PROFILES OF CERTIFICATES

Qcert for Eseal
QTimestamp
Qcert for ESig
QWAC
eDelivery

GENERAL INFORMATION

Type	**General Policy** Specific Policy Procedure Technical Instruction Plan Template
Classification	**Public** Confidential Internal Use
Version	251219
State	Draft in progress **Approved** Retired

VERSION HISTORY

Version	Section and changes	Author
181221	Creation of the specific document of certificate's profiles. It includes all the previous certificate's profiles that were included in their respective CPS. They can be consulted on http://www.firmaprofesional.com/cps	FP
190227	"*2.8. Public Officer with pseudonym certificate's profile*": ● In "*2.8.3.1. Certificate's Extensions*", within the Subject Alternative Name, the OIDs of the Directory Name have been changed. "*5.2. VA Certificate's profile*": ● The extension noCheck of the not qualified VA certificate has been added as optional, and as mandatory for the qualified VA certificate.	FP
190507	"2.7. Public Officer certificate's profile": ● "1.3.6.1.4.1.13177.10.1.22.3.1:DCCF centralised authentication" has been removed for being not qualified. ● "1.3.6.1.4.1.13177.10.1.22.3.2: DCCF centralised pseudonym" for being duplicate information. "2.8. Public Officer with pseudonym certificate's profile": ● The optional field of Subject Alternative Name's mail has been removed.	FP

	● The description of the third OU field has been changed. ● The OID for the "pseudonym" field has been added. For all profiles: ● The extension which indicates the PDS route has been removed for having switched its condition to optional.	
190612	"2.1. Corporate Certificate for professional associates profile" and "2.2. Corporate Certificate for natural persons profile", "organisation" field of the DN: ● Clarifications about the format of the code and number of the RA which issued the certificate have been made. The point 3.3 "Corporate company seal for PSD2 certificate's profile" has been added Modification of point 4.2 in order to add characteristics of the website authentication certificate for PSD2.	FP
200205	Clarification that the certificates are based on The ITU Telecommunication Standardization Sector (ITU-T) standard X.509 version 3 Updated *userNotice* of Corporate Certificates of Corporate Seal PSD2. Updated SSL EV Certificates profile to adapt it to the requirements of CA/Browser Forum, EV Guidelines, v. 1.7.1. Relocation of *keyUsage* and *extendedKeyUsage* extensions for document consistency.	FP
200930	Added portable DCCF and centralized DCCF support for Personal certificates. Added CA / B Forum OIDs to website authentication certificates. An additional OU field is added to the profile of the Corporate Professional Association Member certificates, the interpretation of which is defined by each professional association.	FP
210217	Optional introduction of fields of ISO 17442 part 2 for LEI identifiers: ● 1.3.6.1.4.1.52266.1: for Business Seal and Legal Representative 1.3.6.1.4.1.52266.2: for Legal Representative	FP
210322	Amendment of SSL CA Browser Forum OIDs	FP
211001	● Correction of the Public Officer certificate profile, high level signature: the EKU is removed Minor corrections in the Professional Association Members Certificate profile	FP
220216	● Updated QEVCP-w of ETSI 319 411-2 (2021-11)	FP
220330	● Apple's policy S/Mime modification update	FP

220517	• Electronic Office Certificates OU field removal	FP
220530	• SSL Certificates StateorProvince field removal	FP
221109	• Public Officer Certificate's Key Usage and EKU update	FP
230419	• Correction of error section 2.7	FP
230510	• New profile of Company Seal in Centralized DCCF • Updated Section 5 • Updated references to generic URLs • clarification of optional fields • General review	FP
230828	• Clarifications on the use of the passport # in the electronic signature certificates and elimination of this option in the Corporate Certificate for Voluntary Representative against Public Administration • Stop issuing natural person certificates with email signature since it will be deprecated from 1 September 2023. • Remove eKU "email protection" from personal certificates.	FP
231104	• Adaptation of SSL profiles with the modifications introduced by CABForum	FP
240219	• Remove KU "Data Encipherment"	FP
240520	• Remove of the RFC822 field • Update of the location of the entity on the main page • Information on the removal of some EKUs • Update section 4.1.2	FP
241216	• Update the DN of the corporate certificate profile for a natural person. • Update the key usage of the corporate seal certificate. • Update the DN of the TSU certificate profile.	FP

250502	• Update 2.7.1	ACC
250723	• Updated optional SAN fields in sections 2.8.3 and 2.8.4 • Updated the description of the serial number field in sections 2.1, 2.2, 2.5, 2.6 and 2.7. • Updated the ID and name examples in sections 2.4.1, 2.5.1, and 2.6.1 • Outdated options highlighted in sections 2.1.1, 2.1.2, 2.2.1, 2.2.2, 2.4.2, 2.5.2, 2.6.2, 2.7.2, 2.8.2, 3.1.2, 3.1.3, 3.1.4, 3.2.2, 3.2.3, and 5.1.1.2 • Updated the "user notice" field in all profiles • Updated the "description" field in sections 2.5.1 and 2.6.1	ACC
251219	• Updated using the RFC822NAME field	ACC

Index

1 Introduction

The present document describes the profiles of the certificates issued by Firmaprofesional as Certification Services Provider.

In order to create the certificate's profiles, it has been taken into account the following:

- 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, which repeals Directive 1999/93/CE (from now onwards known as, eIDAS)
- General State Administration Policy for Electronic Signature and Digital Certificates: Annex 2: Digital Certificate's Profiles.
- ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles
- "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" published in https://wwww.cabforum.org/
- The ITU Telecommunication Standardization Sector (ITU-T) standard X.509 version 3.

The profiles of the different certificates issued by Firmaprofesional, based on the Policy that are associated with, are grouped as follows:

A. Electronic Signature Certificates, grouped as:

1. Corporate Certificates:
    - Corporate Certificates for professional associates
    - Corporate Certificates for natural persons
    - Corporate Certificates for Representatives, which can be:
        - Corporate for Representatives of an Entity without Legal Status
        - Corporate for Legal Representatives
        - Corporate for Voluntary Representative
2. Personal Certificates
3. Public Officer Certificates, divided into:
    - Public Officer Certificates
    - Public Officer with pseudonym Certificates

B. Electronic Seal Certificates

1. Public Administration/Entity Seal Certificates
2. Company Seal Certificates

C. Website Authentication Certificates

1. Electronic Office Certificate
2. Secure Service Certificates

D. Secure Service Certificates:

1. CA Certificates
2. VA Certificates
3. TSA Certificates

All the Certification Policies of the certificates are published and can be found on the website www.firmaprofesional.com/cps

2 Description of profiles of Electronic Signature Certificates

NOTE: certificates containing a passport number or another identifier different from the Spanish National Identity Document (DNI), Spanish Foreigner Identification Number (NIE) or Spanish Tax Identification Number (NIF), SHALL NOT BE USED for processing with the Spanish Public Administration.

2.1 Professional Association Members Certificate's profile

2.1.1 Distinguished Name (DN)

DN field	name	Description
CN, Common Name	Name	Name and Surnames of the signatory Additionally the Professional Associate's number can be included preceded by the word "num:'' and separated by "/". *Ej: CN = NAME SURNAME1 SURNAME2 / num:4444*
E, E-mail	*E-mail*	*signatory's e-mail.* *(Optional and not recommended, as it is obsolete according to RFC 5280)*
O, Organization	Organization	Name of the subscriber (company or private or public entity) with which the signer is linked. (Example: Name of the Organization or entity that acts as RA) Additionally the code and number of the RA that issued the certificate will be included, separated by "/".
OU, Organization Unit (Optional)	Organization Unit	It will contain additional information of relevance for the Professional Association Member or the information systems with which it works. The interpretation of this field is defined by each professional association.
T, Title	Title	signatory's Title
ST, State	Geographic Location	signatory's geographic location (eg. Province)
C, Country	Country	Two digit country code, according to ISO 3166-1. By default "ES".
serialNumber	ID Number	Administrative number assigned by national legislation according to the value of the Country field. (*) Ex: "IDCES-99949991H"
SN, surName	Surname	signatory's surname, exactly as it appears on their ID

GN, givenName	First Name	signatory's First name, exactly as it appears on their ID

(*) Coding according to ETSI EN 319 412-1 will be followed. The use of a document other than a DNI, NIE, or NIF will make it impossible to process documents with Spanish public authorities

If the signatory doesn't have their ID (NIF or NIE), they will have to give their Passport Number exactly as it says point 7.1.4 of the CPS.

2.1.2 Common extensions of certificates

Extension	Critical	Values
Subject Alternative Name	-	*RFC822Name: :<signatory's email>* ***(Optional)*** directoryName: • 1.3.6.1.4.1.13177.0.1: First name of the natural person, exactly as it appears on their ID. • 1.3.6.1.4.1.13177.0.2: First surname of the natural person, exactly as it appears on their ID • 1.3.6.1.4.1.13177.0.3: Second surname of the natural person, exactly as it appears on their ID (this field could be empty)
Basic Constraints	Yes	CA:FALSE
Key Usage	Yes	Digital Signature Content Commitment Key Encipherment
Extended Key Usage	-	*eMail Protection* ***(Use prohibited from September 2023)*** TLS Website Client Authentication Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) (**Included** from the 15th of September, 2023)
Subject Key Identifier	-	<ID of the Certificate's Public Key, obtained from its hash>
Authority Key Identifier	-	<ID of the CA Certificate's Public Key, obtained from its hash>
CRL Distribution Points	-	<URI of the CRL>
Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP server> Access Method: Id-ad-calssuers

		Access Location: <URI to access the issuer CA's Certificate>

2.1.3 Extensions of Certificates without DCCF

Extension	Critical	Values
Certificate Policies	-	<OID of the Certification Policy of the Certificate> 1.3.6.1.4.1.13177.10.1.1.2 <URI of the CPS> User Notice: "Éste es un Certificado Corporativo de Colegiado cualificado, para su uso sin DCCF." <OID of the European Certification Policy: 0.4.0.194112.1.0> (Qualified EU Certificates Policy for Qualified Certificates for Natural Persons "QCP-n", without DCCF)
QcStatements	-	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicating Qualified Certificates) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (for a 15 years period) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.1 (qct-esign, indicating that it is a Certificate that creates Digital Signatures).

2.1.4 Extensions of Certificates with DCCF

Extension	Critical	Values
Certificate Policies	-	<OID of the Certification Policy of the Certificates> 1.3.6.1.4.1.13177.10.1.1.1: DCCF portable 1.3.6.1.4.1.13177.10.1.1.3: DCCF centralized <URI of the CPS> User Notice: "Éste es un Certificado Corporativo de Colegiado cualificado, para su uso con DCCF." <OID of the European Certification Policy: 0.4.0.194112.1.2> (Qualified EU Certificates Policy for Qualified Certificates for Natural Persons "QCP-n", with DCCF)

QcStatements	-	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicating Qualified Certificates) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (for a 15 years period) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.1 (qct-esign, indicating that it is a Certificate that creates Digital Signatures). Id-etsi-qcs-QcSSCD: 0.4.0.1862.1.4 (indicating that the Private Key is guarded in a DCCF)

2.2 Natural Persons Certificate's profile

2.2.1 Distinguished Name (DN)

DN field	Name	Description
CN, Common Name	Name	signatory's Name and surnames.
E, E-mail (optional)	*E-mail*	*signatory's e-mail.* *(Optional and not recommended, as it is obsolete according to RFC 5280)*
O, Organization	Organization	Subscriber's Name (Company or Public/Private Entity) with whom the signatory has an entailment. If the Subscriber is self-employed, their Trade Name can be used, their CNAE or IAE. Additionally the code and number of the RA that issued the certificate will be included, separated by "/".
OrganizationIdentifier	Tax ID number of the Organization	Tax ID number of the Organization, exactly as it appears in the Official Records. Coded according to the European Standard ETSI EN 319 412-1 (Ej: VATES-B0085974Z)
OU, Organization Unit	Organization Unit	It will contain one of the following values: • The Department to which the signatory is part of. • Entailment with the Organization.
T, Title	Title	signatory's Title at the Organization.

ST, State	Geographic Location	signatory's geographic location (eg. Province)
C, Country	Country	two digit country code, according to ISO 3166-1. By default "ES".
serialNumber	ID Number	Administrative number assigned by national legislation according to the value of the Country field. (*) Ex: "IDCES-99949991H"
SN, surName	Surnames	signatory's surname, exactly as it appears on their ID
GN, givenName	First name	signatory's First name, exactly as it appears on their ID
1.3.6.1.4.1.4710.1.3.2	NIF of the subscribing organization	NIF number, without ETSI coding (Optional)

(*) If the signatory doesn't have a ID (National ID Number), it shall state its Passport Number exactly as it says in the CPS. The use of a document other than a DNI, NIE or NIF implies the impossibility of processing with the Spanish Public Administrations.

2.2.2 Common extensions of certificates

Extension	Critical	Values
Subject Alternative Name	-	*RFC822Name: :<signatory's email>* ***(Optional)*** directoryName: ● 1.3.6.1.4.1.13177.0.1: First name of the natural person, exactly as it appears on their ID. ● 1.3.6.1.4.1.13177.0.2: First surname of the natural person, exactly as it appears on their ID ● 1.3.6.1.4.1.13177.0.3: Second surname of the natural person, exactly as it appears on their ID(this field could be empty)
Basic Constraints	Yes	CA:FALSE

Key Usage	Yes	Digital Signature Content Commitment Key Encipherment
Extended Key Usage	-	*eMail Protection* (***Use prohibited from September 2023)*** TLS Web Client Authentication Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) (Included from the 15th of September, 2023)
Subject Key Identifier	-	<ID of the Certificate's Public Key, obtained from its hash>
Authority Key Identifier	-	<ID of the CA Certificate's Public Key, obtained from its hash>
CRL Distribution Points	-	<URI of the CRL>
Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP server> Access Method: Id-ad-caIssuers Access Location: <URI to access the issuer CA's Certificate>
QcStatements	-	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicating Qualified Certificates) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (for a 15 years period) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.1 (qct-esign,indicating that it is a Certificate that creates Digital Signatures)

2.2.3 Extensions of Certificates without DCCF

Extension	Critical	Values
Certificate Policies	-	<OID of the Certification Policy of the Certificate> 1.3.6.1.4.1.13177.10.1.2.2 <URI of the CPS> User Notice: "Éste es un Certificado Corporativo de Persona Física cualificado para su uso sin DCCF." <OID of the European Certification Policy: 0.4.0.194112.1.0> (Qualified EU Certificates Policy for Qualified Certificates for Natural Persons "QCP-n", without DCCF)

2.2.4 Extensions of Certificates with DCCF

Extension	Critical	Values
Certificate Policies	-	<OID of the Certification Policy of the Certificate> 1.3.6.1.4.1.13177.10.1.2.1: DCCF portable 1.3.6.1.4.1.13177.10.1.2.3: DCCF centralized <URI of the CPS> User Notice: ""Éste es un Certificado Corporativo de Persona Física cualificado para su uso conjuntamente con un DCCF. " <OID of the European Certification Policy: 0.4.0.194112.1.2> (Qualified EU Certificates Policy for Qualified Certificates for Natural Persons "QCP-n-qscd", with DCCF)
QcStatements	-	Id-etsi-qcs-QcSSCD: 0.4.0.1862.1.4 (indicating that the Private Key is guarded in a DCCF)

2.3 Natural Persons Certificate's profile to sign emails

Profile deprecated from September 1, 2023.

2.4 Profiles of Corporate for Representatives of an Entity without Legal Status Certificate.

2.4.1 Distinguished Name (DN)

DN field	Name	Description
CN, Common Name	Name	See specific table in next section (i.e. 99949991H Nomuno Especimenuno Especimenuno (R:B0085974Z))
OI, OrganizationIdentifier (2.5.4.97)	Official records	Tax ID number, exactly as it appears in the Official Records. Coded according to the European Standard ETSI EN 319 412-1 (VATES-B0085974Z)
O, Organization	Organization	Organization Name, exactly as it appears in the Official Records.

Description (2.5.4.13)	Codification of the public document proving the powers of the signatory or Public Records(*)	Reg:XXX/Hoja:XXX/Tomo:XXX/Sección:XXX/Libro:XXX/Folio:XXX /date: dd-mm-aaaa /Inscription:XXX Notary: Name Surname1 Surname2 /Núm Protocolo: XXX /Authorization Date: dd-mm-aaaa Official Journals: Boletín: XXX /date: dd-mm-aaaa /Resolution number: XXX Other supporting documentation of entity representation.
C, Country	Country	two digit country code, according to ISO 3166-1. By default "ES".
serialNumber	Serial Number	ID (DNI, NIF or NIE) of the signatory according to the european standard ETSI EN 319 412-1 (IDCES-1234567890Z)
SN, surName	Surname	signatory's surname, exactly as it appears on their ID
GN, givenName	Name de Pila	signatory's First name, exactly as it appears on their ID
E, email	e-mail	*signatory's e-mail.* *(Optional and not recommended, as it is obsolete according to RFC 5280)*

(*)The data will be included exactly the same as in the official document, including, if applicable, characters "/".

2.4.1.1 Common Name

Field	Content	Example	Size*
NIF	National ID number	99949991H	10
Name	exactly as it appears in the National ID card	Nomuno	
Surname 1	exactly as it appears in the National ID card	Especimenuno	
Literal	(R:		4

Tax ID Number of the Company	Tax ID Number of the Company, exactly as it appears in the Official Records.	B0085974Z	9
Literal	)		2

*(taking into account the next blank space)

2.4.2 Common extensions of certificates

Extension	Critical	Values
Subject Alternative Name	-	*RFC822Name: :<signatory's email>* ***(Optional)*** directoryName: ● 1.3.6.1.4.1.13177.0.1: First name of the natural person, exactly as it appears on their ID. ● 1.3.6.1.4.1.13177.0.2: First surname of the natural person, exactly as it appears on their ID ● 1.3.6.1.4.1.13177.0.3: Second surname of the natural person, exactly as it appears on their ID(this field could be empty)
Basic Constraints	Yes	CA:FALSE
Key Usage	Yes	Digital Signature Content Commitment Key Encipherment,
Extended Key Usage	-	*eMail Protection (****Use prohibited from September 2023)*** TLS Website Client Authentication Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) (**Included** from the 15th of September, 2023)
Subject Key Identifier	-	<ID of the Certificate's Public Key, obtained from its hash>
Authority Key Identifier	-	<ID of the CA Certificate's Public Key, obtained from its hash>
CRL Distribution Points	-	<URI of the CRL>
QcStatements	-	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicating Qualified Certificates) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (for a 15 years period) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.1 (qct-esign,indicating that it is a Certificate that creates Digital Signatures).

Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP server> Access Method: Id-ad-caIssuers Access Location: <URI to access the issuer CA's Certificate>

2.4.3 Extensions of Certificates without DCCF

Extension	Critical	Values
Certificate Policies	-	<OID of the Certification Policy of the Certificate> 1.3.6.1.4.1.13177.10.1.13.2 <URI of the CPS> User Notice: "Éste es un Certificado Corporativo de Representante de Entidad sin Personalidad Jurídica cualificado." <OID of the European Certification Policy: 0.4.0.194112.1.0> (Qualified EU Certificates Policy for Qualified Certificates for Natural Persons "QCP-n", without DCCF) <OID of the natural person who Represents an Entity without Legal Status Secretariat SGIADSC: 2.16.724.1.3.5.9 >

2.4.4 Extensions of Certificates with DCCF

Extension	Critical	Values
Certificate Policies	-	<OID of the Certification Policy of the Certificate> 1.3.6.1.4.1.13177.10.1.13.1: DCCF portable 1.3.6.1.4.1.13177.10.1.13.3: DCCF centralized <URI of the CPS> User Notice: "Éste es un Certificado Corporativo de Representante de Entidad sin Personalidad Jurídica cualificado en DCCF. <OID of the European Certification Policy: 0.4.0.194112.1.2> (Qualified EU Certificates Policy for Qualified Certificates for Natural Persons "QCP-n-qscd", with DCCF) <OID of the natural person who Represents an Entity without Legal Status Secretariat SGIADSC: 2.16.724.1.3.5.9 >
QcStatements	-	Id-etsi-qcs-QcSSCD: 0.4.0.1862.1.4 (indicating that the Private Key is guarded in a DCCF)

2.5 Profile of the Corporate Certificate for Legal Representatives

2.5.1 Distinguished Name (DN)

DN field	Name	Description
CN, Common Name	Name	See specific table in next section (i.e. 99949991H NOMUNO ESPECIMENUNO (R:B0085974Z))
OI, OrganizationIdentifier	Registry data	NIF, exactly as it appears in the Official Records. Coded according to the European Standard ETSI EN 319 412-1 (VATES-B0085974Z)
O, Organization	Organization	Organization Name, exactly as it appears in the Official Records.
Description (2.5.4.13)	Codification of the public document proving the powers of the signatory or Public Records(*)	Reg:XXX/IRUS[1]:XXXXXX / Hoja:XXX / Tomo:[2]XXX / Sección:XXX / Libro:XXX / Folio[3]:XXX / date: dd-mm-aaaa /Inscripción:XXX Notary: Name Surname1 Surname2 /Núm Protocolo: XXX /Authorization Date: dd-mm-aaaa Official Journals: Boletín: XXX /date: dd-mm-aaaa /Number resolución: XXX
C, Country	Country	two digit country code, according to ISO 3166-1. By default "ES".
serialNumber	Serial Number	Administrative number assigned by national legislation according to the value of the Country field. (**) Ex: "IDCES-99949991H"
SN, surName	Surname	signatory's surname, exactly as it appears on their ID
GN, givenName	Name de Pila	signatory's First name, exactly as it appears on their ID
E, email	e-mail	*signatory's e-mail.* *(Optional and not recommended, as it is obsolete according to RFC 5280)*

[1] IRUS: Mandatory field as of May 9, 2024, due to the entry into force of the electronic registry folio. For those registered before that date, it is optional.

[2] As of May 9, 2024, this field no longer exists in the registry.

[3] As of May 9, 2024, this field no longer exists in the registry.

ISO 17442-2 LEI number (1.3.6.1.4.1.52266.1) (optional)		LEI is a 20-character alphanumeric code based on ISO / IEC 17442 that connects to key reference information that enables the unique identification of legal entities involved in financial transactions.
ISO 17442-2 LEI role (1.3.6.1.4.1.52266.2) (optional)		Role of an individual in the organization described by the certificate.

(*)The data will be included exactly the same as in the official document, including, if applicable, characters "/" (**)In the event that the signatory does not have an ID, the Passport Number will be indicated in the format indicated in the corresponding section of the CPS. The use of a document other than a DNI, NIE or NIF implies the impossibility of processing with the Spanish Public Administrations.

2.5.1.1 Common Name

Field	Content	Example	Size*
NIF	National ID number (DNI, NIF or NIE)	99949991H	10
Name	exactly as it appears in the National ID card	Nomuno	
Surname 1	exactly as it appears in the National ID card	Especimenuno	
Literal	(R:		4
Tax ID Number of the Company	Tax ID Number of the Company, exactly as it appears in the Official Records.	B0085974Z	9
Literal	)		2

*(taking into account the next blank space)

2.5.2 Common extensions of certificates

Extension	Critical	Values

Subject Alternative Name	-	*RFC822Name: :<signatory's email>* ***(Optional)*** directoryName: ● 1.3.6.1.4.1.13177.0.1: First name of the natural person, exactly as it appears on their ID. ● 1.3.6.1.4.1.13177.0.2: First surname of the natural person, exactly as it appears on their ID ● 1.3.6.1.4.1.13177.0.3: Second surname of the natural person, exactly as it appears on their ID(this field could be empty)
Basic Constraints	Yes	CA:FALSE
Key Usage	Yes	Digital Signature Content Commitment Key Encipherment,
Extended Key Usage	-	*eMail Protection (****Use prohibited from September 2023)*** TLS Web Client Authentication Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) (Included from the 15th of September, 2023)
Subject Key Identifier	-	<ID of the Certificate's Public Key, obtained from its hash>
Authority Key Identifier	-	<ID of the CA Certificate's Public Key, obtained from its hash>
CRL Distribution Points	-	<URI of the CRL>
Authority Informacion Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP server> Access Method: Id-ad-caIssuers Access Location: <URI to access the issuer CA's Certificate>

2.5.3 Extensions of Certificates without DCCF

Extension	Critical	Values

Certificate Policies	-	<OID of the Certification Policy of the Certificate> 1.3.6.1.4.1.13177.10.1.11.2 <URI of the CPS> User Notice: "Éste es un Certificado Corporativo de Representante Legal. " <OID of the European Certification Policy: 0.4.0.194112.1.0> (Qualified EU Certificates Policy for Qualified Certificates for Natural Persons "QCP-n", without DCCF) <OID of the natural person who represents the legal person according to Secretariat SGIADSC: 2.16.724.1.3.5.8 >
QcStatements	-	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicating Qualified Certificates) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (for a 15 years period) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.1 (qct-esign,indicating that it is a Certificate that creates Digital Signatures).

2.5.4 Extensions of Certificates with DCCF

Extension	Critical	Values
Certificate Policies	-	<OID of the Certification Policy of the Certificate> 1.3.6.1.4.1.13177.10.1.11.1: DCCF portable 1.3.6.1.4.1.13177.10.1.11.3: DCCF centralized <URI of the CPS> User Notice: "Éste es un Certificado Corporativo de Representante Legal cualificado, en DCCF." <OID of the European Certification Policy: 0.4.0.194112.1.2> (Qualified EU Certificates Policy for Qualified Certificates for Natural Persons "QCP-n-qscd", with DCCF) <OID of the natural person who represents the legal person according to Secretariat SGIADSC: 2.16.724.1.3.5.8 >
QcStatements	-	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicating Qualified Certificates) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (for a 15 years period) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.1 (qct-esign,indicating that it is a Certificate that creates Digital Signatures). Id-etsi-qcs-QcSSCD: 0.4.0.1862.1.4 (indicating that the Private Key is guarded in a DCCF)

2.6 Profile of the Corporate Certificate for Voluntary Representative against Public Administration.

2.6.1 Distinguished Name (DN)

DN field	Name	Description
CN, Common Name	Name	See specific table in next section (i.e. 99949991H Nomuno Especimenuno (R:B0085974Z))
OI, OrganizationIdentifier	Registry data	NIF, exactly as it appears in the Official Records. Coded according to the European Standard ETSI EN 319 412-1 (VATES-B0085974Z)
O, Organization	Organization	Organization Name, exactly as it appears in the Official Records.
Description (2.5.4.13)	Codification of the public document proving the powers of the signatory or Public Records(*)	Reg:XXX/IRUS[4]:XXXXXX / Hoja:XXX / Tomo:[5]XXX / Sección:XXX / Libro:XXX / Folio[6]:XXX / date: dd-mm-aaaa /Inscripción:XXX Notary: Name Surname1 Surname2 /Núm Protocolo: XXX /Authorization Date: dd-mm-aaaa Official Journals: Boletín: XXX /date: dd-mm-aaaa /Number resolución: XXX
C, Country	Country	two digit country code, according to ISO 3166-1. By default "ES".
serialNumber	Serial Number	Administrative number assigned by national legislation according to the value of the Country field. (*) Ex: "IDCES-99949991H"
SN, surName	Surname	signatory's surname, exactly as it appears on their ID
GN, givenName	Name de Pila	signatory's First name, exactly as it appears on their ID
E, email	Email	*signatory's e-mail.* *(Optional and not recommended, as it is obsolete according to RFC 5280)*

[4] IRUS: Mandatory field as of May 9, 2024, due to the entry into force of the electronic registry folio. For those registered before that date, it is optional.

[5] As of May 9, 2024, this field no longer exists in the registry.

[6] As of May 9, 2024, this field no longer exists in the registry.

(*)The data will be included exactly the same as in the official document, including, if applicable, characters "/". In the event that the signatory does not have an ID, the Passport Number will be indicated in the format indicated in the corresponding section of the CPS. The use of a document other than a DNI, NIE or NIF implies the impossibility of processing with the Spanish Public Administrations.

2.6.1.1 Common Name

Field	Content	Example	Size*
NIF	ID Number	99949991H	10
Name	exactly as it appears in the ID	Nomuno	
Surname 1	exactly as it appears in the ID	Especimenuno	
Literal	(R:		4
Tax ID number of the Company	Tax ID number of the Company, exactly as it appears in the Official Records.	B0085974Z	9
Literal	)		2

*(taking into account the next blank space)

2.6.2 Common extensions of certificates

Extension	Critical	Values
Subject Alternative Name	-	*RFC822Name: :<signatory's email>* ***(Optional)*** directoryName: • 1.3.6.1.4.1.13177.0.1: First name of the natural person, exactly as it appears on their ID. • 1.3.6.1.4.1.13177.0.2: First surname of the natural person, exactly as it appears on their ID • 1.3.6.1.4.1.13177.0.3: Second surname of the natural person, exactly as it appears on their ID(this field could be empty)
Basic Constraints	Yes	CA:FALSE
Key Usage	Yes	Digital Signature Content Commitment Key Encipherment,

Extended Key Usage	-	*eMail Protection (**Use prohibited from September 2023)*** TLS Website Client Authentication Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) (Included from the 15th of September, 2023)
Subject Key Identifier	-	<ID of the Certificate's Public Key, obtained from its hash>
Authority Key Identifier	-	<ID of the CA Certificate's Public Key, obtained from its hash>
CRL Distribution Points	-	<URI of the CRL>
QcStatements	-	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicating Qualified Certificates) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (for a 15 years period) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.1 (qct-esign,indicating that it is a Certificate that creates Digital Signatures).
Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP server> Access Method: Id-ad-caIssuers Access Location: <URI to access the issuer CA's Certificate>

2.6.3 Extensions of Certificates without DCCF

Extension	Critical	Values
Certificate Policies	-	<OID of the Certification Policy of the Certificate> 1.3.6.1.4.1.13177.10.1.12.2 <URI of the CPS> User Notice: Este es un Certificado Corporativo de Representante Voluntario cualificado frente a las AAPP." <OID of the European Certification Policy: 0.4.0.194112.1.0> (Qualified EU Certificates Policy for Qualified Certificates for Natural Persons "QCP-n", without DCCF) <OID of the natural person who represents the legal person according to Secretariat SGIADSC: 2.16.724.1.3.5.8 >

2.6.4 Extensions of Certificates with DCCF

Certificate Policies	-	<OID of the Certification Policy of the Certificate> 1.3.6.1.4.1.13177.10.1.12.1: DCCF portable 1.3.6.1.4.1.13177.10.1.12.3: DCCF centralized <URI of the CPS> User Notice: "Este es un Certificado Corporativo de Representante Voluntario cualificado frente a las AAPP, en DCCF." <OID of the European Certification Policy: 0.4.0.194112.1.2> (Qualified EU Certificates Policy for Qualified Certificates for Natural Persons "QCP-n-qscd", with DCCF) <OID of the natural person who represents the legal person according to Secretariat SGIADSC: 2.16.724.1.3.5.8 >
QcStatements	-	Id-etsi-qcs-QcSSCD: 0.4.0.1862.1.4 (indicating that the Private Key is guarded in a DCCF)

2.7 Profile of Personal Certificates

2.7.1 Distinguished Name (DN)

DN field	Name	Description
CN, Common Name	Name	Name and Surnames of the signatory
serialNumber	Serial Number	Administrative number assigned by national legislation according to the value of the Country field. (*) Ex: "IDCES-99949991H"
SN, surName	Surname	signatory's surname, exactly as it appears on their ID
GN, givenName	Name de pila	signatory's First name, exactly as it appears on their ID
C, Country	Country	two digit country code, according to ISO 3166-1. By default "ES".
E, email	Email	*signatory's e-mail.* *(Optional and not recommended, as it is obsolete according to RFC 5280)*

(*)In the event that the signatory does not have an ID, the Passport Number shall be indicated in the format indicated in the corresponding section of the CPS andit shall be coded according to ETSI EN 319 412-1. The use of a document other than the DNI, NIE or NIF implies the impossibility of processing with the Spanish Public Administrations.

2.7.2 Common extensions of certificates

Extension	Critical	Value
Basic Constraints	Yes	CA:FALSE
Key Usage	Yes	Digital Signature Content Commitment Key Encipherment
Extended Key Usage	-	*eMail Protection* (***Use prohibited from September 2023)*** TLS Web Client Authentication Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) (Included from the 15th of September, 2023)
Subject Key Identifier	-	<ID of the Certificate's Public Key, obtained from its hash>
Authority Key Identifier	-	<ID of the CA Certificate's Public Key, obtained from its hash>
CRL Distribution Points	-	<URI of the CRL>
qcStatements	-	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicating Qualified Certificates) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (for a 15 years period) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.1 (qct-esign,indicating that it is a Certificate that creates Digital Signatures).
Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP server> Access Method: Id-ad-calssuers Access Location: <URI to access the issuer CA's Certificate>

Subject Alternative Name	-	*RFC822Name: :<signatory's email>* ***(Optional)*** directoryName: ● 1.3.6.1.4.1.13177.0.1: First name of the natural person, exactly as it appears on their ID. ● 1.3.6.1.4.1.13177.0.2: First surname of the natural person, exactly as it appears on their ID ● 1.3.6.1.4.1.13177.0.3: Second surname of the natural person, exactly as it appears on their ID(this field could be empty)

2.7.3 Certificate extensions without DCCF

Extension	Critical	Value
Certificate Policies	-	<OID of the Certification Policy of the Certificate> 1.3.6.1.4.1.13177.10.1.40.2 <URI of the CPS> User Notice: "Éste es un Certificado Personal de Persona Física cualificado para su uso sin DCCF." <OID of the European Certification Policy: 0.4.0.194112.1.0> (Qualified EU Certificates Policy for Qualified Certificates for Natural Persons "QCP-n", without DCCF)

2.7.4 Certificate extensions with DCCF

Extension	Critical	Value
Certificate Policies	-	<OID of the Certification Policy of the Certificate> 1.3.6.1.4.1.13177.10.1.40.3: DCCF centralized <URI of the CPS> User Notice: "Este es un Certificado Personal de Persona Física cualificado, en DCCF." <OID of the European Certification Policy: 0.4.0.194112.1.2> (Qualified EU Certificates Policy for Qualified Certificates for Natural Persons "QCP-n-qscd", with DCCF).
QcStatements	-	Id-etsi-qcs-QcSSCD: 0.4.0.1862.1.4 (indicates that the private key is kept in a DCCF)

2.8 Profile of the Public Officer Certificate

2.8.1 Distinguished Name (DN)

DN field	Name	Description
O, Organization	Organization	Official Name of the Public Administration or Public Entity subscriber of the certificate, to which the employee has an entailment.
OU, Organization Unit	Description of the certificate	"CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO"(*)
OU, Organization Unit (optional)	Organization Unit	Unit, inside the Organization, to which the certificate's subscriber has an entailment.
OU, Organization Unit (optional)	Certificate Subscriber Identification Number (supposedly unique).	It corresponds to the NRP or NIP
Title (optional)	Title	The position of the natural person, which links them with the Public Administration or Public Entity subscribing the certificate, must be included.
serialNumber(**)	Serial Number	National ID number of the Public Officer, written as defined in ETSI EN 319 412-1
SN, Surname	Surname (Natural Person)	First and second Surname according to ID document (National ID card, NIE) + " - DNI " + National ID number of the Public Officer
GN, Given name	Name	signatory's First name, exactly as it appears on their ID
CN, Common Name	Name, Surname y NIF	Name and Surnames, according to the ID document (National ID/Passport) + " - DNI " + National ID number of the Public Officer's
C, Country	Country	Two digit country code, according to ISO 3166-1. By default "ES".
E, email	E-mail	*signatory's e-mail.* *(Optional and not recommended, as it is obsolete according to RFC 5280)*

(*) All the literals must be introduced in uppercase except for the domain/subdomain and the email, according to "Perfiles de Certificados Electrónicos" de 16 de abril de 2016 del Ministerio de Hacienda y Administraciones Públicas".

(**) SerialNumber = p. ej: IDCES-00000000G. 3 characters to indicate the Document Number (IDC= documento nacional de identidad/NIE) + 2 characters to identify theCountry (ES) + Identity Number (Printable String)) Size [RFC 5280] 64

2.8.2 Common extensions of certificates

Extension	Critical	Values

Subject Alternative Name (optional)	-	*RFC822Name: :<signatory's email> (**Optional)***
Basic Constraints	Yes	CA:FALSE
Key Usage	Yes	Content Commitment Digital Signature Key Encipherment
Extended Key Usage	-	Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) (**Included** from the 15th of September, 2023) *eMail Protection (**Use prohibited from September 2023)*** TLS Web Client Authentication
Subject Key Identifier	-	<ID of the Certificate's Public Key, obtained from its hash>
Authority Key Identifier	-	<ID of the CA Certificate's Public Key, obtained from its hash>
Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP server> Access Method: Id-ad-calssuers Access Location: <URI to access the issuer CA's Certificate>
CRL Distribution Points	-	<URI of the CRL>
Qualified Certificate Statements	Yes	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicating Qualified Certificates) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (for a 15 years period) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.1 (qct-esign,indicating that it is a Certificate that creates Digital Signatures).

2.8.3 Extensions of Certificates with, high level

Extension	Critical	Values

Certificate Policies	-	<OID of the Certification Policy of the Certificate> 1.3.6.1.4.1.13177.10.1.22.1: DCCF portable 1.3.6.1.4.1.13177.10.1.22.3: DCCF centralized <URI of the CPS> User Notice: ● "Éste es un Certificado Cualificado de personal, nivel alto" <OID of the European Certification Policy> ● 0.4.0.194112.1.2 (Qualified EU Certificates Policy for Qualified Certificates for Natural Persons "QCP-n-qscd", with DCCF) <OID Public Officer Certification Policy: 2.16.724.1.3.5.7.1>
Qualified Certificate Statements	Yes	Id-etsi-qcs-QcSSCD: 0.4.0.1862.1.4 (indicating that the Private Key is guarded in a DCCF)
Subject Alternative Name	-	directoryName: OID: 2.16.724.1.3.5.7.1.1 = "certificado electrónico de empleado público de nivel alto" OID: 2.16.724.1.3.5.7.1.2 = <O of the DN> OID: 2.16.724.1.3.5.7.1.3 = <Tax ID number of the subscribing entity> OID: 2.16.724.1.3.5.7.1.4 = <serialNumber of the DN> (optional) OID: 2.16.724.1.3.5.7.1.5 = Certificate Subscriber Identification Number (supposedly unique). It corresponds to the NRP or NIP. (third entry <OU of DN>) OID: 2.16.724.1.3.5.7.1.6 = <Given name> OID: 2.16.724.1.3.5.7.1.7 = <First Surname of the Public Officer> (optional) OID: 2.16.724.1.3.5.7.1.8 = <Second Surname of the Public Officer> (optional) OID: 2.16.724.1.3.5.7.1.9 = <Email of the Public Officer> (optional) OID: 2.16.724.1.3.5.7.1.10 = Unit, inside the Administration, to which the certificate subscriber has an entailment (second entry <OU of the DN>) (optional) OID: 2.16.724.1.3.5.7.1.11 = <Title, T of the DN>

2.8.4 Extensions of Certificates with, medium level

Extension	Critical	Values

Certificate Policies	-	<OID of the Certification Policy of the Certificate> 1.3.6.1.4.1.13177.10.1.22.2 <URI of the CPS> User Notice: "Éste es un Certificado Cualificado de personal, nivel medio." <OID of the European Certification Policy: 0.4.0.194112.1.0> (Qualified EU Certificates Policy for Qualified Certificates for Natural Persons "QCP-n", without DCCF) <OID Public Officer Certification Policy: 2.16.724.1.3.5.7.2>
Subject Alternative Name	-	(optional) otherName-userPrincipalName (UPN): Windows Domain User of the Public Officer directoryName: OID: 2.16.724.1.3.5.7.2.1 = "certificado electrónico de empleado público" OID: 2.16.724.1.3.5.7.2.2 = <O og the DN> OID: 2.16.724.1.3.5.7.2.3 = <Tax ID number of the subscribing entity> OID: 2.16.724.1.3.5.7.2.4 = <ID of the Public Officer> (optional) OID: 2.16.724.1.3.5.7.2.5 = Certificate Subscriber Identification Number (supposedly unique). It corresponds to the NRP or NIP. (third entry <OU of DN>) OID: 2.16.724.1.3.5.7.2.6 = <Given name> OID: 2.16.724.1.3.5.7.2.7 = <First Surname of the Public Officer> (optional) OID: 2.16.724.1.3.5.7.2.8 = <Second Surname of the Public Officer> (optional) OID: 2.16.724.1.3.5.7.2.9 = <Email of the Public Officer> (optional) OID: 2.16.724.1.3.5.7.2.10 = Unit, inside the Administration, to which the certificate subscriber has an entailment (second entry <OU of the DN>) (optional) OID: 2.16.724.1.3.5.7.2.11 = <Title, T of the DN>

2.9 Profile of Public Officer with pseudonym or with professional identification number Certificates

2.9.1 Distinguished Name (DN)

DN field	Name	Description
O, Organization	Organization	Official Name of the Public Administration or Entity subscribing the certificate, to which the Public Officer has an entailment.
OU, Organization Unit	Description of the certificate	"CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO CON SEUDÓNIMO"(*)

OU, Organization Unit (optional)	Organization Unit	Unit, inside the Administration, to which the certificate subscriber has an entailment
OU, Organization Unit (optional)	DIR3 Code of the unit	Ej: E04976701
pseudonym 2.5.4.65	Seudónimo	Ej: NIP 111111111
Title (optional)	Title	The position of the natural person must be included, which links them with the Public Administration or Public Entity subscribing the certificate.
CN, Common Name	pseudonym	"SEUDÓNIMO - " + pseudonym +" - " + organization
C, Country	Country	two digit country code, according to ISO 3166-1. By default "ES".

(*) All the literals must be introduced in uppercase except for the domain/subdomain and the email, according to "Perfiles de Certificados Electrónicos" de 16 de abril de 2016 del Ministerio de Hacienda y Administraciones Públicas".

2.9.2 Common extensions of certificates

Extension	Critical	Values
Basic Constraints	Yes	CA:FALSE
Extended Key Usage	-	Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) (Included from the 15th of September, 2023)
Subject Key Identifier	-	<ID of the Certificate's Public Key, obtained from its hash>
Authority Key Identifier	-	<ID of the CA Certificate's Public Key, obtained from its hash>
Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP server> Access Method: Id-ad-caIssuers Access Location: <URI to access the issuer CA's Certificate>
CRL Distribution Points	-	<URI of the CRL>
Qualified Certificate Statements	Yes	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicating Qualified Certificates) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (for a 15 years period)

2.9.4 Extensions of Certificates with, medium level

Extension	Critical	Values
Key Usage	Yes	Digital Signature Content Commitment Key Encipherment
Extended Key Usage	-	TLS Web Client Authentication
Certificate Policies	-	<OID of the Certification Policy of the Certificate> 1.3.6.1.4.1.13177.10.1.23.2 <URI of the CPS> User Notice: "Éste es un Certificado Cualificado de personal, nivel medio." <OID of the European Certification Policy, corresponding to the policy for qualified EU certificates issued to natural persons "QCP-n", without a DCCF> 0.4.0.194112.1.0 <OID Public Officer with pseudonym Certification Policy, medium level> 2.16.724.1.3.5.4.2
Subject Alternative Name	-	(optional) otherName-userPrincipalName (UPN): Windows Domain User of the Public Officer directoryName: OID: 2.16.724.1.3.5.4.2.1 = "Public Officer with pseudonym Certificate" OID: 2.16.724.1.3.5.4.2.2 = <O of the DN> OID: 2.16.724.1.3.5.4.2.3 = <Tax ID number of the subscribing entity> (Optional) OID: 2.16.724.1.3.5.4.2.9 = <Email of the Civil Servant> (Optional) OID: 2.16.724.1.3.5.4.2.10 = Unit, inside the Public Administration, to which the certificate subscriber has an entailment (second entry <OU of the DN>)(Opcional) (Optional) OID: 2.16.724.1.3.5.4.2.11 = <Title, T of the DN> OID: 2.16.724.1.3.5.4.2.12 = <pseudonym of the DN>
Qualified Certificate Statements		d-etsi-qcs-QcType: 0.4.0.1862.1.6.1 (qct-esign,indicating that it is a Certificate that creates Digital Signatures).

3 Description of profiles of the Electronic Seal Certificate

3.1 Profile of Electronic Seal Certificates for Public Administration or Entity.

3.1.1 Certificate

DN field	Name	Description
O, Organization	Organization	It will contain the name of the Administration to which the body belongs (p.e. "Ministry of Equality")
OI, Organization Identifier	Organization Identifier	Organization Identifier different from the Name. According to ETSI EN 319 412-1 (Eg. VATES +entity's tax number; NTRES-08005.123456789…)
OU, Organization Unit	Organization Unit	"Electronic Seal"
Serial Number	Tax ID Number	Tax ID number of the Public Administration or Public Entity.
SN, Surname (optional)	Surname (Natural Person)	First and second surname (according to National ID card or NIE) + " - DNI " + National ID number of the private key custodian
GN, Given name (optional)	Name (Natural Person)	First Name according to the Private Key custodian's ID (DNI/TIE).
CN, Common Name	System or application name	p.e. "VALIDATION PLATFORM OF THE CITY COUNCIL OF xxx"
C, Country	Country	"ES"

3.1.2 Common extensions of certificates

Extension	Critical	Values
Basic Constraints	Yes	CA:FALSE

Key Usage	Yes	Digital Signature Content Commitment Key Encipherment
Extended Key Usage	-	Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) (Included from the 15th of September, 2023) *eMail Protection* ***(Use prohibited from September 2023)*** TLS Website Client Authentication
Subject Key Identifier	-	<ID of the Certificate's Public Key, obtained from its hash>
Authority Key Identifier	-	<ID of the CA Certificate's Public Key, obtained from its hash>
Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP server> Access Method: Id-ad-calssuers Access Location: <URI to access the issuer CA's Certificate>
CRL Distribution Points	-	<URI of the CRL>
Qualified Certificate Statements	Yes	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicating Qualified Certificates) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (for a 15 years period) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.2 (qct-eseal, it indicates that it is a certificate that creates electronic seals).

3.1.3 Extensions of Certificates, high level

Extension	Critical	Values
Certificate Policies	-	<OID of the Certification Policy of the Certificate> 1.3.6.1.4.1.13177.10.1.21.1: DCCF portable 1.3.6.1.4.1.13177.10.1.21.3: DCCF centralized <URI of the CPS> User Notice: "Certificado cualificado de sello de Administración, órgano o entidad de derecho público, nivel alto." <OID of the Certification Policy according to Secretariat SGIADSC: 2.16.724.1.3.5.6.1> < OID "for EU qualified certificates issued to legal persons" according to ETSI EN 319 411-2: QCP-l-qscd: 0.4.0.194112.1.3>

Qualified Certificate Statements	Yes	Id-etsi-qcs-QcSSCD: 0.4.0.1862.1.4 (indicating that the Private Key is guarded in a DCCF)
Subject Alternative Name	-	*RFC822Name: :<signatory's email>* ***(Optional)*** directoryName: OID: 2.16.724.1.3.5.6.1.1 = "Electronic Seal high level" OID: 2.16.724.1.3.5.6.1.2 = <O of the DN> OID: 2.16.724.1.3.5.6.1 .3 = <serialNumber of the DN> (optional) OID: 2.16.724.1.3.5.6.1 .4 = <Custodian ID> (optional) OID: 2.16.724.1.3.5.6.1 .5 = <CN of the DN> (optional) OID: 2.16.724.1.3.5.6.1 .6 = <Given name> (optional) (optional) OID: 2.16.724.1.3.5.6.1 .7 = <First Surname of the Custodian>(*) (optional) OID: 2.16.724.1.3.5.6.1 .8 = <Second Surname of the Custodian>(*) (optional) (optional) OID: 2.16.724.1.3.5.6.1 .9 = <Email of the Custodian> (optional)

(*) According to the ID or NIE

3.1.4 Extensions of Certificates, medium level

Extension	Critical	Values
Certificate Policies	-	<OID of the Certification Policy of the Certificate> 1.3.6.1.4.1.13177.10.1.21.2 <URI of the CPS> User Notice: "Certificado cualificado de sello de Administración, órgano o entidad de derecho público, nivel medio." <OID of the Certification Policy of theMHAP: 2.16.724.1.3.5.6.2> <OID "for EU qualified certificates issued to legal persons" according to ETSI EN 319 411-2: QCP-l: 0.4.0.194112.1.1>
Subject Alternative Name	-	*RFC822Name: :<signatory's email>* ***(Optional)*** directoryName: OID: 2.16.724.1.3.5.6.2.1 = "Electronic Seal medium level" OID: 2.16.724.1.3.5.6.2.2 = <O of the DN> OID: 2.16.724.1.3.5.6.2.3 = <DN serialNumber> (optional) OID: 2.16.724.1.3.5.6.2.4 = <ID of the custodian> OID: 2.16.724.1.3.5.6.2.5 = <CN of the DN>

		(optional) OID: 2.16.724.1.3.5.6.2.6 = <Given name> (optional) OID: 2.16.724.1.3.5.6.2.7 = <Custodian's First Surname>(*) (optional) OID: 2.16.724.1.3.5.6.2.8 = <Custodian's Second Surname> (*) (optional) OID: 2.16.724.1.3.5.6.2.9 = <Email of the custodian>

(*)According to the ID or NIE

3.2 Profile of the Corporate Company Seal Certificates

3.2.1 Distinguished Name (DN)

DN field	Name	Description
CN, Common Name	Name	It contains the Legal Person's trade name.
serialNumber	Tax ID Number	<Legal Person Tax ID number>
O, Organization	Organization	It contains the exact denomination of the legal person that as it appears in the commercial register, or in case of PSD2 certificates, in the Public Registry of the Competent National Authority of the Member State of origin or resulting from notifications to the EBA (European Banking Authority).
OI, organizationIdentifier	Organization Identifier	Organization Identifier, according to ETSI EN 319 412-1 (Eg. VATES +entity's tax number; NTRES-08005.123456789…) In case of PSD2 certificates, Organization Identifier, according to ETSI TS 119 495
OU, Organization Unit (optional)	Organization Unit	It will contain the Department or Unit
E, Email Address (optional)	Email	It will contain a Company email. *(Optional and not recommended, as it is obsolete according to RFC 5280)*
ST, State	Geographic Location	Geographic location of the subscriber (eg. Province)
C, Country	Country	Two digit country code, according to ISO 3166-1. By default "ES".

ISO 17442-2 LEI number (1.3.6.1.4.1.52266.1) (optional)		LEI is a 20-character alphanumeric code based on ISO / IEC 17442 that connects to key reference information that enables the unique identification of legal entities involved in financial transactions.

(*) According to ETSI EN 319 412-1 and ETSI EN 319 412-3

3.2.2 Extensions of Certificates, with DCCF

Extension	Critical	Values
Basic Constraints	Yes	CA:FALSE
Key Usage	Yes	Digital Signature Content Commitment Key Encipherment (Optional, and only for RSA)
Extended Key Usage	-	*eMail Protection* ***(Use prohibited from September 2023)*** TLS Website Client Authentication Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) (Included from the 15th of September, 2023)
Subject Key Identifier	-	<ID of the Certificate's Public Key, obtained from its hash>
Authority Key Identifier	-	<ID of the CA Certificate's Public Key, obtained from its hash>
Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP server> Access Method: Id-ad-calssuers Access Location: <URI to access the issuer CA's Certificate>
CRL Distribution Points	-	<URI of the CRL>

Certificate Policies	-	<OID of the Certification Policy of the Certificate> 1.3.6.1.4.1.13177.10.1.10.3 <URI of the CPS> User Notice: "Éste es un Certificado Corporativo de Sello Empresarial Cualificado emitido en DCCF." < OID "for EU qualified certificates issued to legal persons" according to ETSI EN 319 411-2: QCP-l: 0.4.0.194112.1.3>
Subject Alternative Name (optional)	-	<Contact Email>
QcStatements	-	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicating Qualified Certificates) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (for a 15 years period) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.2 (qct-eseal,indicating that it is a Certificate that creates Digital Signatures). Id-etsi-qcs-QcSSCD: 0.4.0.1862.1.4 (indicating that the Private Key is guarded in a DCCF)

3.2.3 Extensions of Certificates, without DCCF

Extension	Critical	Values
Basic Constraints	Yes	CA:FALSE
Key Usage	Yes	Digital Signature Content Commitment Key Encipherment (Optional, and only for RSA) Data Encipherment (Optional, and only for RSA)
Extended Key Usage	-	TLS Website Client Authentication *eMail Protection* (***Use prohibited from September 2023)*** Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) (**Included** from the 15th of September, 2023)
Subject Key Identifier	-	<ID of the Certificate's Public Key, obtained from its hash>

Authority Key Identifier	-	<ID of the CA Certificate's Public Key, obtained from its hash>
Authority Information Access	-	Access Method: Id-ad-calssuers Access Location: <URI to access the issuer CA's Certificate> Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP server>
CRL Distribution Points	-	<URI of the CRL>
Certificate Policies	-	<OID of the Certification Policy of the Certificate> 1.3.6.1.4.1.13177.10.1.10.2 <URI of the CPS> User Notice: "Éste es un Certificado Corporativo de Sello Empresarial Cualificado." In case of PSD2 certificate: User Notice "Éste es un Certificado Corporativo de Sello Empresarial Cualificado PSD2." < OID "for EU qualified certificates issued to legal persons" according to ETSI EN 319 411-2: QCP-l: 0.4.0.194112.1.1>
Subject Alternative Name (optional)	-	
QcStatements	-	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicating Qualified Certificates) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (for a 15 years period) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.2 (qct-eseal,indicating that it is a Certificate that creates Digital Seals). In case of PSD2 certificates etsi-psd2-qcStatement according to ETSI TS 119 495

4 Description of the Profiles of the Website Authentication Certificates

4.1 Profile of Electronic Office Certificates

4.1.1 Certificate

DN field	Name	Description
CN, Common Name	Name	Denomination of the domain in which the certificate will be located It must be the same as the one that is located in the Subject Alternative Names Extension
O, Organization	Organization	Official name of the subscribing organization of the certification services
OU, Organization Unit	Organization Unit	"SEDE ELECTRONICA". Not present as of version 220517 of this document. *BR (1.7.9)Prohibited after September 1, 2022*
OU, Organization Unit	Organization Unit	Descriptive name of the headquarters. Not present as of version 220517 of this document. *BR (1.7.9)Prohibited after September 1, 2022*
serialNumber optional)(*)	Serial Number	It will contain the Tax Number of the Entity responsible for the Electronic Office
organizationIdentifier		Organization Identifier According to ETSI EN 319 412-1 (Eg. VATES +entity's tax number; NTRES-08005.123456789…)
C, Country	Country	C= ES
L, Locality		City, Province or State.
businessCategory		Category of the Organization: "Government Entity"

jurisdictionCountryNam e		Jurisdiction	JurisdictionCountryName= “ES”

(*)The field SerialNumber is marked as optional, given that the field OrganizationIdentifier contains the same information

4.1.2 Common extensions of certificates

Extension	Critical	Values
Authority Key Identifier	-	<ID of the CA’s Public Key, obtained from its hash>
Subject Key Identifier	-	<ID of the Certificate’s Public Key, obtained from its hash>
Key Usage	Yes	Digital Signature Key Encipherment
Extended Key Usage	-	TSL web Server Authentication TLS Web Client Authentication
Basic Constraints	Yes	CA:FALSE
CRL Distribution Points	-	<URI of the CRL>
Authority Information Access	-	Access Method: Id-ad-calssuers Access Location: <URI to access the issuer CA’s Certificate> Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP server>
Certificate Policies	-	<URI of the CPS> <OID ca-browser-forum.certificate-policies.extended-validation : 2.23.140.1.1> <OID “EU qualified website authentication certificates” according to ETSI EN 319 411-2: QEVCP: 0.4.0.194112.1.4> <OID of the Certification Policy of the Certificate: 0.4.0.2042.1.4>
Qualified Certificate Statements		Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicating Qualified Certificates) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (for a 15 years period) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.3 (qct-web,indicating that it is a Certificate that creates Digital Signatures).
Subject Alternative Name	-	dNSName: Name of the domain in which the certificate will be located.

cabfOrganizationIdentifier (2.23.140.3.1)	-	Scheme: three-digit scheme identifier (VAT, PSD, ...) Country: ISO 3166-1 two-digit country code Reference: identified of the organization according to the scheme and country

4.1.3 Extensions of Certificates with, high level

Extension	Critical	Values
Certificate Policies	-	<OID of the Certification Policy of the Certificate> 1.3.6.1.4.1.13177.10.1.20.1 *User Notice: "Certificado de Sede Electronica Nivel Alto" (Removed by BRG 2.0.0)* <OID of the Certification Policy of the MHAP 2.16.724.1.3.5.5.1>

4.1.4 Extensions of Certificates, medium level

Extension	Critical	Values
Certificate Policies	-	<OID of the Certification Policy of the Certificate> 1.3.6.1.4.1.13177.10.1.20.2 *User Notice: "Certificado de Sede Electronica Nivel Medio" (Removed by BRG 2.0.0)* <OID of the Certification Policy of the MHAP 2.16.724.1.3.5.5.2>

4.2 Profile of the Server Website SSL Certificates

4.2.1 Distinguished Name (DN)

Field	Values	Description
CN, Common Name	Name	(EVG 9.2.3) Name of a single domain. (BR. 7.1.4.2.2.a) Este dominio debe coincidir con el indicado (o con uno de los indicados) en el Subject Alt Names).
O, Organization	Organization	Official Name of the Certificate Subscriber Organization.

OU, Organizational Unit	Department	Optional until version 6.3 (included)of the present policy. No further present. BR (1.7.9)Prohibited after September 1, 2022
serialNumber (optional)(*)	Tax ID Number	Tax ID Number of the Certificate subscriber Organization
OI, OrganizationIdentifier		Organization Identifier, according to ETSI EN 319 412-1 (Eg. VATES +entity's tax number; NTRES-08005.123456789…) In case of PDS2 certificate Organization Identifier, according to ETSI TS 119 495
businessCategory	Private Organization Government Entity Business Entity Non-Commercial Entity	(EVG 9.2.4) Business Category
L, Locality	City	City, Province or State.
ST, StateOfProvince	Province	Organization Province of Registry. Not present as of version 220530 of this document.
C, Country	Country	Two digit country code, according to ISO 3166-1. By default "ES".
jurisdictionCountryName 1.3.6.1.4.1.311.60.2.1.3	Country	(EVG 9.2.5) Subject Jurisdiction of Incorporation or Registration

(*)The SerialNumber field is marked as optional, given that the field OrganizationIdentifier contains the same information.

The fields (EVG 9.2.X) are specific requirements for the Extended Validation Certificates as defined in CA/Browser Forum.

The indications (BR.X) are requirements of the Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates of the CA/Browser Forum, valid at the time of publication of this document.

4.2.2 Extensions of Certificates

Extension	Critical	Values

Subject Alternative Name	-	URL, Name of the domain or identification of the device or service that owns the keys or the application. (EVG 9.2.2) More than 1 domain can be included, but not wildcards. For multi-domain certificates, the URL will follow the format "*.dominio.com" (This indication is prohibited for EV certificates)
Basic Constraints	Yes	CA:FALSE
Key Usage	Yes	Digital Signature Key Encipherment (Does not appear when certificate keys are in Elliptic Curves)
Extended Key Usage	-	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2) optional
Subject Key Identifier	-	<ID of the Certificate's Public Key, obtained from its hash>
Authority Key Identifier	-	<ID of the CA Certificate's Public Key, obtained from its hash>
Authority Information Access	-	Access Method: Id-ad-caIssuers Access Location: <URI to access the issuer CA's Certificate> Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP server>
CRL Distribution Points	-	<URI of the CRL>
Certificate Policies	-	<OID ca-browser-forum.certificate-policies.baseline-requirements.organization-validated: 2.23.140.1.2.2> (para los certificados SSL OV) (First indicate the Cabforum OID - BRG 2.0.0) <OID ca-browser-forum.certificate-policies.extended-validation : 2.23.140.1.1> (para los certificados EV y PSD2) (First indicate the Cabforum OID - BRG 2.0.0) <OID of the Certification Policy of the Certificate> 1.3.6.1.4.1.13177.10.1.3.1 SSL OV 1.3.6.1.4.1.13177.10.1.3.10 SSL EV / Qualified and PSD2 <URI of the CPS> User Notice: "Este es un Certificado de Servidor Web cualificado con Validación Extendida" (for EV Certificates) Removed by BRG 2.0.0 <OID "EU qualified website authentication certificates" according to ETSI EN 319 411-2: QEVCP-w: 0.4.0.194112.1.4 > (for EV and PSD2 Certificates) <OID of the EV Certification Policy for the certificate: 0.4.0.2042.1.4> (for EV and PSD2 Certificates)

Qualified Certificate Statements (solo para EV y PSD2)	-	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicating Qualified Certificates) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (for a 15 years period) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.3 (qct-web,indicating that it is a Certificate that creates Digital Signatures). In case of PSD2 certificates etsi-psd2-qcStatement according to ETSI TS 119 495
cabfOrganizationIdentifier (for EV and PSD2 only)	-	Scheme: three digits scheme ID Country: ISO 3166-1 country code Reference: organization ID number according to scheme and country

5 Description of profiles of Secure Service Certificates CA, TSA, VA

5.1 Profile of CA Certificates

5.1.1 CA Certificates

5.1.1.1 Distinguished Name (DN)

DN field	Name	Description
CN, Common Name	Name	Common Name of the Organization that provides the Certification Service .
O, Organization	Organization	Denomination (Official Name of the Organization) of the certification service provider (Certificate issuer)(*)
C, Country	Country	C=ES

(*)MINHAP 7. SubCA Certificate 1.4.2 Organization

5.1.1.2 Extensions of Certificates

Extension	Critical	Values
Basic Constraints	Yes	CA:TRUE
Key Usage	Yes	keyCertificateSignature cRLSignature
Extended Key Usage	-	<Variable depending on the type of certificate: serverAuth, clientAuth, timeStamping, OCSPSigning, Smartcard Logon, etc. > *eMail Protection* ***(Use prohibited from September 2023)*** Adobe Authentic Documents Trust, (Included from the 15th of September, 2023)
Subject Key Identifier	-	<ID of the Certificate's Public Key, obtained from its hash>
Authority Key Identifier	-	<ID of the CA Certificate's Public Key, obtained from its hash>
CRL Distribution Points	-	<URI of the CRL>
Certificate Policies	-	policyIdentifier: 1.3.6.1.4.1.13177.10.10.2 or AnyPolicy (2.5.29.32.0) (Optional) cPSURI: http://www.firmaprofesional.com/cps

		userNotice: “Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps”
Authority Information Access	-	accessMethod: Id-ad-calssuers accessLocation: <URI to access the issuer CA’s Certificate> Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP server>

5.1.2 QCA Certificates (Qualified CA)

5.1.2.1 Distinguished Name (DN)

Additionally, the DN of the Qualified CA Certificates (QCA) must fulfill the following requirements:

DN field	Name	Description
OI, Organization Identifier	Organization ID	Organization ID different from the Name As defined in ETSI EN 319 412-1 (Eg. VATES +entity’s tax number; NTRES-08005.123456789…)
OU, Organization Unit (Opcional)	Organization Unit	Service Provider dependent Organization Unit, responsible for issuing the certificate.

5.1.2.2 Extensions of Certificates

Extension	Critical	Values
Certificate Policies	-	policyIdentifier: 1.3.6.1.4.1.13177.10.10.1 o AnyPolicy (2.5.29.32.0) (Optional) cPSURI: http://www.firmaprofesional.com/cps userNotice: “Certificado de Autoridad de Certificación Cualificado. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps”
Authority Information Access	-	accessMethod: Id-ad-ocsp accessLocation: <URI to access the OCSP server> accessMethod: Id-ad-calssuers accessLocation: <URI to access the issuer CA’s Certificate>

5.2 Profile of VA Certificates

5.2.1 VA Certificates

5.2.1.1 Distinguished Name (DN)

DN field	Name	Description
CN, Common Name	Name	Service description
O, Organization	Organization	Name of the Organization that provides the secure service
C, Country	Country	C=ES

5.2.1.2 Extensions of Certificates

Extension	Critical	Values
Basic Constraints	Yes	CA:FALSE
Key Usage	Yes	digitalSignature
Extended Key Usage	-	id-kp-OCSPSigning
Subject Key Identifier	-	<ID of the Certificate's Public Key, obtained from its hash>
Authority Key Identifier	-	<ID of the CA Certificate's Public Key, obtained from its hash>
1.3.6.1.5.5.7.48.1.5 id-pkix-ocsp-nocheck	-	oCSPNoCheck

5.3 Profiles of TSA Certificates

5.3.1 TSA Certificates

5.3.1.1 Distinguished Name (DN)

DN field	Name	Description
CN, Common Name	Name	Must contain an identifier of the TSU that has to identify without doubt the exact TSU, including the client's reference.
O, Organization	Organization	• Firmaprofesional S.A. (always in case of qTSA) • Inclusion of subscriber name, (optionally for non-qualified service)
C, Country	Country	C=ES It must specify the Country where the TSA is located (it doesn't necessarily mean where the TSU is physical located)

5.3.1.2 Extensions of Certificates

Extension	Critical	Values
Basic Constraints	Yes	CA:FALSE
Key Usage	Yes	digitalSignature contentCommitment
Extended Key Usage	Yes	id-kp-timeStamping {1.3.6.1.5.5.7.3.8}
Subject Key Identifier	-	<ID of the Certificate's Public Key, obtained from its hash>
Authority Key Identifier	-	<ID of the CA Certificate's Public Key, obtained from its hash>
CRL Distribution Points	-	<URI of the CRL>
Certificate Policies	-	policyIdentifier: 1.3.6.1.4.1.13177.10.1.4.2 <URI of the CPS> userNotice: "Certificado TSA de Servidor Seguro"
Authority Information Access	-	accessMethod: Id-ad-caIssuers accessLocation: <URI to access the issuer CA's Certificate> accessMethod: Id-ad-ocsp accessLocation: <URI to access the OCSP server>

5.3.2 QTSA Certificates (TSA for Qualified Service)

Additionally, the profile of the TSA for Qualified Service, must fulfill the following requirements:

5.3.2.1 Distinguished Name (DN)

DN field	Name	Description
OI, Organization Identifier	Organization ID	"VATES-A62634068"

5.3.2.2 Extensions of Certificates

Extension	Critical	Values
Certificate Policies	-	policyIdentifier: 1.3.6.1.4.1.13177.10.1.4.1 <URI of the CPS> userNotice: "Certificado de Servicio Seguro de TSA cualificada"
id-ce-privateKeyUsagePeriod 2.5.29.16 (Optional)		Its goal is to limit the validity of the private key: 3 years. This extension is omitted when the certificate is issued in elliptic curves.
Authority Information Access		accessMethod: Id-ad-calssuers accessLocation: <URI to access the issuer CA's Certificate> accessMethod: Id-ad-ocsp accessLocation: <URI to access the OCSP server>

The Qualified Timestamp Tokens, should include an instance of the extension qcStatements, according to the syntax defined in IETF RFC 3739 [i.3], clause 3.2.6.

The extension should include an instance of "esi4-qtstStatement-1" as defined in the Annex B of the ETSI TS 319 422.