REQUERIMIENTOS DE LOS CERTIFICADOS DE SERVIDOR DE TERCEROS EMPLEADOS EN LAS CONEXIONES SEGURAS CON REDSYS

Versión: 1.2

25/03/2013

Referencia RS.RI.SEG.MAN.0004

Redsys · C/ Francisco Sancha, 12 · 28034 · Madrid · ESPAÑA

Autorizaciones y control de versión

AUTOR: Gerencia de Seguridad	VALIDADO POR: Gerencia de Seguridad	APROBADO POR: Gerencia de Seguridad
EMPRESA: Redsys	EMPRESA: Redsys	EMPRESA: Redsys
Firma:	Firma:	Firma:
Fecha: 25/03/2013	Fecha: 25/03/2013	Fecha: 25/03/2013
Comentarios: La gestión de la documentación impresa es responsabilidad de la persona que la imprime. Las versiones impresas de los documentos no garantizan ser la última versión aprobada. Para consultar la última versión acceder a la base de datos de Alejandría.		

Versión	Fecha	Afecta	Breve descripción del cambio
1.0	11/10/2011	Todo	Sustituye al documento PR.CR.150 v1.9 de REDSYS.
1.1	24/05/2012	Anexo A	Incorporación de la CA Raíz R27 y de las CA Intermedias I37, I38 e I39.
1.2	25/03/2013	Anexo A	Incorporación de la CA Raíz R28, R29, R30, R31, R32, R33 y de las CA Intermedias I40, I41, I42, I43, I44, I45, I46, I47, I48, I49 e I50. Baja por caducidad de las CA Intermedias I2 e I11.

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

1.1 Objetivo

Comunicar los requerimientos de los certificados de servidor utilizados por los comercios en su conexión segura (SSL) con REDSYS.

1.2 Estructura

En el capítulo introductorio se da una visión funcional (no técnica) del protocolo SSL y del papel que desempeñan los certificados digitales en este contexto.

A continuación se presentan los requerimientos propiamente dichos.

Finalmente, se recoge en anexos un conjunto de tablas con las CA que REDSYS acepta en sus aplicaciones.

1.3 Audiencia

Este documento está orientado a aquellos comercios que interactúan con las aplicaciones de REDSYS y que requieren una comunicación segura a través de SSL.

2. CONCEPTOS PREVIOS

2.1 Terminología

Criptografía asimétrica: método criptográfico que usa un par de claves para el envío de mensajes. Una clave es *pública* y se puede entregar a cualquier persona. La otra clave es *privada* y el propietario debe guardarla de modo que nadie tenga acceso a ella. La operación que se hace con la una se deshace con la otra.

Si se desea dotar de *confidencialidad* a una información, el remitente utilizará la clave pública del destinatario para cifrarla y, una vez cifrada, sólo la clave privada del destinatario podrá descifrarla.

Si lo que se desea es lograr es la *integridad* de los datos y la *identidad* del remitente, entonces el remitente utilizará su clave privada para *firmar* la información. Cualquiera que disponga de la clave pública del remitente podrá verificar la firma del remitente.

Certificado digital: es un documento digital mediante el cual un tercero confiable (Autoridad de Certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

Autoridad de Certificación (CA): entidad de confianza que da validez a los certificados digitales mediante la firma digital de éstos con su clave privada. La confianza de los usuarios en ella es fundamental para el buen funcionamiento del servicio. También se encarga de firmar y revocar los certificados digitales.

SSL / TLS: Secure Socket Layer / Transport Layer Security. Protocolo de comunicaciones seguras desarrollado por Netscape para permitir confidencialidad y autenticación en Internet.

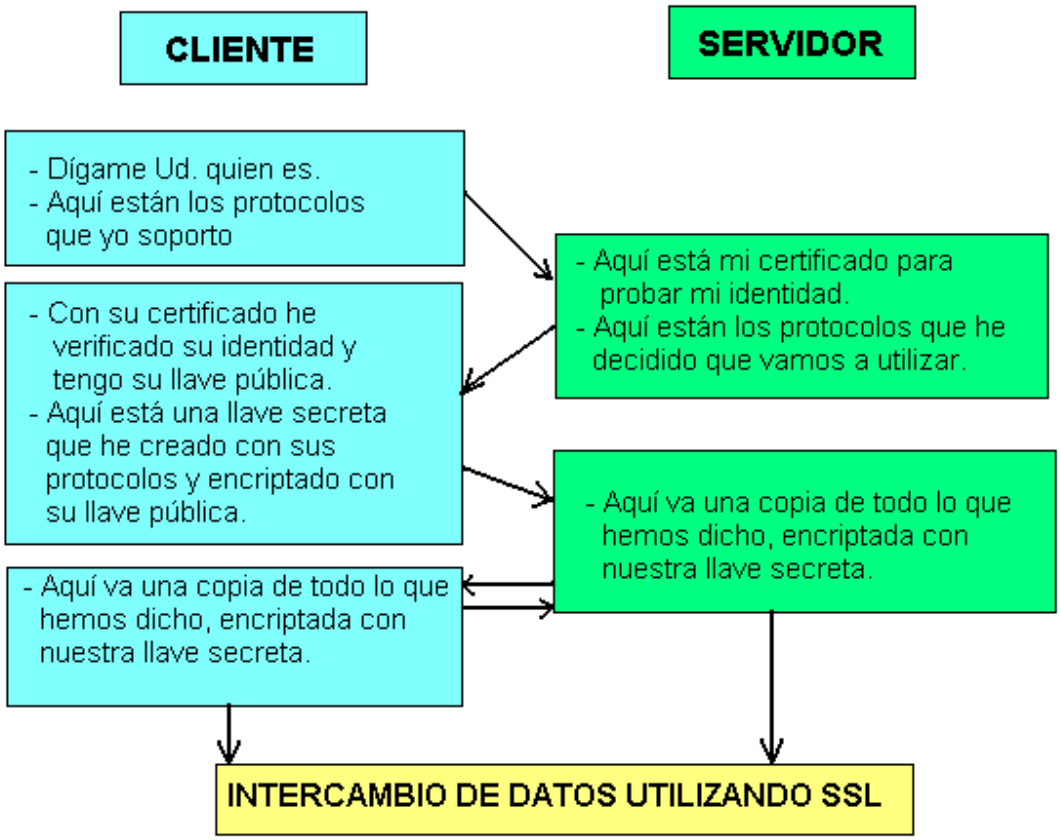
2.2 Necesidad

Debido al auge que en los últimos tiempos ha tenido el comercio electrónico, tanto los comercios como los proveedores de servicio se han visto obligados a garantizar la seguridad de las transacciones por Internet mediante mecanismos robustos que aporten autenticación de (al menos) uno de los extremos (el servidor), y la confidencialidad e integridad de los datos intercambiados.

En este contexto es donde aparecen los protocolos SSL y TLS.

2.3 Cómo funciona SSL / TLS

El gráfico siguiente muestra el proceso del establecimiento de una comunicación segura mediante SSL / TLS:



En resumen, el cliente solicita una comunicación segura al servidor, los extremos intercambian credenciales (certificados digitales) y se ponen de acuerdo sobre los algoritmos de cifrado y la clave que utilizarán para proteger la información intercambiada.

El proceso de autentificación en el protocolo SSL se realiza mediante **Certificados Digitales.**

Un **certificado digital** es un archivo binario que contiene, entre otros, los datos del extremo al que autentica (por ejemplo: el DNS del servidor web), su clave pública, el período de validez del certificado y la firma digital de una entidad de confianza (CA) que legitima ante terceras partes la relación entre los datos de identidad que aparecen en el certificado y la clave pública del mismo.

3. REQUERIMIENTOS

- El certificado de servidor SSL del comercio debe estar emitido por una CA pública reconocida. No se aceptan certificados autofirmados ni emitidos por CAs propietarias.
- REDSYS ha probado el correcto funcionamiento de los certificados de CA que aparecen listadas en el ANEXO A: ENTIDADES DE CERTIFICACIÓN RECONOCIDAS POR REDSYS.
- Dichos certificados de CA se encuentran cargados en los contenedores de certificados de confianza de las aplicaciones de REDSYS.
- En caso de que el comercio quiera hacer uso de un certificado emitido por una CA pública reconocida que no se encuentre en el anexo, deberá ponerse en contacto con su entidad financiera para que sea comprobada su validez e interoperabilidad del mismo con las diferentes aplicaciones.
  - En caso de que la CA sea aceptada, se cargará en las aplicaciones y se incluirá en las tablas correspondientes de este documento. Igualmente se informará al comercio de que puede utilizar certificados de servidor emitidos por dicha Autoridad de Certificación.
  - En caso de que no sea aceptada se informará al comercio para que obtenga uno emitido por la lista de CAs reconocidas por REDSYS.

El tiempo medio necesario para analizar la validez o no de una CA por solicitud de un comercio será de 2 semanas.

4. ANEXO A: ENTIDADES DE CERTIFICACIÓN RECONOCIDAS POR REDSYS

A continuación se muestra el listado de certificados de CA Raíz y CA Intermedia cargados en los contenedores de certificados de REDSYS. Es importante que el comercio al que se conectará de forma segura (SSL) REDSYS, verifique que su jerarquía de CAs está incluida en las tablas siguientes.

CAs Raíz:

ID.	EMPRESA	CAMPO 'ASUNTO'	Nº SERIE	FECHA CAD.
R1	ACE / VeriSign	OU = Class 3 Public Primary Certification Authority O = VeriSign, Inc. C = US	3C 91 31 CB 1F F6 D0 1B 0E 9A B8 D0 44 BF 12 BE	02/08/2028
R2	CyberTrust	CN = GTE CyberTrust Global Root OU = GTE CyberTrust Solutions, Inc. O = GTE Corporation C = US	01A5	14/08/2018
R3	Usertrust	CN = UTN-USERFirst-Hardware OU = http://www.usertrust.com O = The USERTRUST Network L = Salt Lake City S = UT C = US	44BE 0C8B 5000 24B4 11D3 362A FE65 0AFD	09/07/2019
R4	Equifax	CN = Equifax Secure Global eBusiness CA-1 O = Equifax Secure Inc. C = US	01	21/06/2020

R5	Valicert	E = info@valicert.com CN = http://www.valicert.com/ OU = ValiCert Class 2 Policy Validation Authority O = ValiCert, Inc. L = ValiCert Validation Network	01	26/06/2019
R6	Thawte	E = premium-server@thawte.com CN = Thawte Premium Server CA OU = Certification Services Division O = Thawte Consulting cc L = Cape Town S = Western Cape C = ZA	01	01/01/2021
R7	Thawte	E = server-certs@thawte.com CN = Thawte Server CA OU = Certification Services Division O = Thawte Consulting cc L = Cape Town S = Western Cape C = ZA	01	01/01/2021
~~R8~~ (CADUCADO)	~~VeriSign~~	~~OU = Secure Server Certification Authority~~ ~~O = RSA Data Security, Inc.~~ ~~C = US~~	~~02AD 667E 4E45 FE5E 576F 3C98 195E DDC0~~	~~08/01/2010~~
~~R9~~ (CADUCADO)	~~IPSCA~~	~~E = ips@mail.ips.es~~ ~~CN = IPS SERVIDORES~~ ~~OU = Certificaciones~~ ~~O = IPS Seguridad CA~~ ~~L = BARCELONA~~ ~~S = BARCELONA~~ ~~C = ES~~	~~00~~	~~30/12/2009~~
R10	Agencia Catalana de	CN = EC-ACC OU = Jerarquia Entitats de Certificacio	EE2B 3DEB D421 DE14 A862 AC04 F3DD	08/01/2031

	Certificación	Catalanes OU = Vegeu https://www.catcert.net/verarrel (c)03 OU = Serveis Publics de Certificacio O = Agencia Catalana de Certificacio (NIF Q-0801176-I) C = ES	C401	
R11	FNMT	OU = FNMT Clase 2 CA O = FNMT C = ES	36F1 1B19	18/03/2019
R12	Equifax	OU=Equifax Secure Certificate Authority O=Equifax C=US	35DE F4CF	22/08/2018
R13	AddTrust AB	CN = AddTrust External CA Root OU = AddTrust External TTP Network O = AddTrust AB C = SE	01	30/05/2020
R14	Starfield	OU = Starfield Class 2 Certification Authority O = Starfield Technologies, Inc. C = US	00	29/06/2034
R15	Entrust	CN = Entrust.net Secure Server Certification Authority OU = (c) 1999 Entrust.net Limited OU = www.entrust.net/CPS incorp. by ref. (limits liab.) O = Entrust.net C = US	37 4A D2 43	25/05/2019
R16	SwissSign	CN = SwissSign Gold CA - G2 O = SwissSign AG C = CH	00 BB 40 1C 43 F5 5E 4F B0	25/10/2036
R17	DigiCert	CN = DigiCert High Assurance EV Root CA OU = www.digicert.com O = DigiCert Inc	02 AC 5C 26 6A 0B 40 9B 8F 0B 79 F2 AE 46 25 77	10/11/2031

		C = US		
R18	VeriSign	OU = VeriSign Trust Network OU = (c) 1998 VeriSign, Inc. - For authorized use only OU = Class 3 Public Primary Certification Authority - G2 O = VeriSign, Inc. C = US	7D D9 FE 07 CF A8 1E B7 10 79 67 FB A7 89 34 C6	02/08/2028
R19	VeriSign	CN = VeriSign Class 3 Public Primary Certification Authority - G5 OU = (c) 2006 VeriSign, Inc. - For authorized use only OU = VeriSign Trust Network O = VeriSign, Inc. C = US	18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A	17/07/2036
R20	IPSCA	E = global01@ipsca.com CN = ipsCA Global CA Root OU = ipsCA O = IPS Certification Authority s.l. ipsCA L = Madrid S = Madrid C = ES	00	25/12/2029
R21	IPSCA	E = main01@ipsca.com CN = ipsCA Main CA Root OU = ipsCA O = IPS Certification Authority s.l. ipsCA L = Madrid S = Madrid C = ES	00	25/12/2029
R22	RSA	OU = RSA Security 2048 V3 O = RSA Security Inc	0A 01 01 01 00 00 02 7C 00 00 00 0A 00 00 00 02	22/02/2026
R23	Go Daddy	OU = Go Daddy Class 2 Certification Authority O = The Go Daddy Group, Inc. C = US	00	29/06/2034

R24	Camerfirma	CN = Chambers of Commerce Root OU = http://www.chambersign.org O = AC Camerfirma SA CIF A82743287 C = EU	00	30/09/2037
R25	Thawte	CN = thawte Primary Root CA OU = (c) 2006 thawte, Inc. - For authorized use only OU = Certification Services Division O = thawte, Inc. C = US	34 4E D5 57 20 D5 ED EC 49 F4 2F CE 37 DB 2B 6D	17/07/2036
R26	GeoTrust	CN = GeoTrust Global CA O = GeoTrust Inc. C = US	02 34 56	21/05/2022
R27	GlobalSign	CN = GlobalSign Root CA OU = Root CA O = GlobalSign nv-sa C = BE	04 00 00 00 00 01 15 4B 5A C3 94	28/01/2028
R28	FNMT	OU = AC RAIZ FNMT-RCM O = FNMT-RCM C = ES	00 81 BB DD 6B 24 1F DA B4 BE 8F 1B DA 08 55 C4	01/01/2030
R29	Firma Profesional	CN = Autoridad de Certificacion Firmaprofesional CIF A62634068 C = ES	53 EC 3B EE FB B2 48 5F	31/12/2030
R30	Baltimore/CyberTrust	CN = Baltimore CyberTrust Root OU = CyberTrust O = Baltimore C = IE	02 00 00 B9	13/05/2025
R31	Entrust	CN = Entrust.net Certification Authority (2048) OU = (c) 1999 Entrust.net Limited OU = www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O = Entrust.net	38 63 DE F8	24/09/2029
R32	Secure Trust	CN = SecureTrust CA O = SecureTrust Corporation C = US	0C F0 8E 5C 08 16 A5 AD 42 7F F0 EB 27 18 59 D0	31/12/2029

R33	StarCom	CN = StartCom Certification Authority OU = Secure Digital Certificate Signing O = StartCom Ltd. C = IL	01	17/09/2036

CAs Intermedias:

ID	EMPRESA	CAMPO 'ASUNTO'	CAMPO 'EMISOR' [1]	Nº SERIE	FECHA CAD.
~~I1~~ (CADUCADO)	~~ACE / Verisign~~	~~OU = www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign~~ ~~OU = VeriSign International Server CA - Class 3~~ ~~OU = VeriSign, Inc.~~ ~~O = VeriSign Trust Network~~	~~R1~~	~~254B 8A85 3842 CCE3 58F8 C5DD AE22 6EA4~~ ~~78EE 48DE 185B 2071 C9C9 C3B5 1D7B DDC1~~	~~25/10/2011~~
~~I2~~ (CADUCADO)	~~Comodo~~	~~CN = Comodo Class 3 Security Services CA~~ ~~OU = (c)2002 Comodo Limited~~ ~~OU = Terms and Conditions of use: http://www.comodo.net/repository~~ ~~OU = Comodo Trust Network~~ ~~O = Comodo Limited~~ ~~C = GB~~	~~R2~~	~~0200 029A~~	~~28/08/2012~~
I3	Digi-sign	CN = Digi-Sign CA Digi-SSL Xp OU = Terms and Conditions of use: http://www.digi-sign.com/repository O = Digi-Sign Limited L = Dublin S = Dublin C = IE	R3	0B41 F1C4 7162 6DD1 D355 42AF C562 BBCB	09/06/2019

[1] Referencia al campo 'Asunto' de la tabla de CAs Raíz

I4	Starfield Technologies	E = practices@starfieldtech.com CN = Starfield Secure Certification Authority OU = http://www.starfieldtech.com/repository O = Starfield Technologies, Inc. L = Scottsdale S = Arizona C = US	R5	0104	09/06/2024
I5	Thawte	CN = Thawte SSL Domain CA O = Thawte Consulting (Pty) Ltd. C = ZA	R7	3000 0001	04/05/2014
I6	ACE / Verisign	CN = VeriSign Class 3 Secure Server CA OU = Terms of use at https://www.verisign.com/rpa (c)05 OU = VeriSign Trust Network O = VeriSign, Inc. C = US	R1	7533 7D9A B0E1 233B AE2D 7DE4 4691 62D4	19/01/2015
~~I7~~ (CADUCADO)	~~IPSCA~~	~~E = ips@mail.ips.es~~ ~~CN = CLASE B 3 ipsCA IPS Seguridad 2005~~ ~~OU = Certificaciones~~ ~~O = IPS Seguridad CA~~ ~~L = Barcelona~~ ~~S = Barcelona~~ ~~C = ES~~	~~R9~~	~~0090 33~~	~~31/12/2009~~
I8	Agencia Catalana de Certificación	CN = EC-AL OU = Administracions Locals de Catalunya OU = Vegeu https://www.catcert.net/verCIC-2 (c)03 OU = Serveis Publics de Certificacio ECV-2 L = Passatge de la Concepcio 11 08008 Barcelona O = Agencia Catalana de Certificacio (NIF Q-0801176-I) C = ES	R10	3D97 D393 0439 622A 3E1C 4DA6 BED1 730E	08/01/2019
I9	UserTrust	CN = UTN-USERFirst-Hardware OU = http://www.usertrust.com	R13	2621 1BF5 2AEB 51B0 0BFS 9FDD 8D36	30/05/2020

		O = The USERTRUST Network L = Salt Lake City S = UT C = US		DA9E	
I10	Starfield	Número de serie = 10688435 CN = Starfield Secure Certification Authority OU = http://certificates.starfieldtech.com/repository O = Starfield Technologies, Inc. L = Scottsdale S = Arizona C = US	R14	02 01	16/11/2026
~~I11~~ (CADUCADO)	~~Cybertrust~~	~~CN = Cybertrust Educational CA~~ ~~OU = Educational CA~~ ~~O = Cybertrust~~ ~~C = BE~~	~~R2~~	~~04 00 03 FB~~	~~15/03/2013~~
I12	Secure Business Services	CN = Secure Business Services CA O = Secure Business Services, Inc. C = US	R13	0B 1F E5 2C 92 33 C4 B0 78 F1 B8 71 16 7C 64 87	09/07/2019
I13	DigiCert	CN = DigiCert Global CA OU = www.digicert.com O = DigiCert Inc C = US	R15	42 86 AB A0	14/07/2014
I14	SwissSign	CN = SwissSign Server Gold CA 2008 - G2 O = SwissSign AG C = CH	R16	5E CC FA 69 C0 33 27 EF	07/07/2023
I15	DigiCert	CN = DigiCert High Assurance EV CA-1 OU = www.digicert.com O = DigiCert Inc C = US	R17	08 BB B0 25 47 13 4B C9 B1 10 D7 C1 A2 12 59 C5	10/11/2021
I16	VeriSign	CN = VeriSign Class 3 Secure Server CA - G2 OU = Terms of use at https://www.verisign.com/rpa (c)09 OU = VeriSign Trust Network O = VeriSign, Inc.	R18	6E 4F FA B3 C5 E6 69 C4 D1 67 C9 92 AB E8 58 C4	25/03/2019

		C = US			
I17	VeriSign	CN = VeriSign Class 3 Extended Validation SSL SGC CA OU = Terms of use at https://www.verisign.com/rpa (c)06 OU = VeriSign Trust Network O = VeriSign, Inc. C = US	R19	2c 48 dd 93 0d f5 59 8e f9 3c 99 54 7a 60 ed 43	08/11/2016
I18	Go Daddy	SERIALNUMBER = 07969287 CN = Go Daddy Secure Certification Authority OU = http://certificates.godaddy.com/repository O = GoDaddy.com, Inc. L = Scottsdale S = Arizona C = US	R23	03 01	16/11/2026
I19	Camerfirma	SERIALNUMBER = A82743287 CN = CA Camerfirma Express Corporate Server O = AC Camerfirma SA C = ES	R24	08	21/04/2034
I20	Geo Trust	CN = GeoTrust Primary Certification Authority O = GeoTrust Inc. C = US	R12	0d 6e 62	21/08/2018
I21	Geo Trust	CN = GeoTrust Extended Validation SSL CA OU = See www.geotrust.com/resources/cps (c)06 O = GeoTrust Inc C = US	I20	69 48 a2 6b 20 1a a4 21 e8 98 b1 c4 92 c7 c5 8e	29/11/2016
I22	IPSCA	E = ipscalevel1@ipsca.com CN = ipsCA Level 1 CA OU = Certificaciones O = ips Certification Authority L = MADRID S = MADRID C = ES	R20	10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11	24/12/2029

I23	VeriSign	CN = VeriSign Class 3 Extended Validation SSL CA OU = Terms of use at https://www.verisign.com/rpa (c)06 OU = VeriSign Trust Network O = VeriSign, Inc. C = US	R19	5b 77 59 c6 17 84 e1 5e c7 27 c0 32 95 29 28 6b	08/11/2016
I24	Thawte	CN = Thawte SSL CA O = Thawte, Inc. C = US	R25	4D 5F 2C 34 08 B2 4C 20 CD 6D 50 7E 24 4D C9 EC	08/02/2020
I25	Thawte	CN = Thawte DV SSL CA OU = Domain Validated SSL O = Thawte, Inc. C = US	R25	76 10 12 8A 17 B6 82 BB 3A 1F 9D 1A 9A 35 C0 92	18/02/2020
I26	GeoTrust	CN = GeoTrust SSL CA O = GeoTrust, Inc. C = US	R26	02 36 D0	19/02/2020
I27	Agencia Catalana de Certificación	CN = EC-GENCAT OU = Generalitat de Catalunya OU = Vegeu https://www.catcert.net/verCIC-1 (c)03 OU = Serveis Publics de Certificacio ECV-1 O = Agencia Catalana de Certificacio (NIF Q-0801176-I) C = ES	R10	20 BD 3D E0 69 04 3D 25 3E 1C 0B 9C 82 52 F4 22	07/01/2027
I28	Agencia Catalana de Certificación	CN = EC-SAFP OU = Secretaria d'Administracio i Funcio Publica OU = Vegeu https://www.catcert.net/verCIC-2 (c)03 OU = Serveis Publics de Certificacio ECV-2 L = Passatge de la Concepcio 11 08008 Barcelona O = Agencia Catalana de Certificacio (NIF Q-0801176-I)	I27	6F EF 2F 14 F4 4F CC DF 3E 1C 21 16 98 8C 15 36	07/01/2019

		C = ES			
I29	Terena	CN = TERENA SSL CA O = TERENA C = NL	I9	4B C8 14 03 2F 07 FA 6A A4 F0 DA 29 DF 61 79 BA	30/05/2020
I30	Thawte	CN = Thawte SGC CA O = Thawte Consulting (Pty) Ltd. C = ZA	R1	30 00 00 06	13/05/2015
I31	GeoTrust	CN = GeoTrust DV SSL CA OU = Domain Validated SSL O = GeoTrust Inc. C = US	R26	02 36 D2	25/02/2020
I32	VeriSign	CN = VeriSign Class 3 International Server CA - G3 OU = Terms of use at https://www.verisign.com/rpa (c)10 OU = VeriSign Trust Network O = VeriSign, Inc. C = US	R19	64 1B E8 20 CE 02 08 13 F3 2D 4D 2D 95 D6 7E 67	08/02/2020
I33	GeoTrust	CN = RapidSSL CA O = GeoTrust, Inc. C = US	R26	02 36 D1	19/02/2020
I34	ACE / Verisign	OU = www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign OU = VeriSign International Server CA - Class 3 OU = VeriSign, Inc. O = VeriSign Trust Network	R1	46 FC EB BA B4 D0 2F 0F 92 60 98 23 3F 93 07 8F	25/10/2016
I35	UserTrust	CN = PositiveSSL CA O = Comodo CA Limited L = Salford S = Greater Manchester C = GB	R13	4C CD 4A 9A 5B 45 13 21 8C CF 90 2F 8B 2B 51 71	30/05/2020
I36	VeriSign	CN = VeriSign Class 3 Secure Server CA - G3 OU = Terms of use at https://www.verisign.com/rpa (c)10	R19	6E CC 7A A5 A7 03 20 09 B8 CE BC F4 E9 52 D4 91	08/02/2020

		OU = VeriSign Trust Network O = VeriSign, Inc. C = US			
I37	GlobalSign	CN = GlobalSign Domain Validation CA O = GlobalSign nv-sa OU = Domain Validation CA C = BE	R27	04 00 00 00 00 01 1E 44 A5 FA 2C	04/05/2017
I38	VeriSign	CN = VeriSign Class 3 International Server CA - T1 OU = Terms of use at https://www.verisign.com/rpa (c)10 OU = VeriSign Trust Network O = VeriSign, Inc. C = US	R19	6A 64 B0 90 2D CF E7 C6 1B 55 1E D4 F8 D3 E8 29	13/05/2020
I39	DigiCert	CN = DigiCert High Assurance CA-3 OU = www.digicert.com O = DigiCert Inc C = US	R17	08 51 F9 59 81 41 45 CA BD E0 24 E2 12 C9 C2 0E	03/04/2022
I40	Comodo	CN = PositiveSSL CA 2 O = COMODO CA Limited L = Salford S = Greater Manchester C = GB	R13	07 6F 12 46 81 45 9C 28 D5 48 D6 97 C4 0E 00 1B	30/05/2020
I41	Camerfirma	CN = AC Camerfirma Express Corporate Server v3 O = AC Camerfirma SA OU = http://www.camerfirma.com SERIALNUMBER = A82743287 L = Madrid (see current address at www.camerfirma.com/address) E = info@camerfirma.com C = ES	R24	0A	18/01/2019
I42	FNMT	CN = AC Administración Pública SERIALNUMBER = Q2826004J OU = CERES	R28	01	21/05/2022

		O = FNMT-RCM C = ES			
I43	Comodo	CN = COMODO High-Assurance Secure Server CA O = COMODO CA Limited L = Salford S = Greater Manchester C = GB	R13	16 90 C3 29 B6 78 06 07 51 1F 05 B0 34 48 46 CB	30/05/2020
I44	Firma Profesional	CN = AC Firmaprofesional - CA1 O = Firmaprofesional S.A. NIF A-62634068 OU = Jerarquia de Certificacion Firmaprofesional OU = Consulte http://www.firmaprofesional.com L = C/ Muntaner 244 Barcelona E = ca1@firmaprofesional.com C = ES	R29	53 30 15 E0 9A 9E B8 66	16/06/2030
I45	Camerfirma	CN = AC CAMERFIRMA AAPP SERIALNUMBER = A82743287 OU = AC CAMERFIRMA L = MADRID (Ver en https://www.camerfirma.com/address) O = AC CAMERFIRMA S.A. C = ES	R24	0D	20/02/2022
I46	Entrust	CN = Entrust Certification Authority - L1C OU = (c) 2009 Entrust, Inc. OU = www.entrust.net/rpa is incorporated by reference O = Entrust, Inc. C = US	R31	38 63 E9 FC	10/12/2019
I47	UserTrust	CN = OVH Secure Certification Authority O = OVH SAS OU = Low Assurance C = FR	R3	12 92 87 3F D3 F2 25 45 18 09 79 CC 9F 18 0E 05	30/05/2020
I48	StarCom	CN = StartCom Class 2 Primary Intermediate	R33	1A	24/10/2017

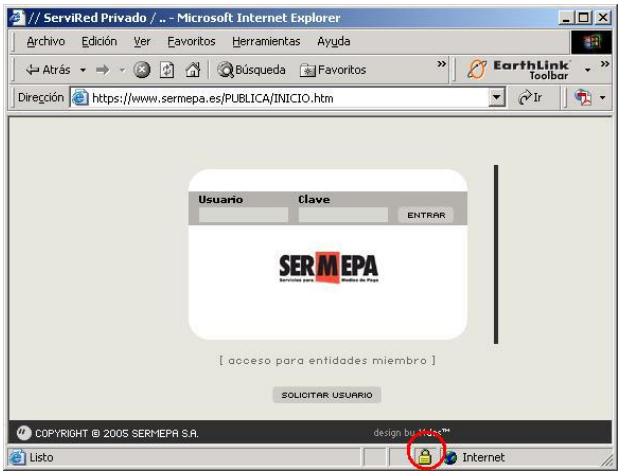
		Server CA OU = Secure Digital Certificate Signing O = StartCom Ltd. C = IL			
I49	StarCom	CN = StartCom Extended Validation Server CA OU = StartCom Certification Authority O = StartCom Ltd. C = IL	R33	35	01/01/2019
I50	T-SYSTEMS	CN = TeleSec ServerPass CA 1 OU = Trust Center Services O = T-Systems International GmbH C = DE	R30	07 27 42 C2	30/11/2017

5. ANEXO B: URL DE LAS CA EMISORAS DE CERTIFICADOS DE SERVIDOR SSL RECONOCIDAS POR REDSYS

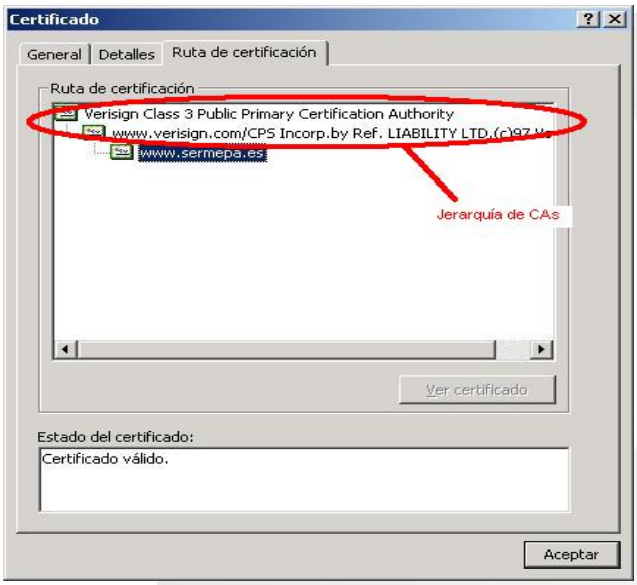
Nombre empresa	URL
ACE/Verisign	http://www.ace.es/
Comodo	http://www.comodogroup.com/index.html
Digi-Sign	http://www.digi-sign.com
Geotrust/ Equifax	http://www.quickssl.com/
Starfield Technologies	http://www.starfieldtech.com/
Thawte	http://www.thawte.com/
IPSCA	http://www.ipsca.com/
Agencia Catalana de Certificación	http://www.catcert.net/
CyberTrust	http://www.cybertrust.com/

6. ANEXO C: QUÉ CA HA EMITIDO MI CERTIFICADO DE SERVIDOR SSL

En caso de que ya se disponga de un certificado de servidor instalado en la web y quiera comprobarse si está en la lista de certificados de CA aceptados por REDSYS, bastará con acceder con el navegador Internet Explorer a la web de forma segura (http**s**:\\...) y hacer doble click sobre el candado que aparece en la esquina inferior derecha.



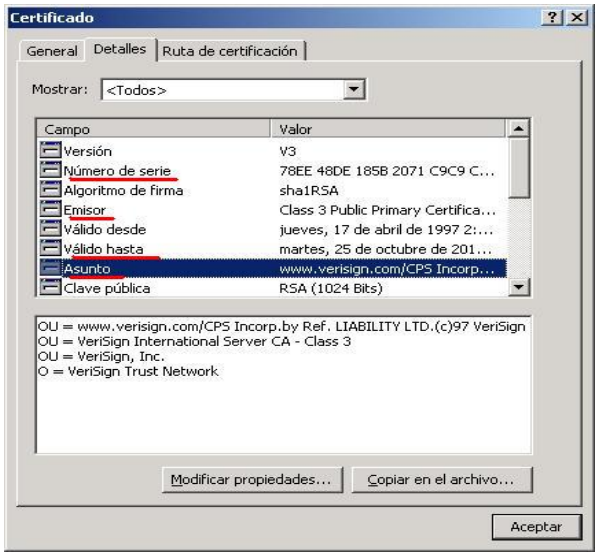
Se abrirá una ventana con la información del certificado digital. En la pestaña "Ruta de certificación" podemos ver la jerarquía de CAs correspondiente.



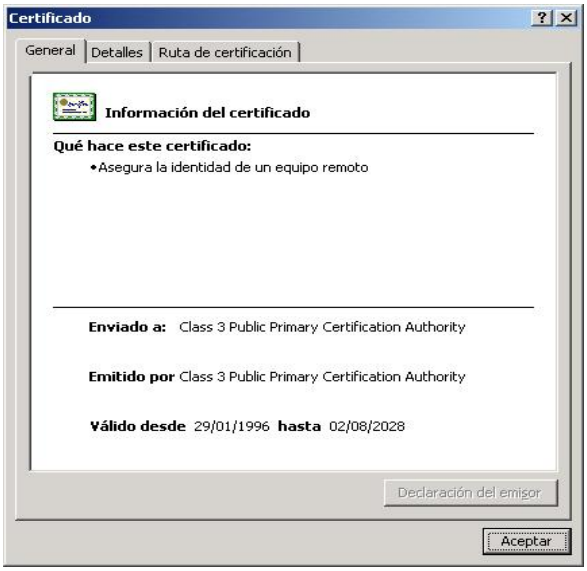
Haremos doble click en cada una de las CA para abrir la correspondiente ventana de certificado, donde poder cotejar sus datos.

La información del certificado se puede ver en la pestaña “Detalles”.

En concreto hay que comprobar que los campos “Número de serie”, “Emisor”, “Asunto” y “Válido hasta” del certificado coinciden con alguno de los del ANEXO A: ENTIDADES DE CERTIFICACIÓN RECONOCIDAS POR REDSYS.



Es necesario realizar esta operación para cada uno de los certificados de CA de la jerarquía, es decir, todos a partir del propio de servidor web (excluido), que es el que se abre al hacer doble click en el candado, hasta llegar al certificado de CA Raíz (incluido) que es aquel que aparece más alto en la pestaña “Ruta de Certificación” y que tiene la peculiaridad que sus campos “Asunto” y “Emisor” coinciden.


Certificado
General
Detalles
Ruta de certificación
Información del certificado
Qué hace este certificado:
•Asegura la identidad de un equipo remoto
Enviado a: Class 3 Public Primary Certification Authority
Emitido por Class 3 Public Primary Certification Authority
Válido desde 29/01/1996 hasta 02/08/2028
Declaración del emisor
Aceptar