

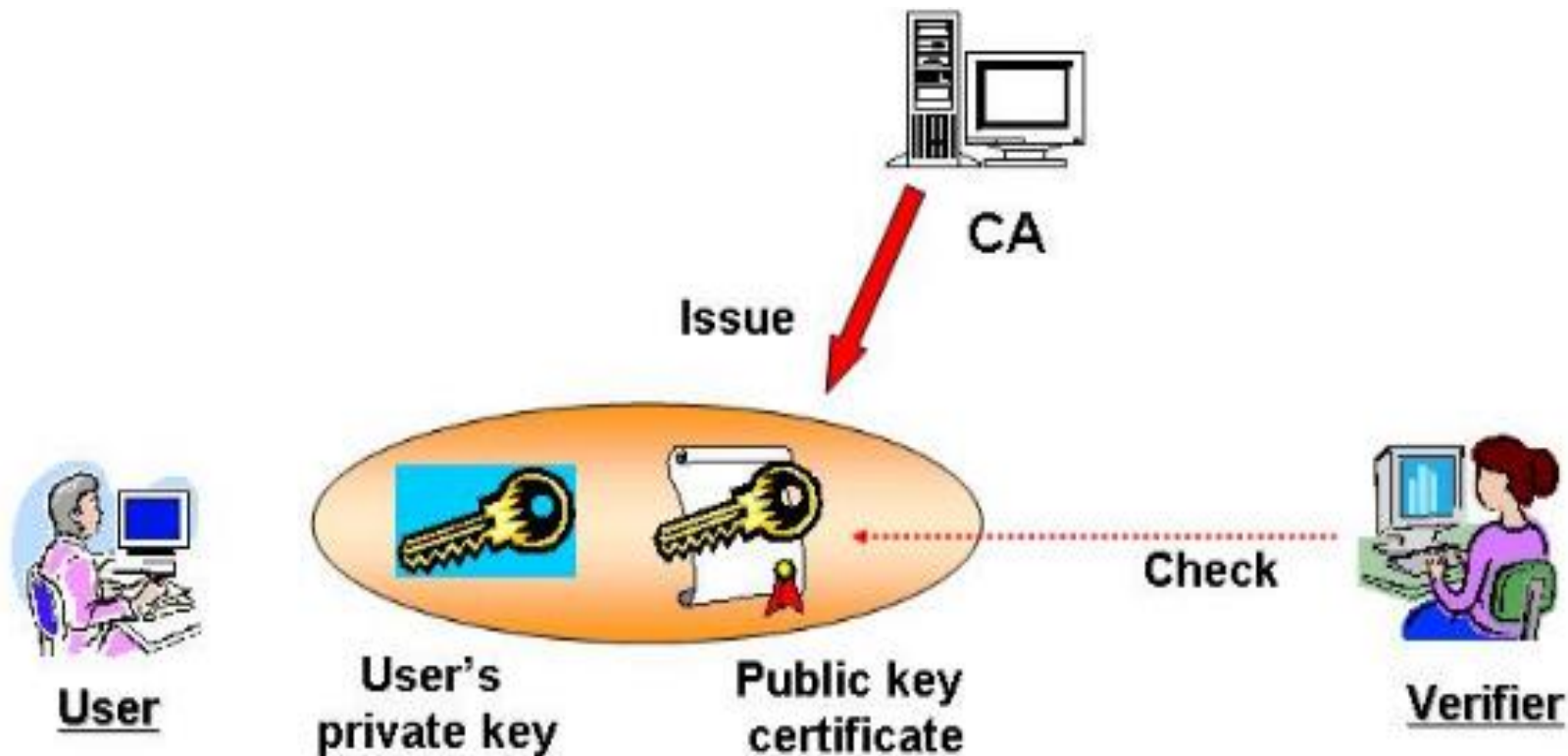


PKI: Trust but Verify!

A presentation by Dmitry Belyavsky, TCI

International conference for ccTLD registries and registrars of CIS, Central and Eastern Europe

Greece, Creta, September 2013



^{*)} **PKI (public-key infrastructure)** is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates

The first (?) case: COMODO

March 2011



One of COMODO partners issued certificates:

Addons.mozilla.org, Login.live.com,
Mail.google.com, www.google.com,
Login.yahoo.com (x3), Login.skype.com

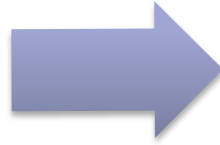


Quick reaction on COMODO side
Certificates are revoked
The Partner is “punished”



To be continued: DigiNotar

June 2011



Certification Authority
DigiNotar issued
certificates for more than 20
sites, Google among them

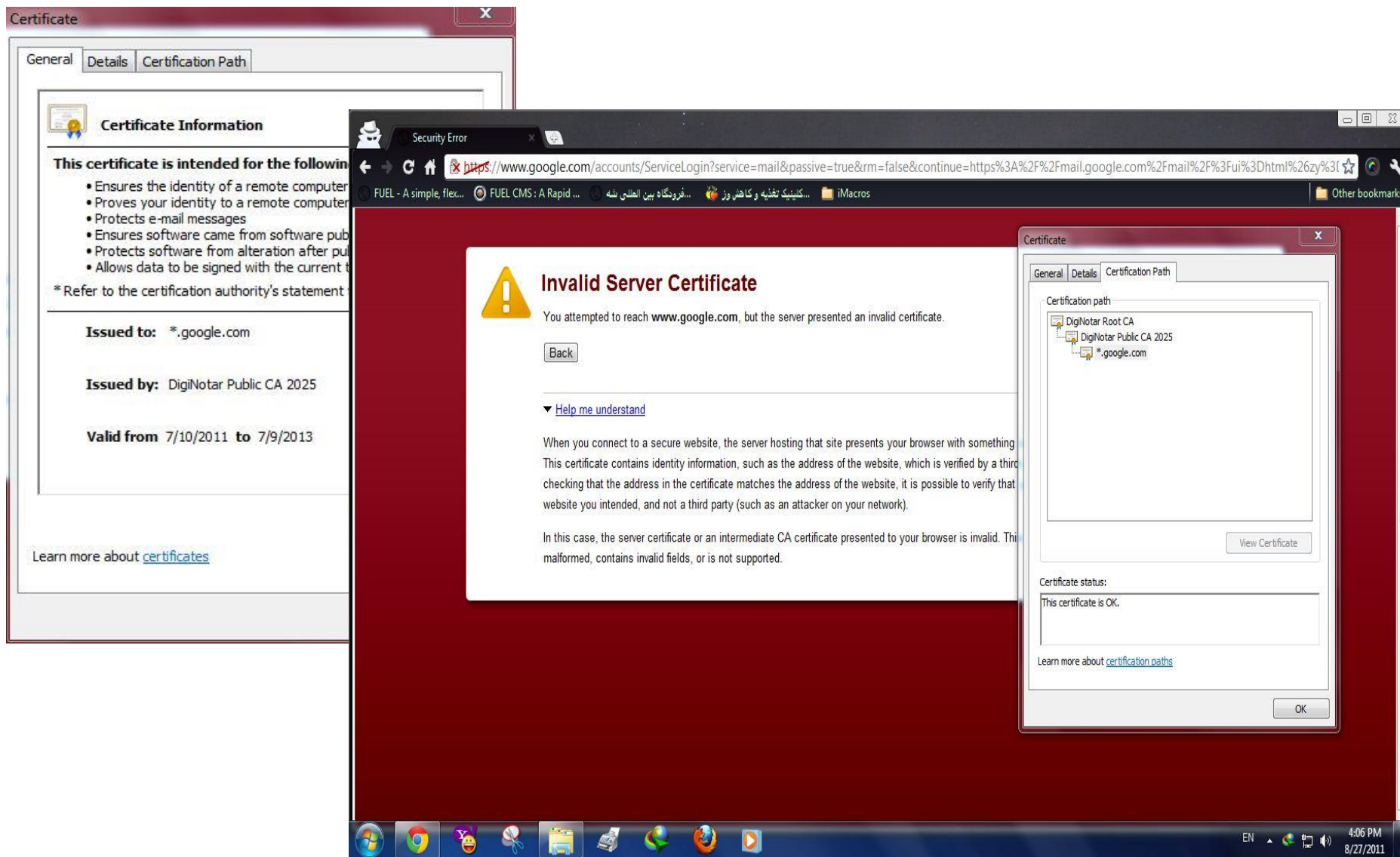


Browsers excluded
DigiNotar certificates for
good
The company went
bankrupt



DigiNotar inactivity
First complaint appeared on
Google forum (Chrome
browser contains the list of
real Google sites
certificates)

More about “DigiNotar case”



The screenshot shows a Windows desktop environment. In the background, a web browser window displays a "Security Error" message from Google. The address bar shows a URL to a Google account login page. The error message states: "Invalid Server Certificate. You attempted to reach www.google.com, but the server presented an invalid certificate." Below the message is a "Back" button and a "Help me understand" link. The text explains that certificates contain identity information and that in this case, the server certificate or an intermediate CA certificate is invalid.

Overlaid on the left is a "Certificate" window showing "Certificate Information". It states: "This certificate is intended for the following:" followed by a list of purposes: "Ensures the identity of a remote computer", "Proves your identity to a remote computer", "Protects e-mail messages", "Ensures software came from software publisher", "Protects software from alteration after publication", and "Allows data to be signed with the current time". It also includes fields for "Issued to: *.google.com", "Issued by: DigiNotar Public CA 2025", and "Valid from 7/10/2011 to 7/9/2013".

Overlaid on the right is another "Certificate" window showing the "Certification Path". The path is: "DigiNotar Root CA" -> "DigiNotar Public CA 2025" -> "*.google.com". The "Certificate status" section indicates "This certificate is OK." and includes a "View Certificate" button.

The Windows taskbar at the bottom shows the Start button, several application icons (including Chrome, Firefox, and a folder), and the system clock indicating 4:06 PM on 8/27/2011.

More about “DigiNotar case”



OSCP requests for the fake *.google.com certificate

Source: FOX-IT, Interim Report, <http://cryptome.org/0005/diginotar-insec.pdf>

2012

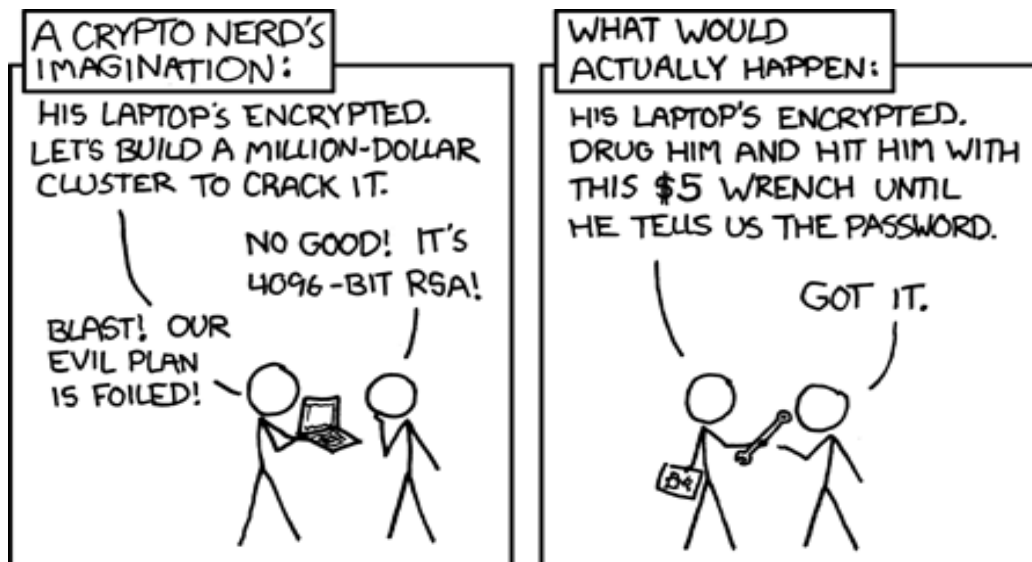
Trustware

issued a certificate for DLP-system

TurkTrust

“incorrectly” issued certificate with extra permissions

2013



Source: <http://xkcd.com/538/>

Five pieces of advice

- ✓ Hide in the network
- ✓ Encrypt your communications
- ✓ Assume that while your computer can be compromised, it would take work and risk on the part of the NSA – so it probably isn't
- ✓ Be suspicious of commercial encryption software, especially from large vendors
- ✓ Try to use public-domain encryption that has to be compatible with other implementations



Bruce Schneier:
“I understand that
most of this is
impossible for the
typical internet user”



DANE (RFC 6698):

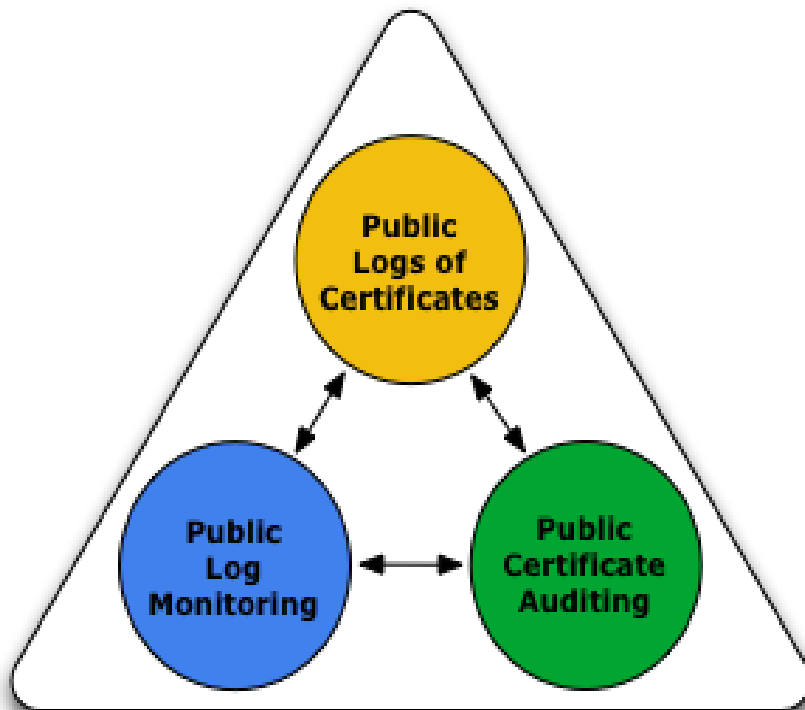
Limited browsers support

Certificate pinning:

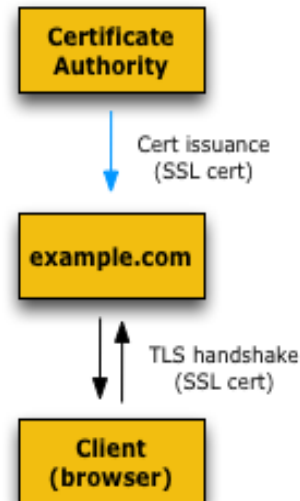
Mozilla Certificate Patrol,
Chrome cache for Google certificates

Certificate transparency (RFC 6962)

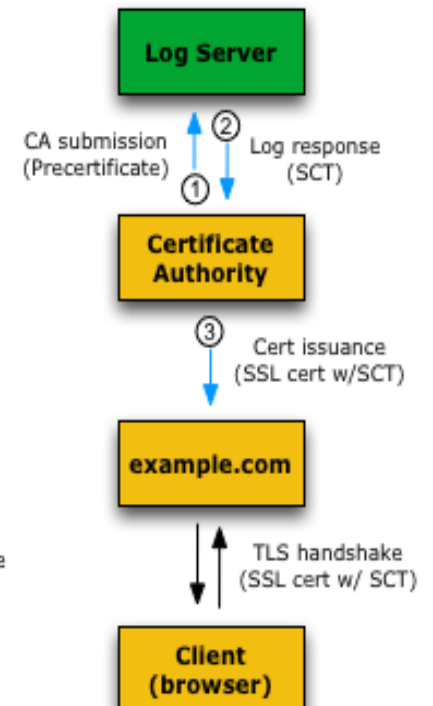
Certificate Transparency: how it works



Current TLS/SSL System

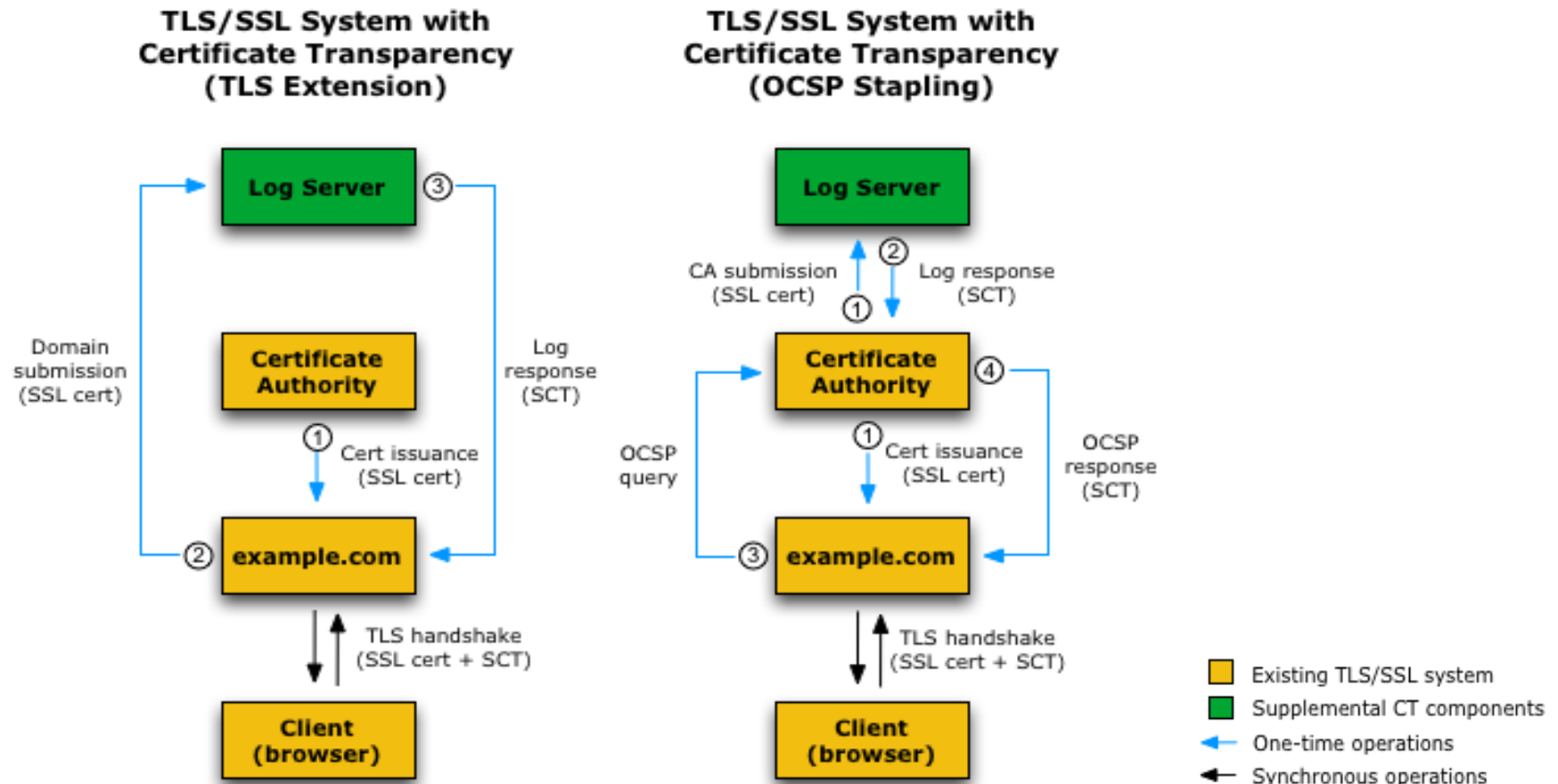


TLS/SSL System with
Certificate Transparency
(X.509v3 Extension)



- Existing TLS/SSL system
- Supplemental CT components
- One-time operations
- ↔ Synchronous operations

Certificate Transparency: how it works





A 4x4 grid of squares, with the top-left square missing, forming a triangular shape.

For today the cryptographic https mechanism is not a guarantee of safety



The weakest element in the safety system provision is

HUMAN FACTOR!



Questions?

Drop 'em at:

beldmit@tcinet.ru