

SE 4472

Information Security

Server Authentication
With
Public-key Infrastructure (PKI)

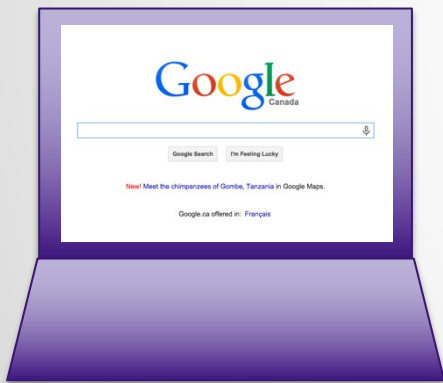


Server Authentication

- Scenario: what happens when you type “google.com” in to your browser?
 - TLS handshake begins
 - ECDHE key agreement
 - Diffie-Hellman needs a signature on the public key to prevent a man-in-the-middle attack
 - Server sends public key and signature
 - How do you verify the signature? With the verification key
 - How do you get the verification key?

Server Authentication

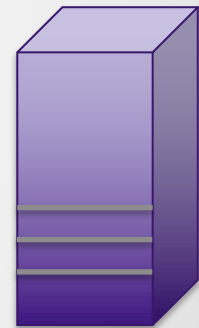
- Scenario: what happens when you type “google.com” in to your browser?



Hi, let's connect securely



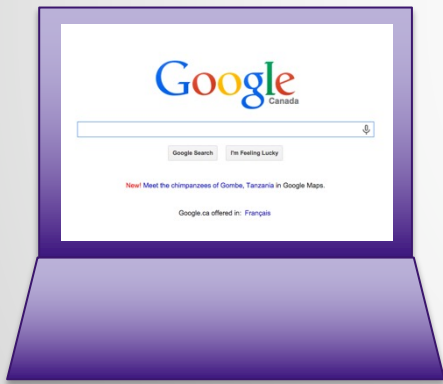
Ok. Here's my public key g^x



Google

Server Authentication

- Scenario: but what if this happens instead?



Hi, let's connect securely

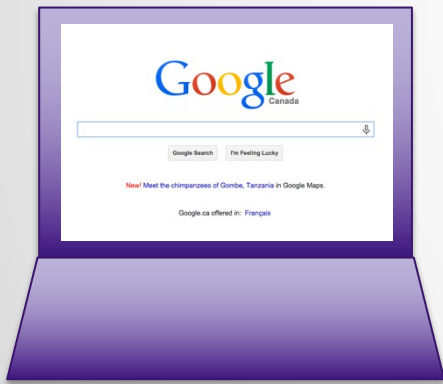


Ok here's my public key g^x



Server Authentication

- Scenario: but what if this happens instead?



How do we get an authentic copy of the server's public encryption key to the user?



Trust

- Key distribution problem
 - Guy with the briefcase handcuffed to his wrist
- Web of trust
 - You have a key, you get people you know to sign your key to endorse it to others
 - When you connect with someone, hopefully they know (and trust) someone who has signed your key
 - E.g., PGP
- Hierarchy of trust
 - There are a few entities in charge of signing keys, and you already somehow magically trust them
 - Who puts them in charge?
 - This is the world of digital certificates

Digital Certificates

Digital Certificates

- A claim made by a *certificate authority*
- Says what the server's public key is
- Signed by the signing key of the certificate authority



Certificate Authority

- An entity that has the authority to issue a certificate
- How do they decide how or whether to issue a certificate?
 - Validation process
- Who grants them the authority to be an authority?
 - Explicitly: your browser does
 - Implicitly: you do

Validation

- Domain validation
 - Prove you control a domain name. Yes? Ok, here's your cert. (cost: low hundreds/yr)
- Organization validation
 - Prove you're company X. (cost: hundreds/yr)
- Extended validation
 - Pay more money, get more validation
 - Expensive
 - Arguably as much of an economic signal (e.g., check out our fancy marble columns in our lobby) as a security measure
 - (cost: thousands/yr)

Certificate: Fields

- Serial number
- Subject Identity
 - Organization name (eg Google), common name (e.g., google.com)
- Public key
 - The server's public key
- Signature algorithm
 - What hash function and padding scheme is used to sign the cert
- Issuer Identity
 - The identity of the authority issuing the certificate
- Validity period
 - Not valid before/not valid after
- Signature
 - Signature on everything above. Signed by issuer.

Certificate Extensions

- Basic Constraints
 - Does this certificate belong to a CA?
- Key Usage:
 - What cryptographic operations can you use the public key for?
 - Digital signatures
 - Key encipherment
 - Sign certificates,
 - Sign certificate revocation lists
- Extended key
 - Indicates purpose of the public key:
 - Server authentication
 - Client email authentication
 - etc

Certificate case: [Google.com](https://www.google.com)

Google's cert 1/5

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1017850149796698209 (0xe2021518535d861)

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=US, O=Google Inc, CN=Google Internet Authority G2

Validity

Not Before: Oct 28 18:49:32 2015 GMT

Not After : Jan 26 00:00:00 2016 GMT

Subject: C=US, ST=California, L=Mountain View, O=Google Inc, CN=*.google.com

Subject
information

Google's cert 2/4

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:ca:41:bd:af:ea:f6:af:44:d8:fe:57:b1:53:52:
a8:e4:ca:63:89:bb:72:ce:2d:45:ed:3d:7c:e9:9a:
fe:1b:81:0b:4a:4c:4b:5d:68:a7:1b:1e:76:38:b1:
dc:d2:ba:d6:e7:01:5f:39:34:87:5b:59:7e:88:4c:
3b:32:79:57:ab:e0:82:0d:c8:da:c4:6f:27:98:1b:
b2:25:e1:7b:f1:44:ca:94:2d:51:c9:dd:ac:2b:b8:
6e:c4:7d:dd:bd:3f:b5:51:1c:a7:25:e5:bd:9d:df:
ef:8e:fa:d4:ce:76:7c:07:74:50:49:a3:43:7b:8b:
fc:f8:6a:4c:1d:00:e7:32:5f:aa:f1:57:5c:6f:21:
d0:8e:0d:42:02:f0:dd:08:f6:6b:75:c3:73:c6:13:
da:f2:0d:97:18:10:0f:c3:bb:63:74:9a:42:79:0a:
0e:ee:a9:4a:73:6b:dc:9e:a8:08:39:d0:99:48:4d:
89:d4:b0:31:1c:eb:18:c8:17:22:fd:6e:85:3f:e6:
b1:64:fc:ca:f7:cb:d7:84:77:e6:02:88:85:6b:ea:
5b:af:eb:be:fc:e2:07:3c:f1:71:b1:b1:f0:0d:80:
81:a0:1b:c6:50:28:32:3c:8e:78:55:76:f8:75:30:
36:64:a2:bf:1c:46:06:ad:46:75:3e:59:b0:cd:bc:
45:93

Exponent: 65537 (0x10001)

Subject
Public key

Google's cert 3/5

X509v3 extensions:

X509v3 Extended Key Usage:

TLS Web Server Authentication, TLS Web Client Authentication

X509v3 Subject Alternative Name:

DNS:*.google.com, DNS:*.android.com, DNS:*.appengine.google.com, DNS:*.cloud.google.com, DNS:*.google-analytics.com, DNS:*.google.ca, DNS:*.google.cl, DNS:*.google.co.in, DNS:*.google.co.jp, DNS:*.google.co.uk, DNS:*.google.com.ar, DNS:*.google.com.au, DNS:*.google.com.br, DNS:*.google.com.co, DNS:*.google.com.mx, DNS:*.google.com.tr, DNS:*.google.com.vn, DNS:*.google.de, DNS:*.google.es, DNS:*.google.fr, DNS:*.google.hu, DNS:*.google.it, DNS:*.google.nl, DNS:*.google.pl, DNS:*.google.pt, DNS:*.googleadapis.com, DNS:*.googleapis.cn, DNS:*.googlecommerce.com, DNS:*.googlevideo.com, DNS:*.gstatic.cn, DNS:*.gstatic.com, DNS:*.gvt1.com, DNS:*.gvt2.com, DNS:*.metric.gstatic.com, DNS:*.urchin.com, DNS:*.url.google.com, DNS:*.youtube-nocookie.com, DNS:*.youtube.com, DNS:*.youtubeeducation.com, DNS:*.yimg.com, DNS:android.clients.google.com, DNS:android.com, DNS:g.co, DNS:goo.gl, DNS:google-analytics.com, DNS:google.com, DNS:googlecommerce.com, DNS:urchin.com, DNS:youtu.be, DNS:youtube.com, DNS:youtubeeducation.com

Extensions

Google's cert 4/5

Authority Information Access:

CA Issuers - URI:<http://pki.google.com/GIAG2.crt>

OCSP - URI:<http://clients1.google.com/ocsp>

X509v3 Subject Key Identifier:

24:9E:07:37:EA:BF:A9:3B:D8:47:0C:E1:1C:97:62:D5:00:91:24:9D

X509v3 Basic Constraints: critical

CA:FALSE

X509v3 Authority Key Identifier:

keyid:4A:DD:06:16:1B:BC:F6:68:B5:76:F5:81:B6:BB:62:1A:BA:5A:81:2F

X509v3 Certificate Policies:

Policy: 1.3.6.1.4.1.11129.2.5.1

Policy: 2.23.140.1.2.2

X509v3 CRL Distribution Points:

Full Name:

URI:<http://pki.google.com/GIAG2.crl>

More extensions

Google's cert 5/5

Signature Algorithm: sha256WithRSAEncryption

08:0d:58:57:dd:8a:b5:4e:36:d6:89:2a:b5:0f:88:a5:01:d0:
21:80:fc:f5:11:8d:d4:08:5a:75:22:ac:5b:23:09:0d:bb:50:
1b:73:90:55:6e:b6:35:d0:4d:d7:43:9d:e4:21:f3:66:8b:9b:
e0:57:7d:40:48:e5:70:f5:20:25:bf:9c:9a:f1:ba:89:bf:33:
2a:61:7e:77:23:95:f9:fa:90:1c:e3:54:f2:8c:aa:f1:5b:df:
62:81:c1:79:3f:b5:c0:6d:75:ca:59:3b:3f:a3:9d:13:e6:3c:
e0:08:cd:2f:b3:9f:af:9c:20:ee:1b:91:6c:f2:bd:c0:db:76:
7b:16:3d:1c:31:cd:0e:c4:03:93:89:56:ca:8a:4d:80:18:85:
86:7b:37:74:cd:e7:c5:72:b5:07:32:9e:35:5c:01:62:5c:7e:
c3:e7:32:5e:9e:61:35:0d:a7:32:40:70:26:75:71:d0:fc:90:
62:eb:ac:0c:1a:61:a2:18:39:1c:8c:06:c5:0a:4f:27:be:e0:
2c:d3:83:cd:c4:7c:67:f9:38:0a:ca:0a:49:7d:5e:59:36:f1:
ed:90:3b:bb:ea:74:87:95:31:16:97:bb:34:60:a9:ac:74:48:
8e:ed:7b:4a:09:10:18:8d:58:8a:ee:34:2f:7c:f2:55:97:3f:
5a:01:9c:07

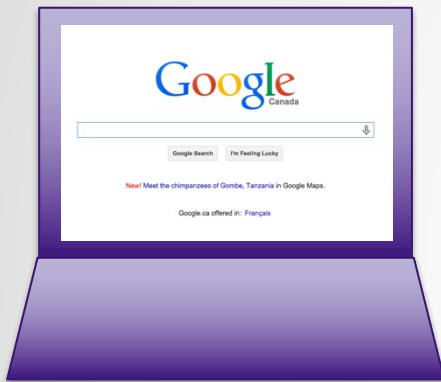
Signature on certificate by CA

Certificate Chains

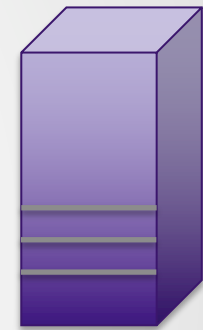
- Ok, so someone signed google.com's public key.
Who signs *their* key?
- Solution: certificate chains
 - Stateless, seamless, transparent
- The end-points of a certificate chain:
 - Starting point: the host (e.g., google.com)
 - End point: a *root* certificate authority that your browser/device trusts (e.g., Geo Trust)
- Why should you trust google.com by trusting GeoTrust (or better yet, your OS)?

Certificate chains

Certificate Chains Example



Hi, let's connect securely



Ok. Here's my public key, **04 5C C2 4B ...** and here's a certificate that endorses it

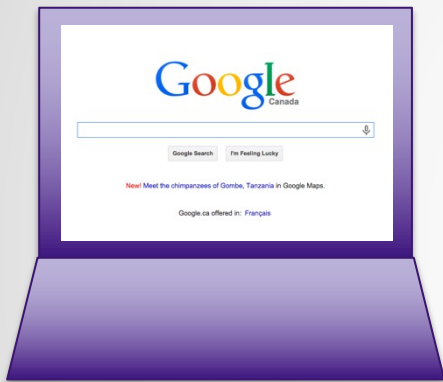


To whom it may concern:

*.google.com's ECDSA signature verification key is:
04 5C C2 4B ...

Yours Sincerely,
Google Internet Authority G2
RSA signature: 27 5C E2 B7 ...

Certificate Chains Example



Ok. So somebody called “Google Internet Authority G2” is claiming this is google.com’s key.

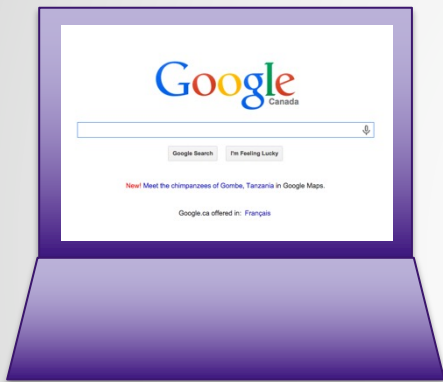
Now I need Google Internet Authority G2’s public key to check the signature!

To whom it may concern:

*.google.com’s ECDSA signature
verification key is:
04 5C C2 4B ...

Yours Sincerely,
Google Internet Authority G2
RSA signature: 27 5C E2 B7 ...

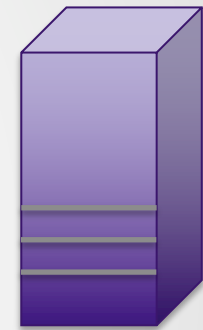
Certificate Chains Example



What Google Internet Authority
G2's public key



It's **9C 2A 04 77...** and here's the
certificate to prove it.



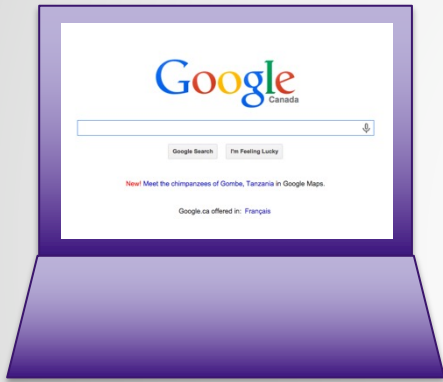
Google

To whom it may concern:

Google Internet Authority G2's
RSA signature verification key is:
9C 2A 04 77...

Yours Sincerely,
Geo Trust Global CA
RSA signature: 27 8C CF E9...

Certificate Chains Example



Ok. So somebody called “Geo Trust Global CA is claiming this is Google Internet Authority G2’s key.

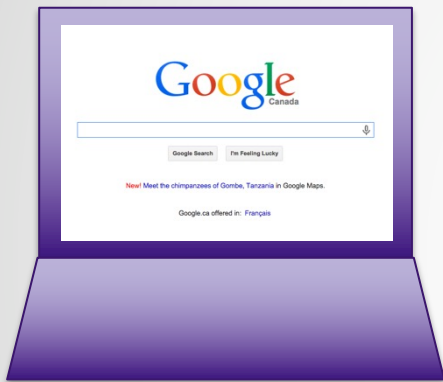
Now I need GeoTrust Global’s public key to check the signature!

To whom it may concern:

Google Internet Authority G2’s
RSA signature verification key is:
9C 2A 04 77...

Yours Sincerely,
Geo Trust Global CA
RSA signature: 27 8C CF E9...

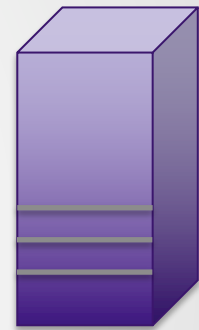
Certificate Chains Example



What Geo Trust Global's public key



It's **35 E3 29 6A...** and here's the certificate to prove it.



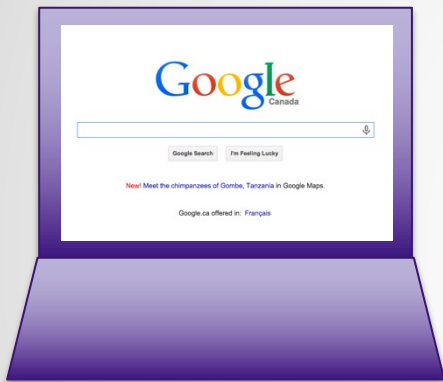
Google

To whom it may concern:

Geo Trust Global's RSA signature
verification key is:
DA CC 18 63...

Yours Sincerely,
Geo Trust Global CA
RSA signature: 35 E3 29 6A...

Certificate Chains Example



Ok. So somebody called “Geo Trust Global CA” is claiming this is Geo Trust Global CA’s key.

Wait a sec. Why should I trust Geo Trust Global to tell me their own key?

To whom it may concern:

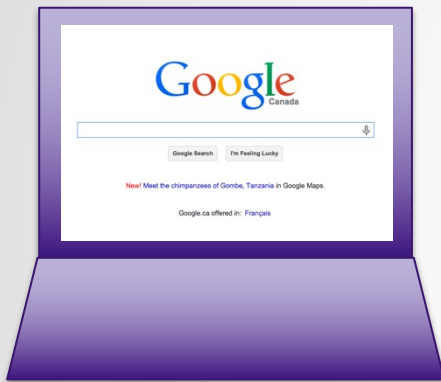
Geo Trust Global’s RSA signature
verification key is:
DA CC 18 63...

Yours Sincerely,
Geo Trust Global CA
RSA signature: 35 E3 29 6A...


Trust Store

- The place in your browser, device or OS where root certificates are stored
 - Demo: let's look at the OSX trust store
- All root CAs are equal in the eyes of your browser, device, OS
 - Any opinions about that?
- Threat scenario: state-level interference with root CA
 - You visit another country. When you try to connect to e.g. Google, a CA local to that country executes a man-in-the-middle attack
 - How?

Certificate



Oh! Geo Trust Global CA's certificate is already on my computer...

 **GeoTrust Global CA**
Root certificate authority
Expires: Saturday, May 21, 2022 at 12:00:00 AM Eastern Daylight Time
✔ This certificate is valid

► **Trust**
▼ **Details**

Subject Name _____
Country US
Organization GeoTrust Inc.
Common Name GeoTrust Global CA

Issuer Name _____
Country US
Organization GeoTrust Inc.
Common Name GeoTrust Global CA

Serial Number 144470
Version 3

Signature Algorithm SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters none

Not Valid Before Tuesday, May 21, 2002 at 12:00:00 AM Eastern Daylight Time
Not Valid After Saturday, May 21, 2022 at 12:00:00 AM Eastern Daylight Time

Public Key Info _____
Algorithm RSA Encryption (1.2.840.113549.1.1.1)
Parameters none
Public Key 256 bytes : DA CC 18 63 30 FD F4 17 ...
Exponent 65537
Key Size 2048 bits

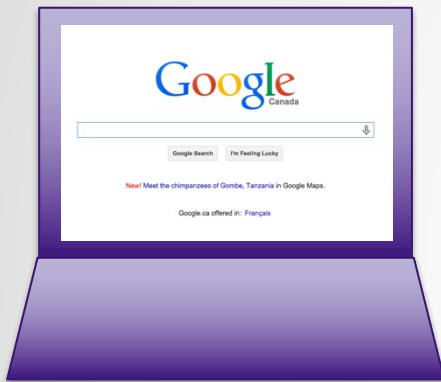
To whom it may concern:

Geo Trust Global's RSA signature verification key is:

DA CC 18 63...

Yours Sincerely,
Geo Trust Global CA
RSA signature: 35 E3 29 6A...

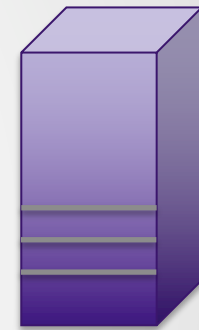
Putting it all Together



Hi, let's connect securely



Ok. Here's my public key, and here's my key certificate chain:



Google

To whom it may concern:

*.google.com's ECDSA signature verification key is:
04 5C C2 4B ...

Yours Sincerely,
Google Internet Authority G2
RSA signature: 27 5C E2 B7 ...

To whom it may concern:

Google Internet Authority G2's
RSA signature verification key is:
9C 2A 04 77...

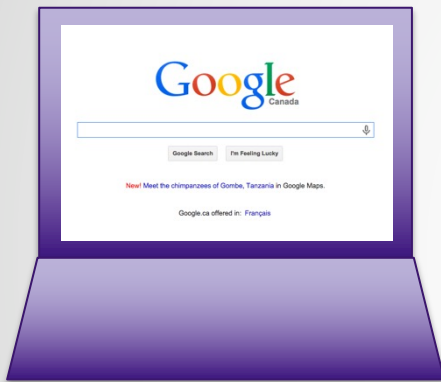
Yours Sincerely,
Geo Trust Global CA
RSA signature: 27 8C CF E9...

To whom it may concern:

Geo Trust Global's RSA signature verification key is:
DA CC 18 63...

Yours Sincerely,
Geo Trust Global CA
RSA signature: 35 E3 29 6A...

Certificate Chains Example



Does this signature verify using this key?

To whom it may concern:

*.google.com's ECDSA signature
verification key is:
04 5C C2 4B ...

Yours Sincerely,
Google Internet Authority G2
RSA signature: 27 5C E2 B7 ...

To whom it may concern:

Google Internet Authority G2's
RSA signature verification key is:
9C 2A 04 77...

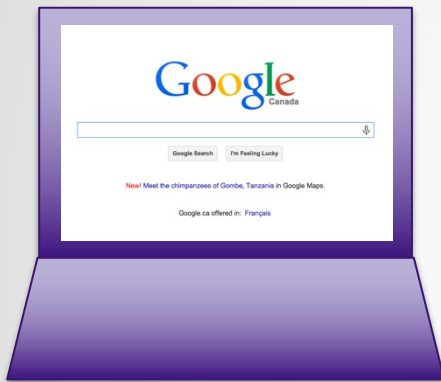
Yours Sincerely,
Geo Trust Global CA
RSA signature: 27 8C CF E9...

To whom it may concern:

Geo Trust Global's RSA signature
verification key is:
DA CC 18 63...

Yours Sincerely,
Geo Trust Global CA
RSA signature: 35 E3 29 6A...

Certificate Chains Example



Does this signature verify using this key?

To whom it may concern:

*.google.com's ECDSA signature
verification key is:
04 5C C2 4B ...

Yours Sincerely,
Google Internet Authority G2
RSA signature: 27 5C E2 B7 ...

To whom it may concern:

Google Internet Authority G2's
RSA signature verification key is:
9C 2A 04 77...

Yours Sincerely,
Geo Trust Global CA
RSA signature: 27 8C CF E9...

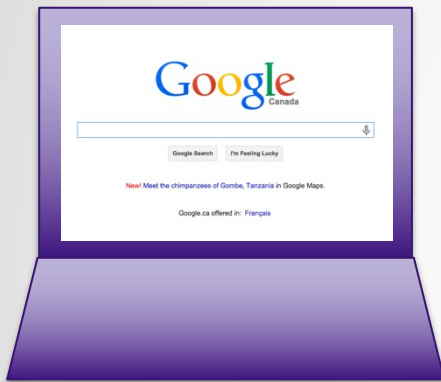
To whom it may concern:

Geo Trust Global's RSA signature
verification key is:
DA CC 18 63...

Yours Sincerely,
Geo Trust Global CA
RSA signature: 35 E3 29 6A...



Certificate Chains Example



Does this signature verify using this key?

To whom it may concern:

*.google.com's ECDSA signature
verification key is:
04 5C C2 4B ...

Yours Sincerely,
Google Internet Authority G2
RSA signature: 27 5C E2 B7 ...

To whom it may concern:

Google Internet Authority G2's
RSA signature verification key is:
9C 2A 04 77...

Yours Sincerely,
Geo Trust Global CA
RSA signature: 27 8C CF E9...

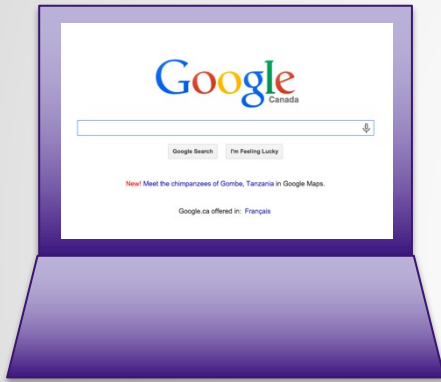
To whom it may concern:

Geo Trust Global's RSA signature
verification key is:
DA CC 18 63...

Yours Sincerely,
Geo Trust Global CA
RSA signature: 35 E3 29 6A...



Certificate Chains Example

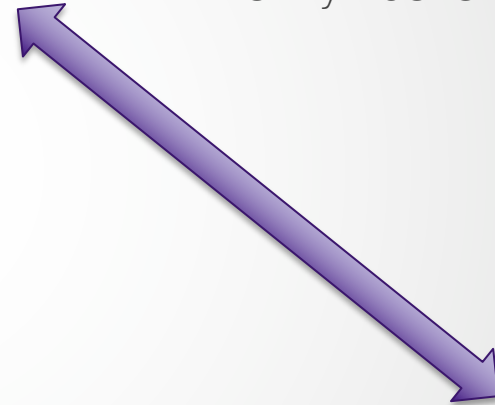


To whom it may concern:

Geo Trust Global's RSA signature
verification key is:
DA CC 18 63...

Yours Sincerely,
Geo Trust Global CA
RSA signature: 35 E3 29 6A...

Do I trust Geo Trust's
key? Yes, this certificate
is my trust store



To whom it may concern:

*.google.com's ECDSA signature
verification key is:
04 5C C2 4B ...

Yours Sincerely,
Google Internet Authority G2
RSA signature: 27 5C E2 B7 ...

To whom it may concern:

Google Internet Authority G2's
RSA signature verification key is:
9C 2A 04 77...

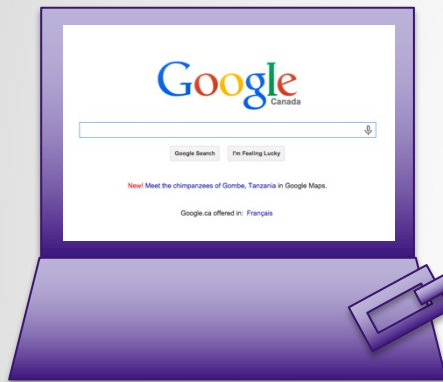
Yours Sincerely,
Geo Trust Global CA
RSA signature: 27 8C CF E9...

To whom it may concern:

Geo Trust Global's RSA signature
verification key is:
DA CC 18 63...

Yours Sincerely,
Geo Trust Global CA
RSA signature: 35 E3 29 6A...

Certificate Chains Example



To whom it may concern:

Geo Trust Global's RSA signature
verification key is:
DA CC 18 63...

Yours Sincerely,
Geo Trust Global CA
RSA signature: 35 E3 29 6A...

A chain of trust has been
established

To whom it may concern:

*.google.com's ECDSA signature
verification key is:
04 5C C2 4B ...

Yours Sincerely,
Google Internet Authority G2
RSA signature: 27 5C E2 B7...

To whom it may concern:

Google Internet Authority G2's
RSA signature verification key is:
9C 2A 01 77...

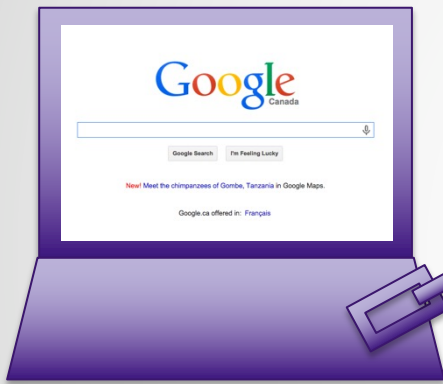
Yours Sincerely,
Geo Trust Global CA
RSA signature: 27 8C CF E...

To whom it may concern:

Geo Trust Global's RSA signature
verification key is:
DA CC 18 63...

Yours Sincerely,
Geo Trust Global CA
RSA signature: 35 E3 29 6A...

Certificate Chains Example



To whom it may concern:

Geo Trust Global's RSA signature
verification key is:
DA CC 18 63...

Yours Sincerely,
Geo Trust Global CA
RSA signature: 35 E3 29 6A...

A chain of trust has been
established, i.e., your
browser trusts
google.com signature
key 04 4C C2 4B....

To whom it may concern:

*.google.com's ECDSA signature
verification key is:
04 5C C2 4B ...

Yours Sincerely,
Google Internet Authority G2
RSA signature: 27 5C E2 B7...

To whom it may concern:

Google Internet Authority G2's
RSA signature verification key is:
9C 2A 01 77...

Yours Sincerely,
Geo Trust Global CA
RSA signature: 27 8C CF E...

To whom it may concern:

Geo Trust Global's RSA signature
verification key is:
DA CC 18 63...

Yours Sincerely,
Geo Trust Global CA
RSA signature: 35 E3 29 6A...

Certificate Pinning

- Directly associate a host with a public key
- “Pin” it in the browser
- Bypasses the certificate chain (you don't have to trust CAs)
- Good for high-assurance applications
 - Malicious CAs (e.g., state-level attacks)
 - Compromised Cas (see e.g., Bit9)

Certificate Revocation

Certificate Revocation

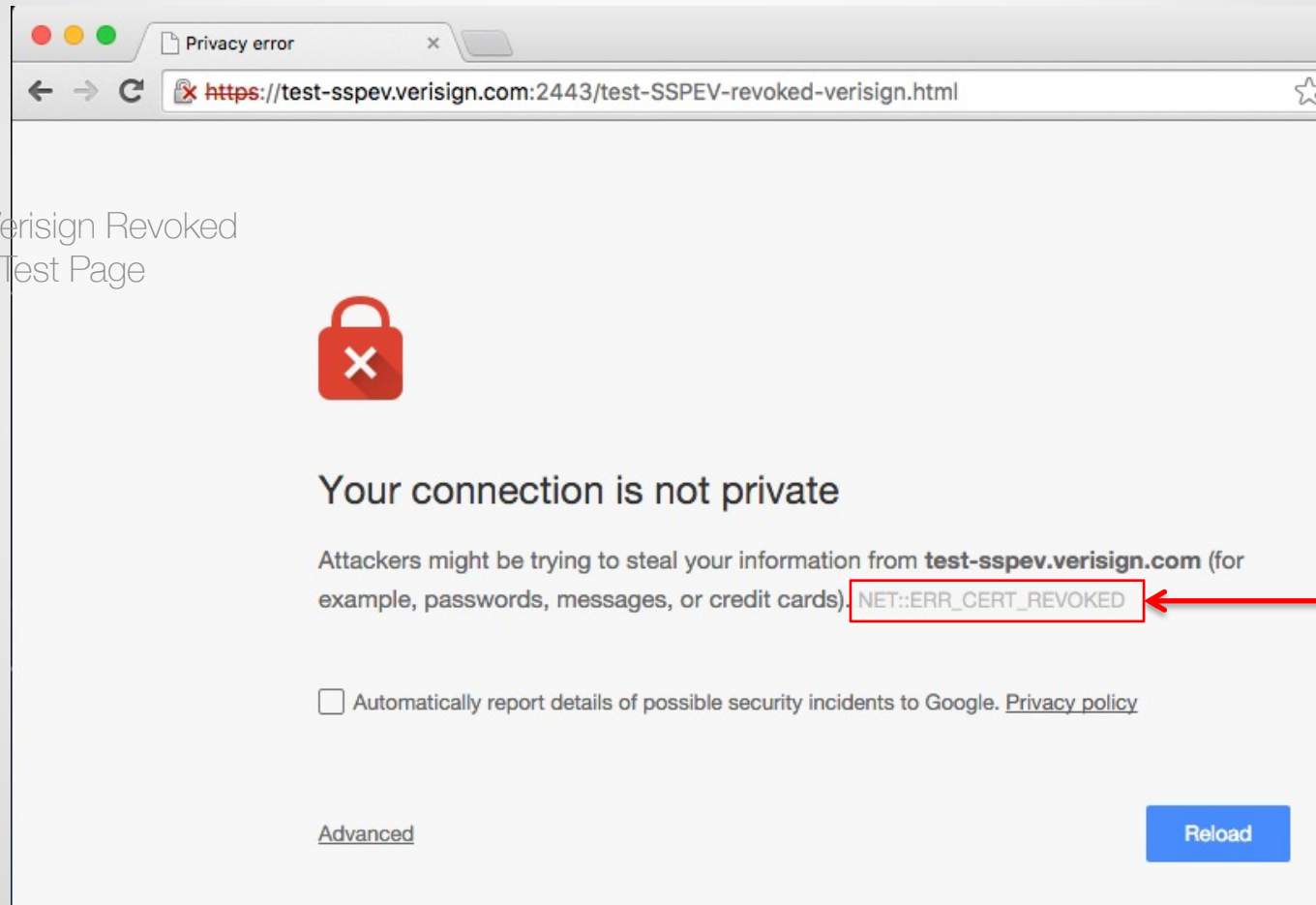
Problem: Sometimes we need to invalidate (revoke) certificates

- Why? All expired certificates are invalid, but not all non-expired certs should be valid.
- Reasons for revocation
 - Company gets hacked (and their private key is compromised)
 - CA gets hacked (and their private key is compromised)
 - New business affiliation/name
 - Company goes out of business
- Security consideration: if you unknowingly trust a revoked certificate, you could get man-in-the-middle

Revoked Certificates


What the users sees:

From the Verisign Revoked
Certificate Test Page



Privacy error

https://test-sspev.verisign.com:2443/test-SSPEV-revoked-verisign.html



Your connection is not private

Attackers might be trying to steal your information from **test-sspev.verisign.com** (for example, passwords, messages, or credit cards). **NET::ERR_CERT_REVOKED**

Automatically report details of possible security incidents to Google. [Privacy policy](#)

[Advanced](#) Reload

Certificate Revocation

There are three main ways a client can check if a certificate has been revoked

- Certificate Revocation Lists
- Requests via the online certificate status protocol (OCSP)
- OCSP stapling

Revocation Mechanisms pt. 1

Certificate Revocation List (CRL):

- Client looks for target certificate in big list of all the revoked certificates
- Issued and signed by CA
- Updated fairly regularly, but not in real-time
- Client has to find, download, and search through them

CRL Example

- Location of Western's CRL (as specified in their certificate):
<http://tj.symcb.com/tj.crl>
- Parse it: `openssl crl -inform DER -in tj.crl -text -noout`
- Contains 3250 entries!

Certificate Revocation List (CRL):

⋮

Version 2 (0x1)

Signature Algorithm: sha256WithRSAEncryption

Issuer: /C=US/O=thawte, Inc./CN=thawte SSL CA - G2

Last Update: Nov 19 09:01:15 2015 GMT

Next Update: Nov 26 09:01:15 2015 GMT

CRL extensions:

X509v3 Authority Key Identifier:

keyid:C2:4F:48:57:FC:D1:4F:9A:C0:5D:38:7D:0E:05:DB:D9:2E:B5:52:60

X509v3 CRL Number:

1478

Revoked Certificates:

Serial Number: 0119B23AAF6FB89DF69F9139E1A5D084

Revocation Date: May 21 13:06:25 2015 GMT

Serial Number: 011BC8CFDD2EA9CEA257E0BC395B668C

Revocation Date: May 26 17:19:20 2015 GMT

Serial Number: 012A260A718016C854F2B4E33DC40942

Revocation Date: Aug 21 21:18:43 2015 GMT

⋮

Serial Number: FA6D7FACDFA4A0F22802B1B7354299

Revocation Date: Sep 23 18:23:48 2015 GMT

Serial Number: FE8C7D2A776CBEED4503EFDBEC6FDF

Revocation Date: Nov 4 10:41:34 2015 GMT

Signature Algorithm: sha256WithRSAEncryption

3a:66:97:dc:d1:1e:cc:e4:bf:b2:02:5d:89:bb:b0:c5:91:db:

ed:cb:c6:0d:7b:ff:c1:a3:23:a7:6b:15:45:2d:7d:63:88:3e:

70:04:b3:83:28:d7:de:a7:60:f7:ec:6d:47:b5:29:25:72:b6:

46:ac:f0:bd:c5:56:e5:7b:36:bc:2b:56:d8:a1:a3:73:73:21:

81:fb:7a:04:b3:2c:ed:09:05:a1:83:dc:d8:cd:f1:1a:4e:64:

f0:dd:06:2d:df:93:94:7b:1f:8c:94:6b:c2:88:09:e8:94:f0:

44:17:a4:91:9a:3a:23:6e:61:64:85:d6:b0:9b:74:89:16:3e:

6d:37:0e:3e:83:c1:c8:31:63:fd:e2:34:67:7d:c5:ed:d9:0b:

8d:ab:8b:11:f9:77:3a:ed:71:74:db:c1:e8:9d:a1:68:ce:9e:

30:1b:8e:9e:97:14:4a:ae:42:d0:c3:12:59:54:b6:5d:ca:d1:

c3:43:8d:d9:66:28:09:9a:6c:ef:03:18:c9:a3:c9:4b:3d:46:

84:f2:3e:ec:59:10:0f:7d:61:93:dc:28:4d:43:d2:fb:73:77:

54:5f:91:c6:57:d1:85:0c:dc:06:ba:27:7c:d6:ba:a5:e8:28:

c4:9d:34:ce:8f:35:77:2c:3a:01:d9:b5:e8:95:c5:86:8b:e7:

8e:f4:48:bc

Revocation Mechanisms pt. 2

Online Certificate Status Protocol (OCSP)

- Created as alternative to CRL's
- Client makes an online request to the CA to check status of a certificate
- CA returns a time-stamped, signed response
- Real-time update. Less work for client. Potentially less work for CA
- Privacy issue: CAs know what website you're visiting!

Revocation Mechanisms pt. 3

OCSP Stapling

- Problem: OCSP requests are not as efficient as they could be:
 - Certificates status requests for high traffic websites can overload CA
 - Also slower for client: they have to connect to a website *and* its CA
- Idea: What if the server makes the OCSP request and then appends, or “staples” the CA’s signed, timestamped response onto the certificate chain
- Resource cost lower for CA and client, and only slightly higher for server
- CA’s don’t know what websites you’re visiting
- Starting to be adopted. Supported by all major CAs and browsers, but requires server admins to enable it