SSL WEB SERVER CERTIFICATES

Certificate Policy

Version: 180719
Classification: Public

Firmado digitalmente por:
FIRMAPROFESIONAL, S.A.

NOTE: This current original document is available in electronic form on the Firmaprofesional website: https://www.firmaprofesional.com/cps

Version History

Version	Changes	Publication date
6.3	(To check for changes in previous versions, please send an email to info@firmaprofesional.com)	17/10/2008
171121	Change of template and number of versions, followed by the YYMMDD format (year, month and day of publication). Inclusion of this section: Section "1.1 General description": ● The explicit reference to the version of *"Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates"* y *"Guidelines for the issuance and management of Extended Validation certificates"* referring to "In force at the time of publication of this policy"is eliminated Section "2.1 Certification Authorities (CA)": ● It is corrected the point that until the version 6.3 (included) of the present policy the emission could be realized from the subordinate CAs "***AC Firmaprofesional – CA1***" and "***AC Firmaprofesional - INFRAESTRUCTURA***" Section "4.3 Verification of long-term information " The content of the information checks is adapted to the life cycle of the certificates. Section "4.4 Certificates Renewal": ● The renewal process is simplified, matching it to the new issuance. Section "5 CERTIFICATES PROFILE": ● The keyUsage "nonRepudiation", which appeared erroneously is eliminated. ● The keyUsage "keyAgreement", used until version 6.3 (included) of the present policy, is added and removed from the current one. ● It is clarified that the field "organizationalUnit" is optional to version 6.3 (included) of this policy and it will be not present in future Adaptation to eIDAS	21/11/2017
180221	● Review regarding Mozilla Root Store Policy Version 2.5. ● Maximum validity of SSL and EV certificates for 2	21/02/2018

	years.	
180517	• Updated “4.5. Subscriber procedure for problem notification” • Updated “4.1. Certificate issue process”: in “a) Request” and “b) Application acceptance”	17/05/2018
180719	Inclusion of the clientAuthentication EKU in the profile	19/07/2018

Index

1. INTRODUCTION

1.1. General description

SSL Web Server Certificates are certificates issued for organizations which apply them for web servers. The purpose of this certificates is to be able to securely authenticate the server on the network and allow users to create a secure connection using standard cryptographic protocols such as SSL or TLS.

SSL Web Server Certificates are qualified certificates as they fulfill the requirements stipulated in annex IV of EU Regulation 910/2014.

In this document are explained the Particular Conditions related to this type of certificate. This Certification Policy is subject to compliance with the General Conditions set out in the Certification Practices Statement (CPS) of Firmaprofesional

Firmaprofesional issues two types of **SSL Web Server Certificates**:

- **Standard SSL Certificates**:
    - They guarantee that a particular domain has been registered in the name of the organization identified in the certificate and that communication between the client's browser and the page server is confidential due to the use of the SSL protocol.
    - They conform to the requirements of the CA / Browser Forum established in the document **"Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates"** in force at the time of publication of this policy.
- **SSL *Extended Validation Certificates* (EV)**:
    - This certificates are issued to web page servers issued according to a specific set of criteria to verify the identity of the organization identified in the certificate.
    - An SSL EV certificate allows browsers that connect to this service to display an additional level of security.This is indicated in the browser by displaying a green background in the browser's address line.
    - ***o*** They conform to the requirements of the CA / Browser Forum established in the document **"Guidelines for the issuance and management of Extended Validation certificates"** in force at the time of publication of the present policy.

In case of any inconsistency between this document and the requirements published by the CA / Browser Forum, the requirements take precedence over this document.

1.2. Document identification

Name:	CP Web Server
Version:	180719
Description:	Certification Policy for Web Server Certificates (SSL)
Issue date:	17/05/2018
OIDs	1.3.6.1.4.1.13177.10.1.3.1 SSL Standard 1.3.6.1.4.1.13177.10.1.3.10 SSL EV / Qualified

Web address	http://www.firmaprofesional.com/cps

Previously, this Certification Policy was called the:

- Type II.C - **SECURE SERVER CERTIFICATES** (1.3.6.1.4.1.13177.10.1.3.1)

1.3. Definitions and acronyms

See corresponding section in the Certification Practices Statement (CPS) of Firmaprofesional (http://www.firmaprofesional.com/cps).

2. PARTICIPATING ENTITIES

2.1. Certification Authorities (CA)

Heretofore, these certificates have been issued by the Subordinated CAs "**AC Firmaprofesional - CA1"** and **"AC Firmaprofesional - INFRASTRUCTURE"**.

From the date of publication of the present version of this policy, these certificates must be issued only by the Subordinated CA "**AC Firmaprofesional - INFRAESTRUCTURA**".

2.2. Registration Authority (RA)

The management of the requests and the issuance of the certificates will be carried out by Firmaprofesional or by an authorized Intermediary.

The Authorized Intermediaries shall be domain registrars entities accredited by ICANN which the Firmaprofesional has a collaboration agreement.

2.3. Applicant

The person who can request these certificates on behalf of an organization is the person that appears as "Administrative Contact" in the official domain registration.

2.4. Subscriber

The certificate subscriber will be the organization that appears as "Registrant" in the official domain registration.

2.5. Third who trust in the Certificates

These certificates are recognized by Microsoft in all its applications, including Internet Explorer, by the Mozilla Foundation, including the Firefox browser and by Apple, including the Safari browser.

Third parties who trust these certificates should have in mind the limitations in their use.

3. CERTIFICATES CHARACTERISTICS

3.1. Validity period of Certificates

- Standard SSL Certificates: Maximum 2 years
- SSL Extended Validation Certificates: Maximum 2 years

3.2. Extended validation Certificates (EV)

SSL EV Web Server Certificates allow browsers that connect to this service to display an additional level of security than standard SSL Web Server Certificates.

For this purpose the certificates are issued according to a specific, rigorous set of criteria to verify the identity of the organization identified in the certificate. These criteria require a thorough verification of the identity of the requesting organization and the person who makes the request. The electronic signature of the application for an SSL EV Web Server Certificate made with a Corporate Representative Certificate issued by Firmaprofesional covers a large part of these requirements.

3.3. Multidomain Certificates

Multidomain Web Server Certificates allow to validate different URLs of the same domain with the same certificate

This functionality is achieved using "Wildcards" for URLs as defined in the **RFC 2818 "HTTP Over TLS" standard**.

According to this standard, you can use the "asterisk" character as a wildcard within a URL.This way, a certificate with the URL "*.domain.com" can be used for any subdomain, such as "subdomain1.domain.com", "subdomain2.domain.com", "www.domain.com", etc ...

The use of wildcards in SSL Web Server Certificates is supported by the major Internet browsers and is very useful when you have many subdomains of the same Internet domain and you want to use a single certificate for all of them.

SSL EV Web Server Certificates can not be multi-domain.

3.4. Domain names

It is not allowed to issue certificates to IP addresses or internal Domain Names, private or reserved.

The use of internationalized domain names (IDNs) is not allowed under this certificate policy.

This measure prevents homographic spoofing attacks.

3.5. Particular use of Certificates

3.5.1. Appropriate uses of certificates

Web Server Certificates can be used to authenticate the identity of a server, and then establish a secure transmission channel between the server and the service user.

In general, these certificates will be used to authenticate a Web Server using the SSL (or TLS) protocol.

3.5.2. Unauthorized use of certificates

No other use than what is established in this Policy and in the Statement of Certification Practices is allowed

The use of this type of certificate for the electronic signature of documents is not allowed. Firmaprofesional has other certificate policies more appropriate for this purpose.

3.5.3. Notification of unauthorized uses, complaints or suggestions.

In case of detecting an unauthorized use of the certificates or have a complaint or suggestion, they must be sent to Firmaprofesional by e-mail to the address soporte@firmaprofesional.com , indicating in the title whether it is an "Unauthorized Use", a "Complaint" or a "Suggestion" and attaching documents to prove the facts explained.

3.6. Rates

Firmaprofesional can establish the rates that it considers opportune to the subscribers, as well as to establish the ways of payment that considers more appropriate in each case. For more details about the prices and conditions of payment of this type of certificates will be necessary to contact with the Commercial Department of Firmaprofesional.

4. OPERATING PROCEDURES

4.1. Certificate issue process

The steps to follow to obtain the certificate are detailed below:

a) Request

In order to request an SSL Web Server Certificate, the organization must be the owner of the domain.

The steps to apply are the following ones:

1. Make in contact with Firmaprofesional or an Authorized Intermediary
2. Send the information listed below by electronic means that Firmaprofesional offers to the applicants (e-mail or web form) :
    - Personal details of the person who will act as a contact: name and surname, position, telephone, email. The data of the person that appears as "Administrative Contact" or "Technical Contact" in the official domain registration must be the same.
    - Domain name (URL for which you want the certificate be issued)
    - Company name, address and ID number

In EV SSL Server Certificates, the above data must be included in a contract signed electronically by a "Corporate Certificate of Legal Representative person" of the requesting organization issued by Firmaprofesional. A contract signed in a handwritten manner by the person with the legal representative position will also be accepted.

In Standard SSL Server Certificates, a person with a legal representative position or an agent of the organization must sign the contract for the provision of electronic certification services. Acceptance and delivery documents must be signed also. The requesting entity must send a scanned copy of the signed contract to Firmaprofesional with a photocopy of the accreditation document (DNI) of the person appointed as a legal representative position.

In both cases, the signature of these documents will mean the person appointed as the legal representative or attorney of the applicant entity will accept the general contracting conditions of Firmaprofesional, the DPC and the PC of the certificate that is delivered.

b) Application acceptance

Notwithstanding what is established in the corresponding Certification Practice Statement (CPS) of Firmaprofesional and in order to ensure that the requesting organization has the control over the domain (URL) that it requests to include in a certificate, the following checks will be made:

1. The authenticated "whois" services are consulted:
    - For "*.es" domains, the following authenticated WHOIS service will be checked: https://www.nic.es/sgnd/domain/publicInformationDominios.action

- For the rest of the domains ending in: com, org, net...or the high level domain (TLD) you can consult which is the authorized WHOIS server information at: http://www.iana.org/domains/root/db/

2. The applicant's data will be verify as "Administrative Contact" or the "Technical Contact" of the domain.

3. Company's data will be validated through one of the following mechanisms:

   - In case of a company with a contractual relationship with Firmaprofesional prior to the application, then the contract previously signed by the two parties is enough.

   - If the company is not a client of Firmaprofesional, a consultation will be carried out to the Business Registry. As an alternative, the company can send the certificate of the Business Registry or Official Certificate where it is registered to Firmaprofesional.

4. The contract can be signed by SMS; for this purpose the mobile number of the legal representative will be requested and the contract will be sent to this telephone number. The contract can also be signed with a digital certificate. If neither of the two previous options is possible, as a last option, the scanned contract with the handwritten signature can be sent.

5. The control of the domain will be confirmed with the applicant by sending a random code via email. The applicant must reply from that email address with the code sent.

   The recipient's email address will be extracted from the domain contact of the registry. It is also possible to send an email to more than one recipient as long as they are identified as representatives of the domain name in the registry.

   If the domain registry is not visible or the data does not match the applicanty company, an email will be sent requesting visibility to the registry.

   Valid email addresses are "admin", "administrator", "webmaster", "hostmaster" or "postmaster" followed by @ and the name of the authorizing domain.

   The random code must be unique, so it is proposed that the operator uses a unique random number generator.

6. RA operator shall store documentary evidence of the validations done. For example by scanning the paper documentation consulted, printing the screen of the electronic records consulted or recording the date, time and interlocutor of the telephone calls carried out.

c) Generation of keys

The signature keys will be generated in the applicant's systems using their own applications compatible with the PKI standards. As usual, Server applications that can be configured with the SSL protocol, such as Microsoft IIS, include tools for generating keys and certificate requests.

The keys must be RSA keys with 2,048 bits as a minimum length.

d) Processing

The applicant will deliver a certificate request in PKCS # 10 format to Firmaprofesional directly or through an authorized Intermediary.

Firmaprofesional will carry out the technical validation of the request in PKCS # 10 and the data in the request will be verified also.

e) Certificate issuance

If the application is electronically signed by a Corporate Certificate of Legal Representative person of Firmaprofesional, it will issue an SSL EV Web Server Certificate; Otherwise, a standard SSL Web Server Certificate will be issued.

On the other hand, EV SSL Web Server Certificate requires the approval of two persons to be issued: the RA Operator responsible of managing the application and the Administrator of the Technical Department responsible of issuing the certificate.

f) Delivery

Firmaprofesional will deliver the certificate to the applicant downloaded by Internet with all the security measures guaranteed.

4.2. Certificates revocation

According to the Certification Practice Statement (CPS)

4.3. Verification of long-term information

The information contained in SSL certificates will be verified at each Certificate issue and renewal.

4.4. Certificate Renewal

The same process as for issuing a new certificate must be followed (4.1 Certificate issuing process)

4.5. Subscriber procedure for problem notification

If the subscriber of Web authentication certificates detects any problem with the certificate, then the subscriber can notify the issue to the following mail address: soporte@firmaprofesional.com

Any email sent to this address is entered into the Customer Service System of Firmaprofesional.

5.CERTIFICATES PROFILE

5.1. Distinguished Name (DN)

Field	Value	Description
CN, Common Name		*(EVG 9.2.3) Name of a single domain.* *(BR 7.1.4.2.2.a) This domain must be the same that has been indicated (or one of the indicated ones) in the Subject Alt Names.*
O, Organization		*Official Name of the Organization that subscribes the certificate*
OU, Organizational Unit		*Optional in this policy to version 6.3 (included) . It is not present hereafter.* *(BR 7.1.4.2.2.i) Optional*
serialNumber		*Tax Identity Number (TIN, in Spanish CIF) of the Subscriber Organization of the certificate*
Organization Identifier		According to the technical standard ETSI EN 319 412-1 (VATES + NIF of the entity)
businessCategory	*Private Organization* *Government Entity* *Business Entity* *Non-Commercial Entity*	(EVG 9.2.4) Business Category
L, Locality		Address of Place of Business: City
ST, StateOfProvince		province of the registered organization
C, Country		Two digit country code according to ISO 3166-1. By default "ES".
Jurisdiction Country Name 1.3.6.1.4.1.311.60.2.1.3		(EVG 9.2.5) Subject Jurisdiction of Incorporation or Registration

Fields (EVG 9.2.X) are specific requirements for Extended Validation certificates as established by the 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, in force at the time of publication of this policy.

5.2. Certificate extensions

Extensión	Crítica	Valores
X509v3 Issuer Alternative Name	-	*URI:http://www.firmaprofesional.com*

X509v3 Subject Alternative Name	-	*URL, domain name or identification of the device or owner's the keys service or the application.* *(EVG 9.2.2) You can include more than 1 domain, but not wildcards.* *For multidomain certificates, the URL will follow the format "* .domain.com" or the IP (this indication is forbidden for EV certificates)*
X509v3 Basic Constraints	*Sí*	*CA:FALSE*
X509v3 Key Usage	*Sí*	*Digital Signature* *Key Encipherment* *Data Encipherment*
X509v3 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)*
X509v3 Subject Key Identifier	-	*<Public key of the certificate, obtained from the hash of the certificate>*
X509v3 Authority Key Identifier	-	*<Public key of the CA certificate, obtained from the hash of the certificate>*
X509v3 Authority Information Access	-	*Access Method 1: Id-ad-ocsp (1.3.6.1.5.5.7.48.1)* *Access Location 1: http://ocsp.firmaprofesional.com* *Access Method 2: id-ad-caissuers (1.3.6.1.5.5.7.48.2)* *Access Location 2: http://crl.firmaprofesional.com/infraestructura.crt*
X509v3 CRL Distribution Points	-	*http://crl.firmaprofesional.com/infraestructura.crl*
X509v3 Certificate Policies	-	*<OID of the certificate policy corresponding to the certificate>* 1.3.6.1.4.1.13177.10.1.3.1 SSL Standard 1.3.6.1.4.1.13177.10.1.3.10 SSL EV / Qualified *<CPS URI>* *User Notice: "Este es un Certificado de Servidor Web cualificado con Validación Extendida" (for EV certificates)* *User Notice: "Este es un Certificado de Servidor Web" (for certificates without EV)* *<OID "EU qualified website authentication certificates" según ETSI EN 319 411-2: QCP-w: 0.4.0.194112.1.4 > (for EV certificates)* *<EVID of EV certificate policy corresponding to certificate: 0.4.0.2042.1.4> (for EV certificates)*
Qualified Certificate Statements (only for EV)	-	*Id-etsi-qcs-QcCompliance:* 0.4.0.1862.1.1 *indicating the qualified certificate* *Id-etsi-qcs-QcRetentionPeriod:* 0.4.0.1862.1.3 *(for 15 years)* *Id-etsi-qcs-QcPDS*[1]*:* 0.4.0.1862.1.5 *(URI: https://www.firmaprofesional.com/cps/pds_en.pdf)* *Id-etsi-qcs-QcType:* 0.4.0.1862.1.6.3 *(**qct-web**, (Indicates that the certificate is useful to create electronic signatures).*

[1] Mandatory in English language. Other QcPDS may be included in other languages.