Certificates

Applied Cryptography

NETS1035 APPLIED CRYPTOGRAPHY - DENNIS SIMPSON ©2020

Introduction

Random Numbers

Symmetric Encryption

Asymmetric Encryption

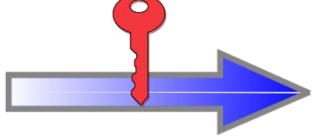
Disk Encryption



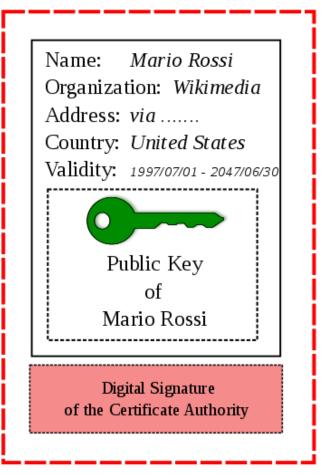
Identity Information and Public Key of Mario Rossi

Name: Mario Rossi Organization: Wikimedia Address: via Country: United States Public Key of Mario Rossi

Certificate Authority verifies the identity of Mario Rossi and encrypts with its Private Key



Certificate of Mario Rossi



Digitally Signed by Certificate Authority

https://en.wikipedia.org/wiki/Public_key_certificate

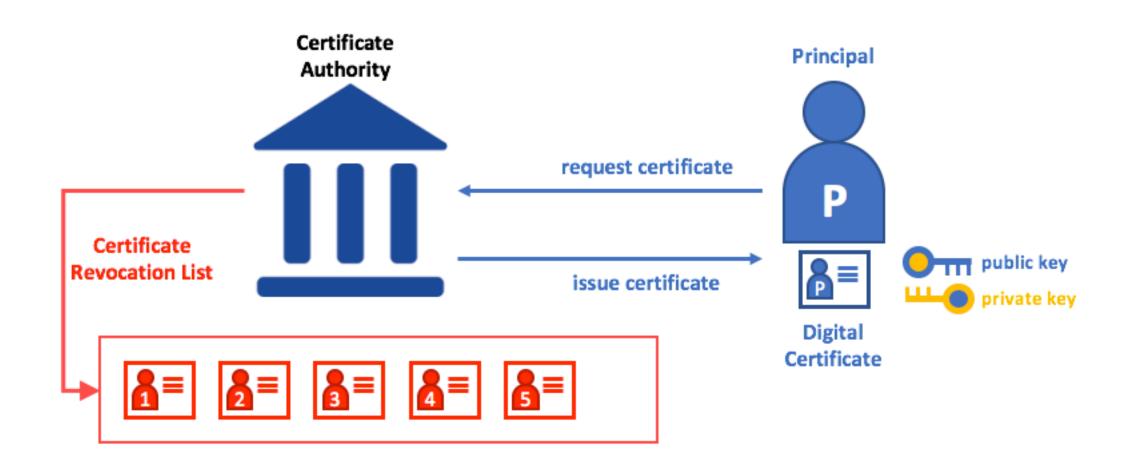
NETS1035 APPLIED CRYPTOGRAPHY - DENNIS SIMPSON ©2020

Public Key Certificates

- A public key certificate (commonly just called a "certificate") is used to provide identification and trust by associating a public key with the subject identified by the certificate (the certificate holder)
- Certificates
 - contents are defined by the X.509 ITU standard
 - describe the identity of a subject, which contains several possible pieces of data including the Common Name (CN) which for a web certificate would be a domain name
 - can be tagged for various allowed uses, such as server certificates, client certificates, signing certificates, etc. with the difference being what the certificate is to be used for, and what is expected to be in the subject information stored in the certificate
 - include a signature from the CA that issued the certificate and guarantees it is valid
 - are tagged to show what identity verification has been done by the certificate issuer
 - have an expiry date and cannot be altered once issued, a new certificate must be issued when an old one expires in order to continue securing communications with that subject

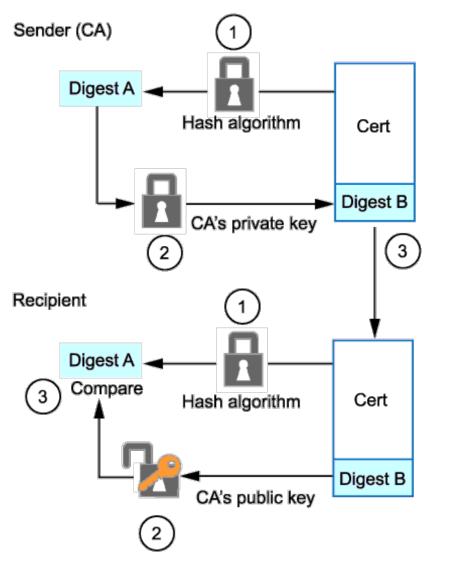






https://hyperledger-fabric.readthedocs.io/en/release-2.0/identity/identity.html

- Using a hash algorithm, the CA generates digest A from the certificate.
- 2. Using the private key, the CA encrypts digest A. The result is digest B, the digital signature.
- The CA sends the digitally signed certificate to the person who requested it.
- Using a hash algorithm, the recipient generates digest A from the certificate.
- Using the CA's public key, the recipient decrypts digest B.
- 3. The recipient compares digest A with digest B. If they match, the recipient knows that the certificate has not been tampered with



https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-digital-certificates-with-pki-overview.html

NETS1035 APPLIED CRYPTOGRAPHY - DENNIS SIMPSON ©2020

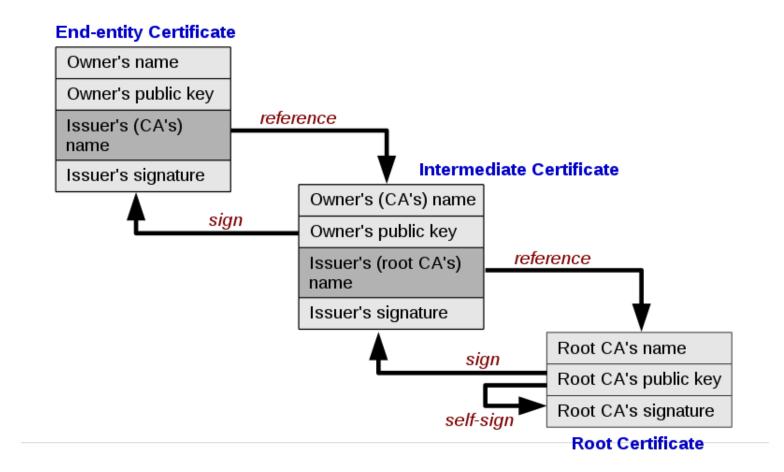
Authorities

- Certificate Authorities (CAs) issue certificates in response to validated certificate signing requests
- Validation of a request may be done by a registration authority or may be done by the same organization that will issue the certificate to the requestor
- An issued certificate will be signed digitally by the CA issuing it so that the public can have confidence that the certificate is valid based on their trust of the CA

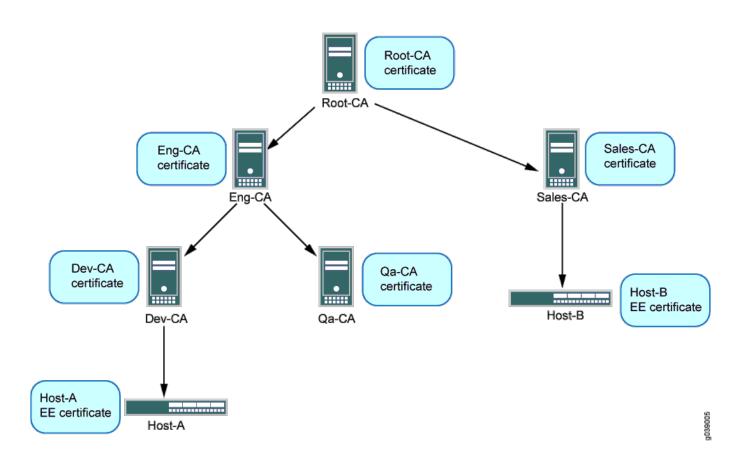


CA Certificates

- A set of CA certificates is included with the operating system
- Root certificates contain the identity information for the CA and the public key of the CA
- The public keys are used to verify CA signatures in other certificates
- CA root certificates are self-signed which is why they are pre-installed as trusted by the operating system and/or specific applications
- May use a chain of authority to increase confidence that the CA is trustworthy
- CAs may cross-sign each other's authority certificates



https://en.wikipedia.org/wiki/Public_key_certificate



https://www.juniper.net/documentation/en_US/junos/topics/example/security-pki-device-certificate-chain-configuring-mx.html

NETS1035 APPLIED CRYPTOGRAPHY - DENNIS SIMPSON ©2020

Chain of Trust

- CA may use a hierarchy of certificates
- Roots may sign intermediate authority certificates
- For a 2-level hierarchy, the intermediates sign the certificate requests that come from the registration authorities
- For a 3-level hierarchy, the intermediates sign further intermediates which sign certificate requests that come from the registration authorities

Certificate Store

- Root certificates and intermediate signing authority certificates are placed in a storage location on the system where they will be used called the certificate store
- Trusted self-signed certificates are placed in a certificate store (as in storage location, not as in buying certificates)
- The certificate store is created when the system is installed
- Where they are stored is operating-system specific, and can also be OS version specific
- openssl can be used to verify if a certificate is trusted

openssl verify -in certfilename.crt

Linux Certificate Store

- Ubuntu installs them as part of the ca-certificates package
- The certificates are kept in /usr/share/ca-certificates
- Certificate files are stored in subdirectories below that to organize them based on how they were approved to be included
- Certificates can be added or removed at your discretion by adding or removing the files and managing the list of enabled certificates with dpkg-reconfigure ca-certificates
- Debian-derived distros use /etc/ssl (/etc/pki/tls for Redhat-derived distros) to hold certificate and key files
- There are links to the root certificates placed in a certs subdirectory, and you can add non-root certificates that are trusted to the certs subdirectory
- Private keys for use on a particular system are placed in a private subdirectory



Windows Certificate Store

- Windows stores them in multiple places dependent on multiple factors but there is a set of them stored in the registry
- If you want to add or remove a root certificate in Windows, you may have to do more than add it to, or remove it from, the registry
- The Windows certificate store is designed to be managed using GUI certificate tools, and is a bit tricky to try to work with, particularly if you are not just using a simple desktop machine
- There are multiple stores, and how they get used depends on the os version, the system config, active directory use, what browser you are using, etc.
- See <u>https://docs.microsoft.com/en-us/windows/win32/seccrypto/system-store-locations</u> for more information





CategoryCategoryCategoryAffirmTrust PremiumCoertificateDec 31, 2028 at 6:59:59SystemCategoryAffirmTrust CommercialcertificateDec 31, 2030 at 9:06:06SystemAffirmTrust NetworkingcertificateDec 31, 2030 at 9:06:06SystemAffirmTrust NetworkingcertificateDec 31, 2030 at 9:06:24SystemAffirmTrust NetworkingcertificateDec 31, 2040 at 9:10:36SystemAffirmTrust PremiumCertificateDec 31, 2040 at 9:00:24SystemAll ItemsAffirmTrust Premium ECCcertificateDec 31, 2040 at 9:00:24SystemSecure NotesAmazon Root CA 1certificateMay 25, 2040 at 8:00:00SystemMy CertificatesAmazon Root CA 2certificateMay 25, 2040 at 8:00:00SystemAmazon Root CA 3certificateMay 25, 2040 at 8:00:00SystemAmazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemAmazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemAmazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemApple Root CA - G2certificateApp 25, 2040 at 8:00:00SystemApple Root CA - G2certificateApp 20:33 at 1:45:38 PMSystemApple Root CA - G2certificateApp 20:39 at 2:10:09					earch
CategoryAAA Certificate ServicescertificateDec 31, 2028 at 6:59:59SystemCategoryActalis Authentication Root CAcertificateSep 22, 2030 at 7:22:02SystemAdmin-Root-CAcertificateNov 10, 2021 at 2:51:07 AMSystemAdmin-Root-CAcertificateDec 31, 2030 at 9:06:06SystemAdmin-Root-CAcertificateDec 31, 2030 at 9:06:06SystemAffirmTrust CommercialcertificateDec 31, 2040 at 9:10:36SystemAffirmTrust PremiumcertificateDec 31, 2040 at 9:10:36SystemAll ItemsAmazon Root CA 1certificateDec 31, 2040 at 9:20:24SystemSecure NotesAmazon Root CA 1certificateMay 25, 2040 at 8:00:00SystemMy CertificatesAmazon Root CA 3certificateMay 25, 2040 at 8:00:00SystemMy CertificatesAmazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemMy CertificatesAnazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemMy CertificatesAnazon Root CA 62certificateMay 25, 2040 at 8:00:00SystemApple Root CA - G2certificateApple 3, 2039 at 2:10:09SystemApple Root CA - G2certificateAppl 3, 2039 at 2:10:09SystemApple Root CA - G2certificateApp 3, 2039 at 2:10:09SystemApple Root CA - G3certificateApp 3, 2039 at 2:10:09SystemApple Root CA - G3certificateApp 3, 2039	 Iogin iCloud Gystem 	Certificate Root certificate authority Expires: Sunday, December 31, 2028 at 6:59:59 PM Eastern Standard Time			
CategoryCategoryCatificateDec 31, 2029 at 7:00:00SystemCategoryAffirmTrust CommercialcertificateDec 31, 2030 at 9:08:06SystemAffirmTrust NetworkingcertificateDec 31, 2030 at 9:08:06SystemAffirmTrust NetworkingcertificateDec 31, 2030 at 9:08:24SystemAffirmTrust PremiumcertificateDec 31, 2040 at 9:00:06SystemAffirmTrust Premium ECCcertificateDec 31, 2040 at 9:20:24SystemAmazon Root CA 1certificateDec 31, 2040 at 9:20:24SystemAmazon Root CA 2certificateMay 25, 2040 at 8:00:00SystemSecure NotesAmazon Root CA 3certificateMay 25, 2040 at 8:00:00SystemMy CertificatesAmazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemMy CertificatesAmazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemAmazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemMy CertificatesApple Root CA - G2certificateMay 25, 2040 at 8:00:00SystemApple Root CA - G2certificateApr 30, 2039 at 2:10:09SystemApple Root CA - G3certificateApr 30, 2039 at 2:19:06System		Name	^ Kind	Expires	Keychain
CategorySystemCategoryAffirmTrust CommercialcertificateDec 31, 2030 at 9:08:06SystemAffirmTrust NetworkingcertificateDec 31, 2030 at 9:08:24SystemAffirmTrust PremiumcertificateDec 31, 2040 at 9:00:06SystemAll ItemsAffirmTrust Premium ECCcertificateDec 31, 2040 at 9:20:24SystemAll ItemsAmazon Root CA 1certificateDec 31, 2040 at 9:20:24SystemAmazon Root CA 2certificateMay 25, 2040 at 8:00:00SystemSecure NotesAmazon Root CA 3certificateMay 25, 2040 at 8:00:00SystemMy CertificatesAmazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemAnszon Root CA 4certificateJun 5, 2033 at 1:45:38 PMSystemAnszon Root CA 4certificateJun 5, 2033 at 1:45:38 PMSystemApple Root CA - G2certificateApr 30, 2039 at 2:10:09SystemApple Root CA - G3certificateApr 30, 2039 at 2:19:06SystemApple Root CA - G3certificateApr 30, 2039 at 2:19:06SystemApple Root CA - G3certificateApr 30, 2039 at 2:19:06SystemApple Root CA - G3certificateDec 31, 2030 at 6:59:59SystemApple Root CA - G3certificateApr 30, 2039 at 2:19:06SystemApple Root CA - G3certificateDec 31, 2030 at 6:59:59SystemApple Root CA - G3certificateDec 31, 2030 at 6:59:59System		😁 AAA Certificate Services	certificate	Dec 31, 2028 at 6:59:59	System Roo
CategoryCategoryAdmin-Root-CAcertificateNov 10, 2021 at 2:51:07 AMSystemCategoryAffirmTrust CommercialcertificateDec 31, 2030 at 9:06:06SystemAffirmTrust NetworkingcertificateDec 31, 2030 at 9:08:24SystemAffirmTrust PremiumcertificateDec 31, 2040 at 9:00:24SystemAll ItemsAffirmTrust Premium ECCcertificateDec 31, 2040 at 9:20:24SystemAmazon Root CA 1certificateJan 16, 2038 at 7:00:00SystemSecure NotesAmazon Root CA 2certificateMay 25, 2040 at 8:00:00SystemMy CertificatesAmazon Root CA 3certificateMay 25, 2040 at 8:00:00SystemMy CertificatesAmazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemKeysAmazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemApple Root CAAmazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemApple Root CAG2certificateMay 25, 2040 at 8:00:00SystemApple Root CAG2certificateJun 5, 2033 at 1:45:38 PMSystemApple Root CA - G2certificateApr 30, 2039 at 2:10:09SystemApple Root CA - G3certificateApr 30, 2039 at 2:19:06SystemApple Root CA - G3certificateApr 30, 2039 at 2:19:06SystemApple Root CA - G3certificateApr 30, 2039 at 2:19:06SystemAtos TrustedRoot 2011certi		C RAIZ FNMT-RCM	certificate	Dec 31, 2029 at 7:00:00	System Roo
CategoryAffirmTrust CommercialcertificateDec 31, 2030 at 9:06:06SystemCategoryAffirmTrust NetworkingcertificateDec 31, 2030 at 9:08:24SystemAffirmTrust PremiumcertificateDec 31, 2040 at 9:10:36SystemAffirmTrust Premium ECCcertificateDec 31, 2040 at 9:20:24SystemAnazon Root CA 1certificateJan 16, 2038 at 7:00:00SystemSecure NotesImazon Root CA 2certificateMay 25, 2040 at 8:00:00SystemMy CertificatesImazon Root CA 3certificateMay 25, 2040 at 8:00:00SystemAmazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemAnszon Root CA 4certificateMay 25, 2040 at 8:00:00SystemAmazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemAnszon Root CA 4certificateMay 25, 2040 at 8:00:00SystemAnszon Root CA 4certificateMay 25, 2040 at 8:00:00SystemAnszon Root CA 4certificateJun 5, 2033 at 1:45:38 PMSystemApple Root CAG2certificateApr 30, 2039 at 2:10:09SystemApple Root CA - G2certificateApr 30, 2039 at 2:10:09SystemApple Root CA - G3certificateApr 30, 2039 at 2:19:06SystemApple Root CA - G3certificateApr 30, 2039 at 2:19:06SystemApple Root CA - G3certificateApr 30, 2039 at 2:19:06SystemApple Root CA - G3certificate <th></th> <th>Actalis Authentication Root CA</th> <th>certificate</th> <th>Sep 22, 2030 at 7:22:02</th> <th>System Roo</th>		Actalis Authentication Root CA	certificate	Sep 22, 2030 at 7:22:02	System Roo
CategorySystemCategoryAffirmTrust Premium ECCcertificateDec 31, 2040 at 9:08:24SystemAll ItemsAffirmTrust Premium ECCcertificateDec 31, 2040 at 9:20:24SystemAll Secure NotesAmazon Root CA 1certificateJan 16, 2038 at 7:00:00SystemMy CertificatesAmazon Root CA 3certificateMay 25, 2040 at 8:00:00SystemMy CertificatesAmazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemKeysAmazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemSecure NotesAmazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemMy CertificatesAmazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemMy CertificatesAmazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemApple Root CACAcertificateJun 5, 2033 at 1:45:38 PMSystemApple Root CAG2certificateApr 30, 2039 at 2:10:09SystemApple Root CA - G2certificateApr 30, 2039 at 2:10:09SystemApple Root CA - G3certificateApr 30, 2039 at 2:10:09SystemApple Root CA - G3certificateApr 30, 2039 at 2:10:09SystemApple Root CA - G3certificateDec 31, 2030 at 6:59:59SystemApple Root CA - G3certificateDec 31, 2030 at 6:59:59SystemApple Root CA - G3certificateDec 31, 2030 at 6:59:59System <th></th> <th>📷 Admin-Root-CA</th> <th>certificate</th> <th>Nov 10, 2021 at 2:51:07 AM</th> <th>System Roo</th>		📷 Admin-Root-CA	certificate	Nov 10, 2021 at 2:51:07 AM	System Roo
CategoryCategoryCategoryAffirmTrust Premium ECCcertificateDec 31, 2040 at 9:10:36SystemM All ItemsAffirmTrust Premium ECCcertificateDec 31, 2040 at 9:20:24SystemAmazon Root CA 1certificateJan 16, 2038 at 7:00:00SystemSecure NotesAmazon Root CA 2certificateMay 25, 2040 at 8:00:00SystemMy CertificatesAmazon Root CA 3certificateMay 25, 2040 at 8:00:00SystemMy CertificatesAmazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemKeysANF Global Root CAcertificateJun 5, 2033 at 1:45:38 PMSystemApple Root CAcertificateJun 5, 2033 at 1:45:38 PMSystemApple Root CA - G2certificateApr 30, 2039 at 2:10:09SystemApple Root CA - G3certificateApr 30, 2039 at 2:19:06SystemApple Root CA - G3certificatePe 9, 2025 at 7:18:14 PMSystemApple Root CA - G3certificateDec 31, 2030 at 6:59:59SystemApple Root CA - G1certificateDec 31, 2030 at 3:38:15SystemApple Root CA - G3certificateDec 31, 2030 at 3:38:15SystemApple Root CA - G3certificateDec 31, 2030 at 3:38:15SystemAtos TrustedRoot 2011certificateDec 31, 2030 at 3:38:15SystemAutoridad de Certificacionrmaprofesional CIF A62634068certificateDec 31, 2030 at 3:38:15System		📷 AffirmTrust Commercial	certificate	Dec 31, 2030 at 9:06:06	System Roo
CategoryCategoryAffirmTrust Premium ECCcertificateDec 31, 2040 at 9:20:24SystemM All ItemsImage: Amazon Root CA 1certificateJan 16, 2038 at 7:00:00SystemM PasswordsImage: Amazon Root CA 2certificateMay 25, 2040 at 8:00:00SystemSecure NotesImage: Amazon Root CA 3certificateMay 25, 2040 at 8:00:00SystemMy CertificatesImage: Amazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemMy CertificatesImage: Amazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemMy CertificatesImage: Amazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemMy CertificatesImage: Amazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemMy CertificatesImage: Amazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemMy CertificatesImage: Amazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemMy CertificatesImage: Amazon Root CA 4certificateJun 5, 2033 at 1:45:38 PMSystemImage: Apple Root CAG2certificateApr 30, 2039 at 2:10:09SystemImage: Apple Root CA - G3certificateApr 30, 2039 at 2:10:09SystemImage: Apple Root CA - G3certificateApr 30, 2039 at 2:19:06SystemImage: Apple Root CA - G3certificateApr 30, 2030 at 6:59:59SystemImage: Apple Root CA - G3certificateDec 31, 2030 at 6:59:59		📷 AffirmTrust Networking	certificate	Dec 31, 2030 at 9:08:24	System Roo
All ItemsCertificateDec 01, 2040 at 3:20:24SystemAll ItemsImazon Root CA 1certificateJan 16, 2038 at 7:00:00SystemSecure NotesImazon Root CA 2certificateMay 25, 2040 at 8:00:00SystemMy CertificatesImazon Root CA 3certificateMay 25, 2040 at 8:00:00SystemMy CertificatesImazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemMy CertificatesImazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemReysImazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemImazon Root CA 4certificateJun 5, 2033 at 1:45:38 PMSystemImazon Root CA 62certificateJun 5, 2039 at 2:10:09SystemImazon Root CA - G2certificateAppla 0, 2039 at 2:10:09SystemImazon Root CA - G3certificateAppla 0, 2039 at 2:19:06SystemImazon Root CA - G3certificateAppla 0, 2039 at 2:19:06SystemImage: Apple Root CA - G3certificateAppla 0, 2039 at 2:19:06SystemImage: Apple Root CA - G3certificateAppla 0, 2039 at 6:59:59SystemImage: Apple Root CA - G3certificateDec 31, 2030 at 6:59:59SystemI		AffirmTrust Premium	certificate	Dec 31, 2040 at 9:10:36	System Roo
Amazon Root CA 2certificateMay 25, 2040 at 8:00:00SystemSecure NotesImazon Root CA 3certificateMay 25, 2040 at 8:00:00SystemMy CertificatesImazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemKeysImazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemANF Global Root CAcertificateJun 5, 2033 at 1:45:38 PMSystemApple Root CAcertificateJun 5, 2033 at 1:45:36 PMSystemApple Root CA - G2certificateApr 30, 2039 at 2:10:09SystemApple Root CA - G3certificateApr 30, 2039 at 2:19:06SystemApple Root CA - G3certificateFeb 9, 2025 at 7:18:14 PMSystemApple Root CA - G3certificateDec 31, 2030 at 6:59:59SystemAtos TrustedRoot 2011certificateDec 31, 2030 at 3:38:15SystemAutoridad de Certificacionrmaprofesional CIF A62634068certificateDec 31, 2030 at 3:38:15System	Category	📷 AffirmTrust Premium ECC	certificate	Dec 31, 2040 at 9:20:24	System Roo
NotesticatedAmazon Root CA 3certificateMay 25, 2040 at 8:00:00SystemMy CertificatesAmazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemKeysAmazon Root CA 4certificateJun 5, 2033 at 1:45:38 PMSystemANF Global Root CAcertificateJun 5, 2033 at 1:45:38 PMSystemApple Root CAcertificateFeb 9, 2035 at 4:40:36 PMSystemApple Root CA - G2certificateApr 30, 2039 at 2:10:09SystemApple Root CA - G3certificateApr 30, 2039 at 2:19:06SystemApple Root CA - G3certificateFeb 9, 2025 at 7:18:14 PMSystemApple Root CA - G3certificateDec 31, 2030 at 6:59:59SystemAtos TrustedRoot 2011certificateDec 31, 2030 at 3:38:15System	\land All Items	📷 Amazon Root CA 1	certificate	Jan 16, 2038 at 7:00:00	System Roo
Secure NotesAmazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemMy CertificatesCertificatesJun 5, 2033 at 1:45:38 PMSystemAns Global Root CAcertificateJun 5, 2035 at 4:40:36 PMSystemApple Root CAcertificateFeb 9, 2035 at 4:40:36 PMSystemApple Root CA - G2certificateApr 30, 2039 at 2:10:09SystemApple Root CA - G3certificateApr 30, 2039 at 2:19:06SystemApple Root CA - G3certificateFeb 9, 2025 at 7:18:14 PMSystemApple Root Cartificate AuthoritycertificateDec 31, 2030 at 6:59:59SystemAtos TrustedRoot 2011certificateDec 31, 2030 at 3:38:15System	/ Passwords	📷 Amazon Root CA 2	certificate	May 25, 2040 at 8:00:00	System Roo
My CertificatesImage: Amazon Root CA 4certificateMay 25, 2040 at 8:00:00SystemKeysImage: ANF Global Root CAcertificateJun 5, 2033 at 1:45:38 PMSystemImage: Apple Root CACertificatesFeb 9, 2035 at 4:40:36 PMSystemImage: Apple Root CA - G2certificateApr 30, 2039 at 2:10:09SystemImage: Apple Root CA - G3certificateApr 30, 2039 at 2:19:06SystemImage: Apple Root CA - G3certificateApr 30, 2039 at 2:19:06SystemImage: Apple Root CA - G3certificateFeb 9, 2025 at 7:18:14 PMSystemImage: Apple Root CA - G1certificateDec 31, 2030 at 6:59:59SystemImage: Autoridad de Certificacionrmaprofesional CIF A62634068certificateDec 31, 2030 at 3:38:15System	Secure Notes	📷 Amazon Root CA 3	certificate	May 25, 2040 at 8:00:00	System Roo
ReysImage: CertificatesJun 5, 2033 at 1:45:38 PMSystemImage: CertificatesApple Root CAcertificateJun 5, 2033 at 1:45:38 PMSystemImage: CertificatesApple Root CAG2certificateApr 30, 2039 at 2:10:09SystemImage: CertificatesApple Root CA - G2certificateApr 30, 2039 at 2:19:06SystemImage: CertificatesApple Root CA - G3certificateApr 30, 2039 at 2:19:06SystemImage: CertificatesSystemCertificate AuthoritycertificateDec 31, 2030 at 6:59:59SystemImage: CertificatesAutoridad de Certificacionrmaprofesional CIF A62634068certificateDec 31, 2030 at 3:38:15System		📷 Amazon Root CA 4	certificate	May 25, 2040 at 8:00:00	System Roo
CertificatesFeb 9, 2035 at 4:40:36 PMSystemCertificatesApple Root CA - G2certificateApr 30, 2039 at 2:10:09SystemApple Root CA - G3certificateApr 30, 2039 at 2:19:06SystemApple Root CA - G3certificateFeb 9, 2025 at 7:18:14 PMSystemApple Root Certificate AuthoritycertificateFeb 9, 2025 at 7:18:14 PMSystemAtos TrustedRoot 2011certificateDec 31, 2030 at 6:59:59SystemAutoridad de Certificacionrmaprofesional CIF A62634068certificateDec 31, 2030 at 3:38:15System		📷 ANF Global Root CA	certificate	Jun 5, 2033 at 1:45:38 PM	System Roo
Apple Root CA - G2CertificateApr 30, 2039 at 2:10:09SystemCartificateApple Root CA - G3CertificateApr 30, 2039 at 2:19:06SystemCartificateApple Root Certificate AuthorityCertificateFeb 9, 2025 at 7:18:14 PMSystemCartificateAtos TrustedRoot 2011CertificateDec 31, 2030 at 6:59:59SystemCartificateAutoridad de Certificacionrmaprofesional CIF A62634068CertificateDec 31, 2030 at 3:38:15System		📷 Apple Root CA	certificate	Feb 9, 2035 at 4:40:36 PM	System Roo
Image: ConstructionCertificateFeb 9, 2025 at 7:18:14 PMSystemImage: Constructed Root 2011CertificateDec 31, 2030 at 6:59:59SystemImage: Constructed Root 2011CertificateDec 31, 2030 at 3:38:15SystemImage: Constructed Root 2011CertificateDec 31, 2030 at 3:38:15SystemImage: Constructed Root 2011Certificationrmaprofesional CIF A62634068CertificateDec 31, 2030 at 3:38:15System		🔤 📴 Apple Root CA - G2	certificate	Apr 30, 2039 at 2:10:09	System Roo
Atos TrustedRoot 2011certificateDec 31, 2030 at 6:59:59SystemAutoridad de Certificacionrmaprofesional CIF A62634068certificateDec 31, 2030 at 3:38:15System		📷 Apple Root CA - G3	certificate	Apr 30, 2039 at 2:19:06	System Roo
Autoridad de Certificacionrmaprofesional CIF A62634068 certificate Dec 31, 2030 at 3:38:15 System		📷 Apple Root Certificate Authority	certificate	Feb 9, 2025 at 7:18:14 PM	System Roo
		TrustedRoot 2011	certificate	Dec 31, 2030 at 6:59:59	System Roo
		📷 Autoridad de Certificacionrmaprofesional CIF A626	34068 certificate	Dec 31, 2030 at 3:38:15	System Roo
Autoridad de Certificación Raiz del Estado Venezolano certificate Dec 17, 2030 at 6:59:59 System		📷 Autoridad de Certificacion Raiz del Estado Venezola	ano certificate	Dec 17, 2030 at 6:59:59	System Roo

NETS1035 APPLIED CRYPTOGRAPHY - DENNIS SIMPSON ©2020

MacOS Certificate Store

- MacOS has a single place where root certificates are stored like Linux, but stores them in keychain files, which are not intended to be directly manipulated
- The MacOS keychain utility is used to view, modify, and extract certificates from the certificate store
- You can drag and drop certificates in and out of the keychain utility



PKI Certificates

- working with them
- openssl has the x509 subcommand which allows us to work with certificate files
- The verify subcommand can be used to check trust for a certificate
- openssl's x509 command also can be used during the creation of certificates

cat certfile | openssl x509 -noout -pubkey cat certfile | openssl x509 -noout -pubkey -subject cat certfile | openssl x509 -noout -pubkey -subject -startdate -enddate cat certfile | openssl x509 -noout -text openssl s_client -connect api.stackexchange.com:443 </dev/null | openssl x509 -text -noout sudo openssl s_server -cert /etc/ssl/certs/ssl-cert-snakeoil.pem -key /etc/ssl/private/ssl-cert-snakeoil.key openssl s_client -connect server:4433 <<<"GET /"</pre>

NETS1035 APPLIED CRYPTOGRAPHY - DENNIS SIMPSON ©2020

• Certificates themselves are not OS-specific, and openssl is a good cross-platform utility for

Certificate Revocation

- Certificates can be revoked or held by the issuing CA
 - Revoked certificates are no longer valid
 - Held certificates may be released and become valid again
- Revoked certificates are added to a CRL by the CA that issued the certificate
- CRLs are published at the discretion of the issuing CA
- There are also ARLs, to revoke CAs which also invalidates every certificate signed by that CA
- CRL checking is supported but not enabled in most of the major browsers and browser suppliers support OCSP as an alternative

CRL

 Certificate Revocation List

ARL

 Authority Revocation List

OCSP

 Online Certificate Status Protocol



Online Certificate Status Protocol

- A lower-overhead request/response protocol, compared to querying CRLs used by web client programs, to check if a certificate is still valid
- Not all browsers use this all the major ones except Chrome support it although it may not be enabled
- Not all certificate suppliers respond to this, some delegate authority to respond to third parties, and some only use it for EV certificates
- It is not encrypted so it is susceptible to data harvesting and man-in-the-middle attacks, as well as replay attacks
- Many clients simply ignore unresponsive OCSP responders



OCSP Stapling

- traffic requiring real-time responses
- save the responses
- making separate OCSP requests
- OCSP responses, this mostly solves the traffic problem
- Major web server software suppliers pretty much all have some form of stapling in place

Both CRL and OCSP validation techniques involve the potential to generate large quantities of

• A solution for this is to have the web server using a certificate make regular OCSP queries and

 Then if a client issues a TLS request with the Certificate Status Request extension enabled, the web server just includes its recent response with the request saving the web client from

Other than the potential for introducing delays in revoking certificates due to server caching of



PKI Certificate Types

- Web certificates are most commonly used to authenticate domain names
- Certificates can be self-signed, meaning they are not trusted to authenticate, unless a user has explicitly chosen to trust them, or the system administrator has installed them as a trusted certificate
- Certificates can be CA signed, in which case they are typically validated by one of several methods by the CA
 - DV certificates only indicate that the certificate holder has control of either the domain's DNS, the domain name's web server, or both
 - OV certificates indicate the CA has done diligence in verifying that the certificate was applied for by the organization described in the certificate
 - IV certificates indicate the CA has done diligence in verifying that the certificate was applied for by the individual identified in the certificate - these are not normally used for web servers but are used for personal messaging
 - EV certificates require more verification on the part of the CA to ensure the certificate's identity does indeed belong to the certificate holder



DV

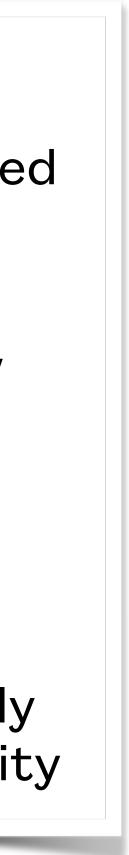
Domain Verified

OV/IV

 Organization/ Individual Verified

EV

 More Diligently Verified Identity



Obtaining Certificates

- Traditionally a manual process involving someone responsible for a domain name making a request for a certificate from a CA
- The requestor creates a CSR file and signs it with their own private key
- The requestor gathers documentation to demonstrate they are who they claim to be and that they have the authority to manage certificates for the domain name
- The requestor sends the CSR file, the documentation, and a cheque to the CA
- They all twiddle their thumbs for a significant time.
- The requestor receives the certificate file from the CA and can now install it where their service software can find it



CSR

• Certificate Signing Request



ACME

- On the internet, the most common use of PKI certificates is to authenticate web servers' domain names
- The ACME protocol provides an automated method to verify domain control and issue certificates based on that verification
- There are 2 ways normally used to demonstrate domain control
 - 1. Verify control of DNS by adding a DNS record
 - 2. Verify control of web server for domain by adding a retrievable document to the web server
- See <u>https://tools.ietf.org/pdf/rfc8555.pdf</u> for an excellent discussion of the ACME protocol and how it fits in with the web's PKI

ACME

Automatic
 Certificate
 Management
 Environment



Letsencrypt

- service or DNS
- for, receive, and install letsencrypt certificates
- Firmware suppliers for routers and such are starting to include letsencrypt client capabilities
- or content for a file to place on the domain web server
- live and that is all the proof they require to believe that you control the domain name for the certificate

• Letsencrypt is a free certificate authority which can be used to obtain DV certificates with the ACME protocol

• It bases certificate signing decisions on whether the applicant can demonstrate control of the domain's web

• The process is fully automated at the letsencrypt server and there are many scripts and programs that can apply

• When applying for a letsencrypt certificate, the letsencrypt servers provide you with data for a DNS TXT record,

• When you ask for the certificate to be issued, the letsencrypt servers verify the web file or DNS TXT record are

• Automation software often only provides the web method and assumes the web server is on the embedded device

Private CA for PK

- of a private CA
- They create a root private keypair, then a self-signed root certificate
- Any machines which should be part of the private PKI will need to add the private root certificate to their trusted certificate store
- VPN packages typically include a private CA capability
- Easy-rsa, <u>CA.pl</u>, and openssl can all be used to create a private CA



• They can then either sign CSRs using their root private key, or create a keypair and CSR and sign it, which supplies the private key and matching certificate as an intermediate authority