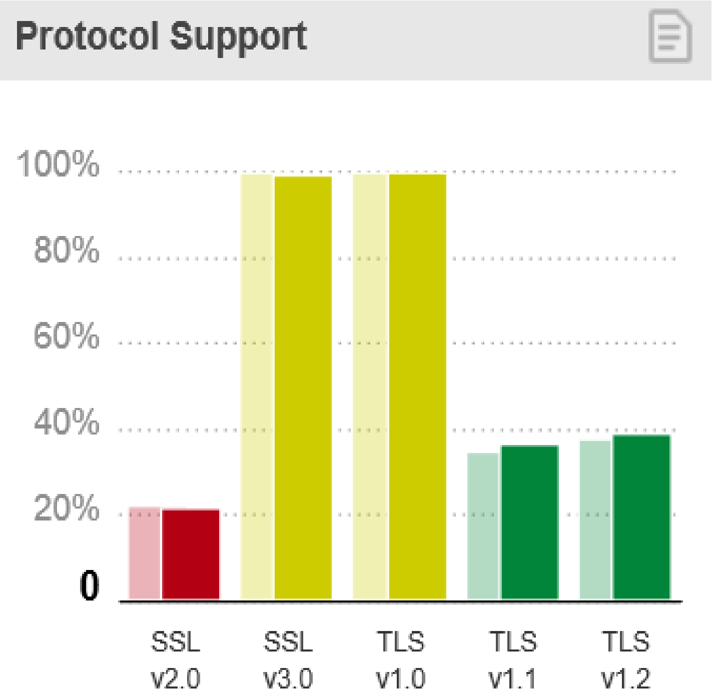
Certificate transparency: New part of PKI infrastructure

A presentation by Dmitry Belyavsky, TCI
BAKU, September 2014

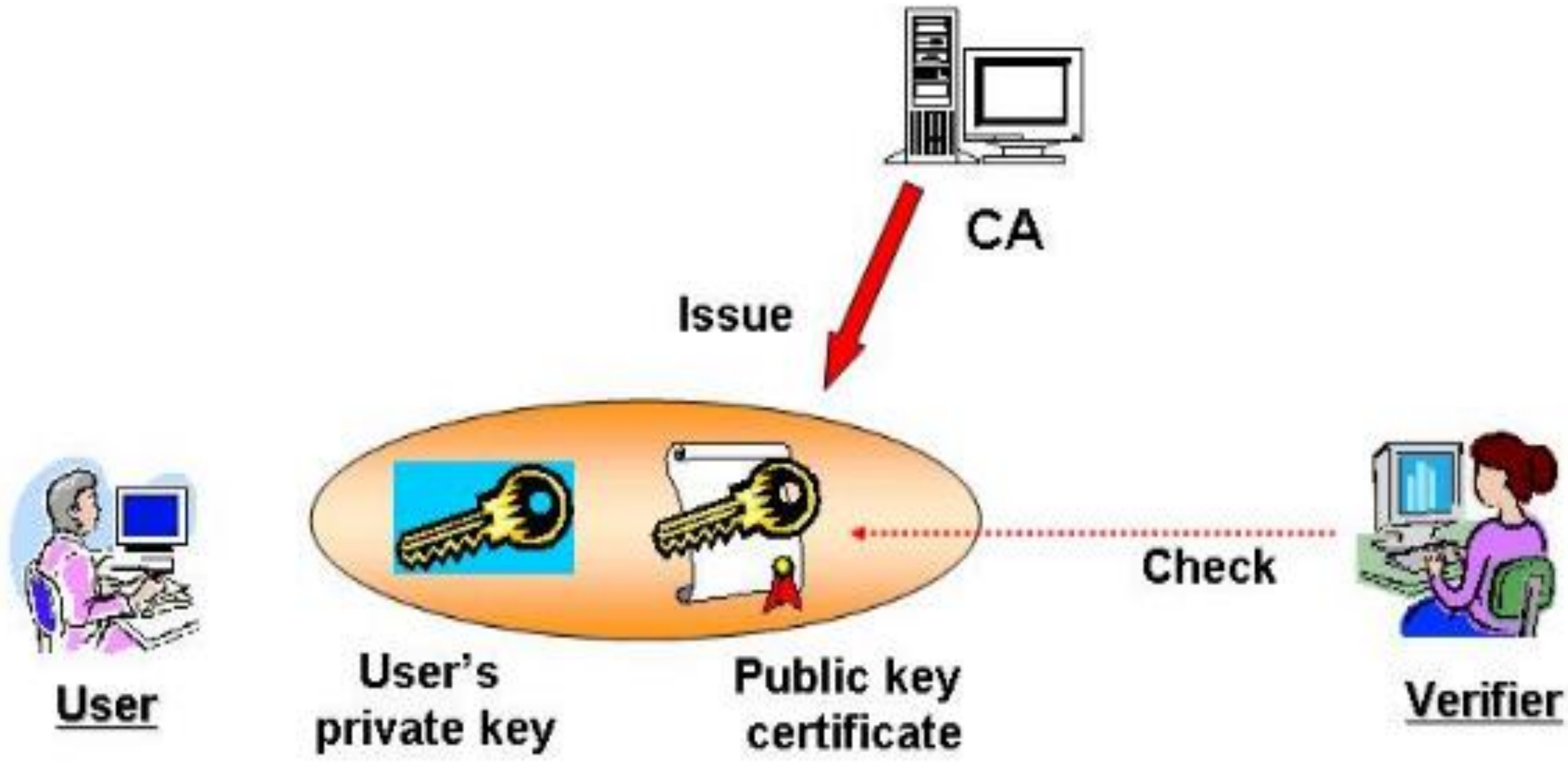
TLS: history

- SSLv2 deprecated by RFC 6176
- SSLv3 still widely supported
- TLS 1.0 in RFC 2246 (1999)
- TLS 1.1 in RFC 4346 (2006)
- TLS 1.2 in RFC 5246 (2008)



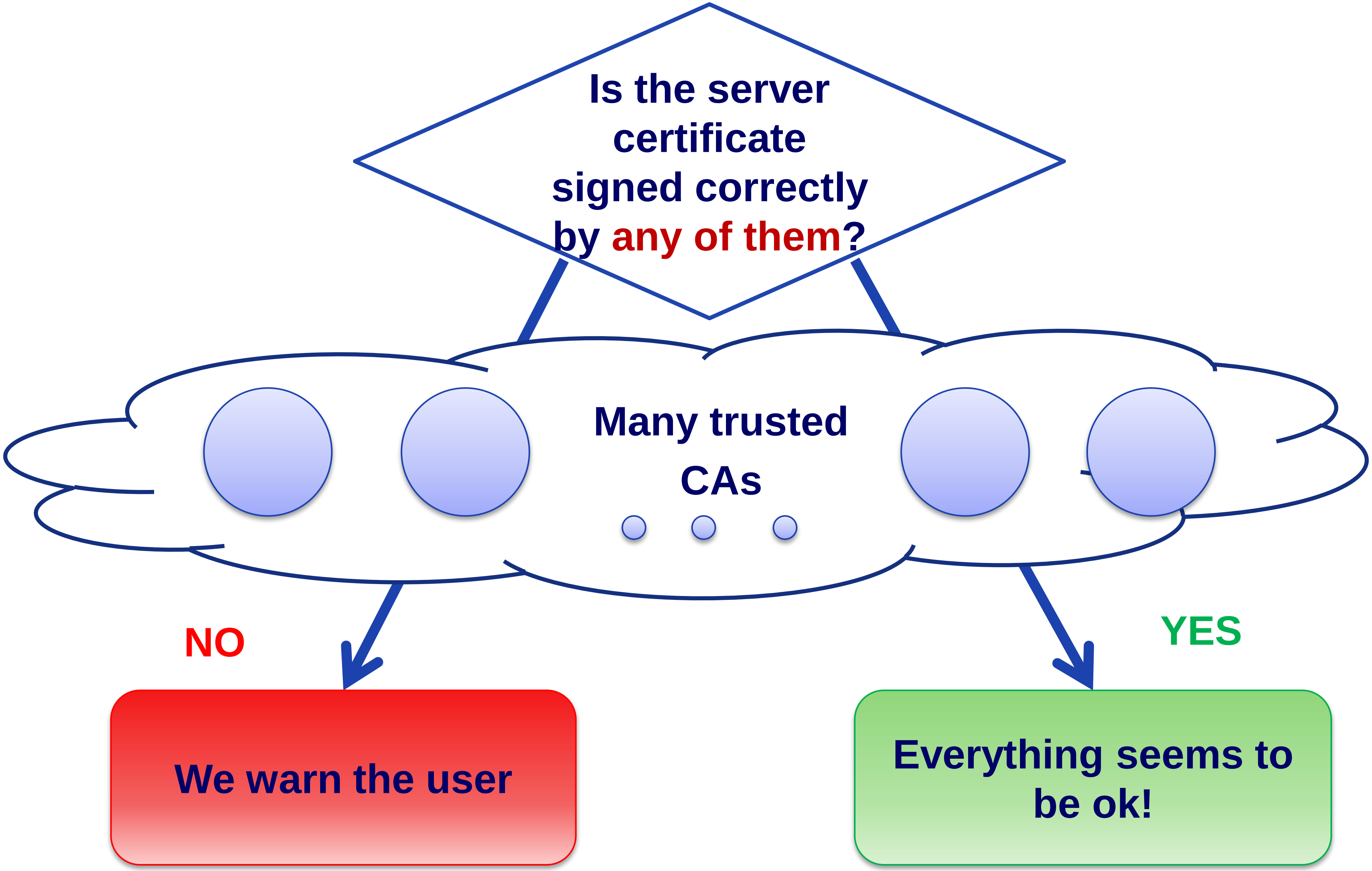
Source: https://www.trustworthyinternet.org/ssl-pulse/

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



Is the server certificate signed correctly by **any of them**?

Many trusted CAs

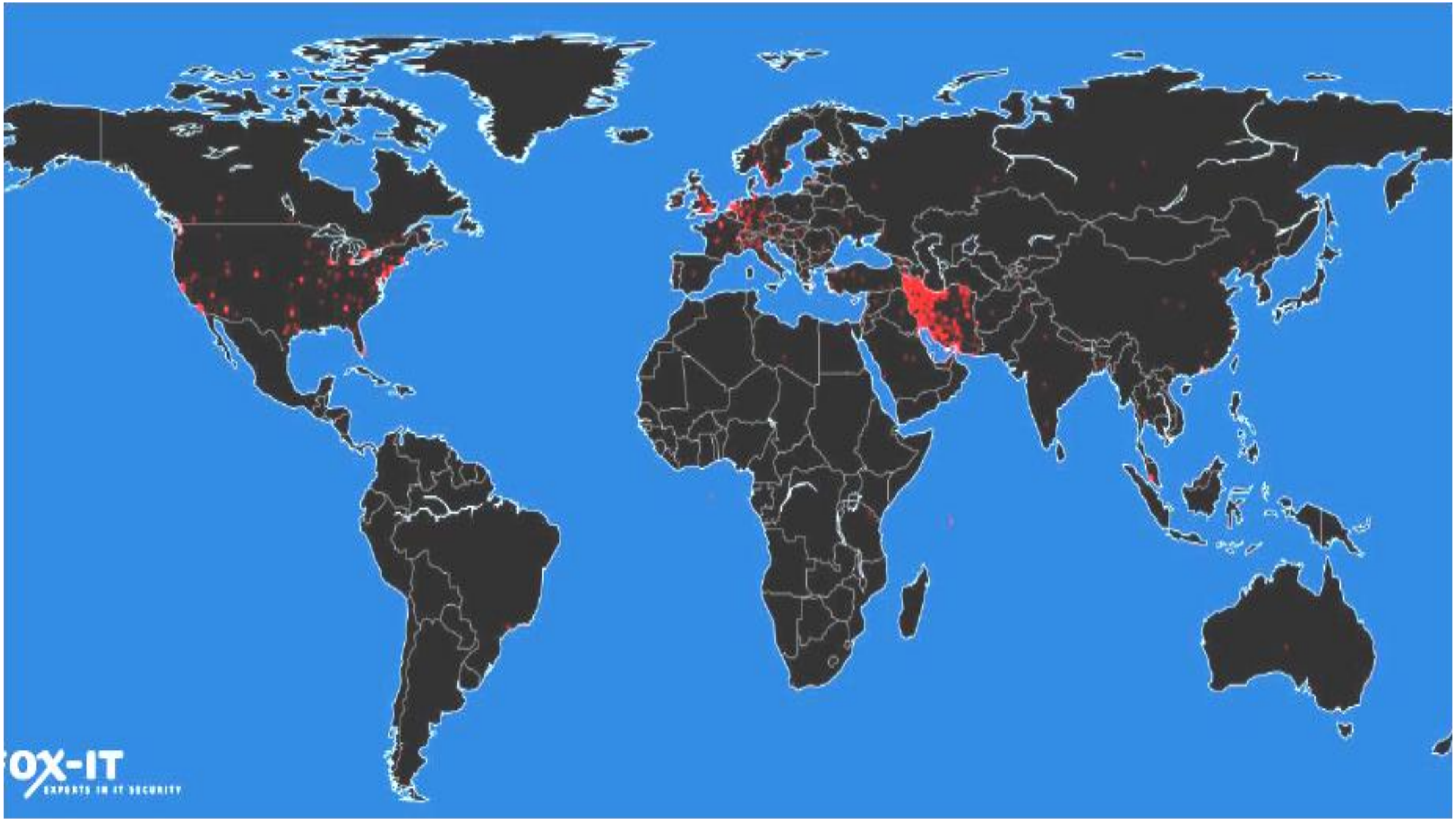
NO

YES

We warn the user

Everything seems to be ok!

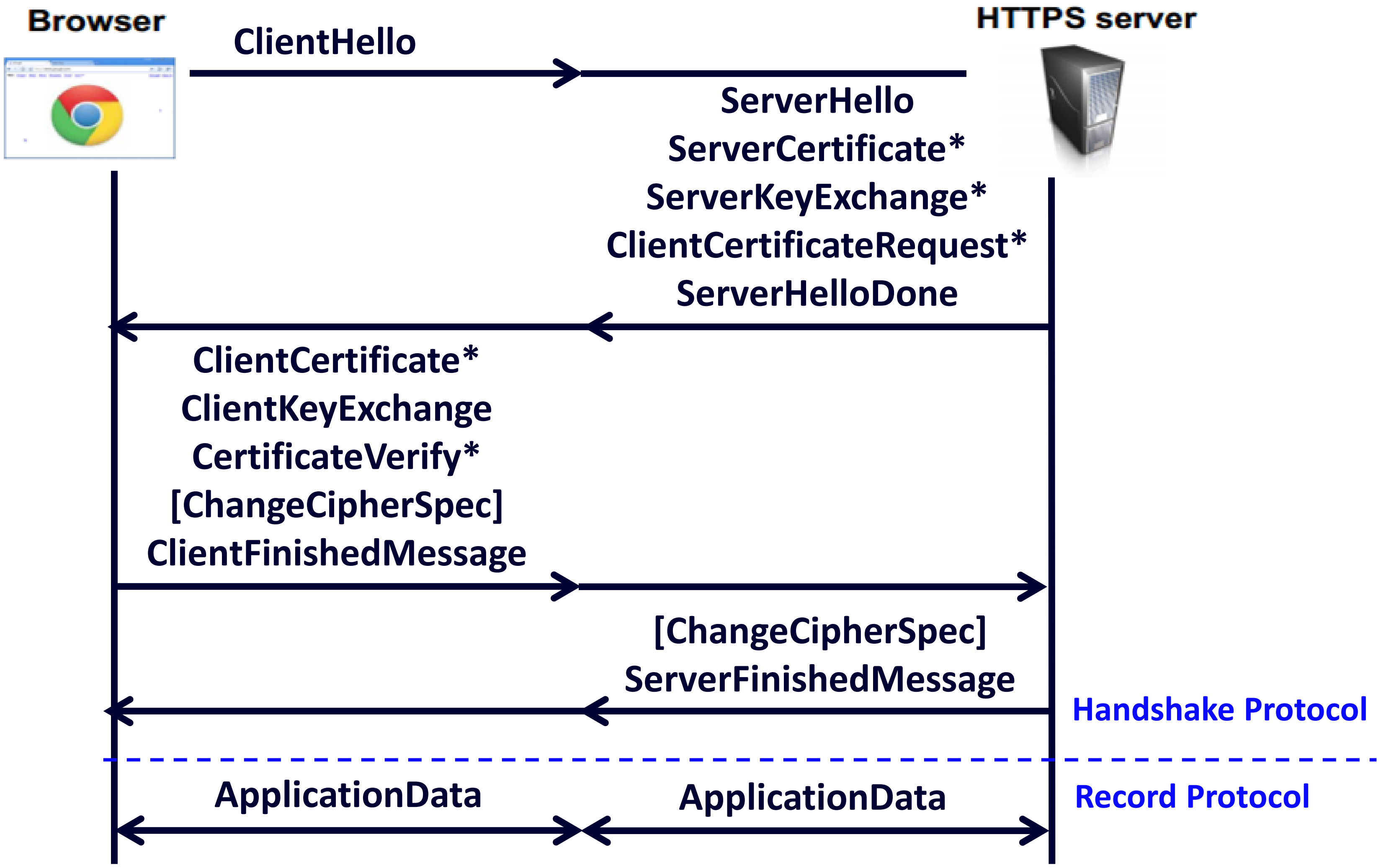
DigiNotar case



OCSP requests for the fake *.google.com certificate

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

TLS: general overview



Browser

HTTPS server

ClientHello

ServerHello
ServerCertificate*
ServerKeyExchange*
ClientCertificateRequest*
ServerHelloDone

ClientCertificate*
ClientKeyExchange
CertificateVerify*
[ChangeCipherSpec]
ClientFinishedMessage

[ChangeCipherSpec]
ServerFinishedMessage

Handshake Protocol

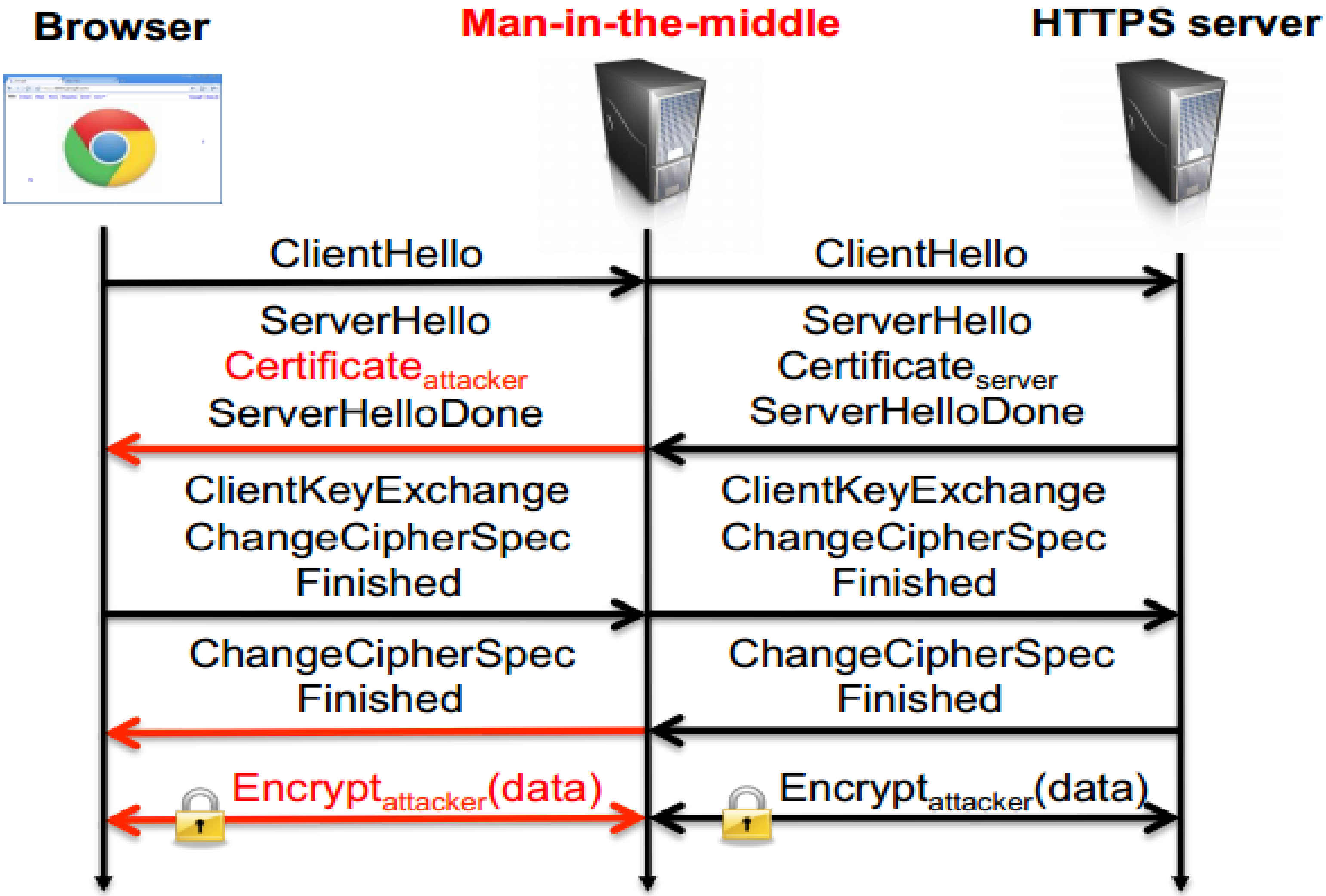
ApplicationData

ApplicationData

Record Protocol

* Optional or situation-depended messages

MITM-attack



Browser

Man-in-the-middle

HTTPS server

ClientHello

ClientHello

ServerHello
Certificate$_{attacker}$
ServerHelloDone

ServerHello
Certificate$_{server}$
ServerHelloDone

ClientKeyExchange
ChangeCipherSpec
Finished

ClientKeyExchange
ChangeCipherSpec
Finished

ChangeCipherSpec
Finished

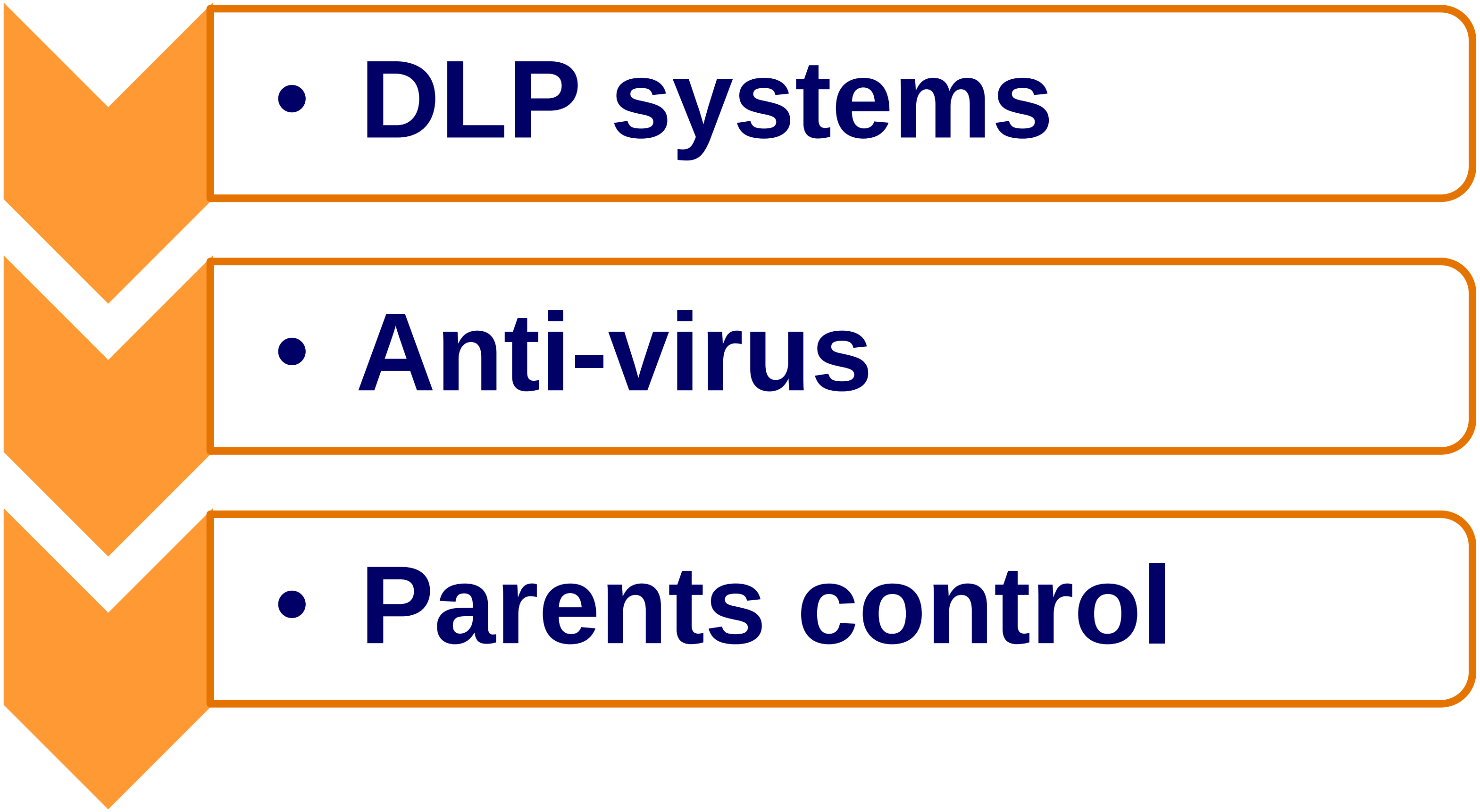
ChangeCipherSpec
Finished

Encrypt$_{attacker}$(data)

Encrypt$_{attacker}$(data)

MITM-attack: positive use

We need traffic analysis!



- DLP systems
- Anti-virus
- Parents control

MITM-attack: detection

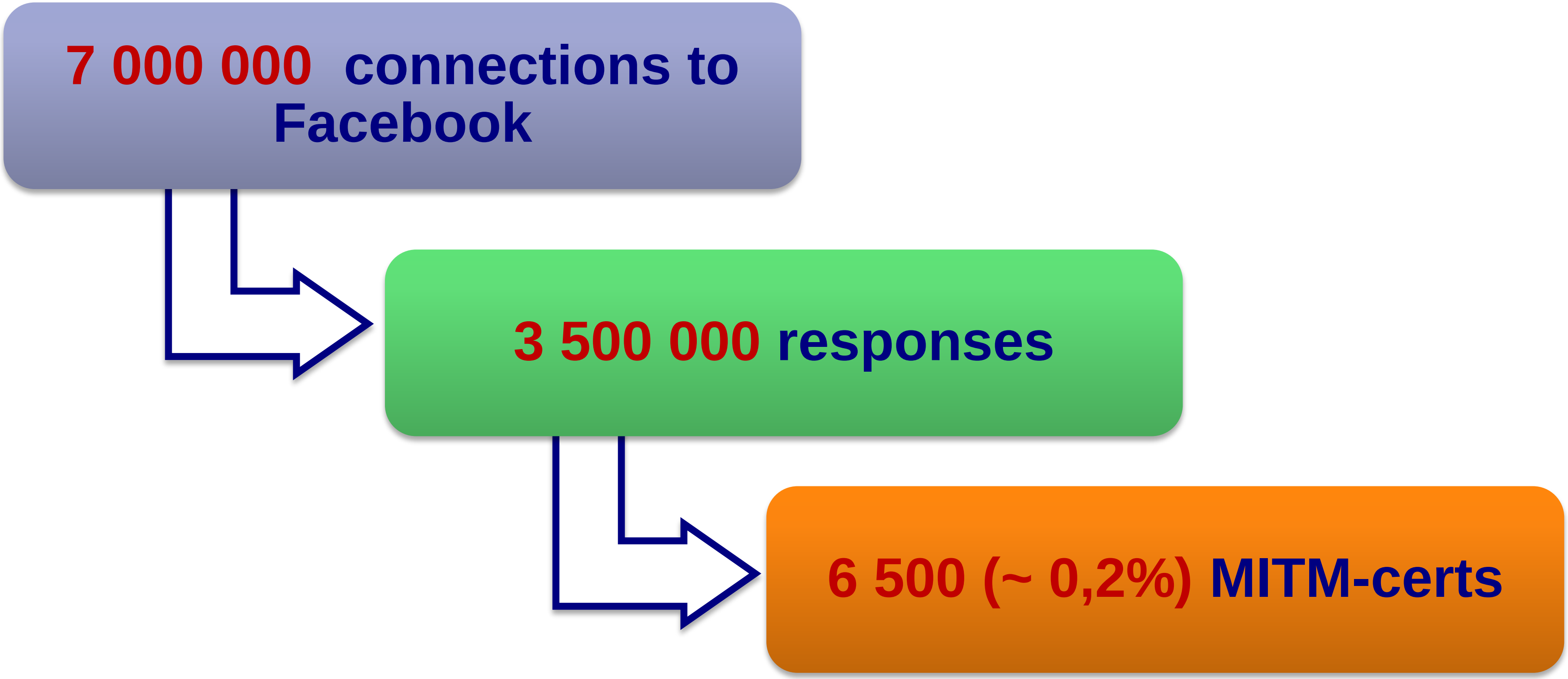
How to detect MITM from server?

Survey: https://www.linshunghuang.com/papers/mitm.pdf

Solution

- Client can send a certificate back to server

MITM-attack: statistics



7 000 000 connections to Facebook

3 500 000 responses

6 500 (~ 0,2%) MITM-certs

Almost all are used positively!

PKI: extra trust

PKI + Independent source = Trusted certificate

Certificate pinning

Chrome cache for Google certificates

Mozilla Firefox 32+

DANE (RFC 6698)

Limited browsers support

Certificate transparency (RFC 6962)

Inspired by Google (Support in Chrome appeared)

One of the authors - Ben Laurie (OpenSSL Founder)

CA support (Comodo, Symantec…)

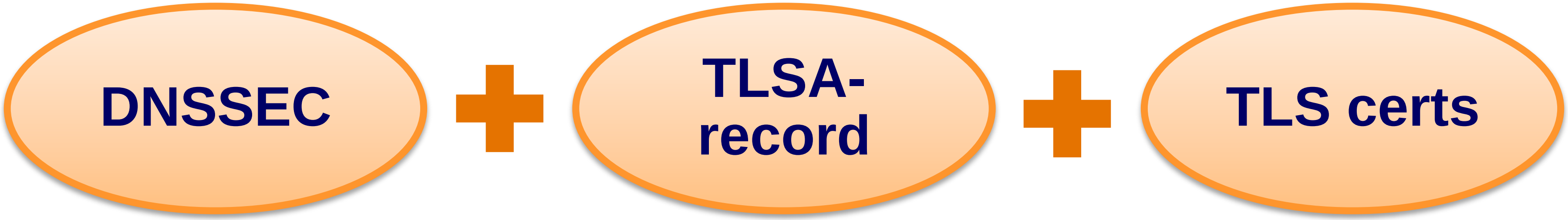
Certificate pinning: how it works

- Limited built-in lists in browsers
- Special plugins

Problems

- Plugins should be installed by each user
- Does not help if you are already under attack
- Popular services have many servers and many certificates

DANE: how it works



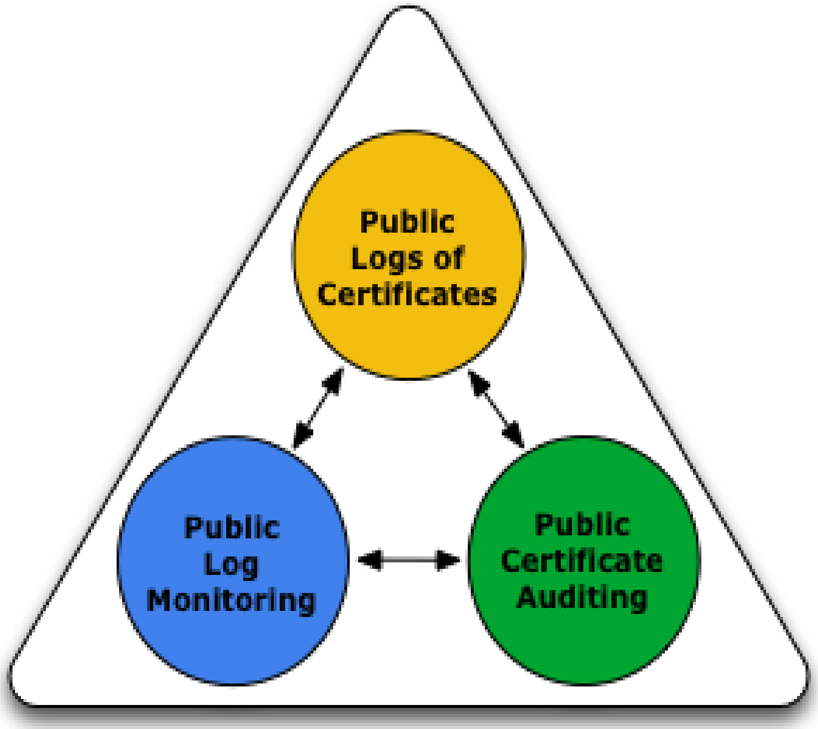
Problems

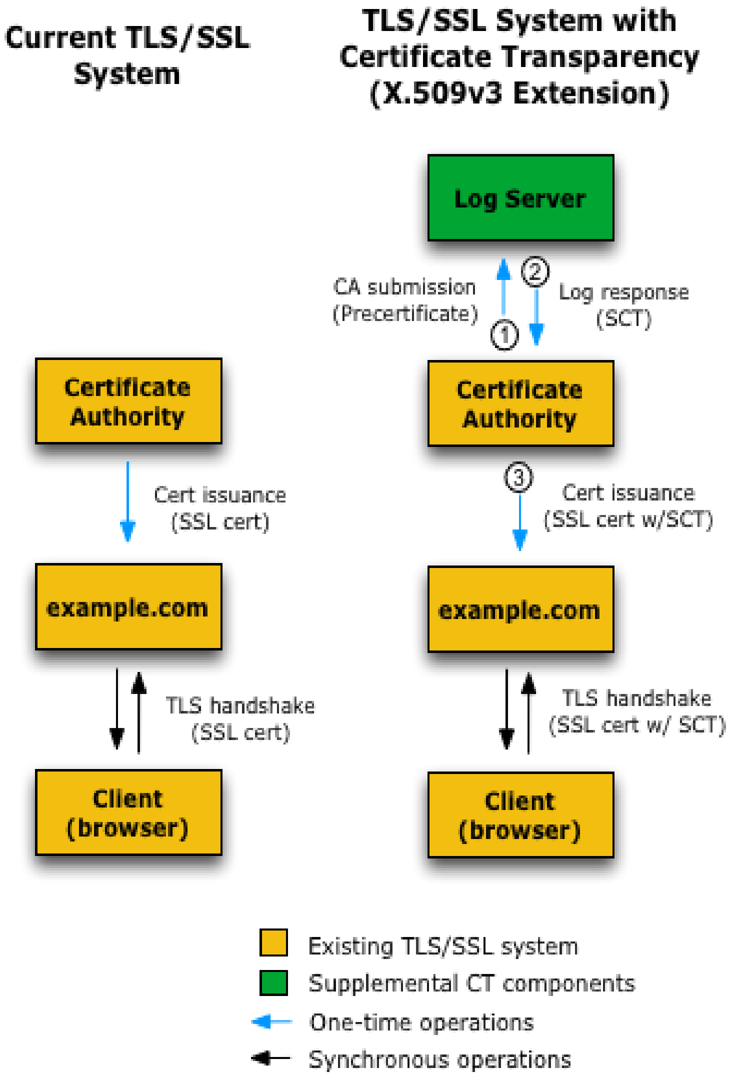
- TLSA record should be added by domain administrator
- Not supported by browsers

Certificate Transparency: how it works

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

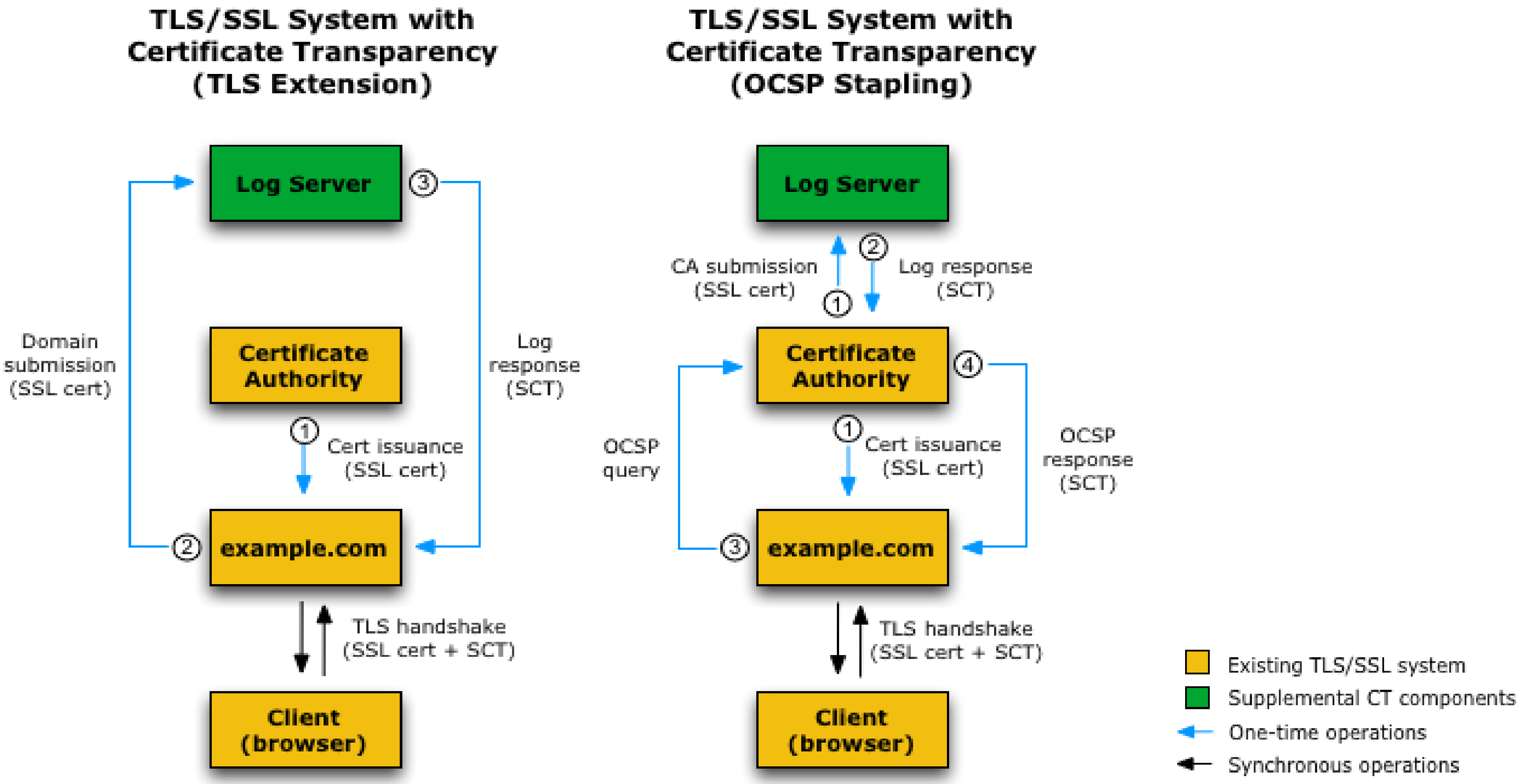
Certificate Transparency: how it works





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

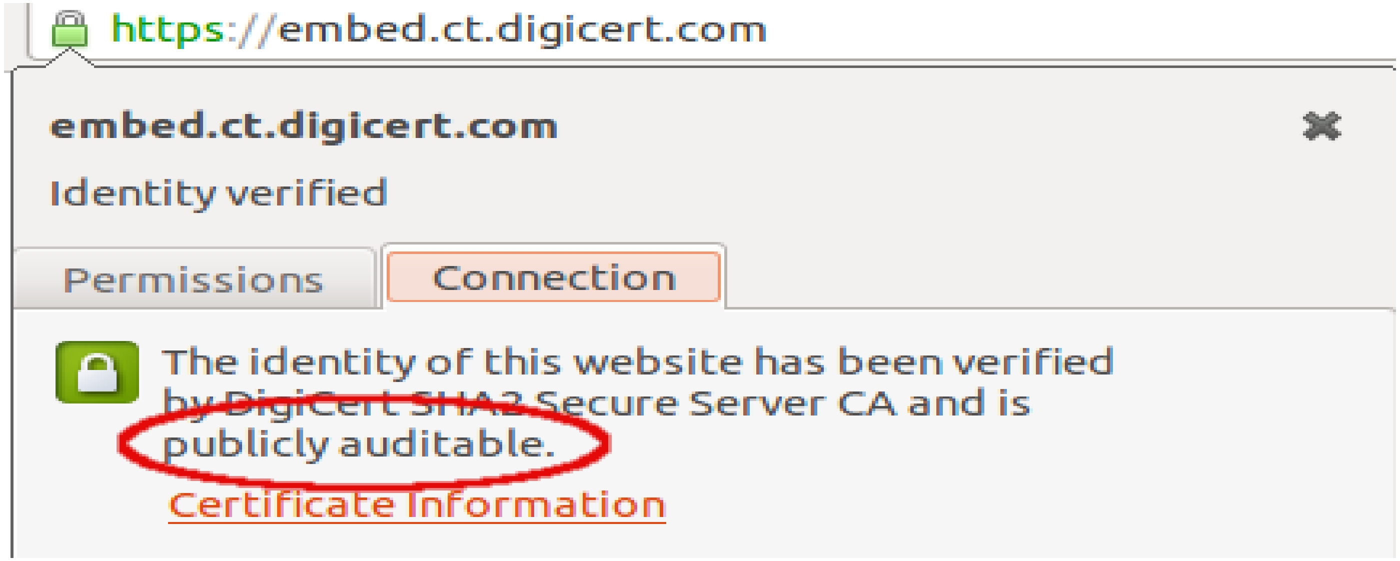
Certificate Transparency how it works



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

Certificate Transparency current state

Google Chrome Support (33+)



https://embed.ct.digicert.com

embed.ct.digicert.com

Identity verified

The identity of this website has been verified by DigiCert SHA2 Secure Server CA and is publicly auditable.

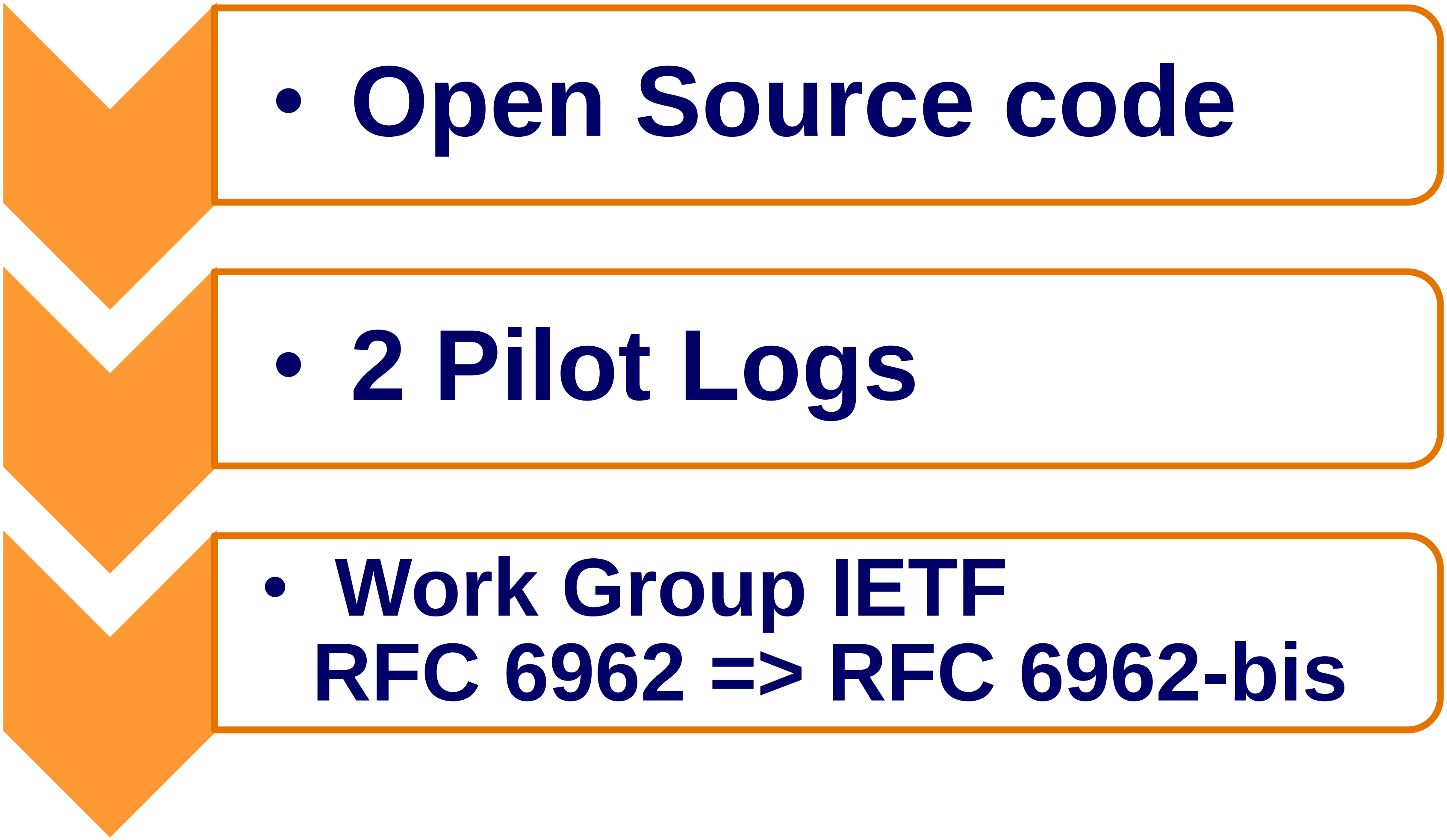
Certificate Information

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
- Work Group IETF
  RFC 6962 => RFC 6962-bis

Certificate Transparency: problems

- Specification is incomplete
- Problems hiding “private” domains
- No technical possibility to limit list of logs

Certificate Transparency: protection from what?

SAVES from MITM attack

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

Does NOT SAVE from HEARTBLEED!

Russian GOST does not save from MITM attacks

Algorithms

SHA-256 >>> GOSTR34.11-2012

Keys

>>> GOST R 34.10-2012

Q&A

Questions?

Drop ‘em at:

beldmit@tcinet.ru