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

Versión: 1.29

22/02/2016

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: 11/12/2014 | Fecha: 11/11/2015 | Fecha: 11/11/2015 |
| <p>Comentarios: La gestión de la documentación impresa es responsabilidad de la persona que la imprime.</p> <p>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.</p> | | |

| 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. |
| 1.3 | 17/07/2013 | Anexo B | Incorporación de entidad Intermedia AlphaSSL GA-C2 cuya raíz es la R27 |
| 1.4 | 11/12/2014 | Anexo B | Incorporación de Entidad Intermedia thawte SSL CA - G2 cuya raíz es R25. SHA256-2048 |
| 1.5 | 23/12/2014 | Anexo B | Incorporación de CA Intermedia I53 Symantec Class 3 EV SSL CA - G3 cuya raíz es R19 |

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



| | | | |
|------|------------|---------|---|
| 1.6 | 08/01/2015 | Anexo B | Incorporación de CA Intermedia I54 AC Componentes Informáticos cuya raíz es R28 |
| 1.7 | 09/01/2015 | Anexo B | Incorporación de CA Intermedias I55, I56, I57 e I58. Baja por caducidad de CA Intermedia I13 |
| 1.8 | 16/01/2015 | Anexo B | Incorporación de CA Intermedia I59 Symantec Class 3 EV SSL CA - G2 cuya raíz es I19 |
| 1.9 | 22/01/2015 | Anexo B | Añadidas la CA Intermedia I60 Entrust Certification Authority - L1K y las Raíces R34 y R35. Baja de I6 por caducidad. |
| 1.10 | 10/02/2015 | Anexo B | Corrección S/N R17. Incorporación CA Intermedia I61 DigiCert SHA2 High Assurance Server CA cuya raíz es R17 |
| 1.11 | 11/02/2015 | Anexo B | Añadida CA Intermedia I62 GeoTrust EV SSL CA - G4 cuya raíz es I20 |
| 1.12 | 16/02/2015 | Anexo B | Añadida CA Intermedia I63 Trustwave Extended Validation CA, Level 3 |
| 1.13 | 16/02/2015 | Anexo B | Añadida CA Intermedia I64 Trustwave Extended Validation SHA256 CA, Level 1 |

La propiedad intelectual de este documento pertenece a Redsys. Queda prohibida su reproducción, venta, o cesión a terceros

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



| | | | |
|------|------------|---------|--|
| 1.14 | 23/02/2015 | Anexo B | Añadida CA Intermedia I65 COMODO RSA Extended Validation Secure Server CA |
| 1.15 | 25/02/2015 | Anexo B | Añadida I66 y actualizada R34 |
| 1.16 | 13/03/2015 | Anexo B | Añadida jerarquía de Izenpe R36 e I67 |
| 1.17 | 20/03/2015 | Anexo B | Añadida CA I68 Go Daddy Secure Certificate Authority – G2 |
| 1.18 | 10/04/2015 | Anexo B | Añadida CA I69 Symantec Class 3 EV SSL SGC CA - G2 |
| 1.19 | 30/04/2015 | Anexo B | Añadida I70 GlobalSign Domain Validation CA - SHA256 - G2 |
| 1.20 | 21/05/2015 | Anexo B | Añadidas I71 y R38 |
| 1.21 | 28/05/2015 | Anexo B | Añadida I72 |
| 1.22 | 01/06/2015 | Anexo B | Añadida I73 y R39 Baja por caducidad I30 Añadida I74, sustituta de I30 |
| 1.23 | 08/06/2015 | Anexo B | Añadida I75 |
| 1.24 | 25/06/2015 | Anexo B | Añadidas I76 e I77. |
| 1.25 | 29/07/2015 | Anexo B | Añadidas R40 e I78. |
| 1.26 | 11/11/2015 | Anexo B | Añadidas I79, I80 |
| 1.27 | 22/12/2015 | Anexo B | Añadidas R41, I81 |
| 1.28 | 04/01/2016 | Anexo B | Añadidas R42, I82 |
| 1.29 | 22/02/2016 | Anexo B | Añadidas R43, R44, I83, I84 |

La propiedad intelectual de este documento pertenece a Redsys. Queda prohibida su reproducción, venta, o cesión a terceros

ÍNDICE DE CONTENIDO

| | |
|--|-----------|
| 1. INTRODUCCIÓN | 1 |
| 1.1 Objetivo | 1 |
| 1.2 Estructura | 1 |
| 1.3 Audiencia | 1 |
| 2. CONCEPTOS PREVIOS | 2 |
| 2.1 Terminología..... | 2 |
| 2.2 Necesidad..... | 2 |
| 2.3 Cómo funciona SSL/TLS | 3 |
| 3. REQUERIMIENTOS | 5 |
| 4. ANEXO A: ENTIDADES DE CERTIFICACIÓN RECONOCIDAS POR REDSYS | 6 |
| 5. ANEXO B: URL DE LAS CA EMISORAS DE CERTIFICADOS DE SERVIDOR SSL RECONOCIDAS POR REDSYS | 29 |
| 6. ANEXO C: QUÉ CA HA EMITIDO MI CERTIFICADO DE SERVIDOR SSL | 30 |

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.

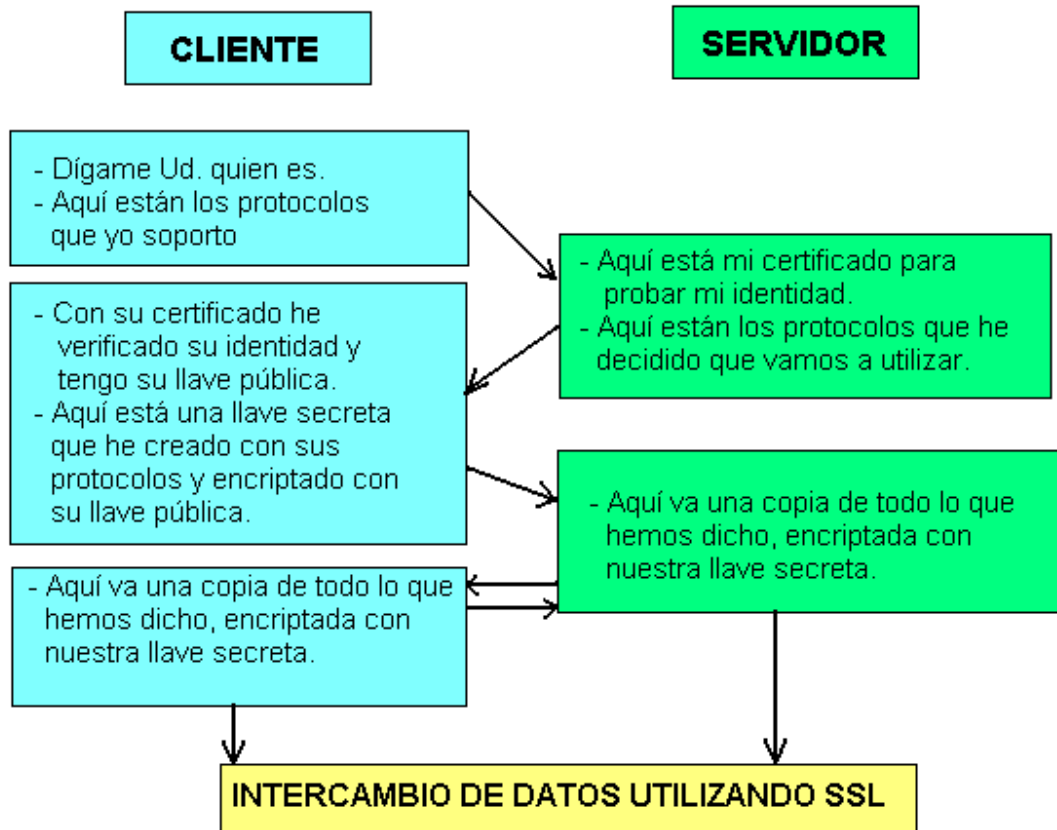
2.2 Necesidad

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 autenticación 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.

CA's Raíz:

| ID. | EMPRESA | CAMPO 'ASUNTO' | Nº SERIE/Huella Digital | 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. | 01 | 21/06/2020 |

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

| | | | | |
|------------------|----------|---|--|-----------------------|
| | | C = US | | |
| 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 | 00 | 30/12/2009 |

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

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

| | | C=ES | | |
|-----|-----------------------------------|---|---|------------|
| R10 | Agencia Catalana de Certificación | CN = EC-ACC OU = Jerarquia Entitats de Certificacio 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 | EE2B 3DEB D421 DE14 A862 AC04 F3DD C401 | 08/01/2031 |
| 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 |

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

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

| | | | | |
|-----|-----------|--|---|------------|
| 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 C = US | 02 ac 5c 26 6a 0b 40 9b 8f 0b 79 f2 ae 46 25 77 | 10/11/2031 |
| 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 | 00 | 25/12/2029 |

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

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

| | | | | |
|----------------|----------------------|--|--|-----------------------|
| | | C = ES | | |
| 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 €4 | 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 | 02 00 00 B9 | 13/05/2025 |

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

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

| | | | | |
|-----|--------------|--|---|------------|
| | | C = IE | | |
| 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 |
| R34 | Entrust | CN = Entrust Root Certification Authority - G2 OU = (c) 2009 Entrust, Inc. - for authorized use only OU = See www.entrust.net/legal-terms O = Entrust, Inc. C = US | 4a 53 8c 28 | 07/12/2030 |
| R35 | Entrust | CN = Entrust Root Certification Authority OU = (c) 2006 Entrust, Inc. OU = www.entrust.net/CPS is incorporated by reference O = Entrust, Inc. C = US | 45 6b 50 54 | 27/11/2026 |
| R36 | Izenpe.com | CN = Izenpe.com O = IZENPE S.A. C = ES | 06 e8 46 27 2f 1f 0a 8f d1 84 5c e3 69 f6 d5 | 13/12/2037 |
| R37 | Go Daddy | CN = Go Daddy Root Certificate Authority - G2 O = GoDaddy.com, Inc. L = Scottsdale S = Arizona | 1b e7 15 | 30/05/2031 |

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

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

| | | | | |
|-----|---|---|---|------------|
| | | C = US | | |
| R38 | VeriSign Universal Root Certification Authority | CN = VeriSign Universal Root Certification Authority OU = (c) 2008 VeriSign, Inc. - For authorized use only OU = VeriSign Trust Network O = VeriSign, Inc. C = US | 40 1a c4 64 21 b3 13 21 03 0e bb e4 12 1a c5 1d | 02/12/2037 |
| R39 | GlobalSign | CN = GlobalSign O = GlobalSign OU = GlobalSign Root CA - R3 | 04 00 00 00 00 01 21 58 53 08 a2 | 18/3/2029 |
| R40 | DigiCert | CN = DigiCert Assured ID Root CA O = DigiCert Inc OU = www.digicert.com C = US | 0c:e7:e0:e5:17:d8:46:fe:8f:e5:60:fc:1b:f0:30:39 | 10/11/2031 |
| R41 | GeoTrust | CN = GeoTrust Primary Certification Authority - G3 OU = (c) 2008 GeoTrust Inc. - For authorized use only O = GeoTrust Inc. C = US | 15 ac 6e 94 19 b2 79 4b 41 f6 27 a9 c3 18 0f 1f | 02/12/2037 |
| R42 | Autoridad de Certificación de la Abogacía | CN = Autoridad de Certificación de la Abogacía O = Consejo General de la Abogacía NIF:Q-2863006I C = ES | 00 90 8b 32 4f c1 90 1a ce b4 c3 38 09 cd cf e4 | 13/06/2030 |
| R43 | FNMT | OU = AC RAIZ FNMT-RCM O = FNMT-RCM C = ES | NS: 5d 93 8d 30 67 36 c8 06 1d 1a c7 54 84 69 07 HD: ec 50 35 07 b2 15 c4 95 62 19 e2 a8 9a 5b 42 99 2c 4c 2c 20 | 01/01/2030 |
| R44 | GeoTrust | CN = GeoTrust Primary Certification Authority | 18 ac b5 6a fd 69 b6 15 3a 63 6c af da fa c4 a1 | 17/07/2036 |

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



| | | | | |
|--|--|-----------------------------|--|--|
| | | O = GeoTrust Inc. C = US | | |
|--|--|-----------------------------|--|--|

CAs Intermedias:

| ID | EMPRESA | CAMPO 'ASUNTO' | CAMPO 'EMISOR' ¹ | Nº SERIE | FECHA CAD. |
|-----------------------------|---------------------------|---|-----------------------------|--|-----------------------|
| 11 (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 |

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

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

| | | | | | |
|------------------|------------------------|---|----|--|------------|
| 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 |
| 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 (caducada) | Thawte | CN = Thawte SSL Domain CA O = Thawte Consulting (Pty) Ltd. C = ZA | R7 | 3000-0001 | 04/05/2014 |
| I6 (Caducado) | 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 | R9 | 0090-33 | 31/12/2009 |

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

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



| | | | | | |
|------------------------------|-----------------------------------|--|---------------|--|-----------------------|
| | | L = Barcelona S = Barcelona C = ES | | | |
| 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 O = The USERTRUST Network L = Salt Lake City S = UT C = US | R13 | 2621 1BF5 2AEB 51B0 0BFS 9FDD 8D36 DA9E | 30/05/2020 |
| 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 |

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

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

| | | | | | |
|-------------------|------------|--|-----|--|------------|
| I13 (CADUCADO) | 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. C = US | R18 | 6E 4F FA B3 C5 E6 69 C4 D1 67 C9 92 AB E8 58 C4 | 25/03/2019 |
| 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 | R24 | 08 | 21/04/2034 |

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

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



| | | | | | |
|-----|-----------|---|-----|---|------------|
| | | O = AC Camerfirma SA C = ES | | | |
| 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 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 |

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

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

| | | | | | |
|----------------|-----------------------------------|---|---------------|--|-----------------------|
| I27 | Agencia Catalana de Certificaci3n | 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 Certificaci3n | 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) C = ES | I27 | 6F EF 2F 14 F4 4F CC DF 3E 1C 21 16 98 8C 15 36 | 07/01/2019 |
| 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 | R19 | 64 1B E8 20 CE 02 08 13 F3 2D 4D 2D 95 D6 7E 67 | 08/02/2020 |

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

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

| | | | | | |
|-----|----------------|---|-----|--|------------|
| | | O = VeriSign, Inc. C = US | | | |
| 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 Incorpor.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 OU = VeriSign Trust Network O = VeriSign, Inc. C = US | R19 | 6E CC 7A A5 A7 03 20 09 B8 CE BC F4 E9 52 D4 91 | 08/02/2020 |
| 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 |

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

| | | | | | |
|----------------|-------------------|---|----------------|--|-----------------------|
| 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 O = FNMT-RCM C = ES | R28 | 01 | 21/05/2022 |
| 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 | R29 | 53 30 15 E0 9A 9E B8 66 | 16/06/2030 |

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

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



| | | | | | |
|-----|------------|--|-----|--|------------|
| | | http://www.firmaprofesional.com L = C/ Muntaner 244 Barcelona E = ca1@firmaprofesional.com C = ES | | | |
| 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 Server CA OU = Secure Digital Certificate Signing O = StartCom Ltd. C = IL | R33 | 1A | 24/10/2017 |
| 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 |

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

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

| | | | | | |
|-----|--------------------------------|---|-----|--|------------|
| I51 | AlphaSSL GA-C2 | CN = AlphaSSL CA - G2 OU = AlphaSSL | R27 | 04 00 00 00 00 01 2f 4e e1 37 02 | 13/04/2022 |
| I52 | THAWTE | CN = thawte SSL CA - G2 O = thawte, Inc. C = US | R25 | 16 87 d6 88 6d e2 30 06 85 23 3d bf 11 bf 65 97 | 31/10/2023 |
| I53 | VeriSign | CN = Symantec Class 3 EV SSL CA - G3 OU = Symantec Trust Network O = Symantec Corporation C = US | R19 | 7e e1 4a 6f 6f ef f2 d3 7f 3f ad 65 4d 3a da b4 | 31/10/2023 |
| I54 | AC Componentes Informáticos | OU = AC Componentes Informáticos O = FNMT-RCM C = ES | R28 | 34 c6 ab 04 4e 36 99 12 51 c8 25 0b 6c 94 d6 c0 | 24/06/2028 |
| I55 | RapidSSL SHA256 CA - G3 | CN = RapidSSL SHA256 CA - G3 O = GeoTrust Inc. C = US | R26 | 02 3a 77 | 20/05/2022 |

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



| | | | | | |
|-----|---|--|-----|---|------------|
| I56 | GeoTrust SSL CA | CN = GeoTrust SSL CA O = GeoTrust, Inc. C = US | R26 | 02 36 d0 | 18/02/2020 |
| I57 | COMODO RSA Certification Authority | CN = COMODO RSA Certification Authority O = COMODO CA Limited L = Salford S = Greater Manchester C = GB | R13 | 27 66 ee 56 eb 49 f3 8e ab d7 70 a2 fc 84 de 22 | 30/05/2020 |
| I58 | COMODO RSA Domain Validation Secure Server CA | CN = COMODO RSA Domain Validation Secure Server CA O = COMODO CA Limited L = Salford S = Greater Manchester C = GB | I57 | 2b 2e 6e ea d9 75 36 6c 14 8a 6e db a3 7c 8c 07 | 12/02/2029 |
| I59 | Verisign | CN = Symantec Class 3 EV SSL CA - G2 OU = Symantec Trust Network O = Symantec Corporation C = US | R19 | 36 65 85 07 7a 88 67 ab 58 f4 a0 94 f8 10 37 33 | 31/10/2023 |
| I60 | Entrust Certification Authority - L1K | CN = Entrust Certification Authority - L1K OU = (c) 2012 Entrust, Inc. - for authorized use only OU = See www.entrust.net/legal-terms O = Entrust, Inc. C = US | R34 | 51 d3 60 ee | 23/10/2024 |
| I61 | DigiCert SHA2 High Assurance Server CA | CN = DigiCert SHA2 High Assurance Server CA OU = www.digicert.com O = DigiCert Inc C = US | R17 | 04 e1 e7 a4 dc 5c f2 f3 6d c0 2b 42 b8 5d 15 9f | 22/10/2028 |
| I62 | GeoTrust EV SSL CA - G4 | CN = GeoTrust EV SSL CA - G4 O = GeoTrust Inc. C = US | I20 | 6e 8a 90 eb cf f0 44 8a 72 0d 08 05 d0 82 a5 44 | 31/10/2023 |
| I63 | Trustwave Extended Validation CA, Level 3 | E = ca@trustwave.com CN = Trustwave Extended Validation CA, Level 3 | R32 | 47 f8 f6 a8 | 24/09/2027 |

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

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

| | | | | | |
|-----|--|---|-----|---|------------|
| | | O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US | | | |
| I64 | Trustwave Extended Validation SHA256 CA, Level 1 | E = ca@trustwave.com CN = Trustwave Extended Validation SHA256 CA, Level 1 O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US | R32 | 00 c1 bd 27 b3 83 95 8d 0d 8b ca 5e 4f 08 d0 09 d9 | 10/10/2024 |
| I65 | COMODO RSA Extended Validation Secure Server CA | CN=COMODO RSA Extended Validation Secure Server CA O=COMODO CA Limited L=Salford ST=Greater Manchester C=GB | I57 | 06:a7:43:80:d4:eb:fe:d4:35:b5:a3:f7:e1:6a:bd:d8 | 11/02/2027 |
| I66 | Entrust Certification Authority - L1E | CN = Entrust Certification Authority - L1E OU = (c) 2009 Entrust, Inc. OU = www.entrust.net/rpa is incorporated by reference O = Entrust, Inc. C = US | R35 | 4c 0e c9 18 | 12/11/2021 |
| I67 | CA de Certificados SSL EV Izenpe | CN = CA de Certificados SSL EV OU = BZ Ziurtagiri publikoa - Certificado publico EV O = IZENPE S.A. C = ES | R36 | 1a 5a 6a 10 37 62 e7 91 4c be a7 ec 33 9a 3a f5 | 20/10/2020 |
| I68 | Go Daddy Secure Certificate Authority – G2 | CN = Go Daddy Secure Certificate Authority - G2 OU = http://certs.godaddy.com/repository/ O = GoDaddy.com, Inc. L = Scottsdale S = Arizona | R37 | 07 | 03/05/2031 |

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

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



| | | | | | |
|--|--|--------|--|--|--|
| | | C = US | | | |
|--|--|--------|--|--|--|

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

Ref RS.RI.SEG.MAN.0004

<PÚBLICO>

22/02/2016

Versión: 1.29

25

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

| | | | | | |
|-----|---|--|-----|--|------------|
| I69 | Symantec Class 3 EV SSL SGC CA - G2 | CN = Symantec Class 3 EV SSL SGC CA - G2 OU = Symantec Trust Network O = Symantec Corporation C = US | R19 | 7a 0f 41 df 1c cd 14 dc b2 69 29 8e e2 2c 6a 35 | 31/10/2023 |
| I70 | GlobalSign Domain Validation CA - SHA256 - G2 | CN = GlobalSign Domain Validation CA - SHA256 - G2 O = GlobalSign nv-sa C = BE | R27 | 04 00 00 00 00 01 44 4e f0 3e 20 | 20/02/2024 |
| I71 | Symantec Class 3 Secure Server SHA256 SSL CA | CN = Symantec Class 3 Secure Server SHA256 SSL CA OU = Symantec Trust Network O = Symantec Corporation C = US | R38 | 69 87 94 19 d9 e3 62 70 74 9d bb e5 9d c6 68 5e | 09/04/2023 |
| I72 | Camerfirma Corporate Server II - 2015 | CN = Camerfirma Corporate Server II - 2015 L = Madrid (see current address at https://www.camerfirma.com/address) SERIALNUMBER = A82743287 O = AC Camerfirma S.A. OU = AC CAMERFIRMA C = ES | R24 | 62 1f f3 1c 48 9b a1 36 | 15/12/2037 |
| I73 | GlobalSign Domain Validation CA - SHA256 - G2 | CN = GlobalSign Domain Validation CA - SHA256 - G2 O = GlobalSign nv-sa C = BE | R39 | 04 00 00 00 00 01 31 89 c6 42 58 | 02/08/2022 |
| I74 | Thawte SGC CA - G2 | CN = Thawte SGC CA - G2 O = Thawte, Inc. C = US | R19 | 18 a2 23 6c d7 27 c7 52 8d f6 7b 4b 85 6e ff ed | 29/07/2020 |
| I75 | Symantec Class 3 Secure Server CA - G4 | CN = Symantec Class 3 Secure Server CA - G4 OU = Symantec Trust Network O = Symantec Corporation C = US | R19 | 51 3f b9 74 38 70 b7 34 40 41 8d 30 93 06 99 ff | 31/10/2023 |

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

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

| | | | | | |
|-----|---|--|-----|---|------------|
| I76 | USERTrust | CN = USERTrust RSA Certification Authority O = The USERTRUST Network L = Jersey City ST = New Jersey C = US | R13 | 13:ea:28:70:5b:f4:ec:ed:0c:36:63:09: 80:61:43:36 | 30/05/2020 |
| I77 | Terena | CN = TERENA SSL CA 2 O = TERENA L = Amsterdam ST = Noord-Holland C = NL | I76 | b0:ff:cf:3a:1d:82:44:98:15:62:9d:64: 88:6a:41:65 | 08/10/2024 |
| I78 | Terena | CN = TERENA SSL CA 3 O = TERENA L = Amsterdam ST = Noord-Holland C = NL | R40 | 08:70:bc:c5:af:3f:db:95:9a:91:cb:6a: ee:ef:e4:65 | 18/11/2024 |
| I79 | STRATO SSL - G2 | C=DE O=STRATO AG OU=Domain Validated SSL CN=STRATO SSL - G2 | R26 | 146044 | 22/05/2022 |
| I80 | GlobalSign Organization Validation CA - SHA256 - G2 | CN = GlobalSign Organization Validation CA - SHA256 - G2 O = GlobalSign nv-sa C = BE | R27 | 04 00 00 00 00 01 44 4e f0 42 47 | 20/02/2024 |
| I81 | GlobalSign Organization Validation CA - SHA256 - G2 | CN = GeoTrust SHA256 SSL CA O = GeoTrust Inc. C = US | R41 | 41 82 12 7d 12 d9 c6 b3 21 39 43 12 56 64 00 b8 | 23/05/2023 |
| I82 | ACA - Certificados Corporativos | CN = ACA - Certificados Corporativos OU = Autoridad de Certificacion de la Abogacia O = Consejo General de la Abogacia NIF:Q-2863006I E = ac@acabogacia.org L = Madrid C = ES | R42 | 79 3b be 52 43 57 d2 fd 42 af d8 84 26 9c ac 62 | 13/06/2017 |

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

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

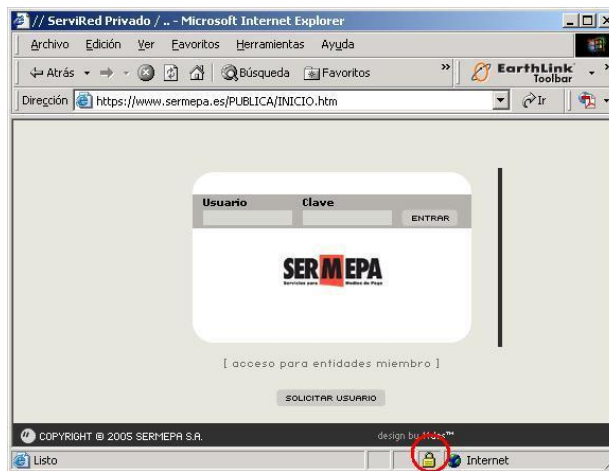
| | | | | | |
|-----|---------------------------|--|-----|--|------------|
| I83 | FNMT | CN = AC Administración Pública SERIALNUMBER = Q2826004J OU = CERES O = FNMT-RCM C = ES | R43 | NS: 02 HD: 73 20 b5 52 7a a9 d4 b0 26 e8 0f 9f 7a 92 e8 a4 a4 a7 24 62 | 21/05/2022 |
| I84 | AlphaSSL CA - SHA256 - G2 | CN = AlphaSSL CA - SHA256 - G2 O = GlobalSign nv-sa C = BE | R27 | 04 00 00 00 00 01 44 4e f0 36 31 | 20/02/2024 |

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

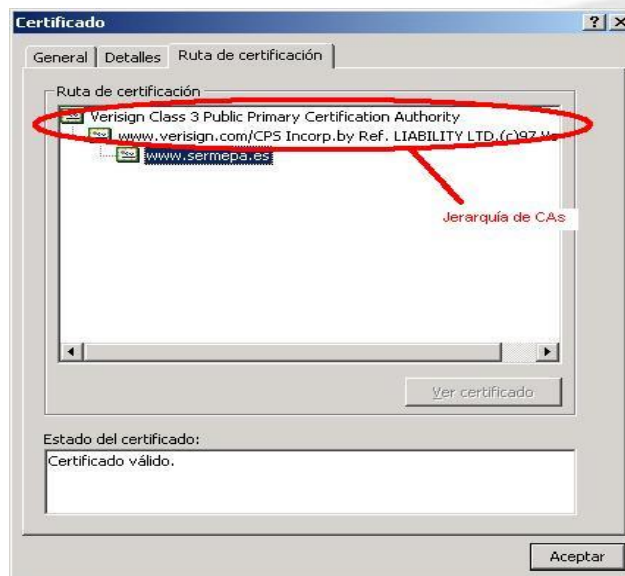
| Nombre empresa | URL |
|-------------------------------------|---|
| ACE/Verisign | http://www.ace.es/ |
| Comodo | http://www.comodogroup.com/index.html |
| Digi-Sign | http://www.digi-sign.com |
| Geotrust/ Equifax | http://www.quickssl.com/ |
| Starfield Technologies | http://www.starfieldtech.com/ |
| Thawte | http://www.thawte.com/ |
| IPSCA | http://www.ipsca.com/ |
| Agencia Catalana de Certificación | http://www.catcert.net/ |
| CyberTrust | http://www.cybertrust.com/ |
| Globalsign | https://www.globalsign.com/ |
| Agencia Valenciana de Certificación | http://www.accv.es/ |
| Izenpe | http://www.izenpe.com |
| Go Daddy | https://certs.godaddy.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 (<https://>...) 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.

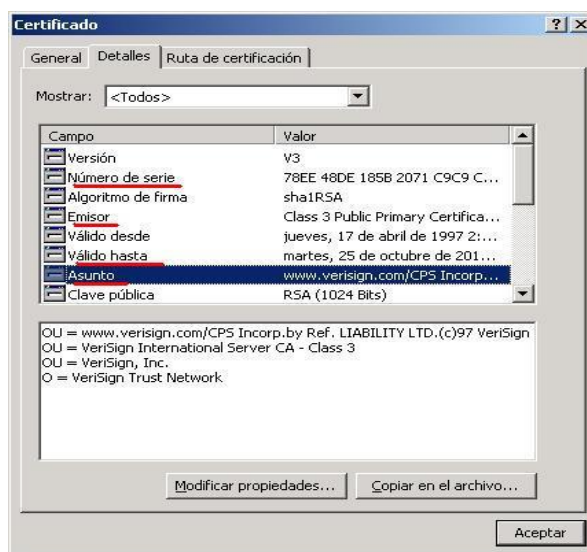


Redsys · C/ Francisco Sancha, 12 · 28034 · Madrid · ESPAÑA

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.

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

