



Certificate Policy (CP)
SSL Secure Web Server Certificates

Version 6.1

Date 20/07/2012


CERTIFICATE POLICY

SSL SECURE WEB SERVER CERTIFICATES

6.1 VERSION

INDEX

1. INTRODUCTION.....	3
1.1 General description.....	3
1.2 Identification of the document.....	4
2. PARTICIPANT ENTITIES.....	5
2.1 Certification Authorities.....	5
2.2 RA	5
2.3 Applicant.....	5
2.4 Subscriber	5
2.5 Third party who relies on the certificates	5
3. CARACTERISTIQUES OF THE CERTIFICATES.....	6
3.1 Certificate's validity period.....	6
3.2 Extended validation certificates (EV).....	6
3.3 Multi Domain certificates.....	6
3.4 Particular use of the Certificates.....	7
3.5 Rates.....	7
4. OPERATIVE PROCEDURES.....	8
4.1 Certificates issuance's process.....	8
4.2 Revocation of the certificates.....	10
4.3 Renovation of the certificates.....	10
5. PROFILE OF THE CERTIFICATES.....	11
5.1 DN.....	11
5.2 Extensions of the certificates.....	11

	Certificate Policy (CP) Certificates of SSL Web Server	
	Version	6.1
	Date	20/07/2012

1 INTRODUCTION

1.1 GENERAL DESCRIPTION

The SSL Secure Web Server certificates are certificates issued to organizations for web servers. The aim of the certificate is to authenticate the server securely in the Internet as well as allow the users to create a secure connection through standard cryptographic protocols as SSL or TLS.

In this document are showed the Particular Conditions refer to this kind of certificate. This certificate policy is subordinated to the fulfilment of the General Conditions exposed in the Certification Practices Statement (CPS) of Firmaprofesional.

Firmaprofesional issues two kinds of SSL Web Server Certificates:


- **Standard SSL Certificate:** They are certificates issued to web servers. The main functions of these certificates are:
 - To certify that a particular domain has been registered in the name of the organization identified in the certificate.
 - To guarantee that the communication between the clients's Browser and the Server Pages is confidential. This is because of the SSL protocol's use.
- **Extended Validation SSL certificates (EV):** They are certificates issued to web servers .These certificates are issued according to a specific set of verification criteria of the organization identity which is identified in the certificate.

An EV SSL certificate allows browsers to be connected to this service showing an additional security level.

The standard SSL certificates issued by Firmaprofesional comply with the [Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.0](#) of the [CA/Browser Forum](#), in effect at the time of publication of this policy.

The EV SSL certificates issued by Firmaprofesional comply with the [Guidelines For The Issuance And Management Of Extended Validation Certificates, Version 1.3](#) of the same entity, in effect at the time of publication of this policy.

The Requirements will have priority over this document in case of any incompatibility between this document and the published Requirements by the CA/Browser Forum.


	Certificate Policy (CP) Certificates of SSL Web Server	
	Version	6.1
	Date	20/07/2012

1.2 IDENTIFICATION OF THE DOCUMENT

Name:	CP SSL Secure Web Server
Version:	6.1
Description:	Certificate Policy for SSL Secure Web Server Certificates
Date of issuance:	20/07/2012
OIDs	1.3.6.1.4.1.13177.10.1.3.1 Standard SSL 1.3.6.1.4.1.13177.10.1.3.10 EV SSL
Location	http://www.firmaprofesional.com/cps

Previously, this Certificate Policy was called:

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

	Certificate Policy (CP) Certificates of SSL Web Server	
	Version	6.1
	Date	20/07/2012

2 PARTICIPANT ENTITIES

2.1 CERTIFICATION AUTHORITIES (CA)

These certificates must be issued by the subordinated CA “**AC Firmaprofesional**”.

2.2 REGISTRATION AUTHORITIES (RA)

The Management of applications and issuances of the certificates will be carried out by Firmaprofesional or by an authorized intermediary.

The authorized intermediaries will be register domain’s entities accredited by ICANN which has a collaboration agreement with Firmaprofesional.

2.3 APPLICANT

The person appearing as “Administrative Contact” will be able to do the application of these certificates on behalf of an organization in the official record of the domain.


2.4 SUBSCRIBER

The subscriber of the certificate will be the organization that appears as “Registrant” in the official record of the domain.

2.5 THIRD PARTY WHO RELIES ON THE CERTIFICATES

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

The third parties that rely on these certificates have to be aware of the limitations in its use.

	Certificate Policy (CP) Certificates of SSL Web Server	
	Version	6.1
	Date	20/07/2012

3 CERTIFICATE'S FEATURES

3.1 CERTIFICATE VALIDITY PERIOD

- Standard SSL Certificates: Between 1 and 5 years.
- Extended Validation SSL Certificates: 27 months.

3.2 EXTENDED VALIDATION CERTIFICATES (EV)

EV SSL Secure Web Server certificates enable browsers that connect to the service to show a higher level of security with respect the Standard SSL Secure Web Server Certificates.

Because of that, the certificates are issued according to a specific set of rigorous criteria for verifying the identity of the organization identified in the certificate rigorous. These criteria require an exhaustive verification of the applicant's organisation identity as well as the person making effective the application. By signing electronically the application with a Corporate Legal Representative Certificate issued by Firmaprofesional, most of these requirements are covered.

3.3 MULTI DOMAIN CERTIFICATES

The Multi Domain Server's Certificate allows to validate different URLs in the same domain with the same certificate.

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

According to this standard the "asterisk" character can be used as a wild card within a URL. Thus, a certificate with a "*.domain.com" URL will be able to be used for any subdomain as "subdomain1.domain.com", "subdomain2.domain.com", "www.domain.com", etc...


The use of "wildcards" in SSL Web Server Certificates is supported by the main Internet Browsers. It is very useful when there are many domains of the same internet's domain and you want to use a single certificate for all.

The EV SSL Secure Web Server Certificates cannot be multi domain according to the requirements established in the [Guidelines For The Issuance And Management Of Extended Validation Certificates, Version 1.3](#)

3.4 PARTICULAR USE OF THE CERTIFICATES

3.4.1 Appropriate uses of the certificates

The Secure Web Server Certificates can be used to authenticate a server's identity as well as to establish a secure transmission channel between the server and the service's user. In general, these certificates are used to authenticate a Web Server through the SSL protocol (or TLS).


	Certificate Policy (CP) Certificates of SSL Web Server	
	Version	6.1
	Date	20/07/2012

3.4.2 Non- authorized uses of certificates

It is not allowed a different use from what is established in this Policy and in the Certification Practices Statement. It is not allowed the use of this kind of certificate for the electronic signature of documents. Firmaprofesional has other appropriate certificate policies for that purpose.

3.5 RATES

Firmaprofesional will be able to establish the rates that are considered appropriate to the subscribers. Also it will be able to establish the means of payment that are considered appropriate in each case. For more details on the price and terms of payment of such certificates will be necessary to consult the Sales Department of Firmaprofesional.

	Certificate Policy (CP) Certificates of SSL Web Server	
	Version	6.1
	Date	20/07/2012

4 OPERATIVE PROCEDURES

4.1 CERTIFICATE ISSUANCE PROCESS

The steps to obtain a certificate are detailed below:

a) Application

The organization must be the holder of the domain in order to apply for a SSL Secure Web Server Certificate.

The steps to make the request are:


1. To contact with Firmaprofesional or with an authorized intermediary.
2. To send, as minimum, the following information through the electronic means (for example email or web form) that Firmaprofesional will place to the applicants disposal:
 - Contact person details: name and surname, position and e-mail. These have to be the same contact details that appear in the domain register as “Administrative Contact”.
 - Name of the domain (URL for which the organization wants to issue the certificate).
 - Trade name and tax code of the organization.

If one wants an EV SSL Secure Web Server Certificate, the previous details should be included in an electronic signed document by a Corporate Legal Representative Certificate of the requesting organization and issued by Firmaprofesional.

b) Acceptance of the application

Following verifications must be done in order to guarantee that the requesting organization has control over the domain (URL) that is requested to be included in a certificate. This is carried out without detriment to what is established in the corresponding Certification Practice Statement (CPS) of Firmaprofesional:

1. The following authenticated *whois* services are consulted:
 - For “*.es” domains, consult the following authenticated WHOIS service: <https://www.nic.es/sgnd/dominio/publicInformacionDominios.action>
 - For the rest of the domains consult on <http://www.iana.org/domains/root/db/> which is the authenticated WHOIS server to look for information about the domain, depending on the Top Level Domain (TLD), or said in another way, depending on whether the domain ends in .com, .org, .net, ...
2. The details of the applicant will be validated as “Administrative Contact” of the domain.

	Certificate Policy (CP) Certificates of SSL Web Server	
	Version	6.1
	Date	20/07/2012

3. The application, electronically signed by the legal representative, will be validated. If this is not possible the organization details will be validated through some of the following mechanisms:

- a. Contractual agreement between the organization and Firmaprofesional, previous to the application.
- b. Consult the Commercial Regsiter.
- c. Manual verification of the organization's details through telephone call.

c) Keypair generation

Signature keys are generated in the applicant's systems using itsown compatible applications with the PKI standards. Generally, web server applications that can be set up with the SSL protocol include tools to generate keys and requests of the certificates.

They must be RSA keys with a minimum length of 2.048 bits.

d) Processing

Applicants shall deliver to Firmaprofesional, directly or through an authorized intermediary, a certificate request in PKCS#10.

Firmaprofesional will perform technical validation of the PKCS#10 requests and the validation of the details that it contains in.


e) Certificate's issuance

Firmaprofesional will issue an EV SSL Web Server Certificate if the application is electronically signed with a Corporate Legal Representative Certificate of Firmaprofesional; in other case it will be issued a standard SSL Web Server Certificate.

Additionally, the EV SSL Web Server Certificate's issuance requires the approval of two people: the RA Operator responsible for managing the request and the Technical Department Manager responsible for issuing the certificate.

f) Delivery

Firmaprofesional will deliver the certificate to the applicant allowing a secure downloading from internet.

	Certificate Policy (CP) Certificates of SSL Web Server	
	Version	6.1
	Date	20/07/2012

4.2 REVOCATION OF THE CERTIFICATES

The subscriber must request for the revocation of his/her certificate in case of lost, compromise of the keypair or other described causes in the CPS.

To request the revocation of the certificate, the subscriber can:

- In office hours:
 - Contact by telephone call or personally with his/her RA.
- Out of office hours:
 - Revoke online his/her certificate in the web page of Firmaprofesional.
 - Call to the revocation service 24X7: 902. 361. 639


For any further information regarding the revocation of certificates, refer to the corresponding section of the CPS.

4.3 RENEWAL OF CERTIFICATES

The request of the SSL Secure Web Server Certificate's renewal can be carried out through the electronic means that Firmaprofesional offer to the applicants (for example e-mail or web form).

If the certificate for which renewal is requested is current or has expired less than thirty (30) calendar days and is not revoked, Firmaprofesional will verify that the applicant is the domain "Administrative Contact" and the renewal process will continue in step c) of section 4.1 Certificate issuance Process.

Otherwise, the renewal will need of all checks from step b) of Section 4.1 Certificate issuance Process.

	Certificate Policy (CP) Certificates of SSL Web Server	
	Version	6.1
	Date	20/07/2012

5 PROFILE OF THE CERTIFICATES

5.1 DISTINGUISHED NAME (DN)

Field	Value	Description
CN, Common Name	Name	<i>Name of the domain</i>
O, Organization	Registered Name	<i>Name of the certificate's subscriber Organization</i>
SN, SerialNumber (opcional)	Organization tax code	<i>Organization tax code of the certificate's subscriber Organization</i>
C, Country	Country	<i>Code of the country with two digits according ISO 3166-1. By default "ES".</i>

5.2 CERTIFICATE EXTENSIONS

Extension	Review	Values
X509v3 Issuer Alternative Name	-	URI:http://www.firmaprofesional.com
X509v3 Subject Alternative Name	-	URL, name of the domain or: - Identification of the device. - Identification of the key or application's holder. For multi domain certificates, the URL will keep the "dominio.com" format or the IP.
X509v3 Basic Constraints	YES	CA: FALSE
X509v3 Key Usage	YES	Digital Signature Non Repudiation Key Encipherment
X509v3 Extended Key Usage	-	Server Authentication (1.3.6.1.5.5.7.3.1)
X509v3 Subject Key Identifier	-	<id of the certificate's public key of the CA, obtained from its hash>
X509v3 Authority Key Identifier	-	<id of the certificate's public key of the CA, obtained from its hash>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI of access to the OCSP service>
X509v3 CRL Distribution Points	-	<URI of the CRL>
X509v3 Certificate Policies	-	<OID of the certification policy corresponding to the certificate> <URI of the CPS> User Notice: This is a Web Server Certificate.