Evaluación de Aprendizaje 3

Marcos Cabral - 42684487

Temas

Certificados digitales

Fechas limites de entregas

ENTREGA	Lunes 23/11/2020	Fecha de Entrega
DEVOLUCION RDOS	Lunes 30/11/2020	Fecha Máxima de Devolución de Resultados
REENTREGA	Jueves 7/12/2020	Fecha de Re-entrega

Consigna

Se ha extraído de un certificado x509 con la siguiente información:

```
Subject Name
C (Country):   AR
L (Locality): Buenos Aires
O (Organization):      Mercadolibre Inc
CN (Common Name):      *.mercadolibre.com.ar
Issuer Name
C (Country):   US
O (Organization):      DigiCert Inc
CN (Common Name):      DigiCert SHA2 Secure Server CA
Issued Certificate
Version:       3
Serial Number: 0F 4D E7 77 D6 71 D8 85 60 66 54 4F 85 B6 F6 5D
Not Valid Before:      2020-02-18
Not Valid After:       2022-02-22
Certificate Fingerprints
SHA1:   43 03 7F C3 B2 B0 D9 E5 70 CD DC 81 B7 B0 19 A5 7A 76 2C EF
MD5:    05 9A 7C 86 30 AB D7 28 C5 86 52 22 99 1B 50 B2
Public Key Info
Key Algorithm: RSA
Key Parameters:        05 00
Key Size:      2048
Key SHA1 Fingerprint:  AB 9D 5D BF 0B A7 E7 E2 BB C4 A5 88 19 74 4B F6 0D D3 A2 20
Public Key:    30 82 01 0A 02 82 01 01 00 A1 26 C0 C0 18 FD 0F 7A 43 75 49 5E 48 ED F1
0D 8F 7B 64 C6 BB 08 8D 6C F2 3B EF AD 30 D4 1F C4 17 82 90 3E 5E BF 80 D0 31 2C 78 CF
80 4F BD D9 54 BF 58 6F 93 9D 42 79 18 F7 AD 90 A3 D8 7D E3 AC E5 B4 54 E9 89 9A 99 E7
A8 9E 4C 15 FF 24 44 66 7F 84 45 68 53 C1 DC 7B 5D 6F 57 1D 3A 1D 7C 65 01 01 4A D5 04
EB EB A4 FA 9C FA D0 3A 91 52 B4 85 6F 78 5A E4 55 D9 C0 6C A2 C4 09 DB 23 17 31 54 9A
3D 02 9B BB A0 5F 0D 9D 6D 7F 43 4F F5 6E 2A E3 89 31 7A D2 5B B4 B8 F1 EF D1 60 0A BF
C9 70 73 63 CA CA 10 D0 AC 72 B0 53 0D 93 38 02 E9 11 25 72 EE EA 61 E2 D6 AA 8A 8A 6C
12 93 16 BB 7B 03 14 7E 4F BB D6 FA A5 D8 4F 4E 8D CC 83 65 43 74 9D 43 C5 89 7E EB CE
5C 0E 47 91 29 CB 04 3A 0D 77 8F AD ED 6E 38 69 8A 88 96 74 63 68 8E FA 31 3D F7 D7 B3
77 08 77 83 85 AD 29 07 4B 02 03 01 00 01
Extension
Identifier:    2.5.29.35
Value: 30 16 80 14 0F 80 61 1C 82 31 61 D5 2F 28 E7 8D 46 38 B4 2C E1 C6 D9 E2
Critical:      No
Subject Key Identifier
Key Identifier:        3A 74 DD 95 69 17 64 0F 5A 52 4E D0 68 92 88 A2 37 79 CC 8B
Critical:      No
```

```
Subject Alternative Names

DNS:    *.mercadolibre.com.ar
DNS:    mercadolibre.com.ar
Critical:       No
Key Usage
Usages:Digital signatureKey encipherment
Critical:       Yes
Extended Key Usage
Allowed Purposes:       Server AuthenticationClient Authentication
Critical:       No
Extension
Identifier:     2.5.29.31
Value: 30 62 30 2F A0 2D A0 2B 86 29 68 74 74 70 3A 2F 2F 63 72 6C 33 2E 64 69 67 69 63
65 72 74 2E 63 6F 6D 2F 73 73 63 61 2D 73 68 61 32 2D 67 36 2E 63 72 6C   30 2F A0 2D A0
2B 86 29 68 74 74 70 3A 2F 2F 63 72 6C 34 2E 64 69 67 69 63 65 72 74 2E   63 6F 6D 2F 73
73 63 61 2D 73 68 61 32 2D 67 36 2E 63 72 6C
Critical:       No
Extension
Identifier:     2.5.29.32
Value: 30 43 30 37 06 09 60 86 48 01 86 FD 6C 01 01 30 2A 30 28 06 08 2B   06 01 05 05 07
02 01 16 1C 68 74 74 70 73 3A 2F 2F 77 77 77 2E 64 69 67 69 63 65 72 74   2E 63 6F 6D 2F
43 50 53 30 08 06 06 67 81 0C 01 02 02
Critical:       No
Extension
Identifier:     1.3.6.1.5.5.7.1.1
Value:  30 6E 30 24 06 08 2B 06 01 05 05 07 30 01 86 18 68 74 74 70 3A 2F 2F 6F 63 73 70
2E 64 69 67 69 63 65 72 74 2E 63 6F 6D 30 46 06 08 2B 06 01 05 05 07 30 02 86 3A 68 74
74 70 3A 2F 2F 63 61 63 65 72 74 73 2E 64 69 67 69 63 65 72 74 2E 63 6F 6D 2F 44 69 67
69 43 65 72 74 53 48 41 32 53 65 63 75 72 65 53 65 72 76 65 72 43 41 2E 63 72 74
Critical:       No
Basic Constraints
Certificate Authority: No
Max Path Length:        Unlimited
Critical:       Yes
Extension
Identifier:     1.3.6.1.4.1.11129.2.4.2
Value: 04 82 01 69 01 67 00 76 00 BB D9 DF BC 1F 8A 71 B5 93 94 23 97 AA 92 7B 47 38 57
95 0A AB 52 E8 1A 90 96 64 36 8E 1E D1 85 00 00 01 70 58 CC A6 45 00 00 04 03 00 47 30
45 02 21 00 DE 66 21 90 07 ED B6 4A 64 0E 88 D1 5C 25 91 8E EF 42 5A 1D 1A CB 72 C2 5B
CB 13 D9 81 2C D1 96 02 20 7E 61 62 D0 56 79 F9 F7 3B B3 00 9C 09 0B 67 87 09 A2 96 5A
78 35 0B AC 9A 37 3D 85 E0 8B AC FE 00 75 00 22 45 45 07 59 55 24 56 96 3F A1 2F F1 F7
6D 86 E0 23 26 63 AD C0 4B 7F 5D C6 83 5C 6E E2 0F 02 00 00 01 70 58 CC A6 84 00 00 04
03 00 46 30 44 02 20 50 21 52 C0 BA 57 13 13 F4 24 03 9D 2A 81 A4 46 D6 D7 B4 65 5E 8F
0F 29 87 32 F0 DD CB 89 2F E0 02 20 41 3D E1 AE 36 16 47 D6 2B 73 1A A9 6E 36 FC FB 9B
8D 0F EF 31 0B 2B 6D 84 DF CD 41 2D 83 D5 A2 00 76 00 51 A3 B0 F5 FD 01 79 9C 56 6D B8
37 78 8F 0C A4 7A CC 1B 27 CB F7 9E 88 42 9A 0D FE D4 8B 05 E5 00 00 01 70 58 CC A6 9D
00 00 04 03 00 47 30 45 02 20 3C CA 51 C3 D7 65 AA 6D 8A 18 01 0E 76 66 F1 91 91 4D 19
62 80 6E 4E 83 3D 22 D2 FE 8C D3 9E A1 02 21 00 EA E8 36 5D C4 35 A8 95 90 BB 93 78 C7
1E 67 5D 10 3C 0D 53 BC B7 F6 2B 67 61 6B D8 6D 3C 83 2E
Critical:       No
Signature
Signature Algorithm:   1.2.840.113549.1.1.11
Signature Parameters: 05 00
Signature:      98 F7 1F 97 97 91 56 25 B5 5B F8 A0 73 C8   AE 45 F8 D6 4A 74 AC 69 CE 3F
DB 0A 4E 04 2E 8E 04 4B 8B 92 F7 21 88 64 69 7F B0 43 24   FB C6 45 FB 3D D9 48 6F A2 62
A8 CB 8C 0A 22 CD 6D 50 31 B2 C6 CF B4 67 B1 BB D8 C4 0C   71 04 8B 73 96 4D 21 49 94 3B
AB D6 CA 15 64 39 31 3F 32 C5 E1 EB DB C4 54 05 D1 39 E1   C4 EB 37 7A 9C 37 27 E4 D1 34
E4 B8 12 26 9A F6 EF 63 AD CA 48 B6 3A E0 78 AB E3 8D 72   6F B7 B5 7F 14 FD AE 1A 80 1B
1F F4 71 24 B4 5D 62 B1 66 D5 71 1B 13 4E DE 9F 8B 6D 77   FE EE 6F C2 1F C0 E3 71 C0 24
BF F0 7E 05 E3 53 A5 FC 60 7E F4 4F C7 30 B4 51 B4 EC C3   A5 CF 0F 75 F0 1D 5E 1E 2A BD
95 80 A1 2D 83 E9 C0 99 65 0A 92 84 C2 E6 09 93 E8 0A B0   C0 ED AD 71 9E 95 74 FD 8F AE
38 6B EE 2A 22 4E 1E D9 E0 26 5C D2 AD 6F E1 75 E5 B7 92 4F 46 5F 0F BA 7C B9 23 E8 1F
```

Se solicita que en base a la información proporcionada responda a los siguientes puntos:

1. ¿ Cual es el sitio web que puede utilizar este certificado ?
2. ¿Cuál es la finalidad principal de configurar este certificado en el servidor web?
3. ¿Puede ser utilizado por tiempo ilimitado? De no ser así indique hasta cuándo puede utilizarse y que ocurrirá con el sitio luego de esa fecha.
4. ¿Con que algoritmo se creó la clave pública de este certificado?

Respuestas

1. El sitio web que puede utilizar este certificado es Mercado Libre (y sus subdominios), específicamente el sitio es mercadolibre.com.ar.
2. La finalidad principal de configurar este certificado en el servidor web es crear un canal de comunicación encriptado, permitiendo que cliente y servidor se transmitan información de forma segura. Además, el certificado permite autenticar la identidad del sitio web, esto permite garantizar a los usuarios o visitantes que no se encuentran en una aplicación o sitio falso.
3. El certificado no puede ser usado por un tiempo ilimitado, ya que el mismo tiene un periodo en el que es válido, y debe ser renovado.

   Este certificado es válido hasta 2020-02-22. Luego de esta fecha, si no se renueva el certificado, lo que ocurrirá es que el certificado y su protocolo serán inválidos. De esta manera, perderá la seguridad de cifrado entre cliente y servidor. Mostrando en el sitio web “Tu conexión con este sitio web no es segura”.
4. El algoritmo utilizado para crear la clave pública de este certificado fue el RSA, con tamaño de 2048 bits.