2026

DECLARACIÓN DIVULGATIVA DE PRODUCTO

SPPS - Servicio de Firma Electrónica Cualificada Remota

ANF AC

© ANF Autoridad de Certificación

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

Teléfono: 932 661 614 (Llamadas desde España)

Internacional +34 933 935 946

Web: www.anf.es

Nivel de Seguridad

Documento Público

Aviso Importante

Dirección: Paseo de la Castellana, 79 - 28046 - Madrid (España)
Teléfono: 932 661 614 (llamadas desde España)
Internacional (+34) 933 935 946
www.anf.es

1. Qué es este servicio

El SPPS de ANF AC permite a un firmante generar **firmas electrónicas cualificadas** de forma remota mediante un **Dispositivo Cualificado de Creación de Firma (QSCD)** gestionado por ANF AC (managed on behalf). El firmante mantiene control exclusivo sobre el uso de su clave privada mediante mecanismos de activación multifactor (2FA + PIN). El servicio cumple con el Reglamento (UE) 910/2014 (eIDAS) y la normativa nacional aplicable (Ley 6/2020).

2. Qué garantiza

- Firma electrónica con valor jurídico cualificado, mientras se cumplan las condiciones de uso y verificación.
- Generación de la clave privada dentro del HSM y protección criptográfica en reposo y en tránsito.
- Trazabilidad y registro de eventos relevantes (uso de clave, autenticaciones, operaciones administrativas).
- Procedimientos de revocación y eliminación de claves tras revocación o caducidad.

3. Componentes técnicos clave

- **HSM:** nShield Connect XC (QSCD).
- **SAM:** Entrust Signature Activation Module.
- **Algoritmos:** RSA 3072 para operaciones de firma; SHA-256/384/512 para resúmenes.
- **Protección de claves:** cifrado en reposo AES-256; backups cifrados (AES-128) y control dual para restauración.
- **Comunicaciones:** TLS 1.2; sincronización horaria vía NTP con referencia ROA.

4. Requisitos para el firmante (qué debe hacer el cliente)

1. Identificación según procedimiento de registro (presencial u OVP) y validación por RA autorizado.
2. Proveer datos personales exigidos: nombre + NIF/NIE/pasaporte u otro identificador legal.
3. Mantener y custodiar: credenciales 2FA (SMS/email u otro factor), PIN de activación y acceso a la pasarela web.
4. Notificar inmediatamente cualquier sospecha de compromiso de credenciales o dispositivo.

5. Cómo funciona (paso a paso, versión resumida)

1. **Registro:** verificación de identidad (presencial u OVP).
2. **Aprovisionamiento:** ANF genera la clave privada **dentro del HSM** y emite el certificado cualificado asociado.
3. **Enlace de activación:** el solicitante recibe un enlace seguro y códigos por SMS/email para completar la configuración.
4. **Configuración:** el firmante establece PIN y factores de autenticación.
5. **Firma:** para cada operación de firma se requiere un **SAD/SAP** (Signature Activation Data / Signature Activation Protocol) que combina factores «algo que sabe» más «algo que posee» y un testigo de sesión; cada activación permite un uso único de la clave para firmar el resumen criptográfico indicado.
6. **Bloqueo/recuperación:** 3 intentos fallidos de activación > bloqueo; desbloqueo mediante proceso de recuperación documentado por ANF.

6. Seguridad, respaldo y control operacional

- Las claves maestras no salen del HSM en texto claro.
- Las copias de seguridad de claves están cifradas y su restauración exige control dual por roles de confianza de ANF AC.
- Registros de auditoría y mecanismos de integridad para detección de manipulación.
- Procedimientos de alta disponibilidad y degradación segura: si la plataforma de auditoría falla, se suspende la emisión/uso hasta restauración conforme a políticas.

7. Revocación, caducidad y borrado

- **Revocación del certificado:** publicación inmediata en CRL/OCSP y borrado de las claves asociadas.
- **Caducidad:** eliminación periódica de claves de certificados vencidos conforme al ciclo de vida definido.
- **Restauración tras siniestro:** restauraciones controladas (control dual, HSM) y registradas en auditoría.

8. Validación por terceros que confían

- Terceros deben validar certificados y estados de revocación mediante los mecanismos publicados por ANF AC (CRL/OCSP).
- Existen limitaciones y perfiles de uso asociados a cada tipo de certificado; terceros que confían deben comprobar dichas limitaciones antes de aceptar una firma.

9. Obligaciones del usuario y riesgos principales

Obligaciones

- Custodiar credenciales, PIN y factores 2FA; usar el servicio según instrucciones.
- Notificar compromisos o pérdidas de credenciales sin demora.

Riesgos

- Bloqueo por intentos erróneos o pérdida de factores; dependencia de disponibilidad del HSM/SSASC (conectividad); necesidad de seguir procesos de recuperación que pueden requerir verificación adicional.

10. Condiciones comerciales y legales

- Tarifas, límites de responsabilidad, indemnizaciones y demás condiciones contractuales figuran en la DPC completa y en los términos de servicio de ANF AC. La PDS resume las características esenciales, pero no sustituye la DPC ni el contrato.

11. Contacto y soporte

- Portal de activación y soporte: https://activatucertificado.anf.es/
- Para información completa, tarifas y repositorios CRL/OCSP consulte la DPC completa y el repositorio legal de ANF AC (referido en la DPC).

ANEXO — Certificados y OIDs relevantes

Tipo	Soporte		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

Lectura recomendada y advertencia final

Esta PDS sintetiza las obligaciones, garantías y limitaciones del SPPS de ANF AC extraídas Política y Prácticas del Servicio de Firma Electrónica Cualificada Remota (SPPS) (OID 1.3.6.1.4.1.18332.3.4.1) disponible en el repositorio legal de ANF AC (https://anf.es/repositorio-legal/). Para decisiones contractuales, operativas o de validación jurídica, remítase al texto íntegro de la política, DPC y a los términos y condiciones de ANF AC.