Forward Secrecy

The Threat

- "Eve" *(cough, NSA, cough)* records multiple years of encrypted messages between Alice and Bob from 2015-2017
  - Can't break them – algorithm & implementation contains no known flaws
- Then, in October 2017, a zero-day exploit allows Eve to steal the encryption key from Alice
- Result: All historical messages saved can be decrypted

Revisiting – Heartbleed

- **Not just a hypothetical concern!**
- **OpenSSL (2014) - CVE-2014-0160** :
  - Allows **remote attackers** to obtain **sensitive information from process memory** via crafted packets that trigger a buffer over-read, as **demonstrated by reading private keys**
  - Allows attacker to recover a private key *today*, and decrypt any & all old encrypted traffic they may have stored

Forward Secrecy

- **Forward Secrecy** – Past sessions are protected against future compromise of secret keys
- **Perfect Forward Secrecy** – Each encryption/decryption key is valid for only one "session"
  - Look for this!

Perfect Forward Secrecy Examples

- Transport Layer Security (TLS)
  - **Ephemeral** Elliptic Curve Diffie-Hellman
    ECDH**E**-RSA, ECDH**E**-ECDSA *(E is for Ephemeral)*
  - **Ephemeral** Diffie-Hellman
    - DH**E**-RSA, DH**E**-DSA
  - *Easy to enable server-side, but can get lost in blizzard of TLS options and backwards compatibility*
- Signal Protocol
  - Double Ratchet Algorithm
    https://signal.org/blog/advanced-ratcheting/
  - Signal messenger, WhatsApp, Facebook Messenger

Transport Layer Security (TLS)

Transport Layer Security (TLS)

- Encryption provided at the application layer
  - Physical layer – Ethernet
  - Network layer – IP
  - Transport layer – TCP
  - Application layer – TLS first, then …
- Common uses: web (HTTPS), email, VOIP, messaging

Transport Layer Security (TLS)

- Two variants
  - Secure Socket Layer (SSL) – **don't use!**
    - SSL 1.0 (never publicly used), SSL 2.0, SSL 3.0
  - Transport Layer Security (TLS) – **modern successor**
    - TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3 *(draft)*

Transport Layer Security (TLS)

- Hybrid encryption scheme
  - Public key encryption for *handshake*
  - Symmetric key encryption for bulk data transport
    - Key is unique per session and negotiated during handshake
  - MACs to provide integrity
    - *Data didn't change in transit*
  - Certificate authorities (CAs) to provide authenticity
    - *I'm communicating with the intended party*
- **Many (many!) choices in specific ciphers & algorithms**

Transport Layer Security (TLS)

HTTPS Client 

 **HTTPS Server**

Client Hello

Version, crypto options, nonce

Server hello + server cert (PKs)

Version, crypto options, nonce, Signed certificate w/ server's public key

Server key exchange (when using DH)

Client key exchange

PreMaster secret encrypted with server's PKs

*Handshake finished. Switch to **negotiated block cipher***

Data Transmission

(HTTP over TLS)

Qualys. SSL Labs

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > cyberlab.pacific.edu

SSL Report: cyberlab.pacific.edu (96.71.204.45)

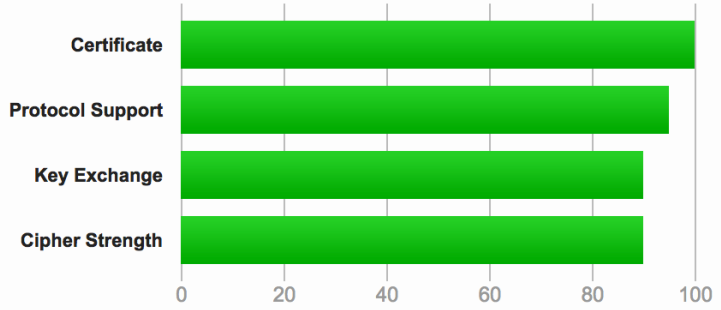
Assessed on: Wed, 11 Oct 2017 06:54:16 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

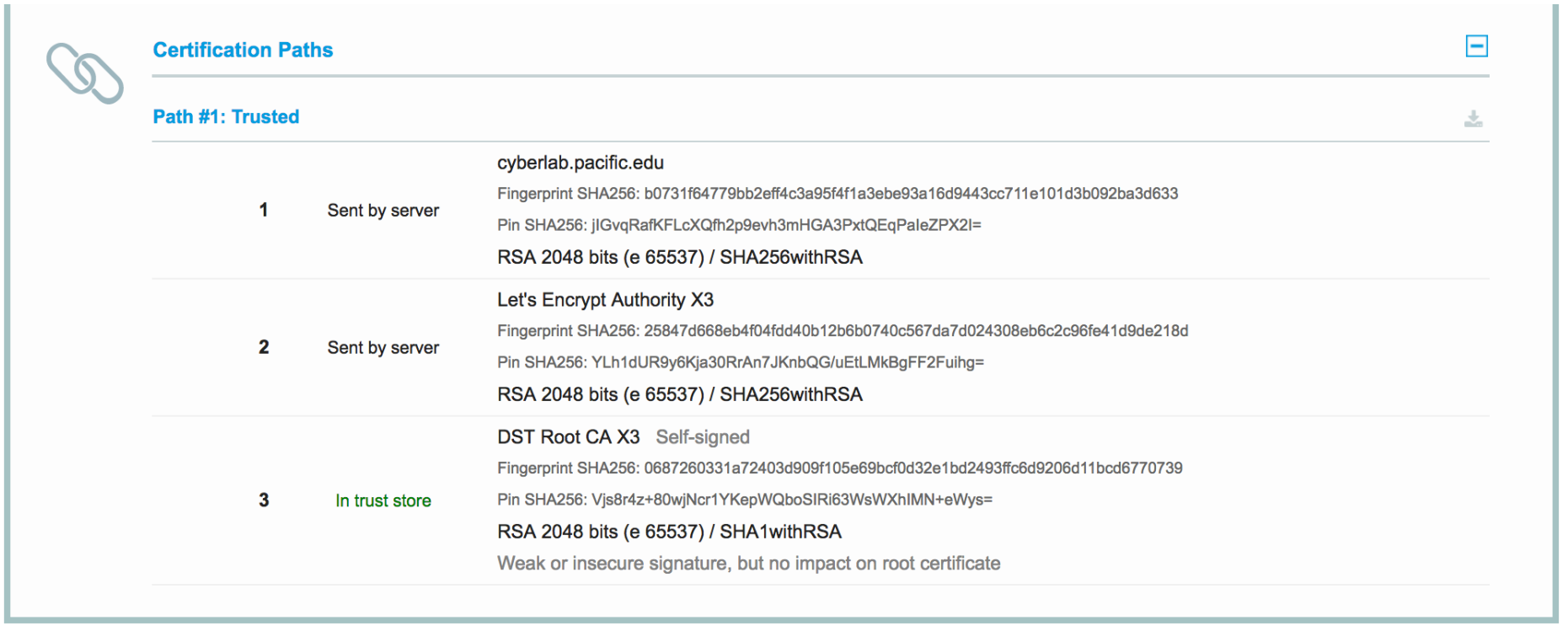
https://www.ssllabs.com/ssltest/analyze.html?d=cyberlab.pacific.edu

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	cyberlab.pacific.edu Fingerprint SHA256: b0731f64779bb2eff4c3a95f4f1a3ebe93a16d9443cc711e101d3b092ba3d633 Pin SHA256: jIGvqRafKFLcXQfh2p9evh3mHGA3PxtQEqPaIeZPX2I=
Common names	cyberlab.pacific.edu
Alternative names	cyberlab.pacific.edu
Serial Number	04f03ad93ab340b00bb933104ab9abdc3dbf
Valid from	Mon, 14 Aug 2017 17:31:00 UTC
Valid until	Sun, 12 Nov 2017 17:31:00 UTC (expires in 1 month and 1 day)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Let's Encrypt Authority X3 AIA: http://cert.int-x3.letsencrypt.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://ocsp.int-x3.letsencrypt.org
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	**Yes**

https://www.ssllabs.com/ssltest/analyze.html?d=cyberlab.pacific.edu



Certification Paths

Path #1: Trusted

1	Sent by server	cyberlab.pacific.edu Fingerprint SHA256: b0731f64779bb2eff4c3a95f4f1a3ebe93a16d9443cc711e101d3b092ba3d633 Pin SHA256: jIGvqRafKFLcXQfh2p9evh3mHGA3PxtQEqPaIeZPX2I= RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	Let's Encrypt Authority X3 Fingerprint SHA256: 25847d668eb4f04fdd40b12b6b0740c567da7d024308eb6c2c96fe41d9de218d Pin SHA256: YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg= RSA 2048 bits (e 65537) / SHA256withRSA
3	In trust store	DST Root CA X3 Self-signed Fingerprint SHA256: 0687260331a72403d909f105e69bcf0d32e1bd2493ffc6d9206d11bcd6770739 Pin SHA256: Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhIMN+eWys= RSA 2048 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

https://www.ssllabs.com/ssltest/analyze.html?d=cyberlab.pacific.edu

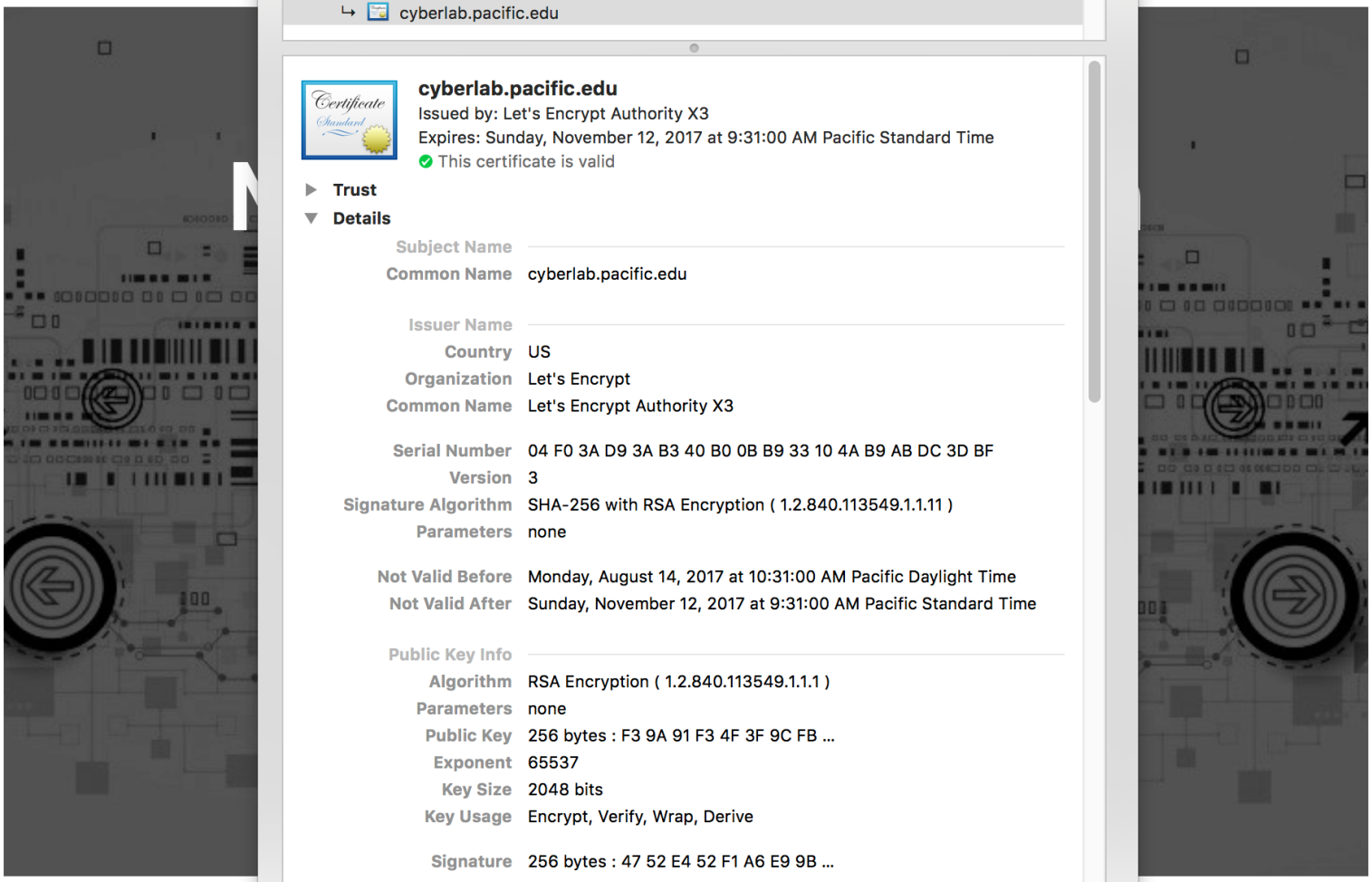
Cipher Suites

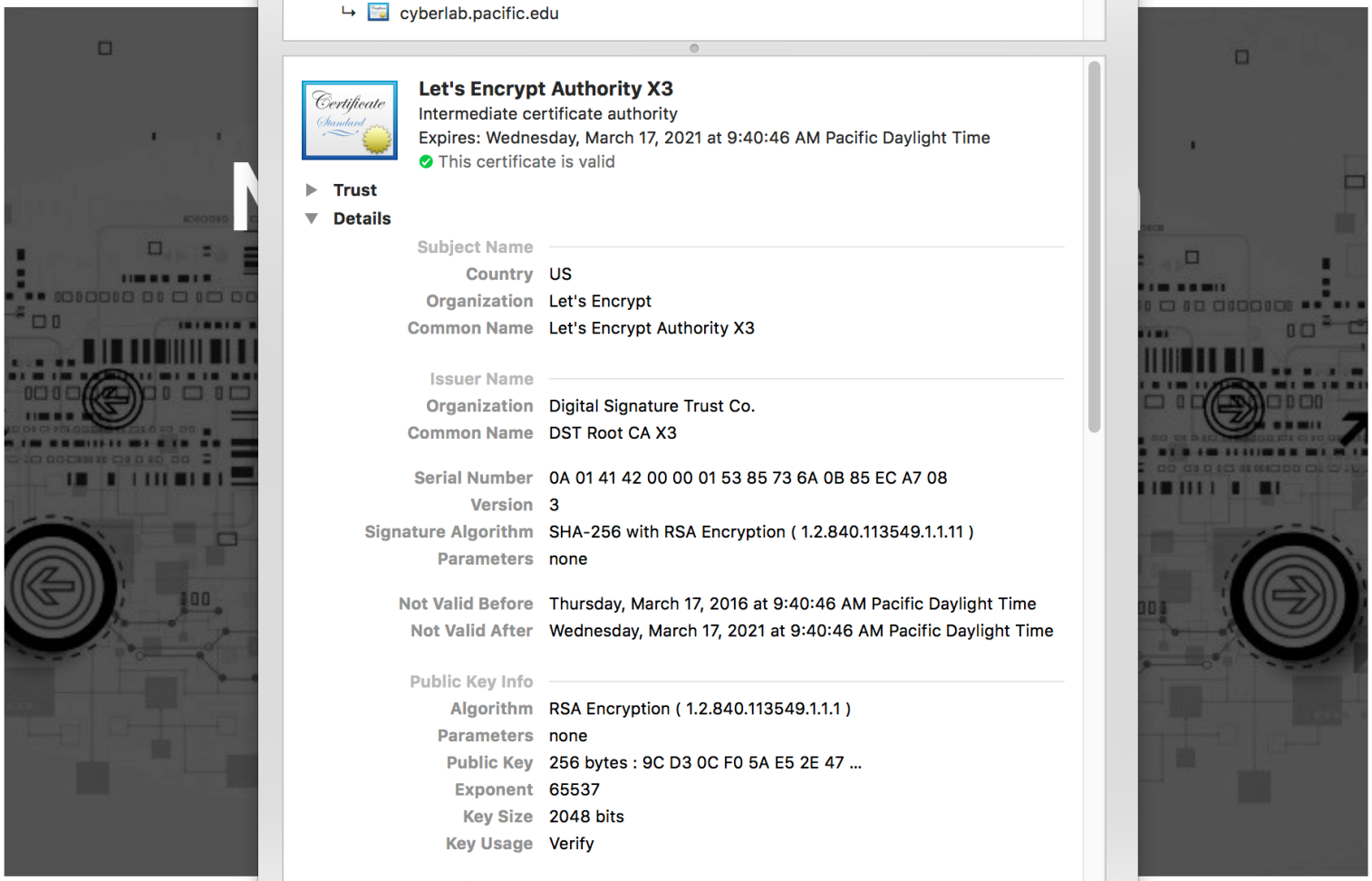
 # TLS 1.2 (suites in server-preferred order)

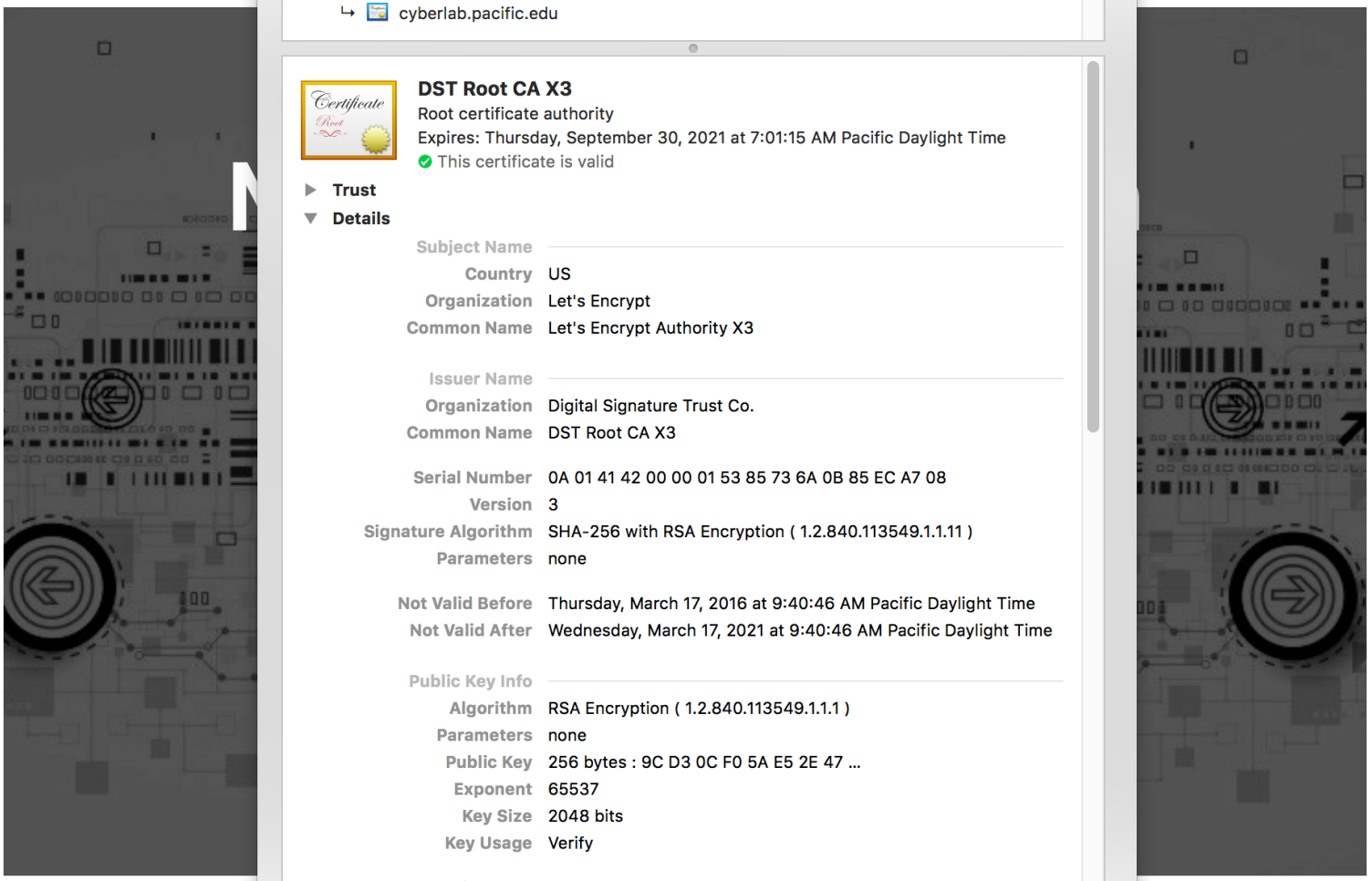
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)		128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)		256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)		128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)		256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		256

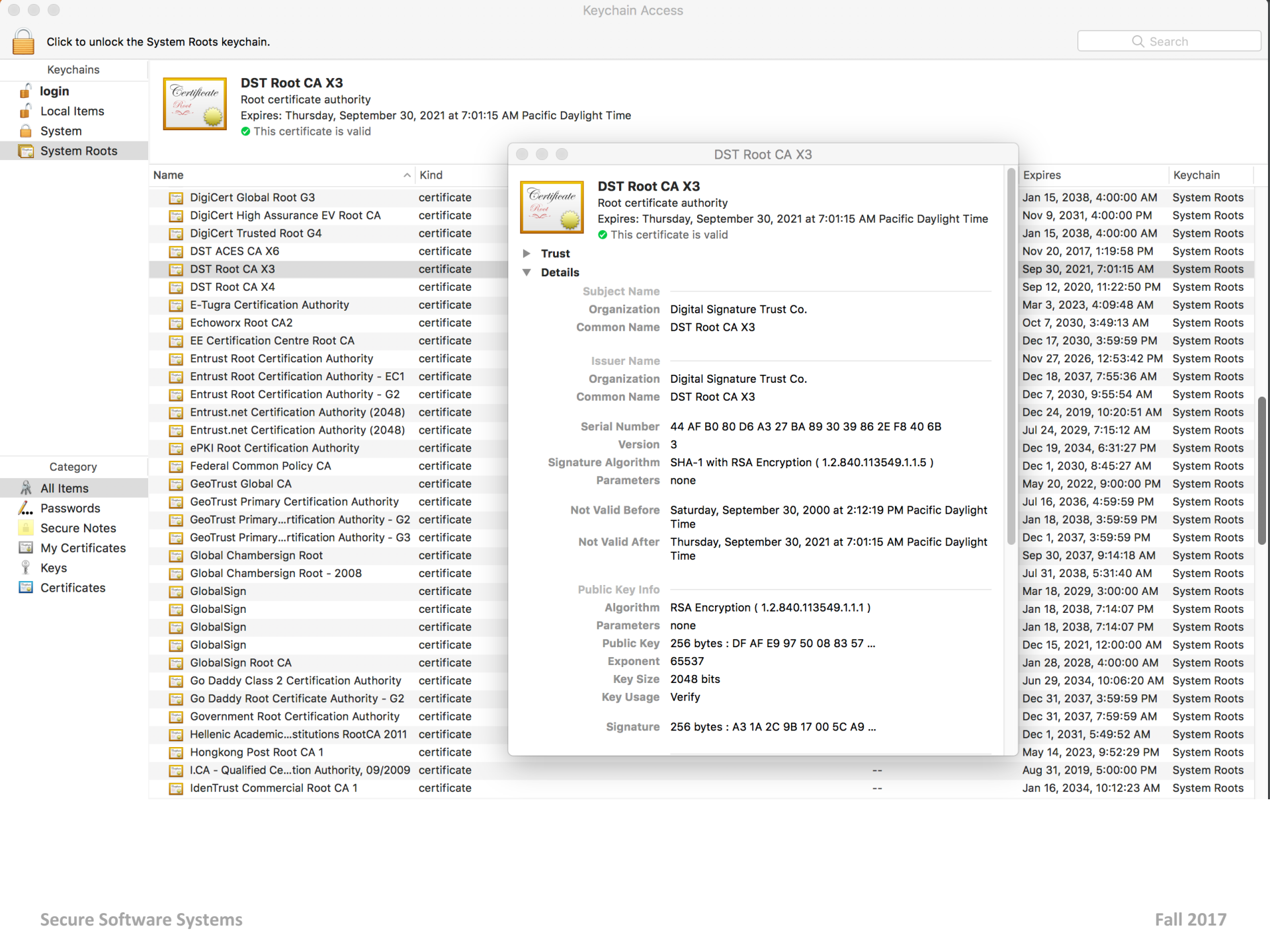
List was much longer (and weaker!) until custom configuration was applied to server

https://www.ssllabs.com/ssltest/analyze.html?d=cyberlab.pacific.edu


cyberlab.pacific.edu
Safari is using an encrypted connection to cyberlab.pacific.edu.
Encryption with a digital certificate keeps information private as it's sent to or from the https website cyberlab.pacific.edu.
DST Root CA X3
Let's Encrypt Authority X3
cyberlab.pacific.edu
cyberlab.pacific.edu
Issued by: Let's Encrypt Authority X3
Expires: Sunday, November 12, 2017 at 9:31:00 AM Pacific Standard Time
This certificate is valid
Trust
Details
Subject Name
Common Name cyberlab.pacific.edu
Issuer Name
Country US
Organization Let's Encrypt
Common Name Let's Encrypt Authority X3
Serial Number 04 F0 3A D9 3A B3 40 B0 0B B9 33 10 4A B9 AB DC 3D BF
Version 3
Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters none
Not Valid Before Monday, August 14, 2017 at 10:31:00 AM Pacific Daylight Time
Not Valid After Sunday, November 12, 2017 at 9:31:00 AM Pacific Standard Time
Public Key Info
Algorithm RSA Encryption (1.2.840.113549.1.1.1)
Parameters none
Public Key 256 bytes : F3 9A 91 F3 4F 3F 9C FB ...
Exponent 65537
Key Size 2048 bits
Key Usage Encrypt, Verify, Wrap, Derive
Signature 256 bytes : 47 52 E4 52 F1 A6 E9 9B ...
Hide Certificate
OK


cyberlab.pacific.edu
Safari is using an encrypted connection to cyberlab.pacific.edu.
Encryption with a digital certificate keeps information private as it's sent to or from the https website cyberlab.pacific.edu.
DST Root CA X3
Let's Encrypt Authority X3
cyberlab.pacific.edu
Let's Encrypt Authority X3
Intermediate certificate authority
Expires: Wednesday, March 17, 2021 at 9:40:46 AM Pacific Daylight Time
This certificate is valid
Trust
Details
Subject Name
Country US
Organization Let's Encrypt
Common Name Let's Encrypt Authority X3
Issuer Name
Organization Digital Signature Trust Co.
Common Name DST Root CA X3
Serial Number 0A 01 41 42 00 00 01 53 85 73 6A 0B 85 EC A7 08
Version 3
Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters none
Not Valid Before Thursday, March 17, 2016 at 9:40:46 AM Pacific Daylight Time
Not Valid After Wednesday, March 17, 2021 at 9:40:46 AM Pacific Daylight Time
Public Key Info
Algorithm RSA Encryption (1.2.840.113549.1.1.1)
Parameters none
Public Key 256 bytes : 9C D3 0C F0 5A E5 2E 47 ...
Exponent 65537
Key Size 2048 bits
Key Usage Verify
Signature 256 bytes : DD 33 D7 11 F3 63 58 38 ...
Hide Certificate
OK

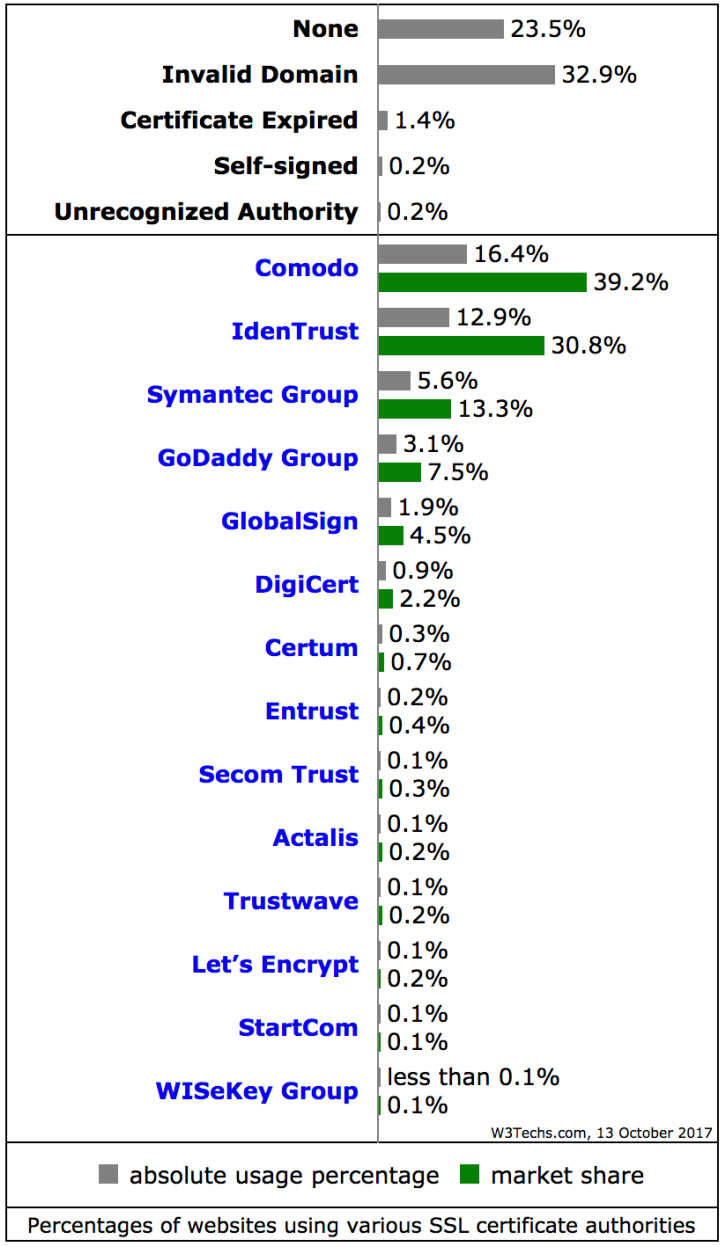

cyberlab.pacific.edu
Safari is using an encrypted connection to cyberlab.pacific.edu.
Encryption with a digital certificate keeps information private as it's sent to or from the https website cyberlab.pacific.edu.
DST Root CA X3
Let's Encrypt Authority X3
cyberlab.pacific.edu
DST Root CA X3
Root certificate authority
Expires: Thursday, September 30, 2021 at 7:01:15 AM Pacific Daylight Time
This certificate is valid
Trust
Details
Subject Name
Country US
Organization Let's Encrypt
Common Name Let's Encrypt Authority X3
Issuer Name
Organization Digital Signature Trust Co.
Common Name DST Root CA X3
Serial Number 0A 01 41 42 00 00 01 53 85 73 6A 0B 85 EC A7 08
Version 3
Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters none
Not Valid Before Thursday, March 17, 2016 at 9:40:46 AM Pacific Daylight Time
Not Valid After Wednesday, March 17, 2021 at 9:40:46 AM Pacific Daylight Time
Public Key Info
Algorithm RSA Encryption (1.2.840.113549.1.1.1)
Parameters none
Public Key 256 bytes : 9C D3 0C F0 5A E5 2E 47 ...
Exponent 65537
Key Size 2048 bits
Key Usage Verify
Signature 256 bytes : DD 33 D7 11 F3 63 58 38 ...
Hide Certificate
OK


Keychain Access
Click to unlock the System Roots keychain.
Search
Keychains
login
Local Items
System
System Roots
DST Root CA X3
Root certificate authority
Expires: Thursday, September 30, 2021 at 7:01:15 AM Pacific Daylight Time
This certificate is valid
Name
Kind
Expires
Keychain
DigiCert Global Root G3 certificate Jan 15, 2038, 4:00:00 AM System Roots
DigiCert High Assurance EV Root CA certificate Nov 9, 2031, 4:00:00 PM System Roots
DigiCert Trusted Root G4 certificate Jan 15, 2038, 4:00:00 AM System Roots
DST ACES CA X6 certificate Nov 20, 2017, 1:19:58 PM System Roots
DST Root CA X3 certificate Sep 30, 2021, 7:01:15 AM System Roots
DST Root CA X4 certificate Sep 12, 2020, 11:22:50 PM System Roots
E-Tugra Certification Authority certificate Mar 3, 2023, 4:09:48 AM System Roots
Echoworx Root CA2 certificate Oct 7, 2030, 3:49:13 AM System Roots
EE Certification Centre Root CA certificate Dec 17, 2030, 3:59:59 PM System Roots
Entrust Root Certification Authority certificate Nov 27, 2026, 12:53:42 PM System Roots
Entrust Root Certification Authority - EC1 certificate Dec 18, 2037, 7:55:36 AM System Roots
Entrust Root Certification Authority - G2 certificate Dec 7, 2030, 9:55:54 AM System Roots
Entrust.net Certification Authority (2048) certificate Dec 24, 2019, 10:20:51 AM System Roots
Entrust.net Certification Authority (2048) certificate Jul 24, 2029, 7:15:12 AM System Roots
ePKI Root Certification Authority certificate Dec 19, 2034, 6:31:27 PM System Roots
Federal Common Policy CA certificate Dec 1, 2030, 8:45:27 AM System Roots
GeoTrust Global CA certificate May 20, 2022, 9:00:00 PM System Roots
GeoTrust Primary Certification Authority certificate Jul 16, 2036, 4:59:59 PM System Roots
GeoTrust Primary...rtification Authority - G2 certificate Jan 18, 2038, 3:59:59 PM System Roots
GeoTrust Primary...rtification Authority - G3 certificate Dec 1, 2037, 3:59:59 PM System Roots
Global Chambersign Root certificate Sep 30, 2037, 9:14:18 AM System Roots
Global Chambersign Root - 2008 certificate Jul 31, 2038, 5:31:40 AM System Roots
GlobalSign certificate Mar 18, 2029, 3:00:00 AM System Roots
GlobalSign certificate Jan 18, 2038, 7:14:07 PM System Roots
GlobalSign certificate Jan 18, 2038, 7:14:07 PM System Roots
GlobalSign certificate Dec 15, 2021, 12:00:00 AM System Roots
GlobalSign Root CA certificate Jan 28, 2028, 4:00:00 AM System Roots
Go Daddy Class 2 Certification Authority certificate Jun 29, 2034, 10:06:20 AM System Roots
Go Daddy Root Certificate Authority - G2 certificate Dec 31, 2037, 3:59:59 PM System Roots
Government Root Certification Authority certificate Dec 31, 2037, 7:59:59 AM System Roots
Hellenic Academic...stitutions RootCA 2011 certificate Dec 1, 2031, 5:49:52 AM System Roots
Hongkong Post Root CA 1 certificate May 14, 2023, 9:52:29 PM System Roots
I.CA - Qualified Ce...tion Authority, 09/2009 certificate -- Aug 31, 2019, 5:00:00 PM System Roots
IdenTrust Commercial Root CA 1 certificate -- Jan 16, 2034, 10:12:23 AM System Roots
Category
All Items
Passwords
Secure Notes
My Certificates
Keys
Certificates
DST Root CA X3
DST Root CA X3
Root certificate authority
Expires: Thursday, September 30, 2021 at 7:01:15 AM Pacific Daylight Time
This certificate is valid
Trust
Details
Subject Name
Organization Digital Signature Trust Co.
Common Name DST Root CA X3
Issuer Name
Organization Digital Signature Trust Co.
Common Name DST Root CA X3
Serial Number 44 AF B0 80 D6 A3 27 BA 89 30 39 86 2E F8 40 6B
Version 3
Signature Algorithm SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters none
Not Valid Before Saturday, September 30, 2000 at 2:12:19 PM Pacific Daylight Time
Not Valid After Thursday, September 30, 2021 at 7:01:15 AM Pacific Daylight Time
Public Key Info
Algorithm RSA Encryption (1.2.840.113549.1.1.1)
Parameters none
Public Key 256 bytes : DF AF E9 97 50 08 83 57 ...
Exponent 65537
Key Size 2048 bits
Key Usage Verify
Signature 256 bytes : A3 1A 2C 9B 17 00 5C A9 ...

Certificate Authorities

- Trusted third party
  - Trusted by owner of certificate (e.g. website)
  - Trusted by party relying on certificate (e.g. visitor)

Certificate Authorities



- Comodo is used by 16.4% of all websites
- Comodo is a SSL certificate authority with a market share of 39.2%
- *October 13 2017 data*

https://w3techs.com/technologies/overview/ssl_certificate/all

Certificate Weaknesses

- **Method 1:** Place desired common name (e.g. “fakebook.com” in a bogus cert
  - Web browsers will validate cert and detect forgery
  - Other software libraries may have broken validation code and miss the forgery!
- **Method 2:** Trick/hack/bribe a CA to issue & sign. Any CA can issue any certificate for any domain!
  - Apple “System Roots” keychain: 168 entries
  - Other players also decide what root CAs to trust
    - Microsoft, Mozilla, Android

Root CA Misuse

- **DigiNotar** (Dutch CA)
  - Attacker signed wildcard cert for *.google.com
  - Used to conduct MITM attack against Google (multiple ISPs in Iran)
  - Issued July 27 2011, detected Aug 27 2011
  - Removed as trusted root CA Aug 29 2011
  - Company bankrupt

Root CA Misue

- **WoSign** (Chinese CA)
  - Issued fake cert in 2016 for *subdomain*.github.com due to shoddy/missing ownership verification process
    - https://www.schrauger.com/the-story-of-how-wosign-gave-me-an-ssl-certificate-for-github-com
  - Backdated SHA-1 certifications
    - Browsers were intentionally blocking weak SHA-1 certs after Jan 1 2016
  - https://wiki.mozilla.org/CA:WoSign_Issues
  - Subsidiary **StartCom/StartSSL** (Isreal)
  - Slowly removed as trusted root CA in 2016-2017 by Google, Mozilla, Apple
    - But still in my Keychain? (?????)

Root CA Misuse

- **Symantec** (US CA)
  - Accused by Google of issuing 30,000 suspect certificates
    - Not 30k attacks, but 30k certs with insufficient validation, audit, assurance, etc…
  - Chrome *Root Certificate Policy* - What **you must do** if you want Google to trust *you*!
    - https://www.chromium.org/Home/chromium-security/root-ca-policy
  - Google issued progressive *death penalty* (Chrome will stop trusting *customer* certs signed by Symantec in late 2018)
  - Aug 2 2017: Symantec sells certificate business to competitor DigiCert for $950 million (cheap!) who will audit and re-certify following best practices

"Intent to Deprecate and Remove: Trust in existing Symantec-issued Certificates" - March 23 2017
https://groups.google.com/a/chromium.org/forum/#!msg/blink-dev/eUAKwjihhBs/rpxMXjZHCQAJ