Procedure of Remotely Qualified Electronic Signature

Paseo de la Castellana, 79 – 28046 - Madrid (España)
Teléfono: 902 902 172 (llamadas desde España)
Internacional (+34) 933 935 946
Fax: (+34) 933 031 611 · Web: www.anf.es

Security Level

Public

DOCUMENT CONTROL:

Version	Modification/creation date	Author / modified by
1.0	2017/03/15	*F. Díaz*

Version	Proposed by	Approved by	Modification date	Approval date	Author

Index

1 Introduction

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

The Public Key Infrastructure (PKI) of ANF AC has been designed and managed in accordance with the legal framework of Regulation [EU] 910/2014 of the European Parliament [eIDAS], and with Law 59/2003 of Electronic Signature of Spain. The PKI of ANF AC is in compliance with the standards ETSI EN 319 411-1 (Part 1: General Requirements), ETSI EN 319 411-2 *(Part 2: Requirements for Trust Service Providers issuing EU Qualified Certificates)*, ETSI EN 319 411 -3 *(Part 3: Policy Requirements for Certification Authorities issuing public key certificates)*, ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI), RFC 3739 *(Internet X.509 Public Key Infrastructure: Qualified Certificates Profile).*

The eIDAS Regulation allows remotely qualified electronic signature (signature server). The remotely qualified electronic signature has been designed respecting the published ETSI / CEN standards for such signatures: prEN 419 241-1: General System requirements; prEN 419 241-2: Protection Profile for QSCD for Server Signing; prEN 419 221-5: Cryptographic module.

ANF AC uses OIDs according to the ITU-T Rec. X.660 standard and the ISO / IEC 9834-1: 2005 standard (Procedures for the Operation of OSI Registration Authorities: General Procedures and ASN.1 Object Identifier tree top arcs). ANF AC is assigned the private company code (SMI Network Management Private Enterprise Codes) 18332 by the international organization IANA -Internet Assigned Numbers Authority-, under the branch iso.org.dod.internet.private.enterprise (1.3.6.1.4.1 -IANA -Registered Private Enterprise-).

ANF Certification Authority offers qualified electronic signature services remotely. This document determines the specific management and administrative procedures that are used for the provision of the service, as well as the systems and products that guarantee that the environment for the creation of electronic signatures is reliable and that the signer has, with a high level of confidence, the exclusive control of the use of their electronic signature creation data.

This document is only one of the various documents that the PKI of ANF AC govern, it details and complements what is defined in the Certification Practices Declaration and its addendum, the profiles of certificates for centralized signature are detailed in the Certification Policies to which your emission is submitted. ANF AC protects and supervises that this PC is compatible and coherent with the rest of the documents it has prepared. All documentation is freely available to users and third persons who trust https://www.anf.es.

2 Certificates for centralized electronic signature

The application, processing, emission and profile of the certificates for centralized electronic signature are detailed in the Certification Policies to which the emission is submitted.

As a general rule, it can be determined that:

- Certificates for centralized electronic signature are exclusively generated in certified signature creation secure devices according to the applicable requirements in accordance with Article 30.3 of the eIDAS Regulation and, therefore, included in the list of qualified devices maintained by the European Commission in compliance with articles 30, 31 and 39 of the eIDAS Regulation.

  https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

  Specifically, ANF AC currently uses devices

  Code = NC 4433E-500

  Model = NShield Solo 500 + F3

  Manufacturer = Thales e-Security, Inc.

Within the QcStatement extension, QcSSCD is activated, which determines that the private key associated with the public key contained in the electronic certificate is in a qualified signature creation device in accordance with Annex II of 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.

- Certificates for centralized electronic signature are exclusively emitted with the qualification of "qualified".

  Within the QcStatement extension, QcCompliance is activated, it refers to a declaration of the emitter in which the qualification with which the certificate is emitted is recorded, and the legal framework to which it is submitted. Specifically, the certificates submitted to this policy, emitted with the qualification of "recognized" (qualified), report:

  "This certificate is issued with the qualification of "qualified" according to Annex I of Regulation (EU) 910/2014 of the European Parliament"

2.1 Signature creation data and Signature activation data

As detailed in the CPS, and in the respective Certification Policy to which the emission of certificates for centralized electronic signature is submitted, the applicant for the certificate follows the same procedure as in any other type of certificate:

- Receives an Identification Act from the Registration Authority, which is signed by the AR and encrypted with a double symmetric key only known by the applicant.
- For the generation of the asymmetric key pair, public and private, the applicant uses the HSM device indicated above.
- For the generation of the request certificate, the applicant uses the same HSM device and the identification act received from the Registration Authority.

The procedure followed by the applicant:

1. Connection through SSL encrypted communication, to the corporate website of ANF AC.
2. The applicant selects the Identification Act and downloads the encrypted document.
3. The reliable server of ANF AC, has an encrypted copy of that act, which was sent by the Registration Authority. The server obtains the hash of the stored encrypted act and obtains the hash of the encrypted act transmitted by the applicant. Both hashes are compared to ensure that they are identical.
4. In case of hash compliance, the reliable server of ANF AC, requires the applicant to input the two symmetric decryption keys of the act.
5. The reliable server of ANF AC deciphers the act, and carries out a verification of the electronic signature of the Operator AR that authenticated it.
6. In case of agreement of signature of the AR, the reliable server of ANF AC requires the applicant to indicate:
    a. Signature activation data that you want to use (PIN). The system includes a library of unauthorized keys (insecure), it requires using a key of at least 8 alphanumeric digits, at least one character must be a capital letter.
    b. If you want to activate the process of Double Authentication Factor (2FA), in case of conformity:
        i. You do not want to activate 2FA
        ii. If you want to receive a token by SMS *(session key)*
        iii. If you want to receive a token by eMail *(session key)*
        iv. If you want to receive a token by Push Notifications *(session key)*

    Session key = different key for each request, it is generated randomly.

7. Once the values indicated in point 6 have been input, the HSM device (SSCD) installed in the reliable server of ANF AC, proceeds to:
    a. generate the pair of asymmetric keys (signature generation data -public and private-), and

b. Prepare the request certificate (CSR), according to PKCS # 10 standard.

8. The PIN selected by the applicant is not stored by ANF AC, it is only used when it is required by the Secure Signature Creation Device.
9. Signature generation data are only accessible by using the Secure Signature Creation Device that keeps them.
10. The interested person receives an email and an SMS as the Identification Act has been activated and the application for emitting a remote signature certificate has been processed. In these communications, the certificate identifier is indicated

This procedure guarantees a high level of trust on the part of the certificate subscriber and guarantees exclusive control of the signature creation data:

- For the transmission of: Identification Act, decryption keys and the signature creation data, a secure electronic communication has been used.
- Only the interested person knows the signature creation data, ANF AC neither store this data nor has the opportunity to do so, therefore, only the signer can use them.
- The signature generation data is generated by the secure signature creation device itself, therefore, this data is safeguarded.
- As in any other type of certificate, the subscriber is sent a notice to the email account and to the mobile that he qualified as personal and secure at the time of authentication before the Registration Authority. In this email, in addition to reporting the certificate identifier, contact details of the Legal Assistance Service of ANF AC are provided.

The procedure followed is basically the same as in any other type of certificate, therefore, the level of security achieved is comparable to that of any other certificates stored in physical HSM device in possession of the signer.

Other technical specifications in document "Via-signature -fortress"

2.2 Emission of electronic certificate and download

The procedure for remote signature certificates is the same as for the other certificates, and information is also sent to the subscriber when the certificate is emitted.

As defined in the CPS and Certification Policies to which the emission of the certificate is submitted.

3 Remote signature server and standards

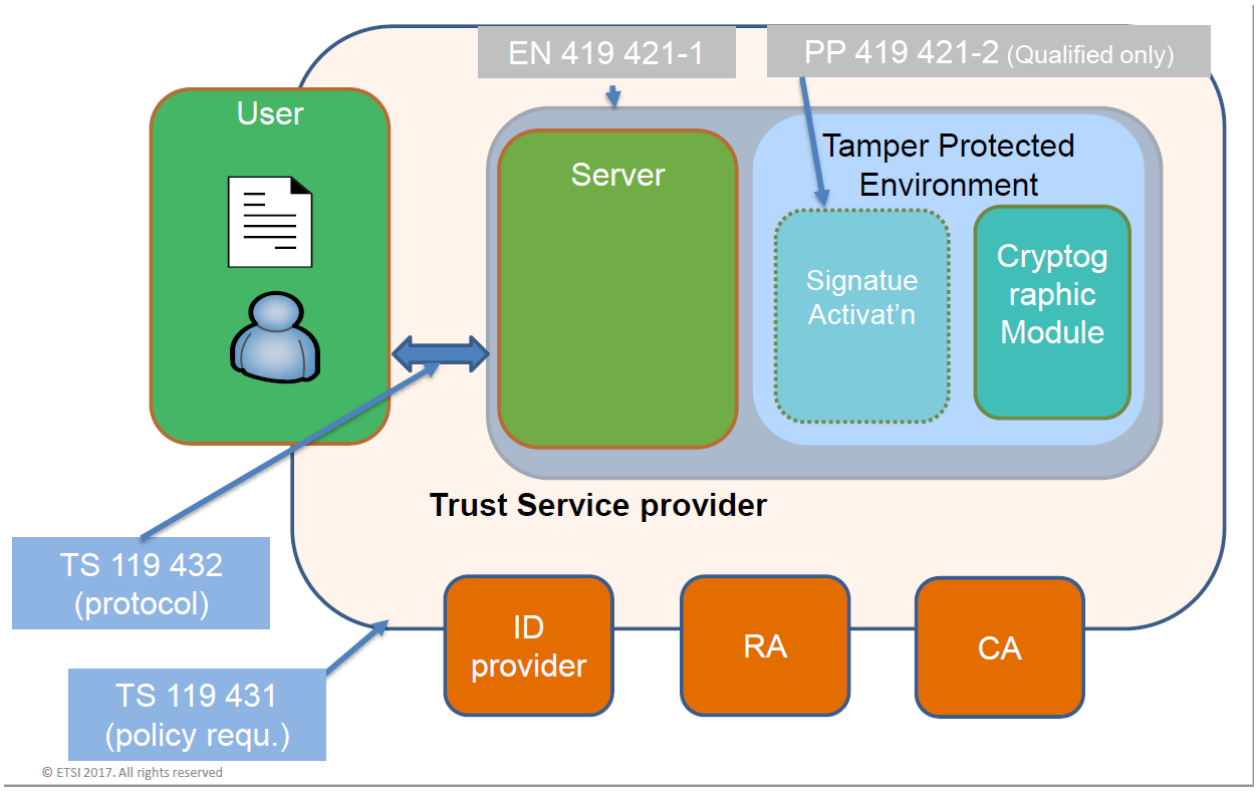
The remote signature server of ANF AC has been developed respecting the ETSI / CEN standards published for such signatures:

- prEN 419 241-1: General System requirements.
- prEN 419 241-2: Protection Profile for QSCD for Server Signing.
- prEN 419 221-5: Cryptographic module. PP for TSP cryptographic modules, in particular its Part 5 PP for cryptographic modules for TSP
- TS 119 431-1: Policy and security requirements for TSP service components operating a remote QSCD / SCD
- TS 119 431-2: Policy and security requirements for TSP service components supporting AdES digital signature creation
- TS 119 432: Protocols for remote digital signature creation

Security Objectives and security requirements for the signature server of ANF AC, detailed in the OID Security Statement 1.3.6.1.4.1.18332.46.8

Functional diagram of the remote signature service

Scope of the remote signature standards.



4 Remote signature procedure

4.1 Selection of the file to be signed

The signer accesses the ANF AC Web service using a secure SSL communication channel.

The signer has the following options:

- Transmit an electronic document to the reliable servers.
- Transmit the hash of an electronic document to the reliable servers.

4.2 Certificate selection

The signatory accesses the ANF AC Web service using a secure SSL communication channel.

Then inputs the certificate identifier (Item 2.1 10)) to select the certificate you want to use.

4.3 2FA authentication control

The remote signature service determines the mode of use established by the signer (Point 2.1 6)):

1. Without 2FA
2. Sending session key by eMail.
3. Sending session key by SMS.
4. Sending session key by Push Notification.

If the signer has activated 2FA, he will receive the session key by the required means. The signer must enter the password in order to continue with the signature process.

Other technical specifications in document "Via-signature -fortress"

Through this procedure, the signer has the option of supplementing the security of the remote signature system with 2FA:

- What I know, signature activation data (PIN)
- What I own, email, mobile, or PC web service.

4.4 Activation of the signature process

Once process 3.2 is completed, the remote signature service allows the signature process to continue by using a secure SSL communication channel. Specifically:

- Shows the signer the file he has requested to sign, and allows him to check content.
- It requires you to enter your PIN (Signature activation data) to activate the signature process.

The remote signature service, using the Signature Creation Secure Device (HSM) and the signer's PIN, proceeds to sign the required file.

Once the file is signed, the signer can proceed to download it.

5 Physical security, facilities, management and operational controls

As defined in the Certification Policy to which the emission of the certificate is submitted.

5.1 Physical security controls

As defined in the CPS of ANF AC.

5.2 Procedural controls

As defined in the CPS of ANF AC.

5.3 Personnel controls

As defined in the CPS of ANF AC.

6 Technical safety controls

6.1 Generation and installation of the key pair

As defined in the CPS of ANF AC.

6.2 Protection of the private key

As defined in the CPS of ANF AC.

6.3 Other aspects of key pair management

As defined in the CPS of ANF AC.

6.4 Activation data

As defined in the CPS of ANF AC.

6.5 IT security controls

As defined in the CPS of ANF AC.

6.6 Life cycle technical controls

As defined in the CPS of ANF AC.

6.7 Network security controls

As defined in the CPS of ANF AC.

6.8 Time sealing

As defined in the CPS of ANF TSA CA.

6.9 Security controls of the cryptographic modules

As defined in the CPS of ANF AC.