference.

1.1.1. NORMATIVE REFERENCES

This document respects and implements the following standards and legal instruments:

- **Regulation (EU) No 910/2014**, as amended by Regulation (EU) 2024/1183 (eIDAS 2)
- Commission Implementing Regulation (EU) 2025/1567
- **ETSI EN 319 401**: General Policy Requirements for Trust Service Providers
- **ETSI TS 119 431-1**: Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev
- **ETSI TS 119 461**: Policy and security requirements for trust service components providing identity proofing of trust service subjects
- **CEN EN 419 241-1**: Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements
- **CEN EN 419 241-2**: Trustworthy Systems Supporting Server Signing – Part 2: Protection profile for QSCD for Server Signing
- **CEN EN 419 221-5**: Protection Profiles for TSP Cryptographic Modules – Part 5: Cryptographic Module for Trust Services

This SSAS Policy and Practice Statement and further fixes and/or updates are approved by the Management Group (see section 9.17.1 of the CPS). Corrections and/or updates shall be published in the form of new versions of this document, replacing any previous version.

1.1.2. QTSP IDENTIFICATION

DigitalSign – Certificadora Digital, S.A.
Largo Pe. Bernardino Ribeiro Fernandes, 26

4835-489 Nespereira, Guimarães
Portugal
E-mail: geral@digitalsign.pt
Support Phone: +351 253 560 650

1.1.3. CONTACT PERSON

Álvaro Matos
DigitalSign – Certificadora Digital, SA.
Largo Padre Bernardino Ribeiro Fernandes, 26
4835-489 Nespereira – Guimarães
Portugal
Email: rqms@digitalsign.pt
Phone: +351 253560650

1.2. DOCUMENT NAME AND IDENTIFICATION

Document Information	
Document Name	Remote QSCD Management Service Policy and Practice Statement
Version/Edition	1.0
OID	1.3.6.1.4.1.25596.7.1.1
Publication Date	15/07/2026
Expiration Date	Upon publication of a newer version
Localization:	https://pki.digitalsign.pt

This document claims conformance to ETSI TS 119 431-1 under the following trust service policy:

Policy	OID
EUSPv2 — EU SSAS Policy (Annex A of ETSI TS 119 431-1)	0.4.0.19431.1.1.4

The EUSPv2 policy incorporates all requirements of the Normalized SSAS Policy (NSP) plus the specific requirements of Regulation (EU) 2024/1183 relating to remote QSCD management (ETSI TS 119 431-1, Annex A).

2. REFERENCES

- ETSI TS 119 431-1: Policy and security requirements for TSP services operating a remote QSCD / SCDev
- ETSI TS 119 432: Protocols for remote digital signature creation
- ETSI TS 119 461: Identity proofing of trust service subjects
- ETSI EN 319 401: General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 / 319 411-2: Requirements for TSPs issuing certificates
- CEN EN 419 241-1, EN 419 241-2, EN 419 221-5
- Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183
- Commission Implementing Regulation (EU) 2025/1567
- CPS: Certification Practice Statement of DigitalSign

3. ACRONYMS AND DEFINITIONS

Acronym	Definition
CA	Certification Authority
CPS	Certification Practice Statement
DTBS/R	Data To Be Signed / Representation
eID	Electronic Identification
EUSPv2	EU SSAS Policy (v2), per ETSI TS 119 431-1, Annex A
HSM	Hardware Security Module
LoIP	Level of Identity Proofing (ETSI TS 119 461)
QSCD	Qualified electronic Signature/Seal Creation Device
SAD	Signature Activation Data
SAM	Signature Activation Module
SAP	Signature Activation Protocol
SCDev	Signature Creation Device
SIC	Signer's Interaction Component
SSAS	Server Signing Application Service
SSASP	Server Signing Application Service Provider
TSP	Trust Service Provider

For other terms, the definitions in ETSI TR 119 001 and ETSI TS 119 431-1, clause 3.1, apply.

4. GENERAL CONCEPTS

4.1. THE SSAS SERVICE

The SSAS operated by DigitalSign enables signers to create qualified electronic signatures and seals whose signature/seal creation data (signing keys) are generated, held and managed by DigitalSign, on behalf and under the (sole) control of the signer, in a remote QSCD.
In accordance with ETSI TS 119 431-1, clause 4.4, the SSAS is broken down into the following component services (for the purpose of classifying requirements only):

- **Signing key generation service** – generates signing keys in the remote QSCD;
- **Certificate linking service** – links certificates issued by DigitalSign CAs with the corresponding signing keys;
- **eID means / identity linking service** – links the signer's eID means reference (or, for one-time signing keys, the verified identity) with the corresponding signing keys, in order to provide sole control;
- **Signature activation service** – verifies the Signature Activation Data (SAD) and activates the corresponding signing key through the Signature Activation Module (SAM);
- **Signing key deletion service** – destroys signing keys in a way that ensures they can no longer be used.
- **eID means provision service** – prepares and provides or makes eID means available to the signers.

4.2. PARTICIPANTS

4.2.1. SSASP

DigitalSign is the SSASP and maintains overall responsibility for the service, including where parts of the service are supported by other parties.

4.2.2. SUBSCRIBER AND SIGNER

The signer associated with a signing key can be a natural person, a natural person identified in association with a legal person, or a legal person. The relationship between signer and subscriber is equivalent to the relationship between subject and subscriber described in ETSI EN 319 411-1, clause 5.4.2, and in the CPS (section 1.3.3).

4.2.3. RELYING PARTIES

As defined in section 1.3.4 of the CPS.

4.3. RELATION TO CERTIFICATE ISSUANCE

The SSAS is operated in conjunction with, but is a trust service distinct from, the issuance of qualified certificates by the DigitalSign CAs identified in the CPS (section 1.1.1). Where the SSAS supports proof of possession or signer authentication assertions towards the registration service of the issuing CA, the requirement REG-6.3.1-01 of ETSI EN 319 411-1 is supported as described in section 7.2.1 of this document.

5. SSAS POLICY

5.1. OVERVIEW

This SSAS Policy defines the set of rules under which DigitalSign operates the management of remote QSCDs, in accordance with ETSI TS 119 431-1, policy EUSPv2.

5.2. IDENTIFICATION

As defined in section 1.2 of this document.

5.3. USER COMMUNITY AND APPLICABILITY

The community of users of the SSAS includes subscribers, signers and relying parties of qualified electronic signatures and seals created through the DigitalSign remote signature solution, supported by qualified certificates issued by the DigitalSign CAs under the policies identified in the CPS and Certification Profile List (namely QCP-n-qscd and QCP-l-qscd).

5.4. CONFORMANCE

DigitalSign claims conformance of the SSAS with the EUSPv2 policy of ETSI TS 119 431-1, taking into account the adaptations specified in Commission Implementing Regulation (EU) 2025/1567. DigitalSign is subject to independent conformity assessment (see section 7.6) in order to demonstrate that the SSAS fulfils the obligations defined in section 6 and has implemented the controls described in section 7.

6. OBLIGATIONS AND LIABILITY

6.1. SSASP OBLIGATIONS

DigitalSign operates the SSAS and assumes responsibility for the requirements described in section 7 of this document, as well as the provisions of applicable national and European legislation. DigitalSign undertakes, namely, to:

- generate, manage and, where applicable for back-up purposes only, duplicate the signature/seal creation data only on behalf and at the request of the signatory/creator of the seal (Articles 29a(1)(a)-(b) and 39a of the amended Regulation);
- ensure that duplication for back-up purposes maintains the same level of security as the original datasets and does not exceed the minimum needed to ensure continuity of the service;
- generate and use signing keys exclusively in a certified QSCD, operated in the configuration described in its certification guidance documentation, and comply with any requirements identified in the certification report of the specific remote QSCD (Article 29a(1)(c));
- ensure that the signing keys are used under the sole control of the signer (control, in the case of seals), through a certified Signature Activation Module and Signature Activation Protocol;
- publicly disclose this document through an online means available on a 24×7 basis.

6.2. SUBSCRIBER AND SIGNER OBLIGATIONS

Subscribers and signers must, in addition to the obligations set out in the CPS (section 9.6.3) and in the applicable Subscriber Agreement:

- keep the eID means and authentication factors used for signature activation under their exclusive control, and not disclose or share them;
- immediately request the blocking/deletion of the signing key and the revocation of the associated certificate upon suspicion of compromise or loss of control of the eID means or authentication factors;
- use the service only for lawful purposes and in accordance with the terms and conditions.

6.3. RELYING PARTY OBLIGATIONS

As defined in the CPS (sections 4.5.2 and 9.6.4).

6.4. LIABILITY

As defined in the CPS (sections 9.7 to 9.9), which apply to the SSAS mutatis mutandis.

7. REQUIREMENTS ON SSAS PRACTICES

This section follows the structure of ETSI TS 119 431-1, clauses 5 and 6 and Annex A. Where a requirement is common to all DigitalSign trust services, reference is made to the corresponding section of the CPS.

7.1. PRACTICE STATEMENT, PUBLICATION AND REPOSITORY

This document, together with the CPS and the applicable terms and conditions, is publicly available at https://pki.digitalsign.pt on a 24×7 basis (see CPS, sections 2.1 to 2.4). The applicable terms and conditions are readily identifiable for a given signing key and for the associated certificate.

The signature algorithms and parameters applied, including the algorithms applied for key pair generation, are those identified in the CPS (sections 6.1.5 and 7.1.3) and in the Certification Profile List.

7.2. SIGNING KEY INITIALIZATION

7.2.1. SIGNING KEY GENERATION

Signing keys are generated in a **QSCD certified in accordance with Regulation (EU) No 910/2014 (as amended), Annex II**:

- QSCD product: Entrust **nShield Solo XC Hardware Security Module v12.60.15**
- Certification reference: **A-SIT-VIG-25-090 / A-SIT / 10/03/2026**
- The QSCD is operated in the configuration described in the applicable certification guidance documentation, and DigitalSign complies with any requirements identified in the certification report of the device.

The cryptographic module supporting the QSCD conforms to EN 419 221-5. Cryptographic algorithms and key lengths comply with the requirements referenced in EN 419 241-1 and with the parameters identified in the CPS. Key generation ceremonies and dual-control requirements follow CPS sections 6.1.1 and 5.2.2.

Where the SSAS and the certificate generation service are managed separately, the SSAS supports requirement REG-6.3.1-01 of ETSI EN 319 411-1 by providing proof of possession / an assertion of the authentication of the signer linked to the private key.

7.2.2. IDENTITY PROOFING AND EID MEANS / IDENTITY LINKING

The identity proofing of the signer fulfils the requirements of the **extended Level of Identity Proofing (LoIP) as defined in ETSI TS 119 461**. Identity proofing is performed in accordance with the CPS (section 3.2), through physical presence, notified eID means, remote videoconference identification, EUDI wallet.

The signing key is linked to the signer's eID means reference (or, in the case of one-time signing keys, directly to the verified identity). DigitalSign ensures that the person identification data linked to the eID means reference or identity is the same as that linked to the subject of the associated certificate, and protects the integrity of the links between the signing key and the eID means reference / identity.

The eID means and authentication mechanism conform to EN 419 241-1, clauses A.2.1 and A.2.2, for assurance level **substantial or higher**, including two-factor authentication combining knowledge factor defined by the signer and possession factor (OTP app/device, Wallet), as per CPS section 6.4.1.

7.2.3. CERTIFICATE LINKING

Certificates issued by the DigitalSign CAs are linked to the corresponding signing keys in accordance with EN 419 241-1 (SRC_SKS.1.2, .1.4, .1.5). The integrity of such links is protected within the trustworthy system.

7.2.4. EID MEANS PROVISION

The eID means is securely passed to the signer; associated user activation data is securely prepared and distributed separately from the eID means, through an independent channel (see CPS, section 6.4.2).

7.3. SIGNING KEY LIFE-CYCLE

7.3.1. SIGNATURE ACTIVATION

Signing keys are used exclusively in the certified QSCD identified in section 7.2.1. Signature activation is performed through a **Signature Activation Protocol (SAP)** verified by a **Signature Activation Module (SAM)** operating within the tamper-protected environment of the QSCD, ensuring sole control of the signer at **Sole Control Assurance Level 2 (SCAL2)** as defined in EN 419 241-1.

- SAM certification: **Entrust Signature Activation Module (A-SIT-VIG-25-090)**
- The SAD binds together the signer's authentication, the signing key and the DTBS/R(s), and is protected in integrity and confidentiality during collection, transmission and use.
- Signing keys are usable only in those cases for which the signer's consent has been obtained.
- The SSAS ensures that the public key certificate is valid (not expired, not revoked) before using the corresponding signing key.

For authentication linked directly to the identity (one-time signing keys): the SAD contains the unique identifiers of the signature session and of the identity verification process; the signature session ends at most 30 minutes after the end of the identity verification process (SIG-A.5-09); the SAP includes an explicit action of the signer to approve the authorization to sign the specific documents referenced in the SAD (SIG-6.3.1-15/16).

7.3.2. SIGNING KEY DELETION

Signing keys are destroyed, in a way that ensures they can no longer be used: (i) when the associated certificate is revoked; (ii) when requested by the signer; (iii) for one-time signing keys, immediately after the end of the signature session. Backup copies are deleted in accordance with EN 419 241-1 (SRG_KM.7.3). Key destruction follows CPS section 6.2.10.

7.3.3. SIGNING KEY BACKUP AND RECOVERY

Signing keys may be duplicated **for back-up purposes only**, at the request and on behalf of the signatory, ensuring that: (i) the security of the duplicated datasets is at the same level as the original datasets; and (ii) the number of duplicated datasets does not exceed the minimum needed to ensure continuity of the service. Backup and recovery operations require dual control by personnel in trusted roles (see CPS, sections 6.2.4 and 6.2.6).

7.4. SSAS MANAGEMENT AND OPERATION

Domain	TS 119 431-1	Implementation
Internal organization	OVR-6.8.1-01	CPS section 5.2; Management Group (CPS 9.17.1)
Risk assessment	EN 319 401 cl. 5 (OVR-6.4.1-01)	DigitalSign has an information security management system based on the standard ISO/IEC 27001, ensuring that facilities, procedures, personnel, equipment and products comply with all regulatory and safety requirements applicable to the exercise of its activity
Physical security	OVR-6.4.2-01/02	CPS section 5.1; the requirements of ETSI EN 319 411-1 (OVR-6.4.2-02 to -10) apply mutatis mutandis to signing key generation and activation management
Procedural controls	OVR-6.4.3-01A	CPS section 5.2
Personnel controls	OVR-6.4.4-01 to -03	CPS section 5.3
Audit logging	OVR-6.4.5-01 to -07	CPS section 5.4, complemented by SSAS-specific audit data per EN 419 241-1 (SRG_AA.1/.2/.3/.7/.8): all security events, SAP transactions, signature activations, key life-cycle events
Records archival	OVR-6.4.6-01	Audit data records relating to the SSAS are retained for at least seven (7) years after any certificate based on these records ceases to be valid
Key changeover	6.4.7	No policy requirement
Compromise and disaster recovery	OVR-6.4.8-01	CPS section 5.7
Termination	OVR-6.4.9-01/02	CPS section 5.8, applied to the SSAS; termination plan includes secure destruction of signing keys or, where legally permitted and requested, transfer arrangements
Systems and security management	OVR-6.5.1-01, OVR-6.5.2-01/02	EN 419 241-1 SRG_M.1, SRG_SO.1/.2 Detailed descriptions of implemented operation security controls are available as internal document(s)
Computer security	OVR-6.5.3-01A/02	CPS section 6.5; system monitoring per EN 419 241-1 SRG_AA.6.1
Life cycle security	OVR-6.5.4-01	CPS section 6.6
Network security	OVR-6.5.5-01 to -03	CPS section 6.7

Cryptographic controls	OVR-6.8.5-01/02	Cryptographic techniques are managed throughout their lifecycle and selected in accordance with the Agreed Cryptographic Mechanisms endorsed by the ECCG and published by ENISA; algorithms and parameters as identified in the CPS (sections 6.1.5 and 7.1.3)

7.5. TERMS AND CONDITIONS, PRIVACY AND OTHER LEGAL MATTERS

Terms and conditions applicable to the SSAS are made available to subscribers and relying parties in accordance with EN 319 401, clause 6.2 (OVR-6.8.4-01), through Subscriber Agreement. Privacy of personal information, compliance with applicable law, accessibility (disabilities) and remaining business and legal matters are governed by CPS section 9, which applies mutatis mutandis.

7.6. COMPLIANCE AUDIT AND OTHER ASSESSMENT

The provision of Qualified Trust Services is subject to an external audit performed at least every 12 months by a Conformity Assessment Body (CAB) and the qualified status is supervised by GNS (Gabinete Nacional de Segurança), the Portuguese National Supervisory Body

ANNEX A – CONFORMANCE MAPPING (INFORMATIVE)

Cross-reference between ETSI TS 119 431-1 (V1.3.1) requirements and this document / the CPS, to support conformity assessment:

TS 119 431-1 clause	Requirement group	This document	CPS
5.1	Practice statement	1, 7.1	1.5, 2
5.2 / A.2	Policy identification (EUSPv2)	1.2, 5.2	-
5.3	Participants	4.2	1.3
6.1	Publication and repository	7.1	2
6.2.1 / A.4	Signing key generation	7.2.1	6.1
6.2.2 / A.7	eID means / identity linking; identity proofing (extended LoIP)	7.2.2	3.2
6.2.3	Certificate linking	7.2.3	-
6.2.4	eID means provision	7.2.4	6.4
6.3.1 / A.5, A.6	Signature activation (SAM/SAP, SAD, SCAL2)	7.3.1	4.12, 6.2
6.3.2	Signing key deletion	7.3.2	6.2.10
6.3.3	Backup and recovery	7.3.3	6.2.4
6.4	Facility, management and operational controls	7.4	5
6.5	Technical security controls	7.4	6
6.6	Compliance audit	7.6	8
6.7 / 6.8	Business and legal matters; terms and conditions	7.5	9
A.3	QSCD certification reference; certification report requirements	7.2.1	-