Sujeto

Nombre común: calamarilng.com

Emisor

País / Región: GB
Estado / Providencia: Greater Manchester
Localidad: Salford
Empresa: Sectigo Limited
Nombre común: Sectigo RSA Domain Validation Secure Server CA
Número de serie: 41 0F 34 EC AA 3A C5 C8 3B 24 71 9F 67 3A DC 1F
Version: 3
Algoritmo de frima: SHA-256 con encriptación RSA (1.2.840.113549.1.1.11)
Parametros Ninguno
No valido antes de: jueves, 29 de octubre de 2020, 7:00:00 p. m. hora estándar de Colombia
Novalido despues de: sábado, 30 de octubre de 2021, 6:59:59 p. m. hora estándar de Colombia

Información de clave pública

Algoritmo: Encriptación RSA (1.2.840.113549.1.1.1)
Parámetros: Ninguno
Clave Pública: 256 bytes: B4 24 33 68 DD C6 C3 73 89 56 E1 63 7C 82 3B 48 65 14 4A 41 ED 5F E7 E8 69 B7 6E 08 DC F6 BD 97 F5 1B 73 FC 74 06 9F 50 E4 22 ED 40 78 DD 11 C6 CA B5 4A 0D B2 03 CC 04 A2 1B 50 2E 88 8C 71 A4 A5 E2 66 90 10 8B F7 C9 36 94 92 85 93 EB CE 61 D7 D2 6B 11 5B B8 2C 4F A4 9F EA CD 3E A5 1B EA 0A 21 2B 5F 0A 7E EF 5A 0D 07 B4 A1 5C 8F 78 61 18 E9 29 64 C5 4D 24 99 A7 39 54 ED BC 57 CF A0 B6 C1 FC 5A 18 A7 BB E1 6C 30 4C 2C F6 18 D6 A4 46 59 08 CF 24 23 57 04 C8 82 76 05 64 ED 7F D1 82 C1 9C 3D B6 04 F7 A2 FF A0 17 1D E9 3A 34 CA 71 9C 51 6A 89 E9 D5 9D 43 BA F4 32 24 0B 1C 4F 1C 0A 3E 20 3E 74 7A 86 9B 13 65 9B FC E0 D2 8E A1 0D 67 0A 71 5F 60 61 C6 E1 15 EA 23 86 5F 56 76 9A D8 F0 80 B4 A2 98 33 8D 59 88 7E BB A4 4D 94 E4 95 70 36 4E 70 89 40 80 CB 0F D4 DB C1 49

Exponente: 65537
Tamaño de la clave: 2.048 bits
Uso de la clave: encriptar, verificar, Ajustar, derivar
Firma: 256 bytes: 49 AE 72 69 0E C3 62 5C 67 44 EA 22 FB FE 94 50 EF 88 4D 10 8E 8D 5B 11 3C 8C 32 24 D2 06 80 52 2A BB 56 4E FC C2 2B BC AD 89 8B D8 5B E6 19 DE D5 23 CA DE FF 57 10 EE 0E 22 80 EC F3 0B 4E 9D 6B 84 3F E6 4A CB CD 3E CD BC C9 1A 6E 87 DF 23 EC 10 1B 17 15 58 B9 B7 A1 12 56 F3 BA 97 56 D7 67 61 42 1C 0B E4 FF C0 47 7A 2D 5E 4D 4A 98 6E 8E 33 98 AA 72 01 B0 05 8D 1C 40 27 E1 7C C7 5A 66 1D E0 16 38 FB A4 02 EC E7 F6 1D 2E AB 4C EA E7 07 C7 68 E1 4C A3 1F 70 25 00 0C 52 7F 58 7C E1 33 33 9A 02 03 AA 54 56 FC BA 33 17 60 D0 4D 5C 62 3E 08 DE 9D 8C 04 C9 01 CA A4 4F F5 77 ED 60 91 0D BC 2A F2 7B FA 91 3E A0 F1 E0 84 AA D6 15 9B 40 C4 2A F3 F4 44 4D 73 DD 86 E6 E8 36 99 18 E5 DA 28 2C 44 AD E2 08 86 4B 79 E3 FF 53 3F 9B E9 F0 C6 4E 02 C1 B0 28 B8 71 9A AC D5 F9 FF

Extensión:	Uso de la clave (2.5.39.15)
Crítico:	Sí
Uso:	Firma digital, Encriptación de la clave
Extensión:	Restricciones básicas (2.5.29.19)
Crítico:	Sí
Uso:	No
Extensión:	Uso de clave ampliada (2.5.29.37)
Crítico:	No
Objetivo 1	Autenticación de servidor (1.3.6.1.5.5.7.3.1)
Objetivo 2	Autenticación de cliente (1.3.6.1.5.5.7.3.2)
Extensión:	Identificador de clave del sujeto (2.5.29.14)
Crítico:	No
Número de clave:	09 97 60 FD B7 20 5B 00 85 15 49 4D 7B FD 22 FF 56 BF F5 D6
Extensión:	Identificador de clave de entidad (2.5.29.35)
Crítico:	No
Número de clave:	8D 8C 5E C4 54 AD 8A E1 77 E9 9B F9 9B 05 E1 B8 01 8D 61 E1
Extensión:	Nombre alternativo del sujeto (2.5.29.17)
Crítico:	No
Nombre DNS	calamarilng.com
Nombre DNS	www.calamarilng.com
Extensión:	Políticas del certificado (2.5.29.32)
Crítico:	No
ID de la política #1:	(1.3.6.1.4.1.6449.1.2.2.7)
ID de la calificador #1:	Instrucción de prácticas de certificación (1.3.6.1.5.5.7.2.1):
Identificador URI CPS:	https://sectigo.com/cps
ID de la política #1:	(2.23.140.1.2.1)
Extensión:	Lista de marcas de fecha y hora del certificado firmado incrustado (1.3.6.1.4.1.11129.2.4.2)
Crítico:	No
Version CT:	1
ID de clave de acceso:	7D 3E F2 F8 8F FF 88 55 68 24 C2 C0 CA 9E 52 89 79 2B C5 0E 78 09 7F 2E 6A 97 68 99 7E 22 F0 D7
Fecha y hora:	viernes, 30 de octubre de 2020, 2:24:09 p. m. hora estándar de Colombia
Algoritmo de firmas	SHA-256 ECDSA
Firma	70 bytes: 30 44 02 20 09 0F D7 69 DD A5 DB 63 99 28 C2 15 80 25 A6 6E 87 16 C8 B4 8D A7 B7 84 90 12 B6 C5 69 B7 2A 29 02 20 52 BE 63 6A CD 5E CD A8 58 4B 84 C8 5A D0 D4 87 C6 C2 A7 BF 9A ED 1F 7C B9 C7 AC F4 99 A4 94 8E
Extensión:	
Crítico:	
Método núm 1:	
URI:	
Método núm 2:	
URI:	

Huellas digitales

SHA-256:	40 B7 4B 20 4A C8 E8 8F 5E F9 16 17 B1 7A 67 AB D5 67 6A 76 A6 D8 54 A3 76 1D 1C EF 72 DC F3 39
SHA-1:	DB B0 D0 7B 40 1B 77 35 EE 64 32 A1 80 B9 03 E6 FF D1 ED EA