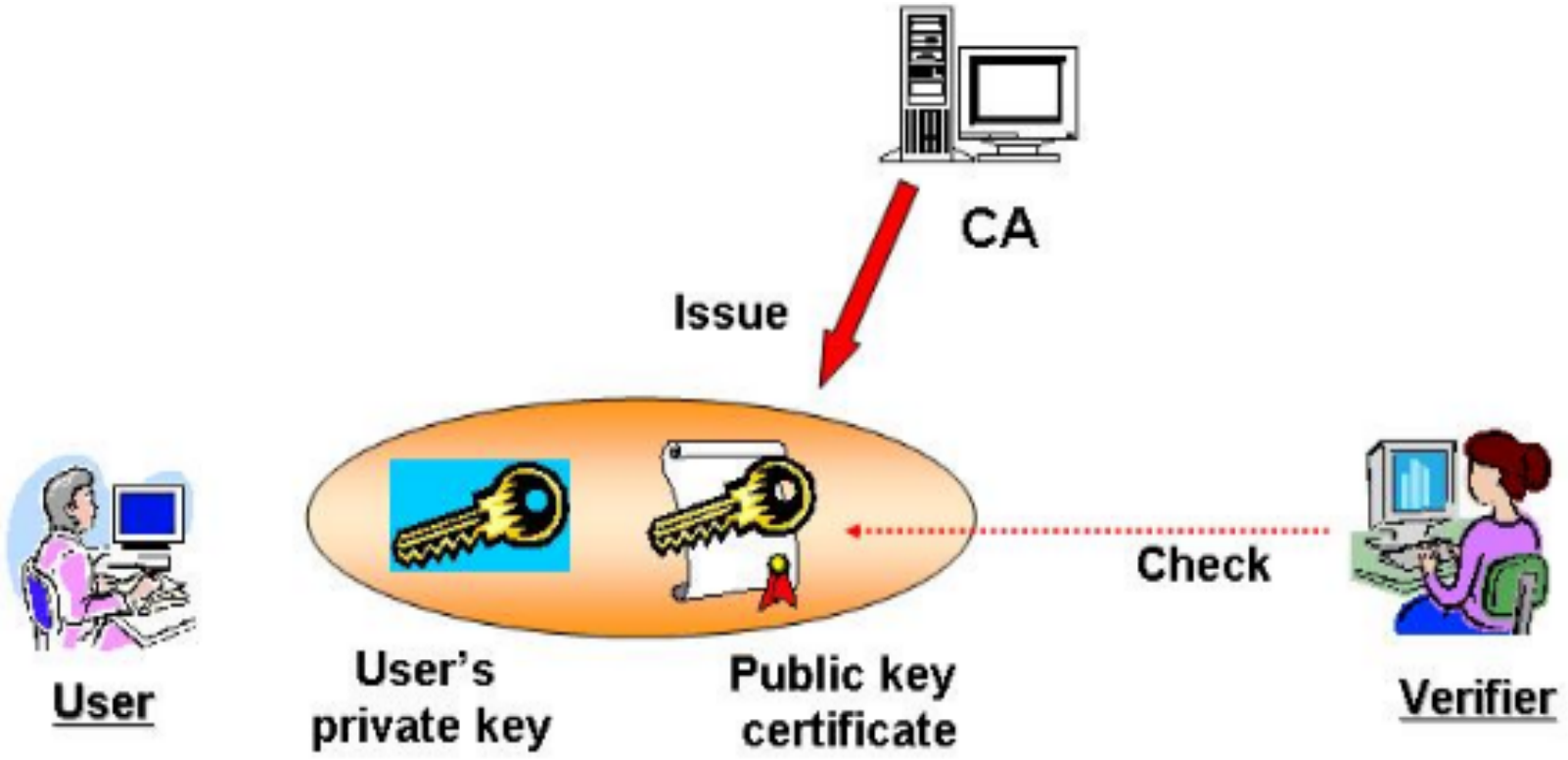
Certificate transparency: New part of PKI infrastructure

A presentation by Dmitry Belyavsky, TCI

ENOG 7
Moscow, May 26-27, 2014

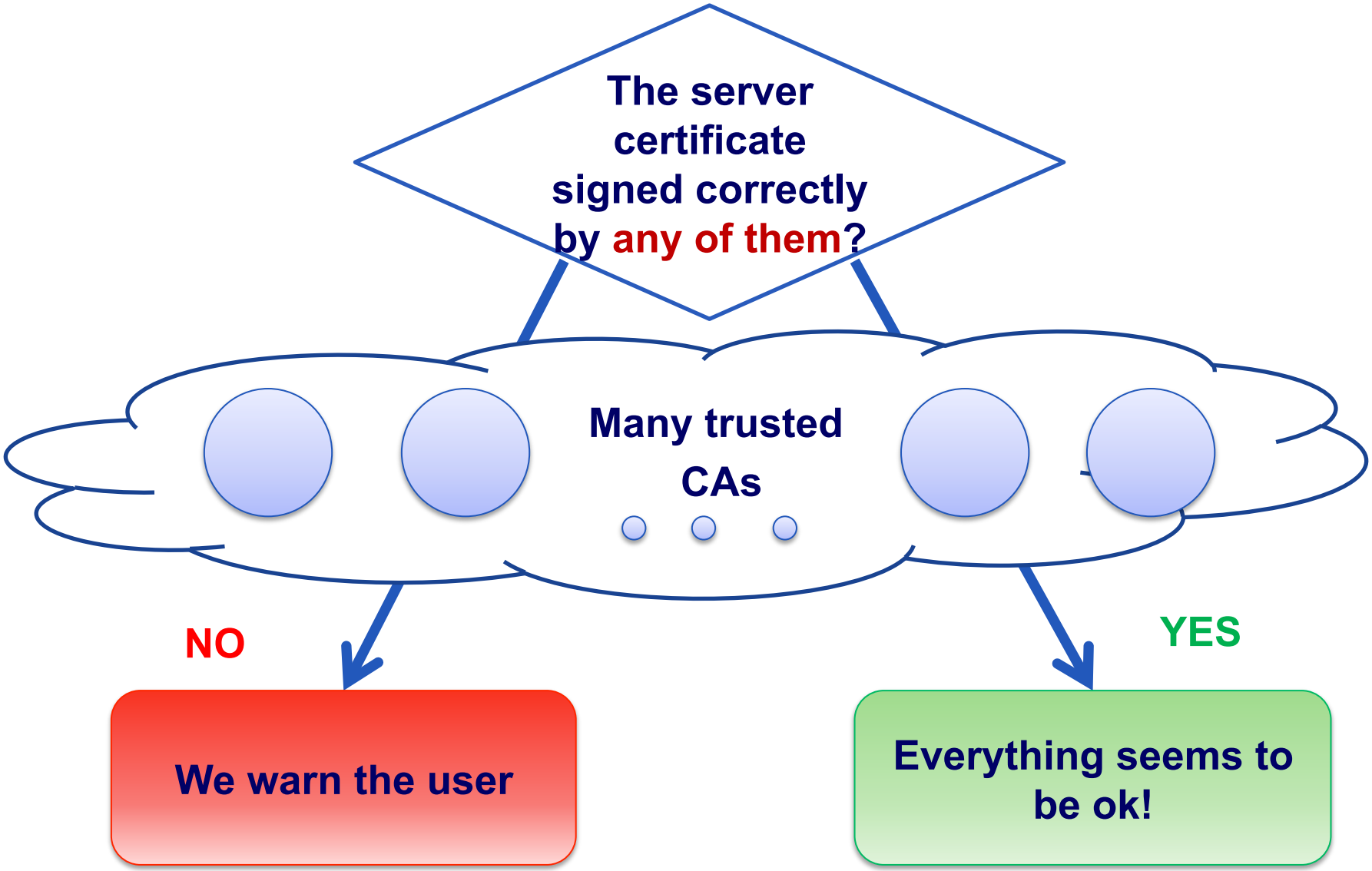
Technical Centre of Internet

About PKI *)



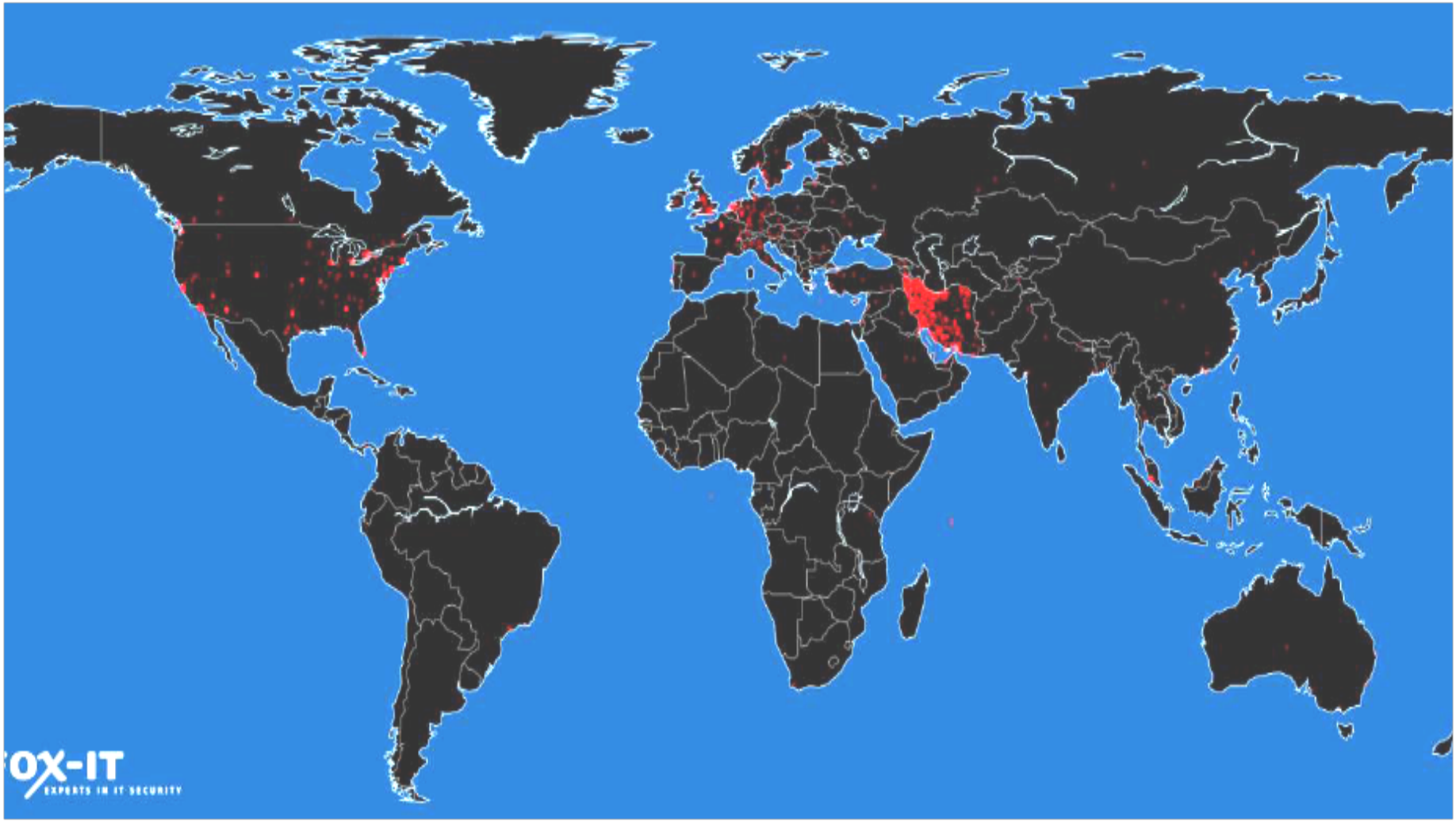
*) **PKI (public-key infrastructure)** is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates

Check the server certificate



Technical Centre of Internet

DigiNotar case



OCSP requests for the fake *.google.com certificate

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

Technical Centre of Internet

PKI: extra trust

DANE (RFC 6698)

Limited browsers support

Certificate pinning

Mozilla Certificate Patrol,
Chrome cache for Google certificates

Certificate transparency (RFC 6962)

Inspired by Google (Support in Chrome appeared)
One of the authors - Ben Laurie (OpenSSL Founder)
CA support – Comodo

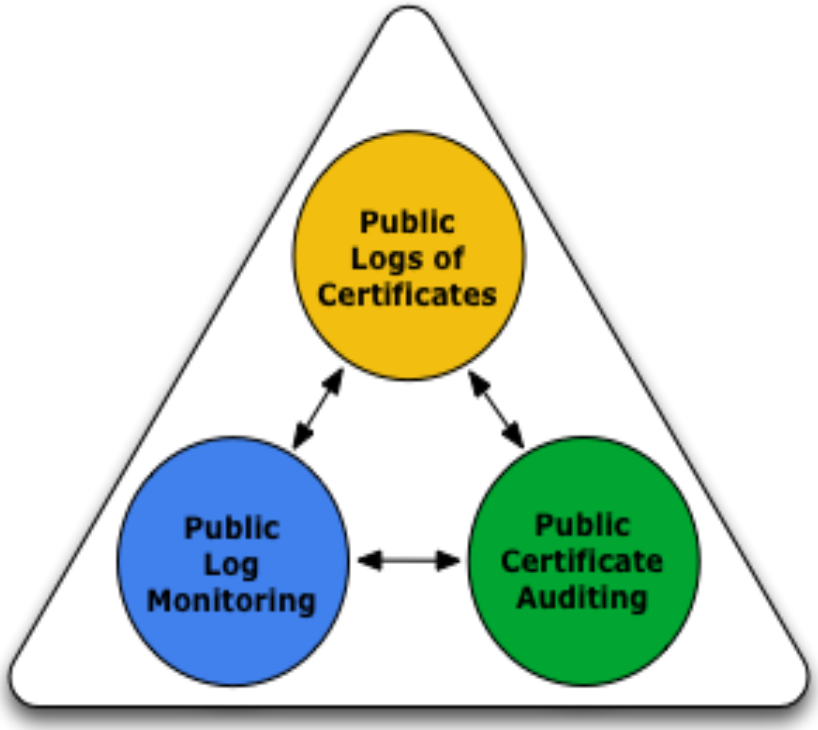
Technical Centre of Internet

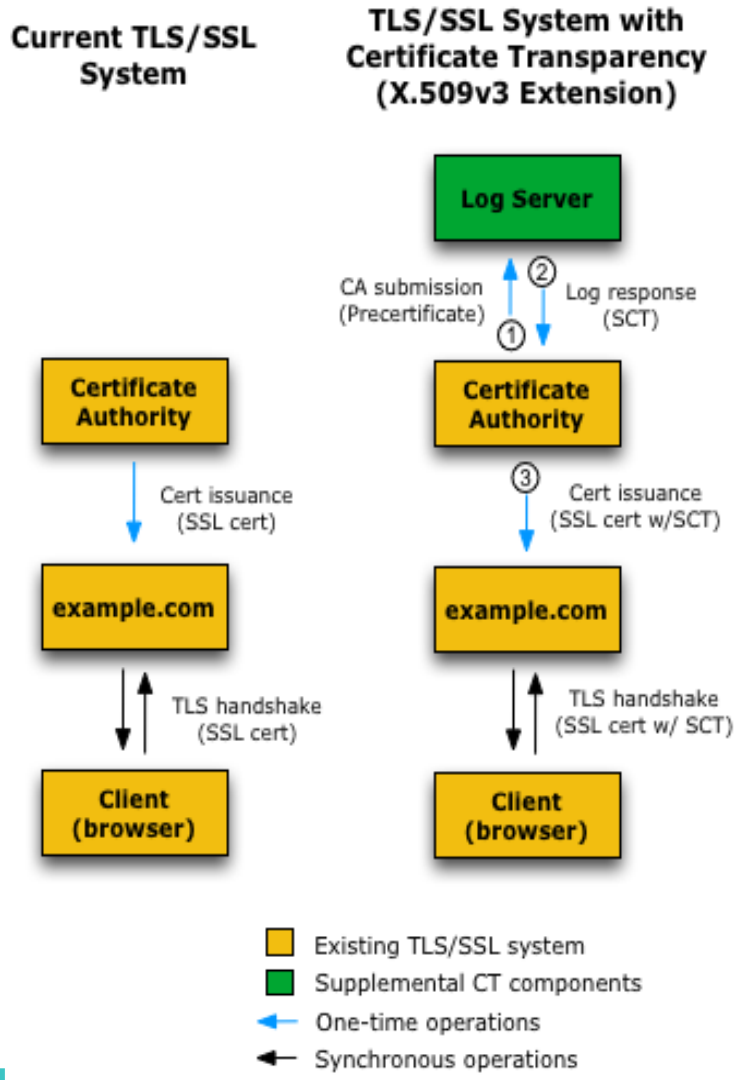
Certificate Transparency: how it works

	• Log accepts cert => SCT
Client	•Is SCT present and signed correctly?
Client	•Is SCT present and signed correctly?
Auditor	•Does log server behave correctly?
Monitor	•Any suspicious certs?

Technical Centre of Internet

Certificate Transparency: how it works

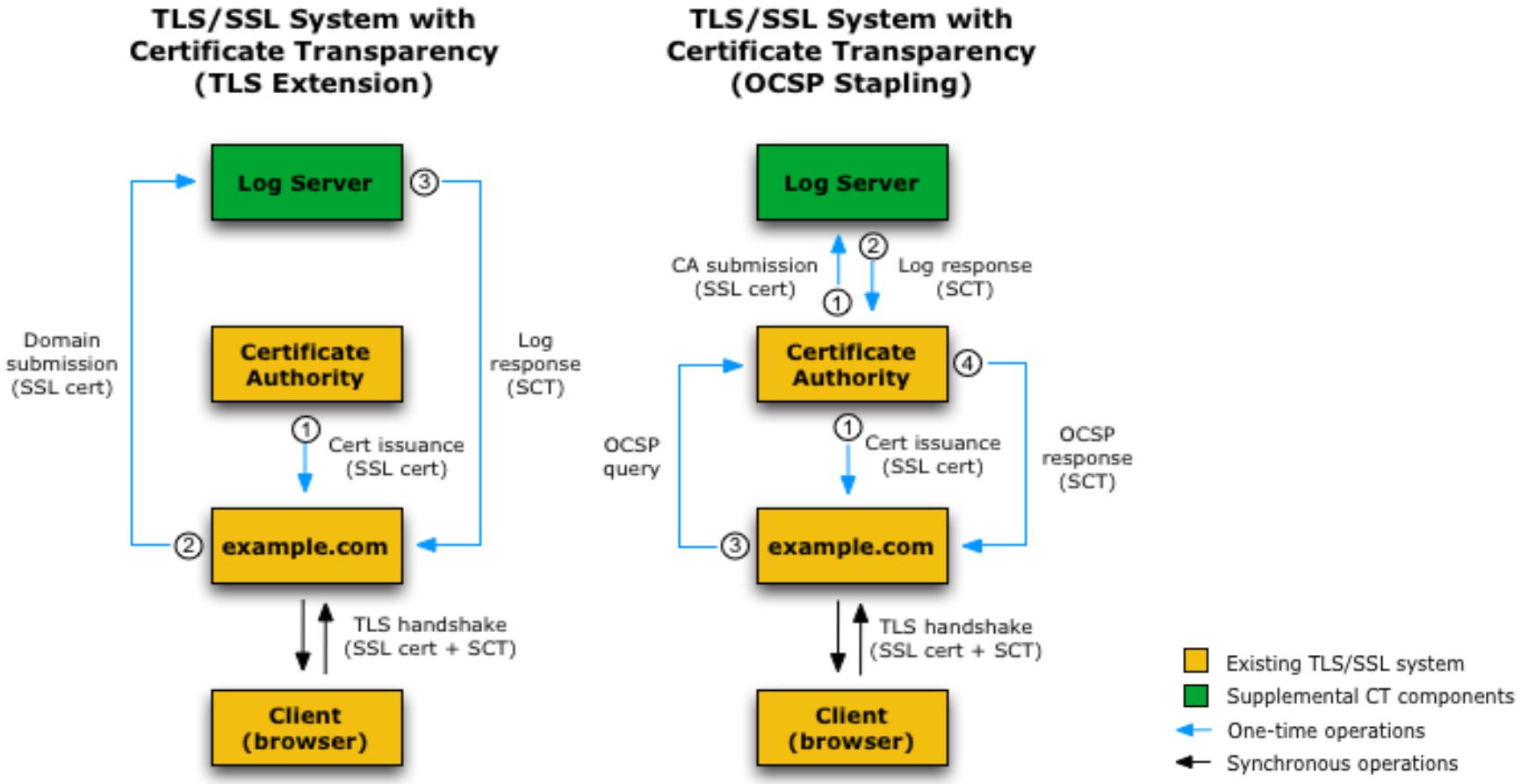




Source: http://www.certificate-transparency.org

Technical Centre of Internet

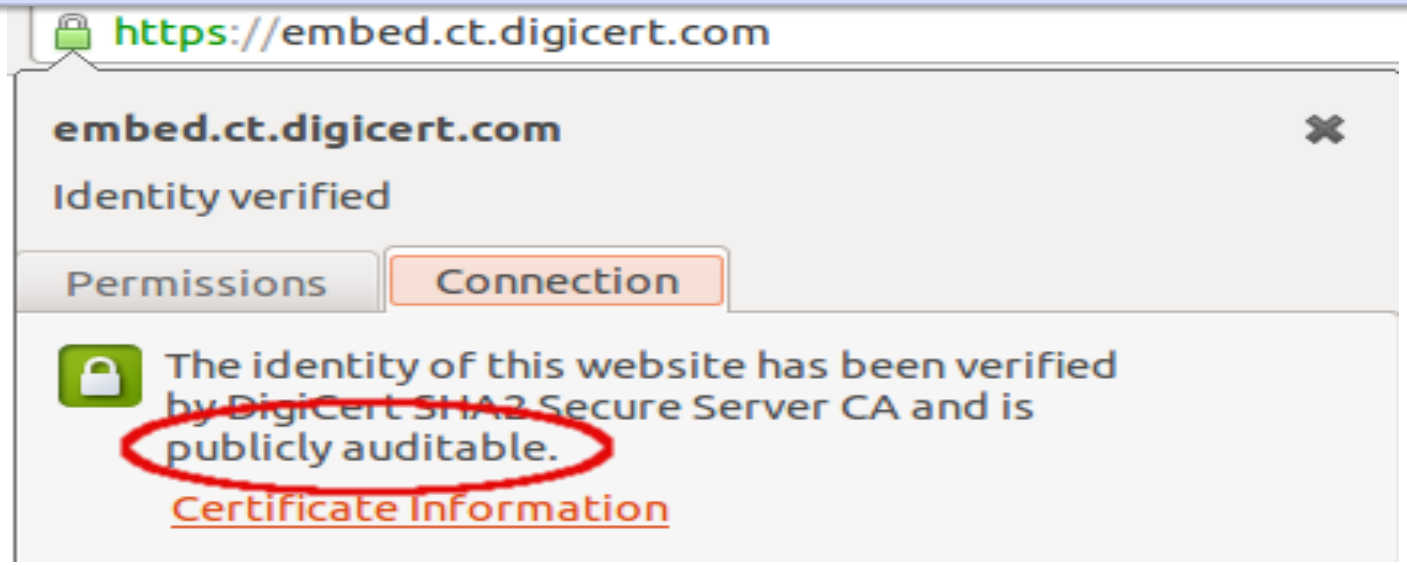
Certificate Transparency how it works



Source: http://www.certificate-transparency.org

Certificate Transparency current state

Google Chrome Support (33+)



http://www.certificate-transparency.org/certificate-transparency-in-chrome

Google Cert EV plan

http://www.certificate-transparency.org/ev-ct-plan

Certificate Transparency current state

Open source code

2 pilot logs

Certificate Transparency: protect from what?

SAVE from MITM attack

- ✓ Warning from browser
- ✓ Site owner can watch logs for certs

Do NOT SAVE from HEARTBLEED!

Certificate transparency and Russian GOST crypto

Russian GOST does not save from the MITM attack

Algorithm

SHA-256 >>> GOSTR34.11-2012

Key

>>> GOST R 34.10-2012

Q&A

Questions?

Drop ‘em at:

beldmit@tcinet.ru