2.1.

The stream cipher described in Definition 2.1.1 can easily be generalized to work in alphabets other than the binary one. For manual encryption, an especially useful one is a stream cipher that operates on letters.

1. Develop a scheme which operates with the letters A, B,..., Z, represented by the numbers 0,1,...,25. What does the key (stream) look like? What are the encryp- tion and decryption functions?

Answer:

Key stream in this case is a stream of (randomly generated) characters from A, B, .. Z

Encryption function:

Yi = xi + zi mod 26 (zi is randomly generated alphabet between 0, 1, 2, …25)

Decryption function:

Xi = yi - zi mod 26 (zi is randomly generated alphabet between 0, 1, 2, …25)

Have to use '-' in the Decryption function to make sure that after substituting yi in the decryption equation, we get back xi.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

2. Decrypt the following cipher text:

bsaspp kkuosp

which was encrypted using the key:

rsidpy dkawoa

1.Decrypting bsaspp:

For b

Xi = b-r mod 26

= 1-17 mod 26 = -16 mod 26 = 10 mod 26 = 10 = K

For s

Xi = s-s mod 26

= 18-18 mod 26 = 0 = A

For a

Xi = a-i mod 26

= 0-8 mod 26 = 18 mod 26 = 18 = S

For s

Xi = s-d mod 26

= 18-3 mod 26 = 15 mod 26 = 15 = P

For p

Xi = p-p mod 26

= 15-15 mod 26 = 0 = A

For s

Xi = p-y mod 26

= 15-24 mod 26 = 17 mod 26 = 17 = R

Word bsaspp decrypts to Kaspar
1.Decrypting kkuosp

For K
Xi = k-d mod 26
= 10-3 mod 26 = 7 mod 26 = 7 = H
For s
Xi = k-k mod 26
= 10-10 mod 26 = 0 = A
For a
Xi = u-a mod 26
= 20-0 mod 26 = 20 mod 26 = 20 = U
For s
Xi = o-w mod 26
= 14-22 mod 26 = 18 mod 26 = 18 = S
For p
Xi = s-o mod 26
= 18-14 mod 26 = 4 mod 26 = 4 = E
For s
Xi = p-a mod 26
= 15-0 mod 26 = 15 mod 26 = 15 = P

Word kkuosp decrypts to Hausep

Full Name came out to be : Kasper Hausep

3. How was the young man murdered?

Answer : Though the word decrypts to Kaspar Hausep but as per online content available is for Kasper Hauser.
As per https://www.livescience.com/44375-the-mystery-of-kaspar-hauser.html

“ It is widely believed that Hauser stabbed himself (probably for attention) and had simply injured himself more grievously than he had intended.”

2.2. Assume we store a one-time key on a CD-ROM with a capacity of 1 Gbyte. Discuss the real-life implications of a One-Time-Pad (OTP) system. Address issues such as life cycle of the key, storage of the key during the life cycle/after the life cycle, key distribution, generation of the key, etc.

Answer:
Issues:
1. The size of the data that we can encrypt has to be the same as key length. In this case, because we cannot have more than 1 Gbyte of key length, we cannot encrypt more than 1 Gigabyte of data.
2. Another issue is that because the key is stored on CD-ROM, if the CD-ROM is lost or damaged, we might permanently lose access to the data and will never be able to decrypt it.
3. The key must be exchanged and stored securely on both sender and receiver’s side.
4. Generation of the key must be done by a true random number generator algorithm.

2.3. Assume an OTP-like encryption with a short key of 128 bit. This key is then being used periodically to encrypt large volumes of data. Describe how an attack works that breaks this scheme.

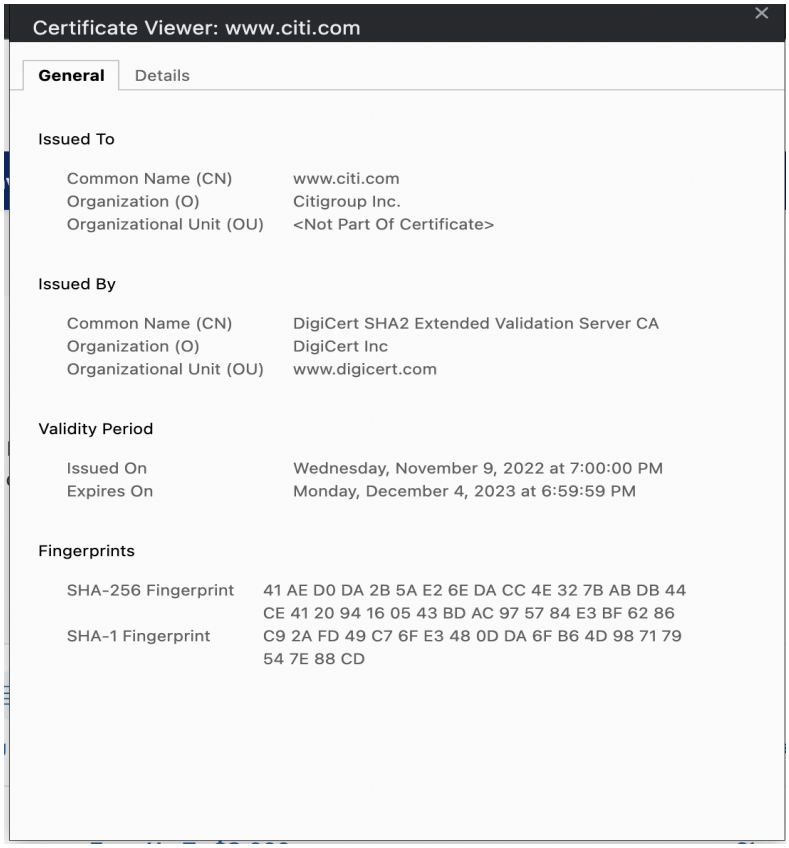
Answer:
In this case, the attacker might use the patterns in the underlying text to recover parts of the key.
Another point is if the attacker knows some part of the plaintext, he might be able to even generate the whole key and decrypt the complete plaintext as well.

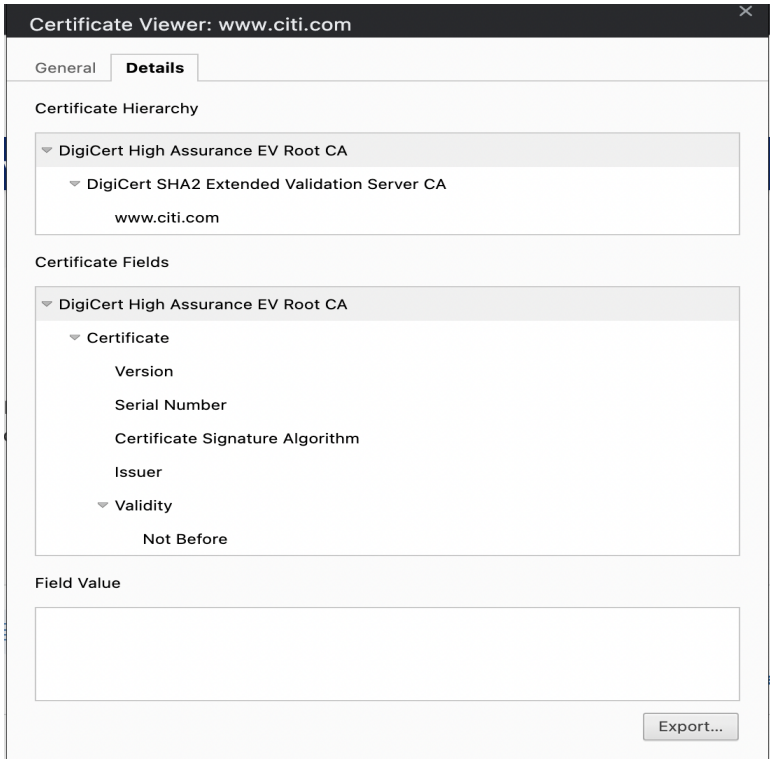
2.4. At first glance it seems as though an exhaustive key search is possible against an OTP system. Given is a short message, let's say 5 ASCII characters represented by 40 bit, which was encrypted using a 40-bit OTP. Explain exactly why an exhaus- tive key search will not succeed even though sufficient computational resources are available. This is a paradox since we know that the OTP is unconditionally secure. That is, explain why a brute-force attack does not work.
Note: You have to resolve the paradox! That means answers such as "The OTP is unconditionally secure and therefore a brute-force attack does not work" are not valid.

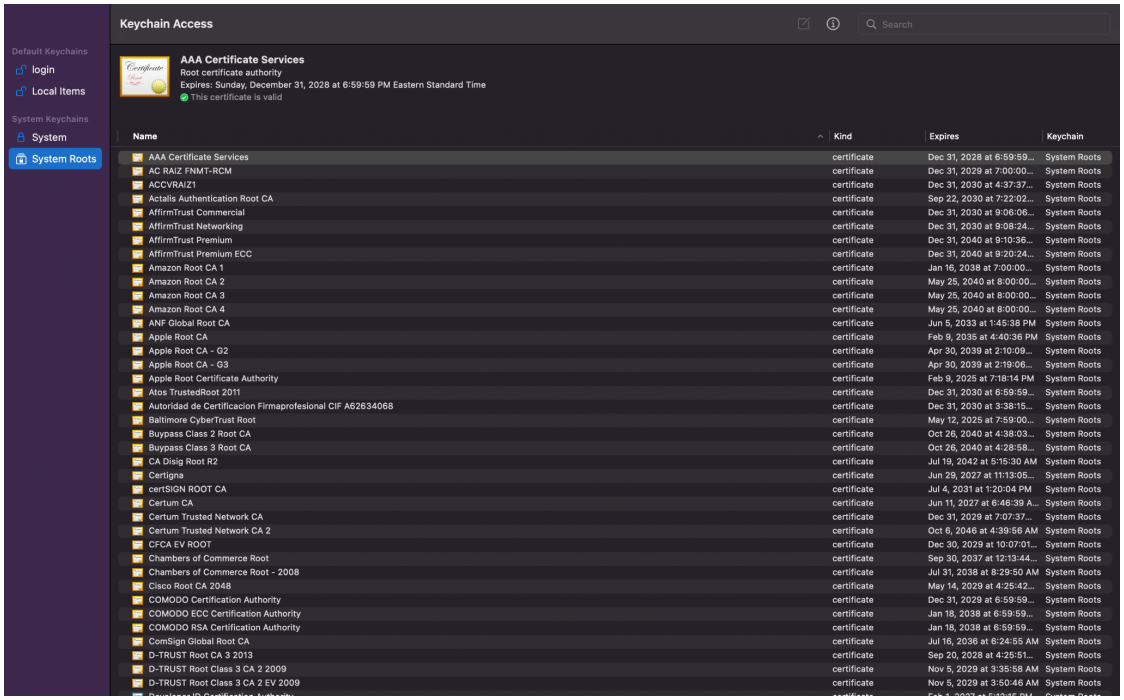
Answer:
One problem with exhaustive key search is that there is no way to know what the right answer is, which means no way to identify the correct key.
With OTP based encryption, there is a 50/50 chance of 0 bit turning into a 0 or 1 and a 50/50 chance of 1 bit turning into a 0 or 1. So, the odds of getting back the plaintext are the worst.

Step 3 Seeing is believing. Let's look at how these actual digital certificates and the trusted root certificate store look through the eyes of Google Chrome.
a. In Google Chrome, go to www.citibank.com.
b. Click the lock at the far left of the URL bar.
c. Click Certificate (Valid).
A window, with tabs, will open up. In the General tab, notice the certificate information. In the Details tab, notice all of the fields and values for the digital certificate. In the Certification Path tab, notice the hierarchy of CAs.
The certificate the website gives the browser is known as a leaf certificate, because it's at the end of the hierarchy, and it is signed by an intermediate CA's certificate. The intermediate CA's certificate is signed by a root certificate. The root certificate is self-signed and is trusted by browsers.
Using this hierarchy, browsers don't have to manage large amounts of root certificates. It enables the root CA to delegate signing to intermediate CAs without sharing the root master signing private key. It also enables the root CA to revoke an intermediate CA's certificate in the event of a mistake or malicious action, instead of revoking the root CA's certificate, which would cause immediate problems in browsers worldwide.
d. Click OK to close the certificate window.
e. At the upper-right corner of the browser window, click the Customize And Control Google Chrome
Button (three vertical dots).
f. Click Settings.
g. In the Privacy And Security section, click Security, and scroll down to the Advanced section.
h. Click Manage Certificates, and then click each tab in the dialog. You're now looking through Chrome's trusted root certificate store, which since Chrome debuted in 2009, always used the root store of the system it was on. On Windows systems, Chrome used the Microsoft Trusted Root Program. On macOS systems, Chrome used the Apple Root Certificate program. It was announced at the end of October 2020 that Chrome has plans in the works to create and use its own dedicated certificate root store.
Read this for further details: www.zdnet.com/article/chrome-will-soon-have-its-own-dedicated-certificate-root-store/

Answer:
Certificate Screenshot:


Certificate Viewer: www.citi.com
General
Details
Issued To
Common Name (CN) www.citi.com
Organization (O) Citigroup Inc.
Organizational Unit (OU) <Not Part Of Certificate>
Issued By
Common Name (CN) DigiCert SHA2 Extended Validation Server CA
Organization (O) DigiCert Inc
Organizational Unit (OU) www.digicert.com
Validity Period
Issued On Wednesday, November 9, 2022 at 7:00:00 PM
Expires On Monday, December 4, 2023 at 6:59:59 PM
Fingerprints
SHA-256 Fingerprint 41 AE D0 DA 2B 5A E2 6E DA CC 4E 32 7B AB DB 44 CE 41 20 94 16 05 43 BD AC 97 57 84 E3 BF 62 86
SHA-1 Fingerprint C9 2A FD 49 C7 6F E3 48 0D DA 6F B6 4D 98 71 79 54 7E 88 CD

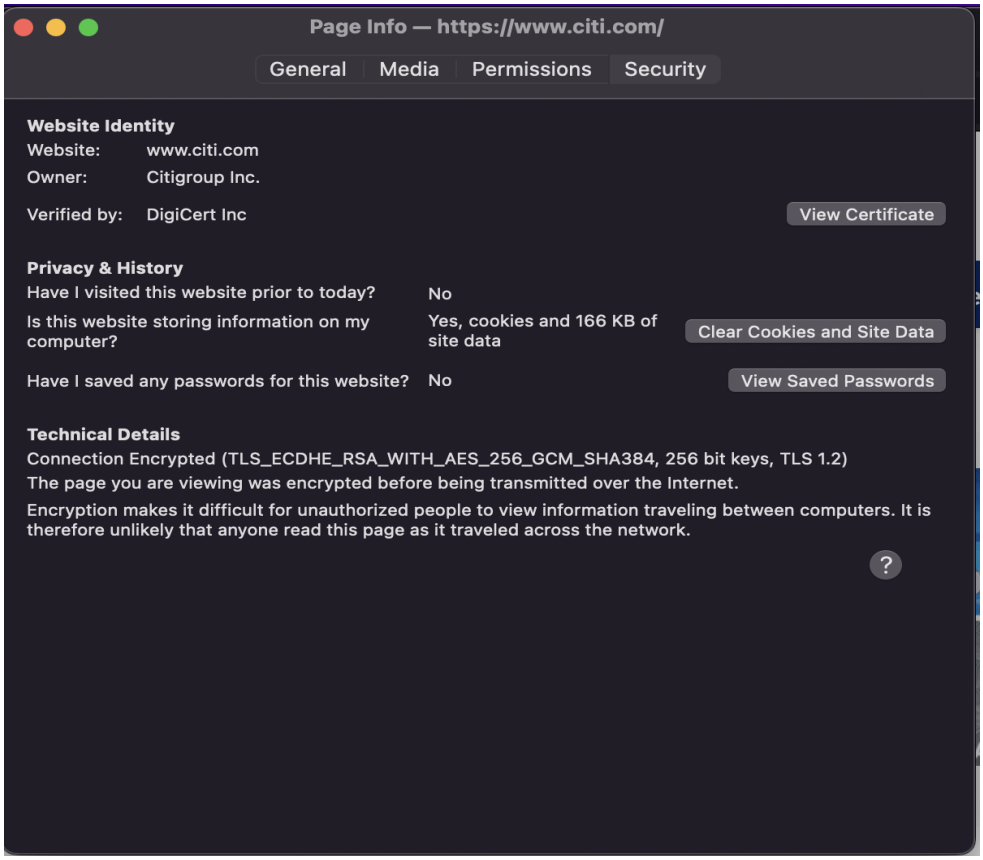

Certificate Viewer: www.citi.com
General
Details
Certificate Hierarchy
DigiCert High Assurance EV Root CA
DigiCert SHA2 Extended Validation Server CA
www.citi.com
Certificate Fields
DigiCert High Assurance EV Root CA
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before
Field Value
Export...

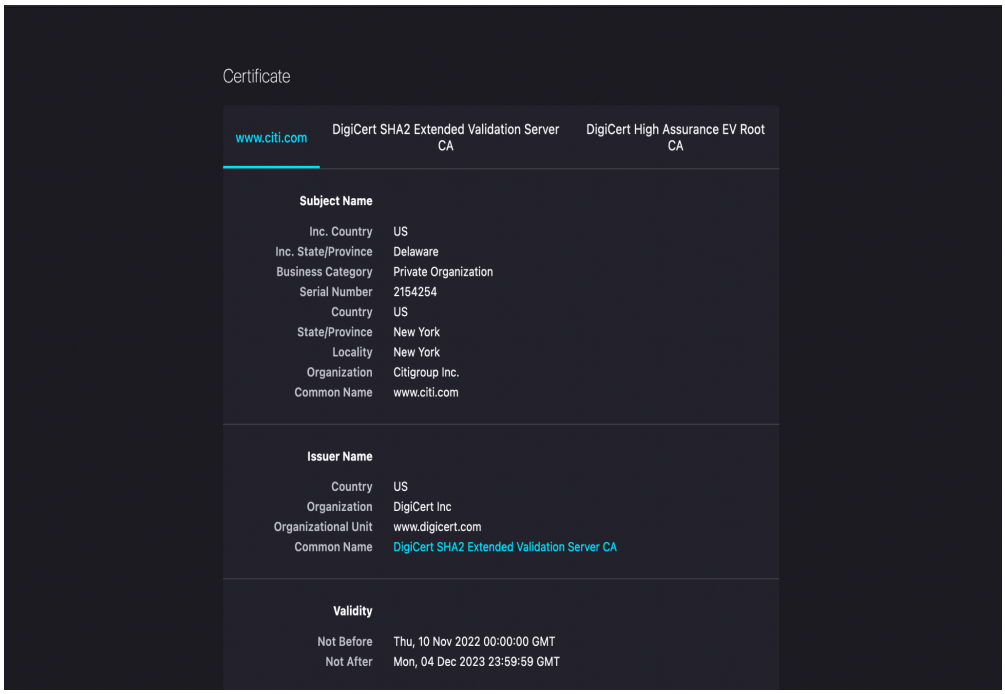


Step 4 Now let's look at how digital certificates and the trusted root certificate store look through the eyes of Mozilla Firefox.

a. In Mozilla Firefox, go to www.citibank.com.
b. Click the lock at the far left of the URL bar.
c. Click the arrow near Connection Secure.
d. Click More Information.
e. Click the View Certificate button.
f. Go through the information in all three tabs, which includes information about the certificate, the CA, and that CA's root.
g. On the upper-right corner of the browser window, click the Open menu button (three horizontal lines).
h. Click Options.
i. In the pane at the left, click Privacy & Security.
j. Scroll all the way down, and in the Certificates section, click the View Certificates... button.
k. Click each tab at the top. You're now looking through Firefox's trusted root certificate store.

Answer:


Page Info — https://www.citi.com/
General
Media
Permissions
Security
Website Identity
Website: www.citi.com
Owner: Citigroup Inc.
Verified by: DigiCert Inc
View Certificate
Privacy & History
Have I visited this website prior to today? No
Is this website storing information on my computer? Yes, cookies and 166 KB of site data
Clear Cookies and Site Data
Have I saved any passwords for this website? No
View Saved Passwords
Technical Details
Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256 bit keys, TLS 1.2)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.
?


Certificate
www.citi.com
DigiCert SHA2 Extended Validation Server CA
DigiCert High Assurance EV Root CA
Subject Name
Inc. Country US
Inc. State/Province Delaware
Business Category Private Organization
Serial Number 2154254
Country US
State/Province New York
Locality New York
Organization Citigroup Inc.
Common Name www.citi.com
Issuer Name
Country US
Organization DigiCert Inc
Organizational Unit www.digicert.com
Common Name DigiCert SHA2 Extended Validation Server CA
Validity
Not Before Thu, 10 Nov 2022 00:00:00 GMT
Not After Mon, 04 Dec 2023 23:59:59 GMT

Subject Alt Names

DNS Name	www.citi.com
DNS Name	prod.report.nacustomerexperience.citi.com
DNS Name	www2.citibank.com
DNS Name	www1.citibank.com
DNS Name	www.creditcards.citi.com
DNS Name	www.citiretailservices.com
DNS Name	www.citigroup.com
DNS Name	www.citibank.com
DNS Name	www.citibank.co.uk
DNS Name	oncampus.citi.com
DNS Name	icg.citi.com
DNS Name	creditcards.citi.com
DNS Name	ccsi.citi.com

Public Key Info

Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	C6:1C:25:01:51:50:3F:6C:D6:81:06:6A:99:4E:1E:CE:5C:2D:D2:9F:42:3D:...

Miscellaneous

Serial Number	09:4C:4E:6A:CB:B9:9D:AD:35:CF:BC:59:49:40:79:B0
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Fingerprints

SHA-256	41:AE:D0:DA:2B:5A:E2:6E:DA:CC:4E:32:7B:AB:DB:44:CE:41:20:94:16:05...
SHA-1	C9:2A:FD:49:C7:6F:E3:48:0D:DA:6F:B6:4D:98:71:79:54:7E:88:CD

Basic Constraints

Certificate Authority	No

Key Usages

Purposes	Digital Signature, Key Encipherment

Extended Key Usages

Purposes	Server Authentication, Client Authentication

Subject Key ID

Key ID	36:97:19:71:8E:2F:4C:5D:A7:E7:95:6F:A0:38:36:49:0F:ED:BC:2C

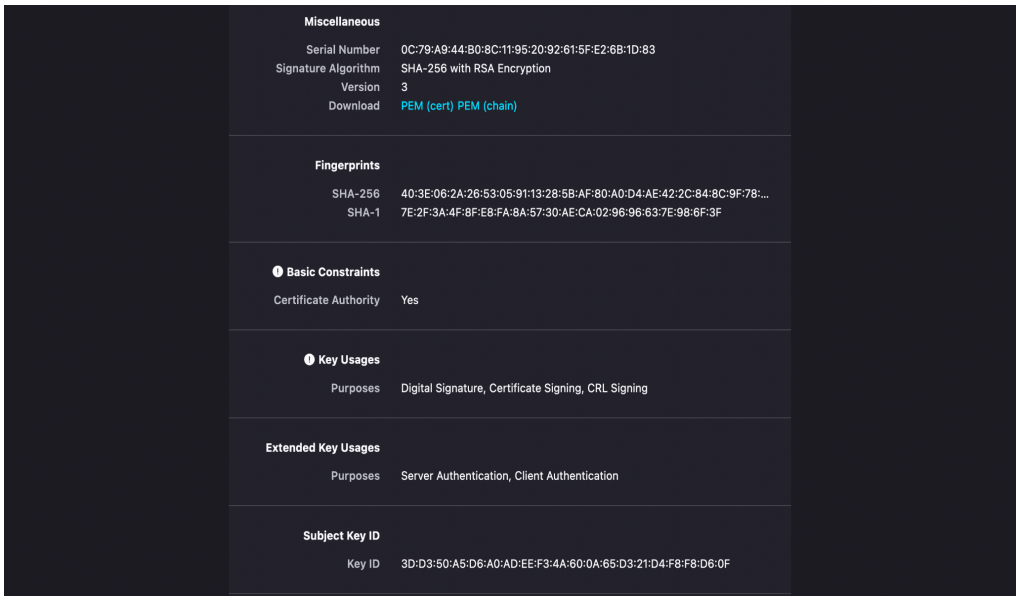
Authority Key ID

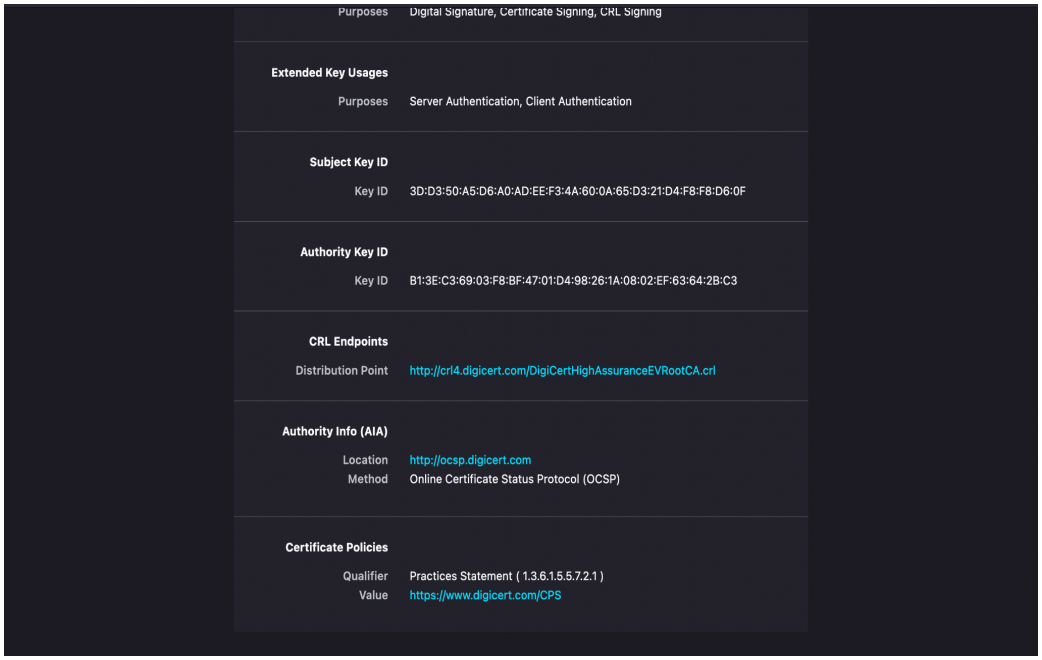
Key ID	3D:D3:50:A5:D6:A0:AD:EE:F3:4A:60:0A:65:D3:21:D4:F8:F8:D6:0F

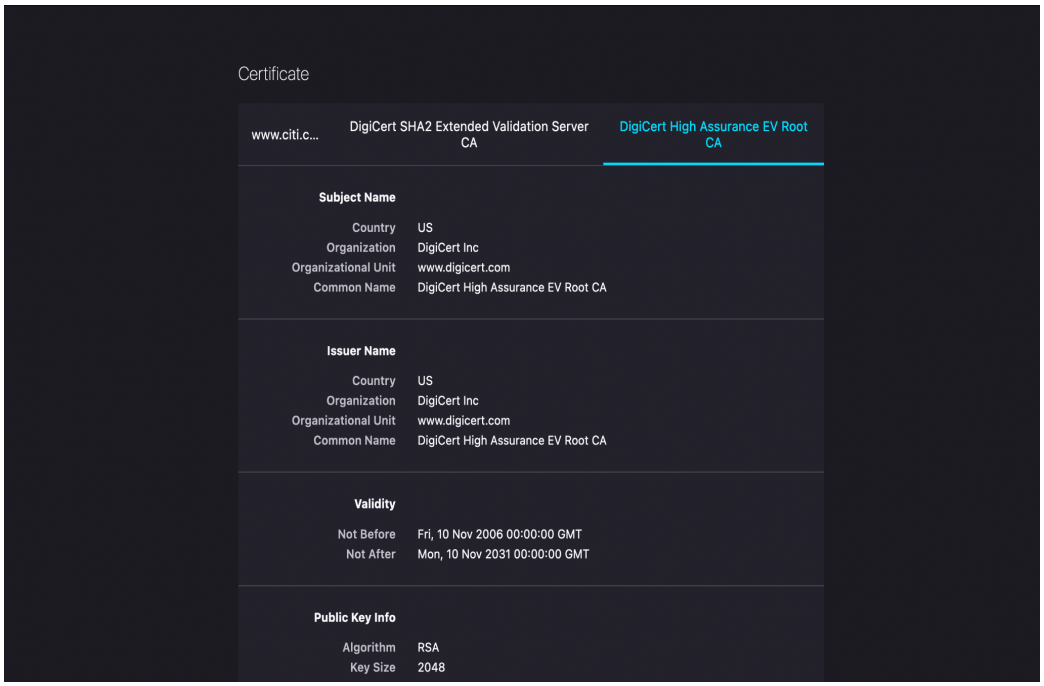
CRL Endpoints

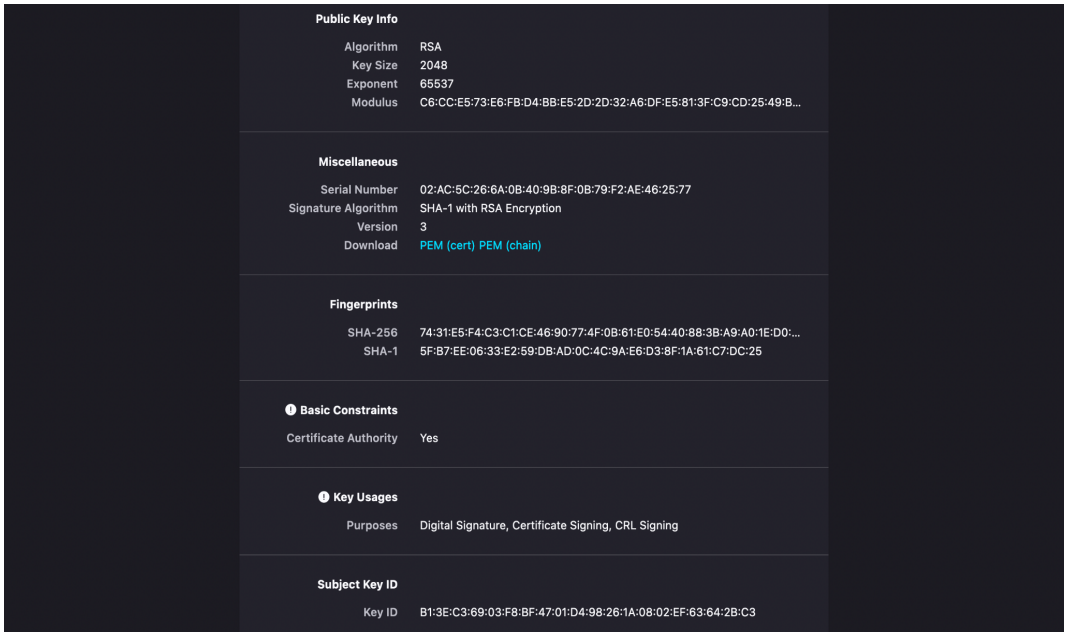
Distribution Point	http://crl3.digicert.com/sha2-ev-server-g3.crl
Distribution Point	http://crl4.digicert.com/sha2-ev-server-g3.crl

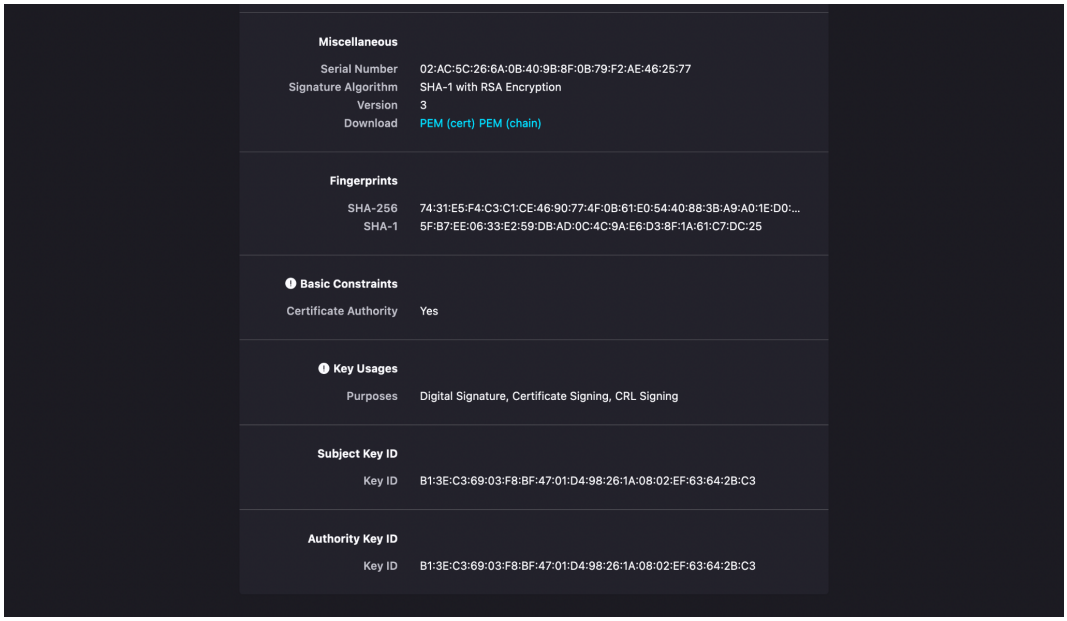

www.citi.c...
DigiCert SHA2 Extended Validation Server CA
DigiCert High Assurance EV Root CA
Subject Name
Country US
Organization DigiCert Inc
Organizational Unit www.digicert.com
Common Name DigiCert SHA2 Extended Validation Server CA
Issuer Name
Country US
Organization DigiCert Inc
Organizational Unit www.digicert.com
Common Name DigiCert High Assurance EV Root CA
Validity
Not Before Tue, 22 Oct 2013 12:00:00 GMT
Not After Sun, 22 Oct 2028 12:00:00 GMT
Public Key Info
Algorithm RSA
Key Size 2048
Exponent 65537
Modulus D7:53:A4:04:51:F8:99:A6:16:48:4B:67:27:AA:93:49:D0:39:ED:0C:B0:B0...

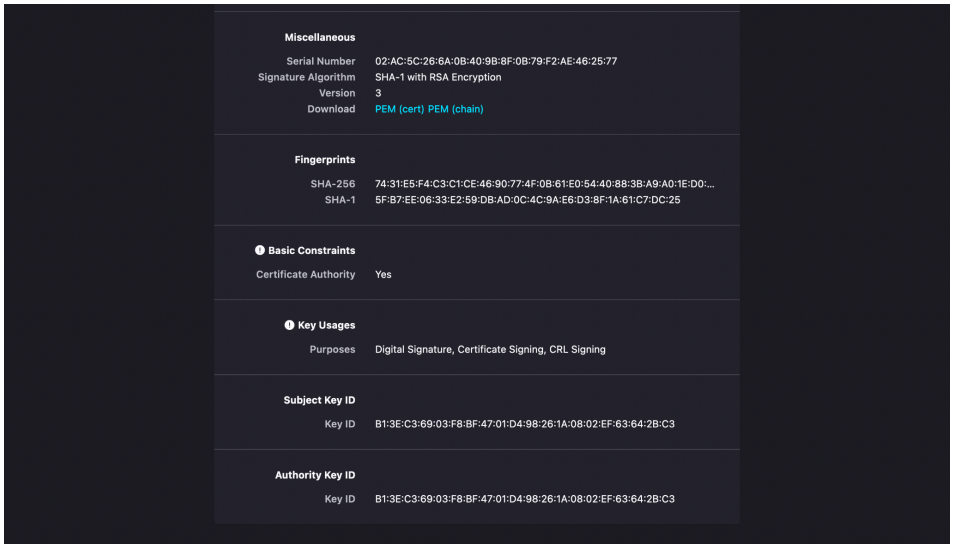

Miscellaneous
Serial Number 0C:79:A9:44:B0:8C:11:95:20:92:61:5F:E2:6B:1D:83
Signature Algorithm SHA-256 with RSA Encryption
Version 3
Download PEM (cert) PEM (chain)
Fingerprints
SHA-256 40:3E:06:2A:26:53:05:91:13:28:5B:AF:80:A0:D4:AE:42:2C:84:8C:9F:78:...
SHA-1 7E:2F:3A:4F:8F:E8:FA:8A:57:30:AE:CA:02:96:96:63:7E:98:6F:3F
Basic Constraints
Certificate Authority Yes
Key Usages
Purposes Digital Signature, Certificate Signing, CRL Signing
Extended Key Usages
Purposes Server Authentication, Client Authentication
Subject Key ID
Key ID 3D:D3:50:A5:D6:A0:AD:EE:F3:4A:60:0A:65:D3:21:D4:F8:F8:D6:0F

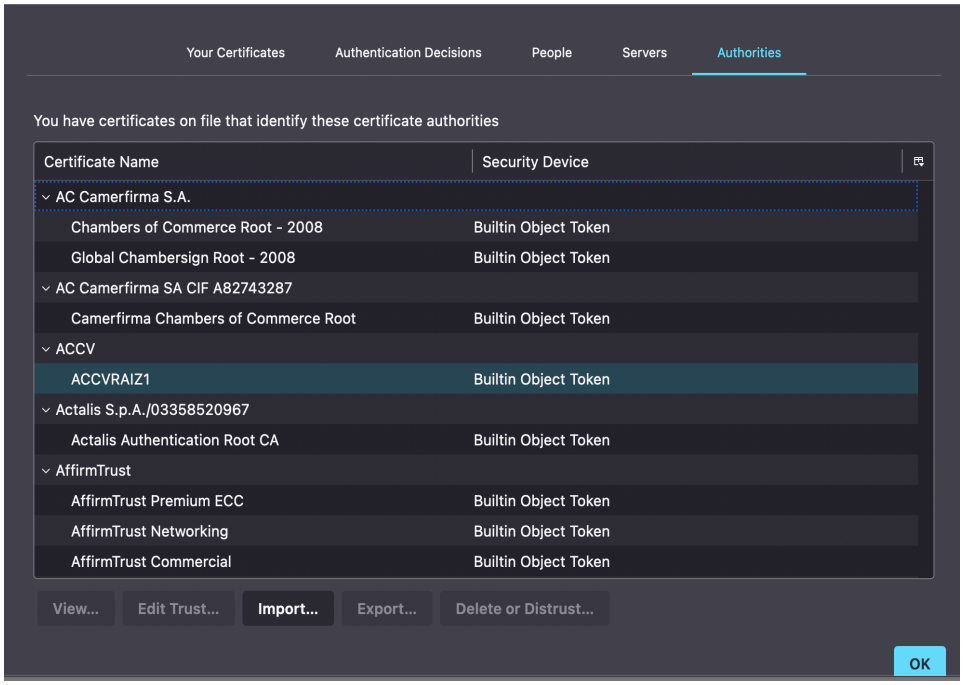

Purposes
Digital Signature, Certificate Signing, CRL Signing
Extended Key Usages
Purposes
Server Authentication, Client Authentication
Subject Key ID
Key ID
3D:D3:50:A5:D6:A0:AD:EE:F3:4A:60:0A:65:D3:21:D4:F8:F8:D6:0F
Authority Key ID
Key ID
B1:3E:C3:69:03:F8:BF:47:01:D4:98:26:1A:08:02:EF:63:64:2B:C3
CRL Endpoints
Distribution Point
http://crl4.digicert.com/DigiCertHighAssuranceEVRootCA.crl
Authority Info (AIA)
Location
http://ocsp.digicert.com
Method
Online Certificate Status Protocol (OCSP)
Certificate Policies
Qualifier
Practices Statement (1.3.6.1.5.5.7.2.1)
Value
https://www.digicert.com/CPS

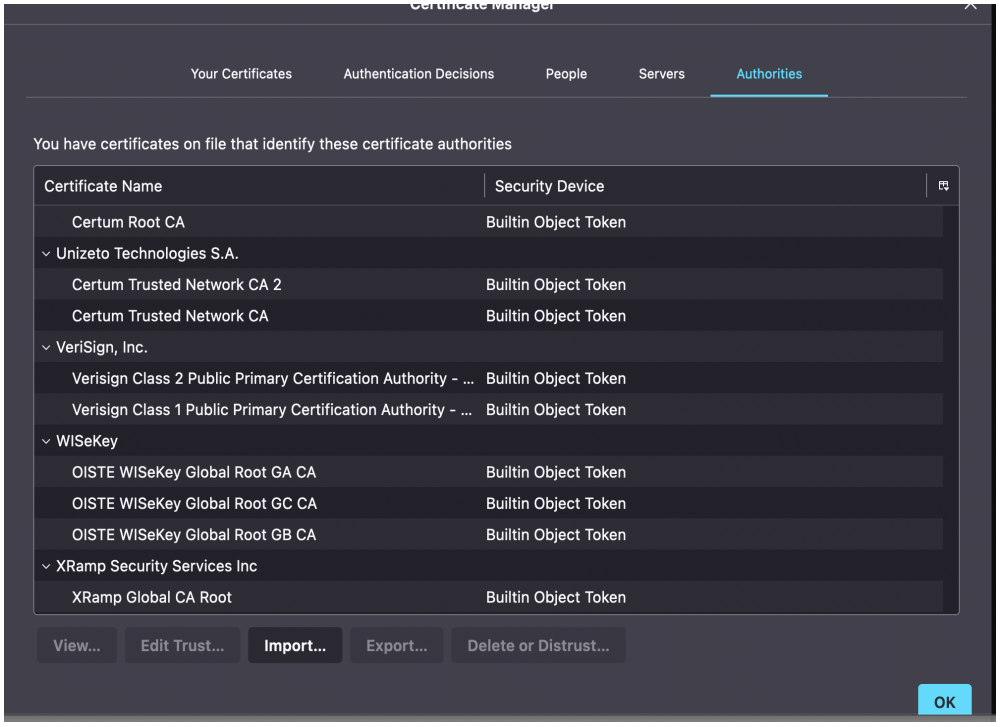

Certificate
www.citi.c...
DigiCert SHA2 Extended Validation Server CA
DigiCert High Assurance EV Root CA
Subject Name
Country
US
Organization
DigiCert Inc
Organizational Unit
www.digicert.com
Common Name
DigiCert High Assurance EV Root CA
Issuer Name
Country
US
Organization
DigiCert Inc
Organizational Unit
www.digicert.com
Common Name
DigiCert High Assurance EV Root CA
Validity
Not Before
Fri, 10 Nov 2006 00:00:00 GMT
Not After
Mon, 10 Nov 2031 00:00:00 GMT
Public Key Info
Algorithm
RSA
Key Size
2048

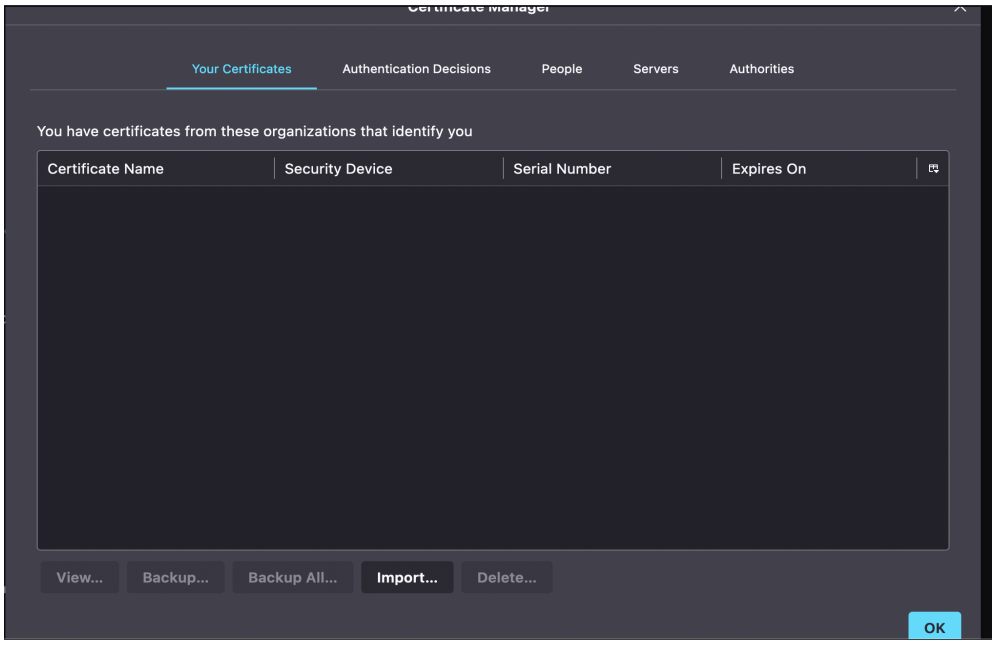

Public Key Info
Algorithm RSA
Key Size 2048
Exponent 65537
Modulus C6:CC:E5:73:E6:FB:D4:BB:E5:2D:2D:32:A6:DF:E5:81:3F:C9:CD:25:49:B...
Miscellaneous
Serial Number 02:AC:5C:26:6A:0B:40:9B:8F:0B:79:F2:AE:46:25:77
Signature Algorithm SHA-1 with RSA Encryption
Version 3
Download PEM (cert) PEM (chain)
Fingerprints
SHA-256 74:31:E5:F4:C3:C1:CE:46:90:77:4F:0B:61:E0:54:40:88:3B:A9:A0:1E:D0:...
SHA-1 5F:B7:EE:06:33:E2:59:DB:AD:0C:4C:9A:E6:D3:8F:1A:61:C7:DC:25
Basic Constraints
Certificate Authority Yes
Key Usages
Purposes Digital Signature, Certificate Signing, CRL Signing
Subject Key ID
Key ID B1:3E:C3:69:03:F8:BF:47:01:D4:98:26:1A:08:02:EF:63:64:2B:C3

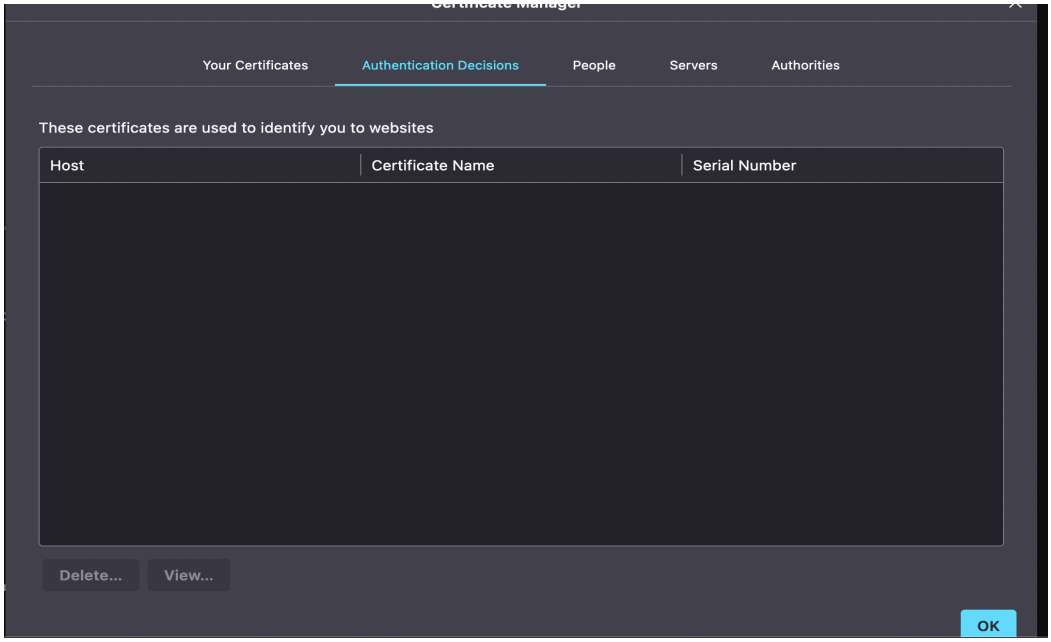

Miscellaneous
Serial Number 02:AC:5C:26:6A:0B:40:9B:8F:0B:79:F2:AE:46:25:77
Signature Algorithm SHA-1 with RSA Encryption
Version 3
Download PEM (cert) PEM (chain)
Fingerprints
SHA-256 74:31:E5:F4:C3:C1:CE:46:90:77:4F:0B:61:E0:54:40:88:3B:A9:A0:1E:D0:...
SHA-1 5F:B7:EE:06:33:E2:59:DB:AD:0C:4C:9A:E6:D3:8F:1A:61:C7:DC:25
Basic Constraints
Certificate Authority Yes
Key Usages
Purposes Digital Signature, Certificate Signing, CRL Signing
Subject Key ID
Key ID B1:3E:C3:69:03:F8:BF:47:01:D4:98:26:1A:08:02:EF:63:64:2B:C3
Authority Key ID
Key ID B1:3E:C3:69:03:F8:BF:47:01:D4:98:26:1A:08:02:EF:63:64:2B:C3

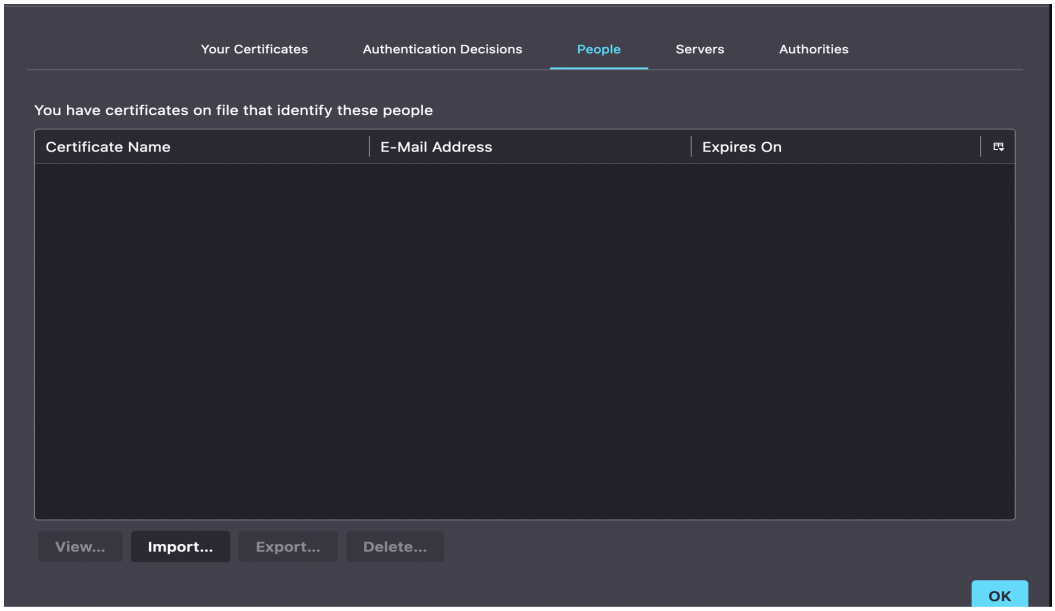

Miscellaneous
Serial Number 02:AC:5C:26:6A:0B:40:9B:8F:0B:79:F2:AE:46:25:77
Signature Algorithm SHA-1 with RSA Encryption
Version 3
Download PEM (cert) PEM (chain)
Fingerprints
SHA-256 74:31:E5:F4:C3:C1:CE:46:90:77:4F:0B:61:E0:54:40:88:3B:A9:A0:1E:D0:...
SHA-1 5F:B7:EE:06:33:E2:59:DB:AD:0C:4C:9A:E6:D3:8F:1A:61:C7:DC:25
Basic Constraints
Certificate Authority Yes
Key Usages
Purposes Digital Signature, Certificate Signing, CRL Signing
Subject Key ID
Key ID B1:3E:C3:69:03:F8:BF:47:01:D4:98:26:1A:08:02:EF:63:64:2B:C3
Authority Key ID
Key ID B1:3E:C3:69:03:F8:BF:47:01:D4:98:26:1A:08:02:EF:63:64:2B:C3

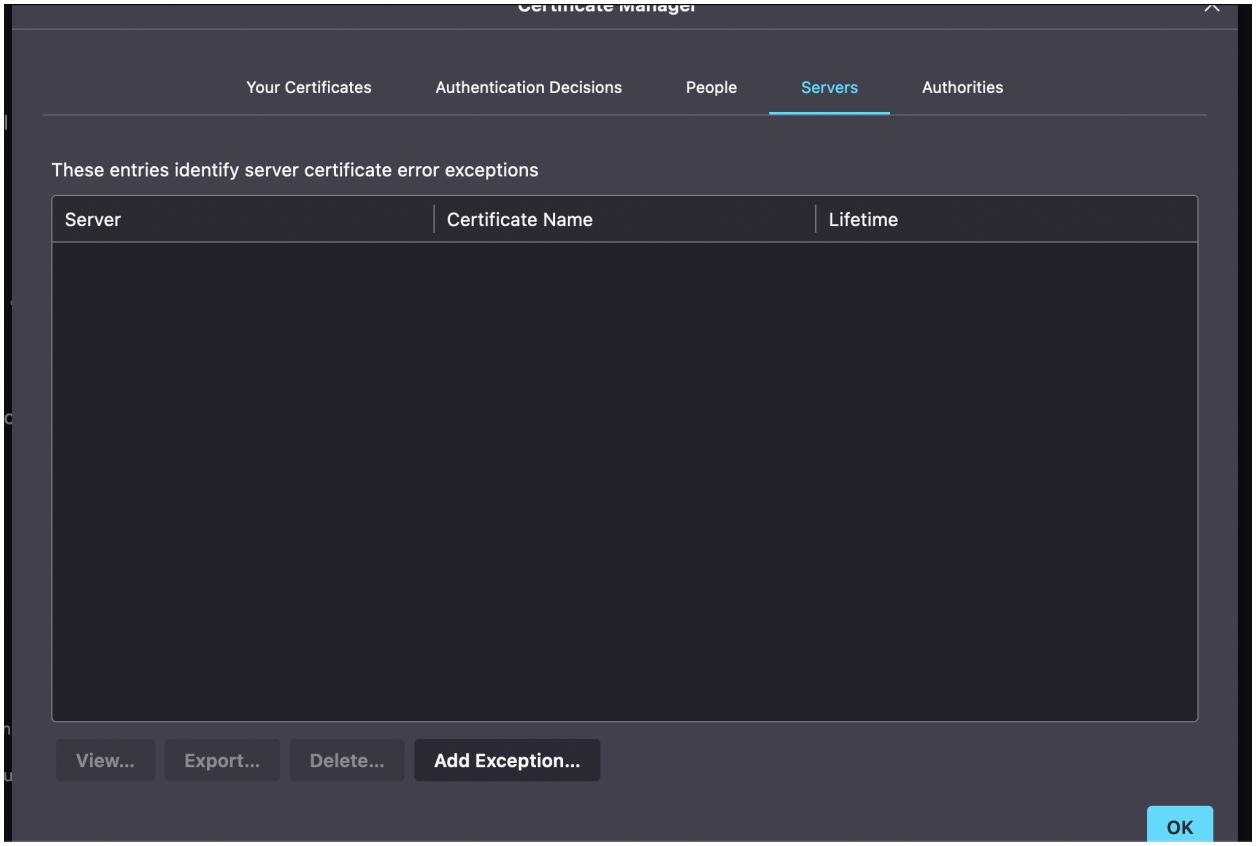

Your Certificates
Authentication Decisions
People
Servers
Authorities
You have certificates on file that identify these certificate authorities
Certificate Name
Security Device
AC Camerfirma S.A.
Chambers of Commerce Root - 2008 Builtin Object Token
Global Chambersign Root - 2008 Builtin Object Token
AC Camerfirma SA CIF A82743287
Camerfirma Chambers of Commerce Root Builtin Object Token
ACCV
ACCVRAIZ1 Builtin Object Token
Actalis S.p.A./03358520967
Actalis Authentication Root CA Builtin Object Token
AffirmTrust
AffirmTrust Premium ECC Builtin Object Token
AffirmTrust Networking Builtin Object Token
AffirmTrust Commercial Builtin Object Token
View...
Edit Trust...
Import...
Export...
Delete or Distrust...
OK


Certificate Manager
Your Certificates
Authentication Decisions
People
Servers
Authorities
You have certificates on file that identify these certificate authorities
Certificate Name
Security Device
Certum Root CA
Builtin Object Token
Unizeto Technologies S.A.
Certum Trusted Network CA 2
Builtin Object Token
Certum Trusted Network CA
Builtin Object Token
VeriSign, Inc.
Verisign Class 2 Public Primary Certification Authority - ...
Builtin Object Token
Verisign Class 1 Public Primary Certification Authority - ...
Builtin Object Token
WISeKey
OISTE WISeKey Global Root GA CA
Builtin Object Token
OISTE WISeKey Global Root GC CA
Builtin Object Token
OISTE WISeKey Global Root GB CA
Builtin Object Token
XRamp Security Services Inc
XRamp Global CA Root
Builtin Object Token
View...
Edit Trust...
Import...
Export...
Delete or Distrust...
OK


Certificate Manager
Your Certificates
Authentication Decisions
People
Servers
Authorities
You have certificates from these organizations that identify you
Certificate Name
Security Device
Serial Number
Expires On
View...
Backup...
Backup All...
Import...
Delete...
OK


Your Certificates
Authentication Decisions
People
Servers
Authorities
These certificates are used to identify you to websites
Host
Certificate Name
Serial Number
Delete...
View...
OK


Your Certificates
Authentication Decisions
People
Servers
Authorities
You have certificates on file that identify these people
Certificate Name
E-Mail Address
Expires On
View...
Import...
Export...
Delete...
OK


Certificate Manager
Your Certificates
Authentication Decisions
People
Servers
Authorities
These entries identify server certificate error exceptions
Server
Certificate Name
Lifetime
View...
Export...
Delete...
Add Exception...
OK