# Remote Qualified Electronic Signature Service (SPPS)

## Practices Statement and Service Policy





Paseo de la Castellana,79 -28046- Madrid (Spain)

Telephone: 932 661 614

www.anf.es

**Security Level**

*Public Document*

---

**Important Notice**



Address: Paseo de la Castellana, 79 - 28046 - Madrid (Spain)

Teléfono: 932 661 614

www.anf.es

# INDEX

# 1. Introduction

ANF Certification Authority [ANF AC] is a legal entity established under Organic Law 1/2002 of March 22 and registered with the Ministry of the Interior under national number 171.443 and Tax Identification Number (NIF) G-63287510.

The Public Key Infrastructure (PKI) of ANF AC adheres to the guidelines of Regulation [EU] 910/2014 of July 23, 2014, of the European Parliament and the Council (hereinafter referred to as "eIDAS"), and Law 6/2020 of November 11, governing certain aspects of electronic trust services.

## 1.1. Objective and scope

This document outlines the Policy and Practices for the Qualified Remote Electronic Signature Service (SPPS) provided by ANF AC. It is an integral part of the ANF AC Certification Practice Statement (CPS) as a Qualified Trust Service Provider (QTSP).

The centralized certificate management system and remote signature service of ANF AC involve the management, on behalf of the signer, of their signature creation device. In this way, subscribers can use qualified certificates whose private keys are securely hosted and managed in a QSCD device (under the "managed on behalf" model). This facilitates the remote generation of qualified electronic signatures while ensuring that the signer retains exclusive control over their signature keys at all times.

This document describes the most relevant aspects of the remote signature service and the operation of the components that manage signature creation devices remotely on behalf of the signer. It also includes a declaration of the safeguard measures for the infrastructure and the technical and non-technical security controls applied to the systems involved in providing the service.

This Policy and Practice Statement applies to the keys of all qualified electronic signature certificates defined in the ANF AC CPS as "centralized" certificates or certificates in centralized storage.

This document has been structured based on the ETSI TS 119 431 technical specification.

## 1.2. Overview of the service

The remote qualified electronic signature generation system of ANF AC consists of the following components:

1. **nShield Connect XC HSMs**
2. **Entrust Signature Activation Module (SAM)**, which ensures that the user maintains exclusive control over their signature keys.
3. **DELL tamper-proof servers**, which protect the physical infrastructure of the solution.
4. **Signature software developed by ANF AC**

These components are integrated to provide a reliable and secure remote qualified electronic signature service. The nShield Connect XC HSMs securely store the keys; the Entrust SAM ensures that only the key holder can activate and use the keys; the tamper-proof DELL servers reinforce the physical integrity of the platform; and ANF AC's signature software coordinates the remote generation of qualified electronic signatures.

## 1.3. Document Name and Identification

| | | | |
|---|---|---|---|
| **Document name** | Service Practices and Policy of the Remote Qualified Electronic Signature Service (SPPS) | | |
| **Version** | 1.1 | | |
| **OID** | 1.3.6.1.4.1.18332.3.4.1<br>0.4.0.19431.1.1.3 - EUSCP: EU SSASC Policy | | |
| **Approval date** | 23/12/2024 | **Publication date** | 23/12/2024 |
| **Related CPS** | ANF AC Certification Practices Statement (CPS) of ANF AC<br>OID 1.3.6.1.4.1.18332.1.9.1.1 | | |

### 1.3.1. Policy Administration

As established in ANF AC CPS.

### 1.3.2. Reviews

| Version | Changes | Approval | Publication |
|---|---|---|---|
| 1.1. | Annual review | 23/12/2024 | 23/12/2024 |
| 1.0. | Document creation | 19/02/2023 | 19/02/2023 |

## 1.4. Participating Entities

In the provision and use of the Trust Services regulated in this CPSP, the following parties are involved:

1. **ANF AC** - Remote signature service provider (SSASP)
2. **Registration Authority (RA)**
3. **Subscribers and signers of the certificates**
4. **Relying parties**

### 1.4.1. ertification Authorities (CA) – Server Signing Application Service Provider (SSASP)

The remote signature application service component (SSASC) is part of the services operated by ANF AC and enables the provision of remote electronic signature services to signers holding a centralized qualified electronic signature certificate, as established in the ANF AC CPS.

ANF AC acts as the server signature application service provider (SSASP) and does not delegate any part of this service to external entities. In its capacity as SSASP, ANF AC develops, implements, enforces, and updates this document, which contains the Policy and Practice Statement for SPPS.

### 1.4.2. Registration Authority (RA)

As established in ANF AC CPS.

### 1.4.3. Subscriber and signers

The Signers are natural persons who maintain exclusive control over the signature creation data associated with the Certificates they hold. The Signer is the individual who creates the electronic signature and must be identified by their full name, NIF (Tax Identification Number), NIE (Foreigner Identification Number), or passport number.

The Subscriber of a Certificate can be distinct from the Signer when there is a representative relationship or affiliation with an Organization, in which case the Organization acts as the Subscriber, or in the case of Electronic Seal Certificates. However, each Specific Certification Policy Statement will determine the potential distinction between the roles of Signer and Subscriber.

### 1.4.4. Relying parties

Relying parties are natural or legal persons, other than the Signer or Subscriber, who receive and/or use the certificates or electronic signatures issued by ANF AC.

The centralized certificates covered by this Policy comply with the requirements established in Law 6/2020 and the eIDAS Regulation, and are recognized by @firma, the electronic validation and signature platform of the Spanish Government.

Relying parties must consider the limitations of use, both quantitative and qualitative, specified in the CPS, in this document, and in the certificate itself.

## 1.5. Use of Certificates

As provided in the current Certification Practice Statement (CPS) of ANF AC and in the corresponding Certification Policy (CP) for each certificate.

## 1.6. Definitions and acronyms

### 1.6.1. Definitions

In addition to the definitions provided in the ANF AC CPS, the following terms, as defined in ETSI TS 119 431-1, are included for the interpretation of this document:

**Electronic identification (eID):** The process of using a person's identification data in electronic format that uniquely represents a natural or legal person, or a natural person representing a legal entity.

**Electronic identification means:** A tangible and/or intangible unit that contains a person's identification data and is used for authentication in online services.

**Reference to electronic identification means:** Data used in the SSASC as a reference to electronic identification means that enable the authentication of a signer.

**Qualified electronic signature/seal creation device (QSCD):** A signature creation device that meets the requirements of Annex II of Regulation (EU) No 910/2014.

**Remote signature creation device:** A signature creation device used remotely by the signer and operated on their behalf under their exclusive control.

**Server Signature Application Service Component (SSASC):** A service component operated by a TSP, consisting of a server signature application (SSA) and a QSCD/SCDev, used for creating electronic signatures on behalf of the signer.

**Server Signature Application Service Provider (SSASP):** A TSP that operates an SSASC.

**Signature Creation Device (SCDev or SCD):** Configured hardware or software used to create an electronic signature.

### 1.6.2. Acronyms

**EUSPv2:** EU SSAS Policy v2

**QSCD:** Qualified Electronic Signature/Seal Creation Device

**SAD:** Signature Activation Data

**SAM:** Signature Activation Module

**SAP:** Signature Activation Protocol

**SCDev:** Signature Creation Device

**SP:** SSAS Policy

**SSAS:** Server Signature Application Service

**SSASP:** Server Signature Application Service Provider

**TW4S:** Trustworthy System Supporting Server Signing

# 2. Repositories and Information Publication

## 2.1. Repositories

As established in ANF AC CPS.

## 2.2. Publication of Certification Information

As established in ANF AC CPS.

## 2.3. Timing and Frequency of Publication

As established in ANF AC CPS.

## 2.4. Access Controls to Repositories

As established in ANF AC CPS.

# 3. Identification and Authentication

## 3.1. Name registration

As provided in the current Certification Practice Statement (CPS) of ANF AC and in the corresponding Certification Policy (CP) for each certificate.

## 3.2. Initial Identity Validation

As provided in the current Certification Practice Statement (CPS) of ANF AC and in the corresponding Certification Policy (CP) for each certificate.

## 3.3. Identification and Authentication for Key Renewal Requests

As provided in the current Certification Practice Statement (CPS) of ANF AC and in the corresponding Certification Policy (CP) for each certificate.

## 3.4. Identification and Authentication for Revocation Requests

As provided in the current Certification Practice Statement (CPS) of ANF AC and in the corresponding Certification Policy (CP) for each certificate.

# 4. Operational Requirements for the Signature Key Lifecycle

The request, processing, acceptance, renewal, modification, and revocation of the centralized certificate are governed by the provisions set forth in the Certification Practice Statement (CPS) and the Certification Policy (CP) applicable to each certificate type.

This document only describes the specific aspects that affect the remote signature service and centralized certificates, complementing the provisions already established in the corresponding CPS and CP..

## 4.1. Initialization of Signature Keys

ANF Autoridad de Certificación, in the provision of its server signing service, uses cryptographic devices for signature creation and protection classified as qualified (QSCD), in compliance with Regulation (EU) No. 910/2014 of the European Parliament and of the Council of July 23, 2014, on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation), which repeals Directive 1999/93/EC.

The HSMs used are certified under Common Criteria EAL4+ (AVA_VAN.5 and ALC_FLR.2), and the SSASC solution employed aligns with the security requirements established in standard EN 419 241-1, allowing it to operate as a Trustworthy System Supporting Server Signing (TW4S) with Sole Control Level 2 (SCAL2).

### 4.1.1. Signature Key Generation

The Server Signature Application Service (SSASC) of ANF AC uses proprietary signature software in combination with the Entrust Signature Activation Module (SAM), installed on tamper-proof servers, along with an nShield Connect XC cryptographic module (HSM) classified as QSCD. This HSM has been validated to meet at least the requirements of FIPS 140-2 Level 3 or FIPS 140-3 Level 3, enabling all cryptographic operations with the signers' keys and ensuring the exclusive control of each key holder.

Initialization and management operations of the cryptographic module require dual control. Once the registration process is completed, the user's 2048-bit RSA keys are generated within the HSM. Until the certificate is issued by ANF AC, these keys remain in an inactive state and cannot be used.

Alongside the signer's key, a certificate request in PKCS#10 format is generated, serving as proof of possession of the private key during the registration and certificate issuance process with the Certification Authority. Once the certificate has been issued and validated, the keys are activated, enabling the generation of qualified electronic signatures.

If backups are required, the keys are encrypted and stored outside the HSM using the AES algorithm with a 128-bit key derived from an internal master key of the HSM. This ensures the confidentiality and integrity of the keys throughout their lifecycle.

### 4.1.2. Association of the Signer's Electronic Identification Means

Once the request has been processed through an authorized operator of a Face-to-Face Verification Office (OVP) in AR Manager, the applicant receives an email with a unique link granting access to the web confirmation gateway (https://activatucertificado.anf.es/).

In this gateway, the applicant must enter two previously provided confirmation codes: one sent via SMS and the other via email. Subsequently, the applicant can review the application details and must set up their credentials with two-factor authentication, as well as a PIN, which will act as the certificate's activation data.

Once the applicant confirms the request, the system instructs the Server Signature Application Service (SSASC) to generate the signature key pair and registers the request. This request is then sent to ANF AC servers for review by the

Issuance Decision Officers. Following this, ANF AC proceeds with issuing the electronic certificate and requests the SSASC to link it with the generated key pair.

The use of the private key is contingent upon the activation of two authentication factors of different categories. Additionally, the SSASC ensures the integrity of the keys and associated metadata by managing them within an encrypted database.

### 4.1.3. Association of the Signer's Certificate

Once the registration and issuance processes of the signer's certificate are completed, the certificate is imported into the Server Signature Application Service (SSASC). The SSASC verifies that the public key included in the certificate matches the one stored in the system. If a match is confirmed, the certificate is linked to the signer's key pair, thus forming the signature identity (composed of the certificate and the private key generated within the QSCD device).

Until the certificate is effectively associated with its corresponding key pair, the signature identity remains incomplete, and the SSASC does not allow the keys to be used for signing. Once both elements are linked, the signer's key becomes operational for signature operations, provided the required authentication factors have been activated.

The SSASC protects the integrity of the signers' keys and associated metadata through secure storage and ensures the validity of each signature identity by applying registration procedures that maintain the traceability and integrity of the information.

### 4.1.4. Provision of the Signer's Identification Means

When the signer confirms their request through the secure web gateway of ANF Certification Authority (ANF AC), a process is initiated to configure their electronic identification means, including credentials and two-factor authentication. At that time, a code or seed required for generating one-time passwords (OTP) is created and associated with the signer, without storing this information in plain text.

The Server Signature Application Service (SSASC) retains only the essential information needed to validate the OTPs generated by the signer, ensuring the confidentiality of their access data and preventing the exposure of keys or passwords in readable format.

## 4.2. Use of Keys and Certificates

### 4.2.1. Activation of Signature Keys

For each use of the signature key, the signer must send a Signature Activation Data (SAD) message through the Signature Activation Protocol (SAP). This message includes two authentication factors of different categories and a session witness. Prior to this, the signer identifies themselves with their username and at least one authentication factor to obtain the session witness.

The signer's keys can only be activated if the HSM is operational.

The SSASC validates the SAD and, only when the signer has been properly authenticated (using credentials and authentication factors), the key becomes active. Once activated, the SSASC allows a single use to sign the cryptographic hash contained in the SAD; after completing the operation, the key is deactivated, requiring a new SAD for each subsequent signature.

The SAP protocol is designed to prevent man-in-the-middle and replay attacks. The SAD message incorporates safeguards against impersonation, session theft, duplication, credential theft, phishing, and guessing through encryption techniques, electronic signatures, hash functions, random numbers, and the use of two authentication factors of different types (something the signer knows and something the signer possesses).

If the signer enters their activation factor incorrectly three consecutive times, access to the remote key is blocked. The key can only be unlocked through a recovery process sent to the signer's email address.

All communications with the SSASC are protected using TLS 1.2.

The SSASC access controls ensure that a signer cannot access the keys of other users or system functionalities beyond those necessary for signing or personal management.

Additionally, the SSASC maintains the expiration date and revocation status of the certificate associated with the key. If the certificate has expired or is revoked, the use of the key is denied.

Finally, the signers' keys are stored encrypted using AES (256 bits) derived from a master key of the cryptographic module. The SAM module, along with the HSM, enables the generation of electronic signatures under the RSA PKCS#1 v1.5 standard with SHA-256, SHA-384, or SHA-512 hash functions, ensuring the integrity and authenticity of the signed data.

### 4.2.2. Deletion of Signature Keys

The signer's keys are immediately deleted when their certificate is revoked.

Periodically, ANF AC executes a process to remove the keys of signers whose associated certificate has expired.

Signers may request the revocation of their certificate following the procedures established in the ANF AC CPS. In all cases, the revocation or expiration of the certificate results in the destruction of the associated keys.

#### 4.2.2.1. Backup and Restoration of Signature Keys

The signers' keys are protected by the master key of the cryptographic module and can only be used when the module is active. During the backup of signers' keys, the AES encryption algorithm with a 128-bit key length is used. Periodic backups are made of the SSA database, which references the signers' keys, as well as other infrastructure keys necessary to ensure service continuity in case of an incident, while keeping the number of backups to the essential minimum.

The SSASC infrastructure keys are stored in encrypted containers. The cryptographic module containing the SSASC master key, responsible for protecting all signers' keys, requires dual control for its operation, backup, and restoration. This master key never leaves the cryptographic module in plain text.

# 5. Physical, Management, and Operational Security Controls

## 5.1. Physical Security Controls

As established in ANF AC CPS.

## 5.2. Controles de procedimientos

As established in ANF AC CPS.

## 5.3. Personnel Controls

The SSA implements the following management roles:

- **Security Officer:** Has overall responsibility for administering and implementing security policies and has access to security information.
- **System Administrators:** Are responsible for installing, configuring, and maintaining the TW4S, but with controlled access to security information.
- **System Operators:** Are responsible for the day-to-day operation of the TW4S, as well as backup and restoration operations.
- **System Auditor:** Is authorized to review the TW4S files and audit records to verify that system operations are aligned with the security policy.

ANF AC assigns these roles to qualified personnel and implements all segregation-of-duties controls defined in section 6.2.1.2 of the CEN EN 419 241-1 standard.

## 5.4. Security Audit Procedures

According to the provisions established in the CPS of ANF AC and, in particular, for the remote electronic signature service:

The Server-Side Signature Application Service (SSASC) logs at least the following events:

- Initialization, startup, shutdown, and system configuration changes.
- Key management events for the signer (generation, activation, use, deactivation, and destruction).
- Use of the signers' keys.
- Signer authentications (including failed attempts).
- Changes related to signature activation data (e.g., PIN changes).
- Startup, shutdown, and reconfiguration of auditing functions.
- System accesses by administrative users.

The SSASC generates a continuous audit record in which it is only possible to add new events, with no possibility to delete or modify existing ones. To protect each record entry and the record as a whole, techniques are applied that chain each event to the previous one, preventing any tampering with the recorded data. Periodically and during startup, the SSASC verifies the integrity of this record, also providing a functionality that allows a user with the auditor role to perform the same check on demand.

In order to guarantee the accuracy of the audit events' date and time, the system clock is synchronized via NTP, using the Real Observatory of the Navy (ROA) as a reference, and controls are implemented to detect incidents that could affect this synchronization.

In case the auditing functions become unavailable, the SSASC will automatically suspend the processing of new requests, ensuring that no operation is carried out without proper control..

## 5.5. Information Archiving

As established in ANF AC CPS.

## 5.6. Key Change

As established in ANF AC CPS.

## 5.7. Key Compromise and Disaster Recovery

As established in ANF AC CPS.

## 5.8. Termination

As established in ANF AC CPS.

# 6. Technical Security Controls

According to the provisions established in the CPS of ANF AC, except for the following issues specific to the qualified remote signature service:

## 6.1. Operations and Systems

The organization has procedures in place to operate the SSASC correctly and securely.

The SSA software component, the Entrust SAM, and the HSM module are operated in accordance with their manuals for installation, management, and operation to meet the security objectives defined in the Security Statement of their certification as a QSCD device.

## 6.2. Computing Security Controls

ccording to the provisions established in the CPS of ANF AC.

The SSASC is monitored, and alerts are generated and sent to system administrators when events that may impact its availability or compromise its security are detected.

# 7. Profiles of certificates, CRL and OCSP

## 7.1. Certificate profile

### 7.1.1. Version number

As established in ANF AC CPS.

### 7.1.2. Certificate extensions

The extensions used for each type of certificate issued under this policy are published in the document titled "ANF AC Certificate Profiles" on the ANF AC website (https://anf.es/repositorio-legal/).

### 7.1.3. Algorithm object identifiers

As established in ANF AC CPS.

### 7.1.4. Name forms

As established in ANF AC CPS.

### 7.1.5. Name restrictions

As established in ANF AC CPS.

### 7.1.6. Certificate policy object identifier

Under the provisions established in this document, the following types of certificates are issued, along with their corresponding OIDs:

| Type | Support | | OID |
|---|---|---|---|
| **Clase 2 de Persona Física** | QSCD. Servicio Centralizado | | 1.3.6.1.4.1.18332.3.4.1.5.22 |
| **Corporativo de Colegiado** | QSCD. Servicio Centralizado | | 1.3.6.1.4.1.18332.3.4.1.11.22 |
| **Representante Legal de Persona Jurídica** | QSCD. Servicio Centralizado | | 1.3.6.1.4.1.18332.2.5.1.14 |
| **Representante Legal de Entidad sin Personalidad Jurídica** | QSCD. Servicio Centralizado | | 1.3.6.1.4.1.18332.2.5.1.15 |
| **Representante Legal para administradores únicos y solidarios** | QSCD. Servicio Centralizado | | 1.3.6.1.4.1.18332.2.5.1.13 |
| **Sello Electrónico** *(QSealC)* | QSCD. Servicio Centralizado | | 1.3.6.1.4.1.18332.25.1.1.9 |
| **Sello Electrónico AA.PP.** *(QSealC AA.PP.)* | Nivel Alto | QSCD. Servicio Centralizado | 1.3.6.1.4.1.18332.25.1.1.11 |
| **Sello Electrónico PSD2** *(QSealC PSD2)* | QSCD. Servicio Centralizado | | 1.3.6.1.4.1.18332.25.1.1.7 |

#### 7.1.7. Using the Policy Constraints extension

As established in ANF AC CPS.

#### 7.1.8. Syntax and semantics of policy qualifiers

As established in ANF AC CPS.

#### 7.1.9. Processing semantics of the critical Certificate Policies extension

As established in ANF AC CPS.

### 7.2. CRL Profile

As established in ANF AC CPS.

### 7.3. OCSP Profile

As established in ANF AC CPS.

# 8. Compliance audits and other controls

## 8.1. Frequency of audits

As established in ANF AC CPS.

## 8.2. Qualification of the auditor or evaluator

As established in ANF AC CPS.

## 8.3. Relationship between the auditor and the audited authority

As established in ANF AC CPS.

## 8.4. Aspects covered by the evaluation

As established in ANF AC CPS.

## 8.5. Actions to be taken as a result of the detection of deficiencies

As established in ANF AC CPS.

# 9. Other business and legal matters

## 9.1. Fees

As established in ANF AC CPS.

## 9.2. Financial liabilities

As established in ANF AC CPS.

## 9.3. Confidentiality of commercial information

As established in ANF AC CPS.

## 9.4. Protection of personal information

As established in ANF AC CPS.

## 9.5. Intellectual property rights

As established in ANF AC CPS.

## 9.6. Representations and warranties

As established in ANF AC CPS.

## 9.7. Disclaimers of warranties

As established in ANF AC CPS.

## 9.8. Limitations of liability

As established in ANF AC CPS.

## 9.9. Indemnities

As established in ANF AC CPS.

## 9.10. Term and termination

As established in ANF AC CPS.

## 9.11. Individual notices and communications with participants

As established in ANF AC CPS.

## 9.12. Amendments

As established in ANF AC CPS.

## 9.13. Dispute resolution provisions

As established in ANF AC CPS.

## 9.14. Governing Law

As established in ANF AC CPS.

## 9.15. Compliance with applicable law

As established in ANF AC CPS.

## 9.16. Miscellaneous provisions

As established in ANF AC CPS.

## 9.17. Other provisions

As established in ANF AC CPS.