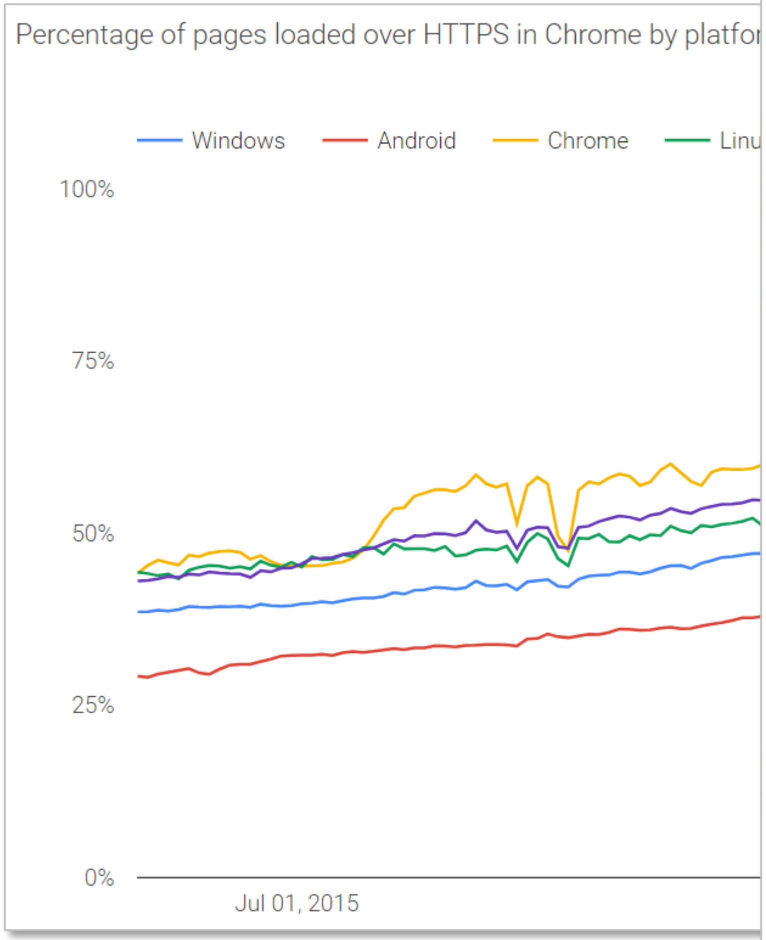
UiO : Department of Informatics
University of Oslo

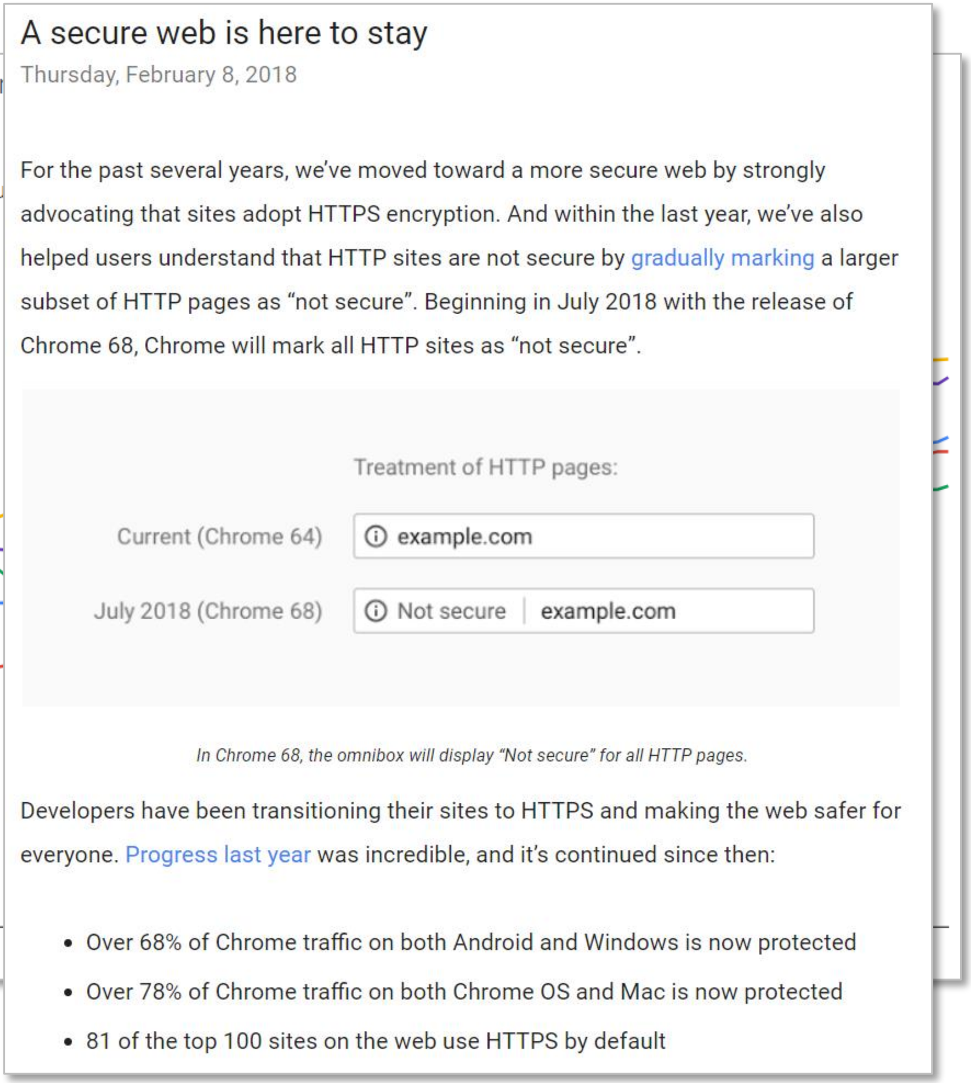
Nils Gruschka

CA Authorization:
Fixing a Problem or Shifting it Elsewhere?

UNIVERSITAS OSLOENSIS MDCCCXI

Motivation: HTTPS usage





A secure web is here to stay

Thursday, February 8, 2018

For the past several years, we've moved toward a more secure web by strongly advocating that sites adopt HTTPS encryption. And within the last year, we've also helped users understand that HTTP sites are not secure by gradually marking a larger subset of HTTP pages as "not secure". Beginning in July 2018 with the release of Chrome 68, Chrome will mark all HTTP sites as "not secure".

In Chrome 68, the omnibox will display "Not secure" for all HTTP pages.

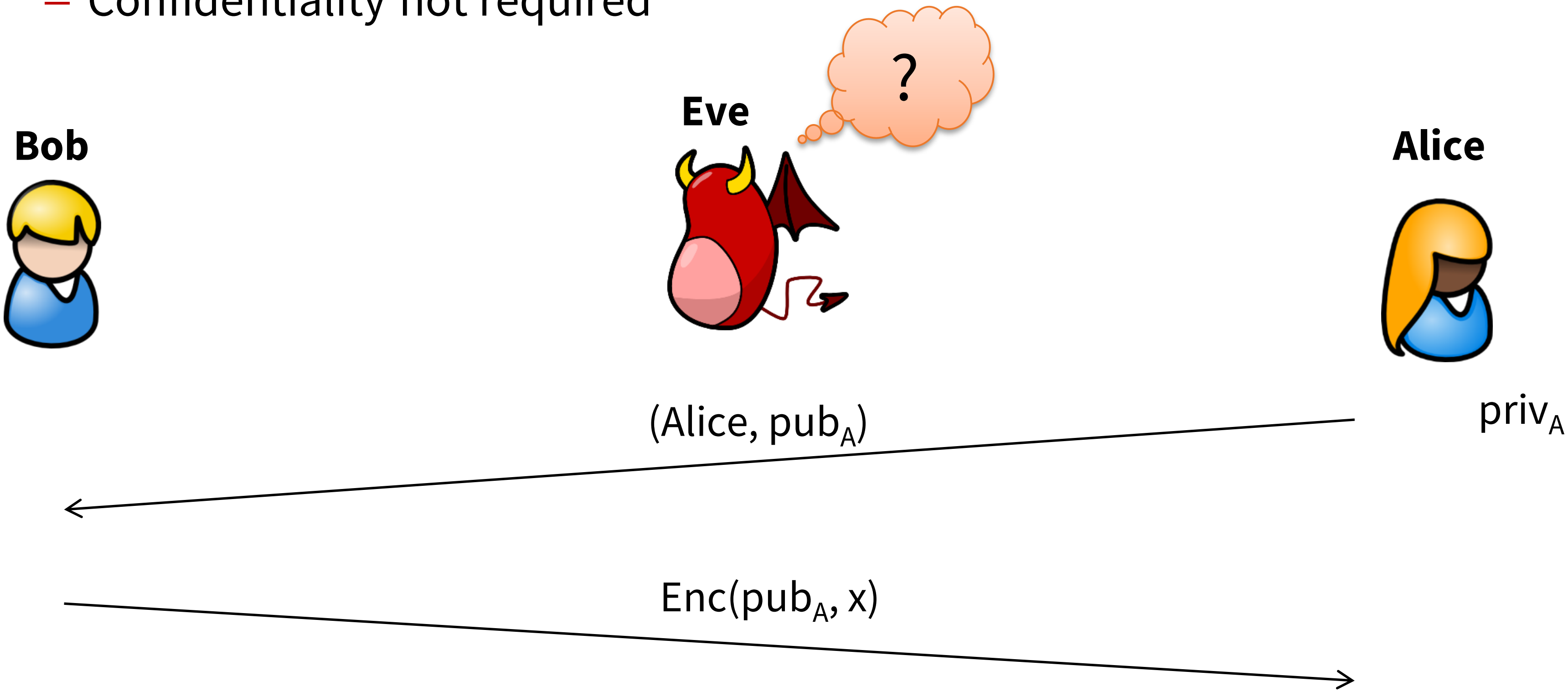
Developers have been transitioning their sites to HTTPS and making the web safer for everyone. Progress last year was incredible, and it's continued since then:

- Over 68% of Chrome traffic on both Android and Windows is now protected
- Over 78% of Chrome traffic on both Chrome OS and Mac is now protected
- 81 of the top 100 sites on the web use HTTPS by default

Source: https://transparencyreport.google.com/https/overview?hl=en
https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html

Attack on Key Exchange (Encryption)

- Exchange of public key:
  - Confidentiality not required



?

Eve

Bob

Alice

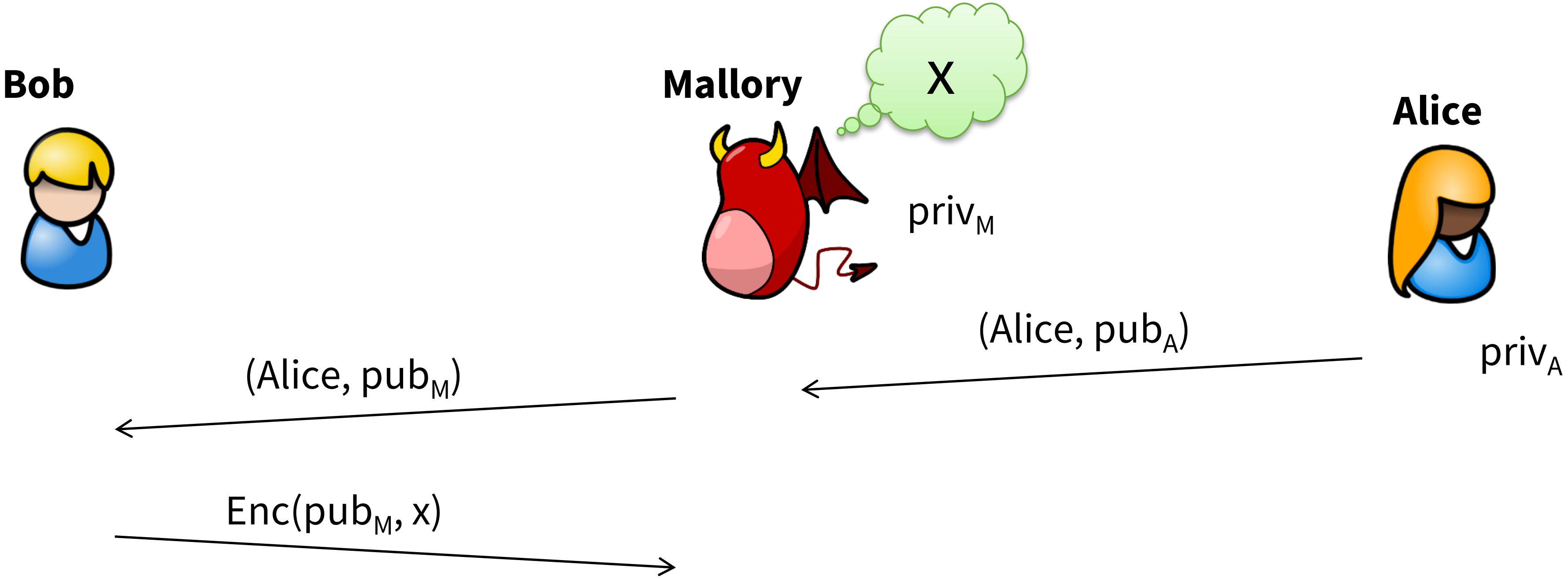
(Alice, pub_A)

$priv_A$

Enc(pub_A, x)

Attack on Key Exchange (Encryption)

- Exchange of public key:
  - Confidentiality not required
  - Integrity/authenticity highly required



Bob

Mallory

X

$priv_M$

Alice

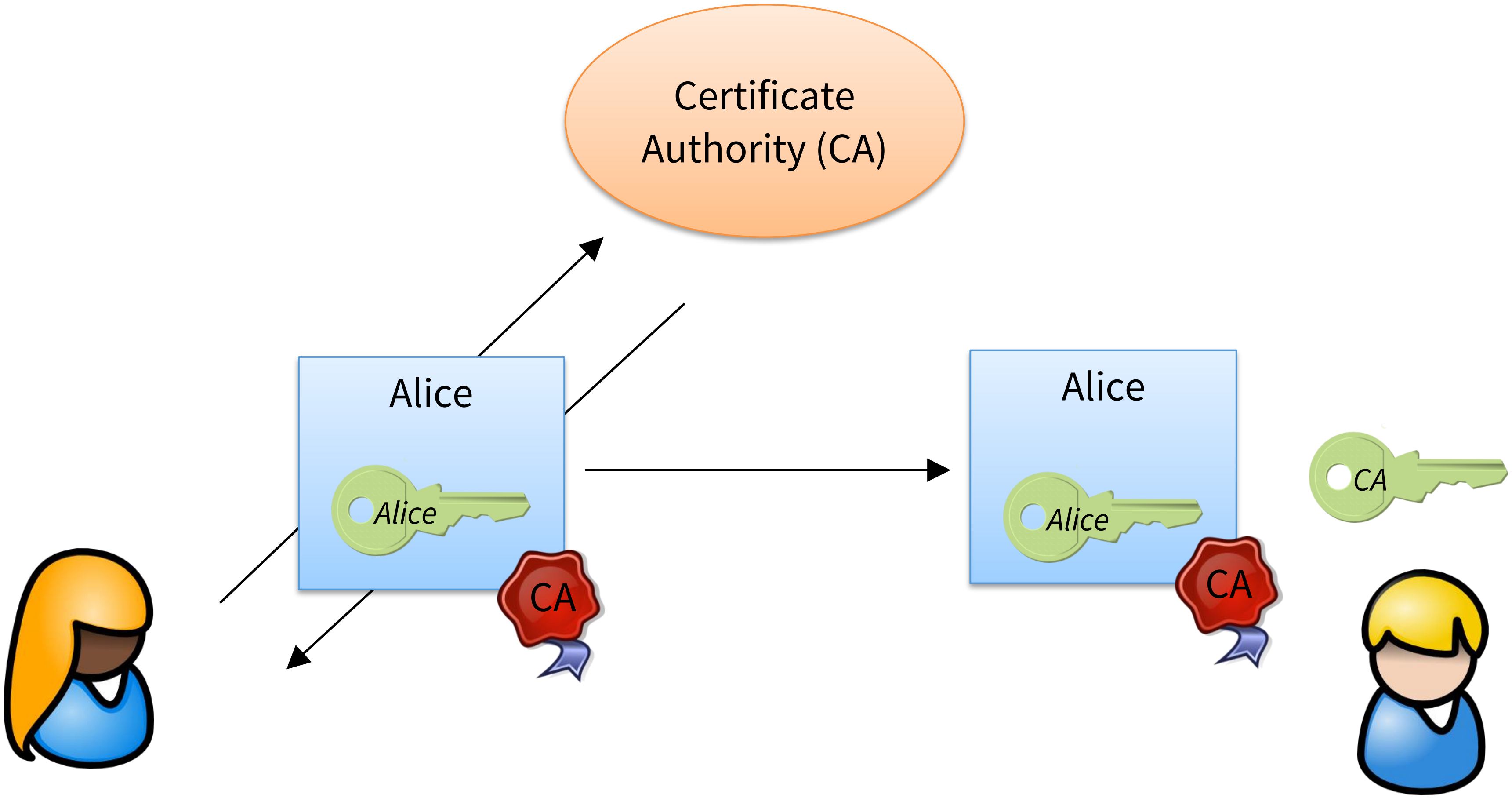
$(Alice, pub_A)$

$priv_A$

$(Alice, pub_M)$

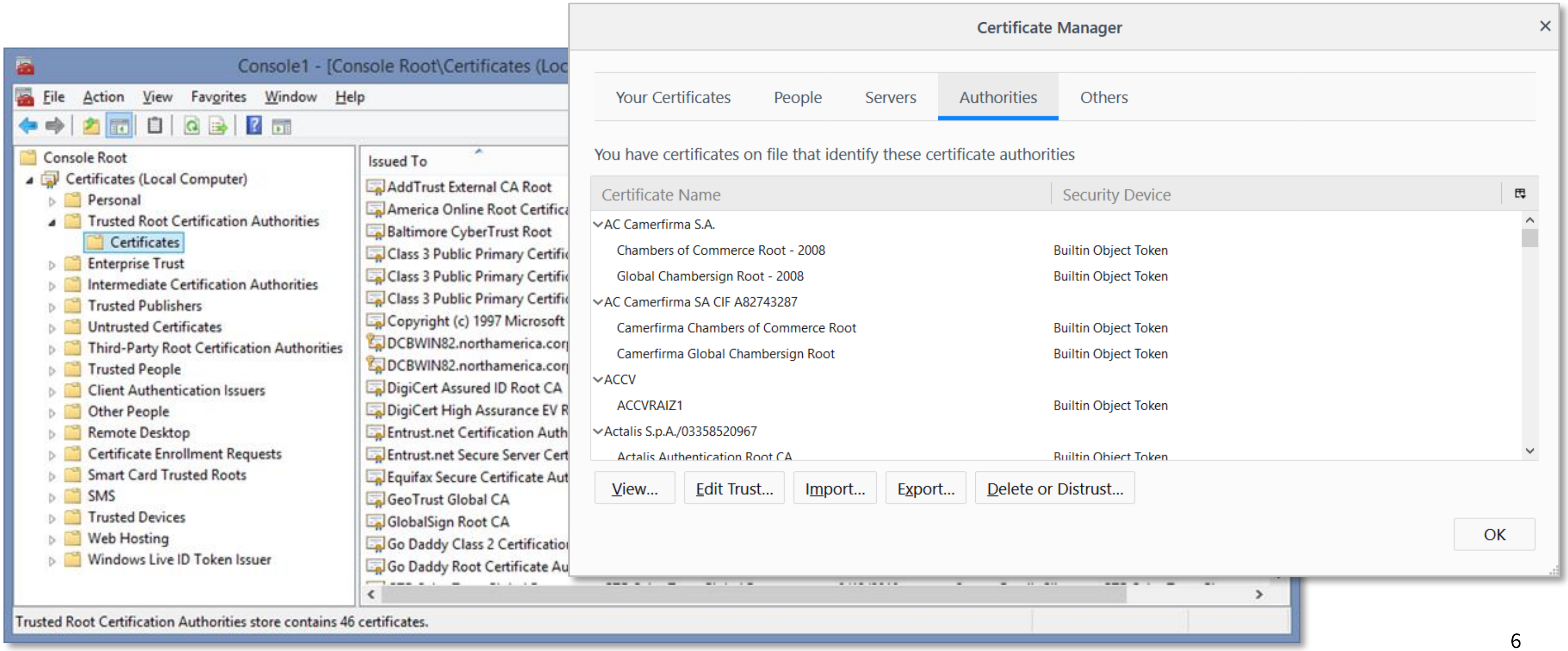
$Enc(pub_M, x)$

Certificates



Certificate Trust

- How obtains Bob the public key of the CA?
- A set of trusted CAs (root store) is included in the OS or the application (e.g. browser)



Console1 - [Console Root\Certificates (Loc

- Console Root
  - Certificates (Local Computer)
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Client Authentication Issuers
    - Other People
    - Remote Desktop
    - Certificate Enrollment Requests
    - Smart Card Trusted Roots
    - SMS
    - Trusted Devices
    - Web Hosting
    - Windows Live ID Token Issuer

Issued To

- AddTrust External CA Root
- America Online Root Certifica
- Baltimore CyberTrust Root
- Class 3 Public Primary Certific
- Class 3 Public Primary Certific
- Class 3 Public Primary Certific
- Copyright (c) 1997 Microsoft
- DCBWIN82.northamerica.cor
- DCBWIN82.northamerica.cor
- DigiCert Assured ID Root CA
- DigiCert High Assurance EV R
- Entrust.net Certification Auth
- Entrust.net Secure Server Cert
- Equifax Secure Certificate Aut
- GeoTrust Global CA
- GlobalSign Root CA
- Go Daddy Class 2 Certificatio
- Go Daddy Root Certificate Au

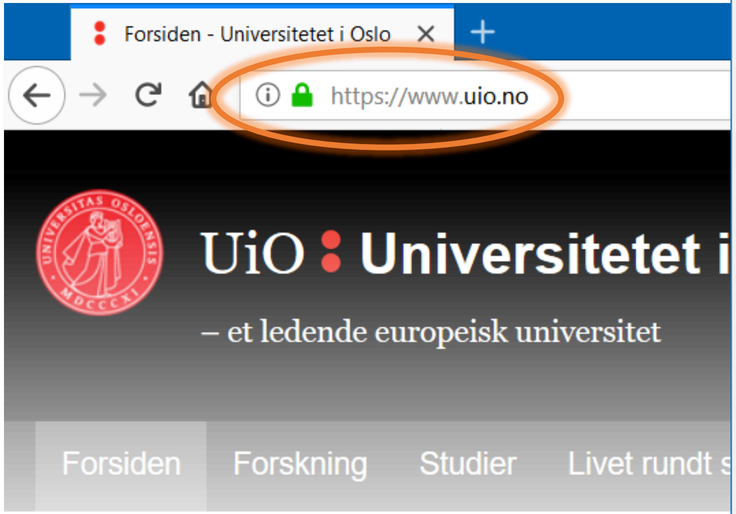
Trusted Root Certification Authorities store contains 46 certificates.

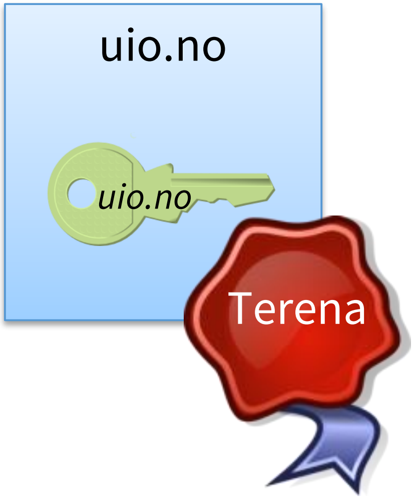
Certificate Manager

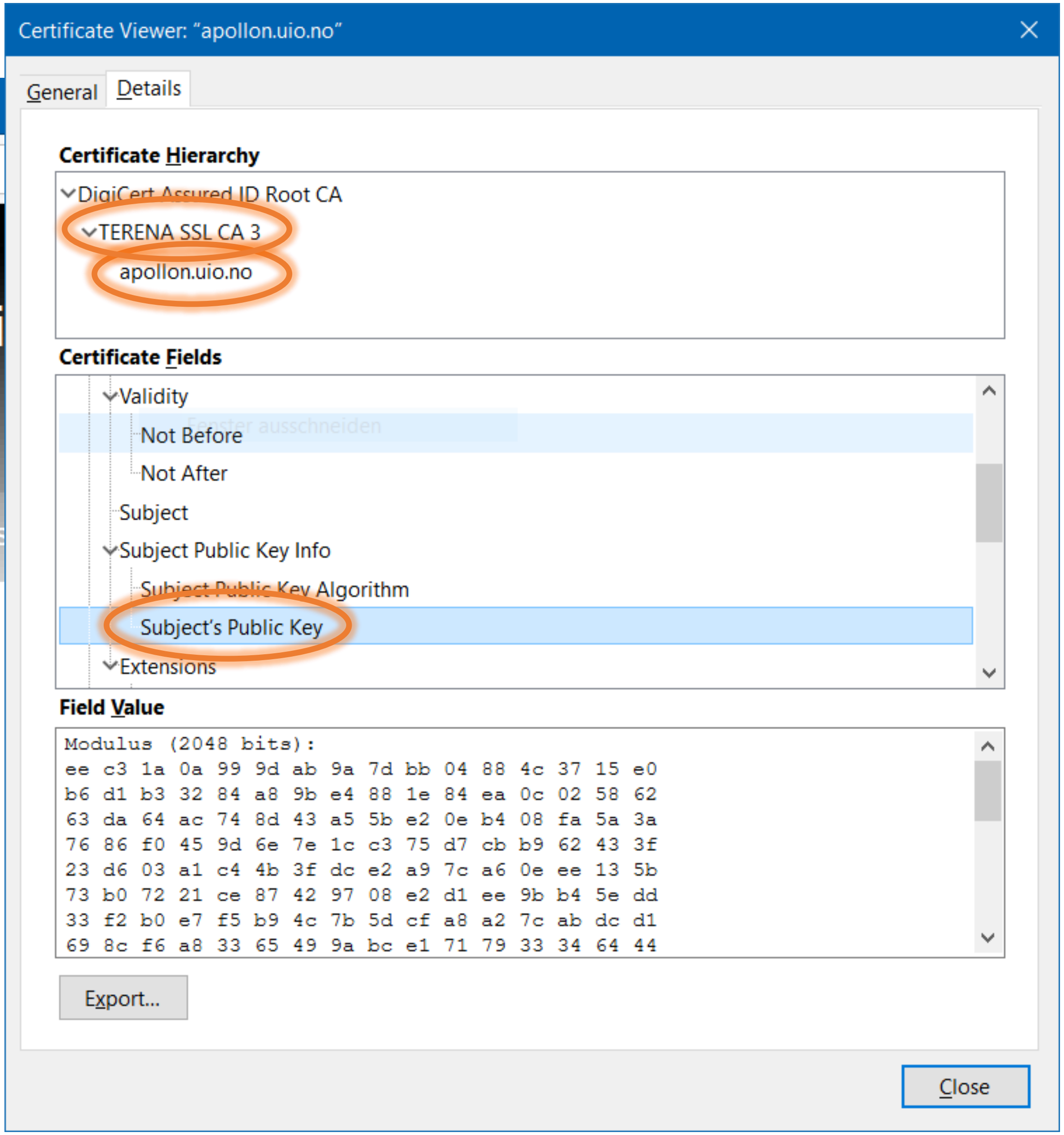
You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce Root	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token
ACCV	
ACCVRAIZ1	Builtin Object Token
Actalis S.p.A./03358520967	
Actalis Authentication Root CA	Builtin Object Token

Certificates on the Web







Certificate Viewer: "apollon.uio.no"

General | Details

Certificate Hierarchy

- DigiCert Assured ID Root CA
  - TERENA SSL CA 3
    - apollon.uio.no

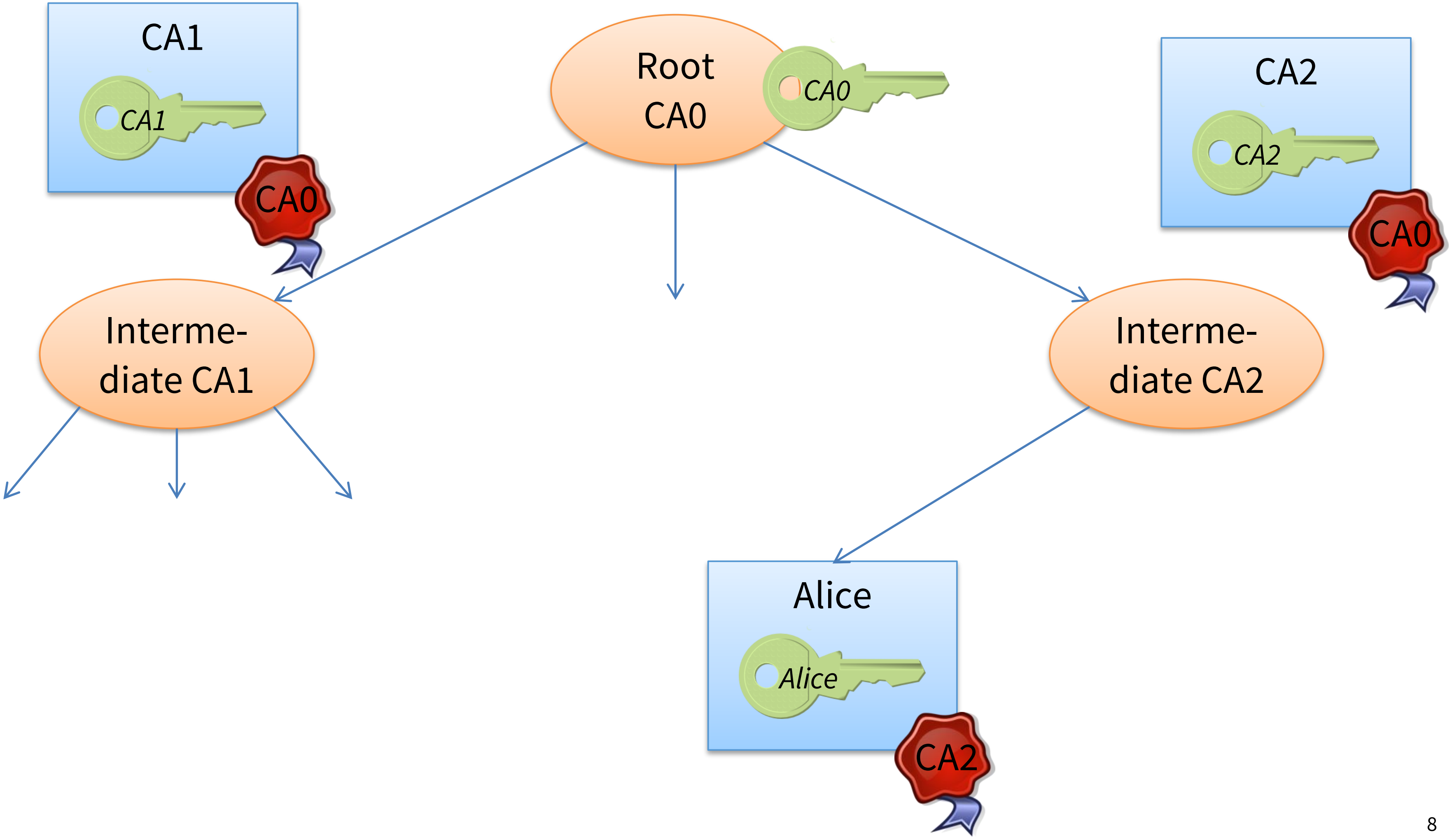
Certificate Fields

- Validity
  - Not Before
  - Not After
- Subject
- Subject Public Key Info
  - Subject Public Key Algorithm
  - Subject's Public Key
- Extensions

Field Value

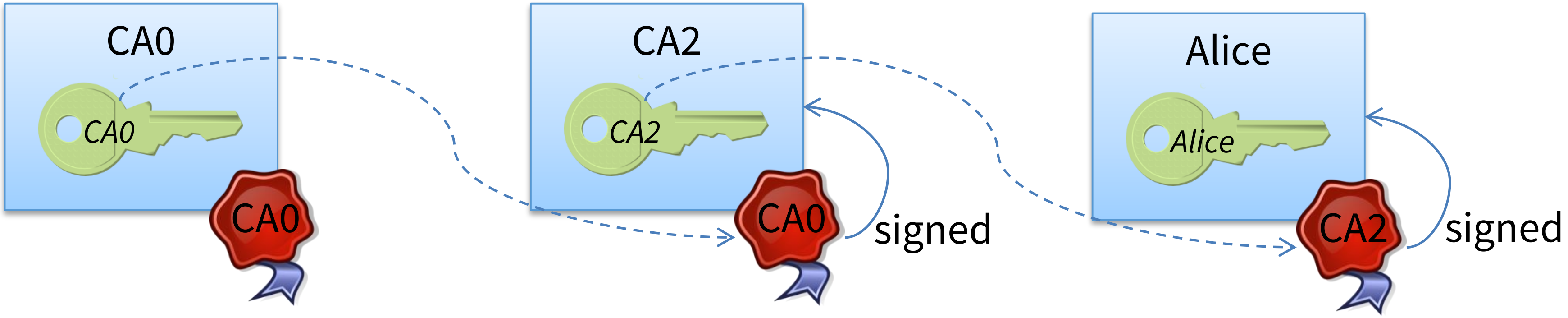
```
Modulus (2048 bits):
ee c3 1a 0a 99 9d ab 9a 7d bb 04 88 4c 37 15 e0
b6 d1 b3 32 84 a8 9b e4 88 1e 84 ea 0c 02 58 62
63 da 64 ac 74 8d 43 a5 5b e2 0e b4 08 fa 5a 3a
76 86 f0 45 9d 6e 7e 1c c3 75 d7 cb b9 62 43 3f
23 d6 03 a1 c4 4b 3f dc e2 a9 7c a6 0e ee 13 5b
73 b0 72 21 ce 87 42 97 08 e2 d1 ee 9b b4 5e dd
33 f2 b0 e7 f5 b9 4c 7b 5d cf a8 a2 7c ab dc d1
69 8c f6 a8 33 65 49 9a bc e1 71 79 33 34 64 44
```

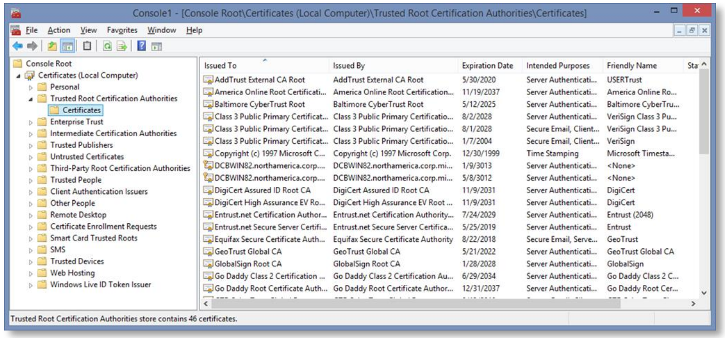
Certificate Trust



Certificate Trust

- When to trust a certificate?
- → a signature chain from a trusted root CA exists



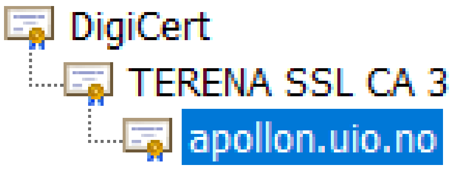


Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]

- Console Root
  - Certificates (Local Computer)
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Client Authentication Issuers
    - Other People
    - Remote Desktop
    - Certificate Enrollment Requests
    - Smart Card Trusted Roots
    - SMS
    - Trusted Devices
    - Web Hosting
    - Windows Live ID Token Issuer

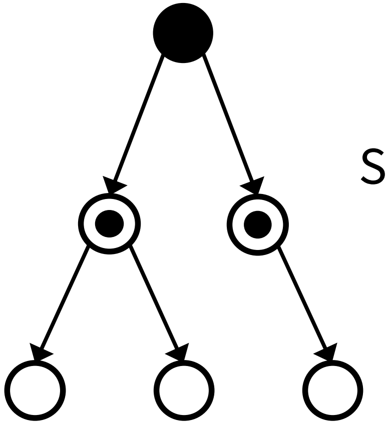
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Sta
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenticati...	USERTrust	
America Online Root Certificati...	America Online Root Certification...	11/19/2037	Server Authenticati...	America Online Ro...	
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenticati...	Baltimore CyberTru...	
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/2/2028	Server Authenticati...	VeriSign Class 3 Pu...	
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Secure Email, Client...	VeriSign Class 3 Pu...	
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	1/7/2004	Secure Email, Client...	VeriSign	
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timesta...	
DCBWIN82.northamerica.corp....	DCBWIN82.northamerica.corp.mi...	1/9/3013	Server Authenticati...	<None>	
DCBWIN82.northamerica.corp....	DCBWIN82.northamerica.corp.mi...	5/8/3012	Server Authenticati...	<None>	
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Server Authenticati...	DigiCert	
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/9/2031	Server Authenticati...	DigiCert	
Entrust.net Certification Author...	Entrust.net Certification Authority...	7/24/2029	Server Authenticati...	Entrust (2048)	
Entrust.net Secure Server Certifi...	Entrust.net Secure Server Certifica...	5/25/2019	Server Authenticati...	Entrust	
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Serve...	GeoTrust	
GeoTrust Global CA	GeoTrust Global CA	5/21/2022	Server Authenticati...	GeoTrust Global CA	
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Server Authenticati...	GlobalSign	
Go Daddy Class 2 Certification ...	Go Daddy Class 2 Certification Au...	6/29/2034	Server Authenticati...	Go Daddy Class 2 C...	
Go Daddy Root Certificate Auth...	Go Daddy Root Certificate Author...	12/31/2037	Server Authenticati...	Go Daddy Root Cer...	

Trusted Root Certification Authorities store contains 46 certificates.

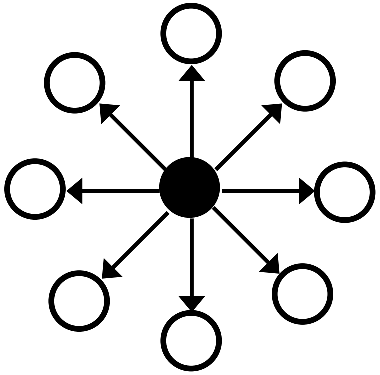


- DigiCert
  - TERENA SSL CA 3
    - apollon.uio.no

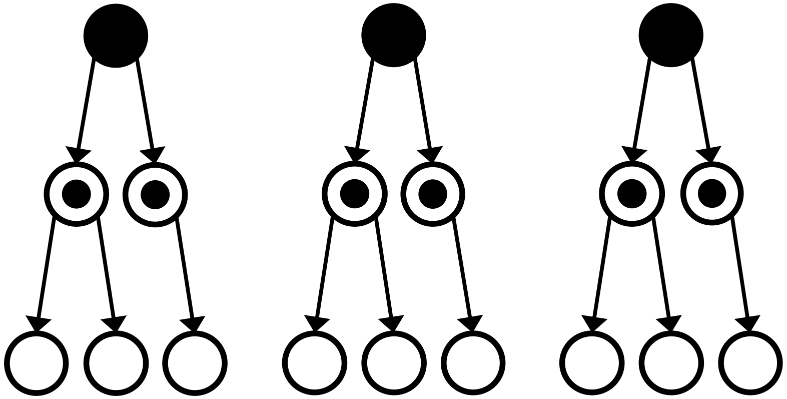
Trust Models



Strict hierarchy
e.g. DNSSEC



User-centric PKI
e.g. PGP



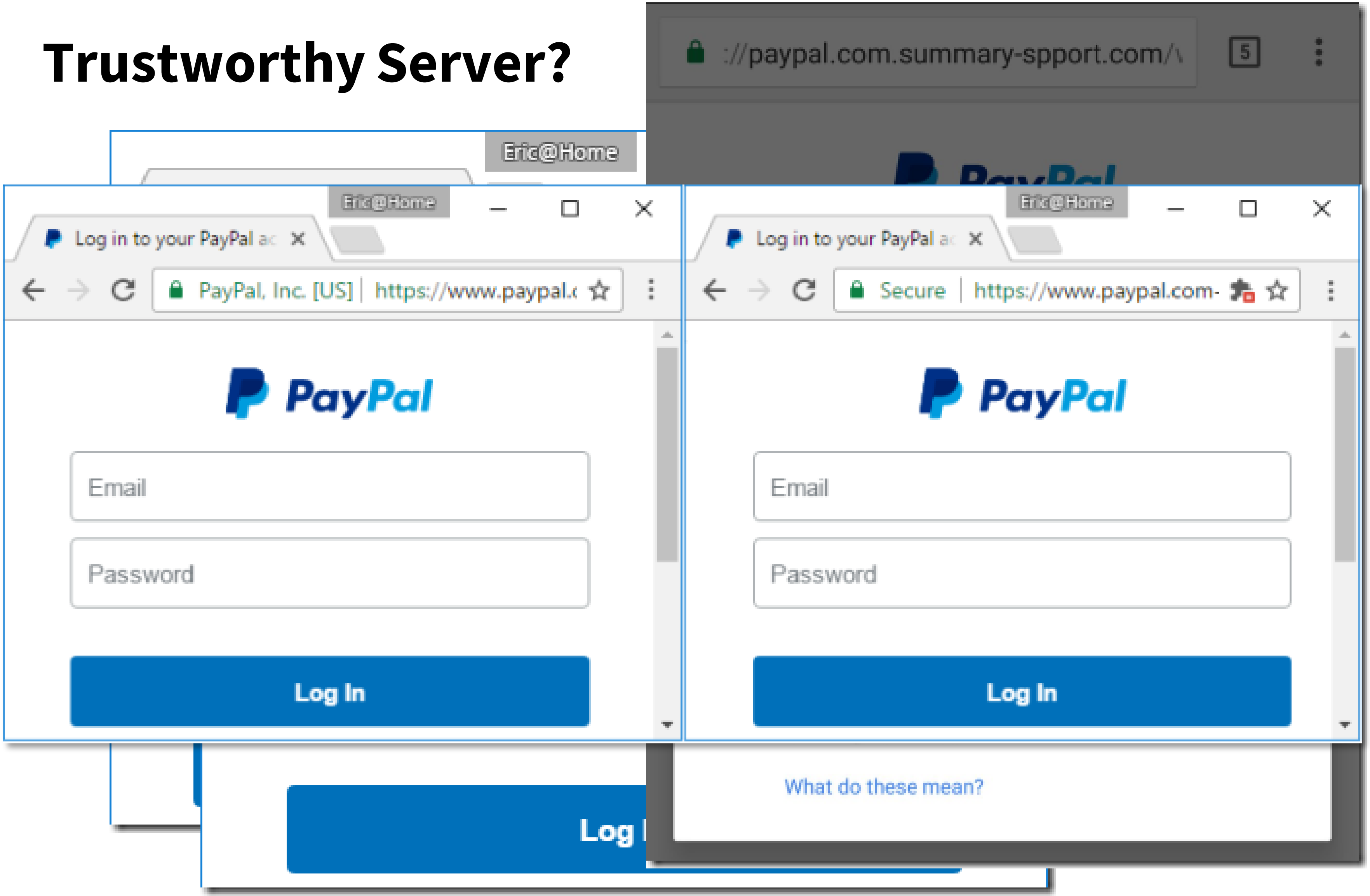
Isolated strict hierarchies
e.g. Web PKI

Problems with PKI / Certificate Security

- Fundamental issue:
  - Trusted certificate ≠ trustworthy server
- Threats:
  - Downgrade attack
  - Misconfigured client
  - Compromised server/certificate
  - Compromised
  - Sloppy
  - Rogue

  } certificate authority

Trustworthy Server?



Source: https://textslashplain.com/2017/01/16/certified-malice/

Compromised Certificate

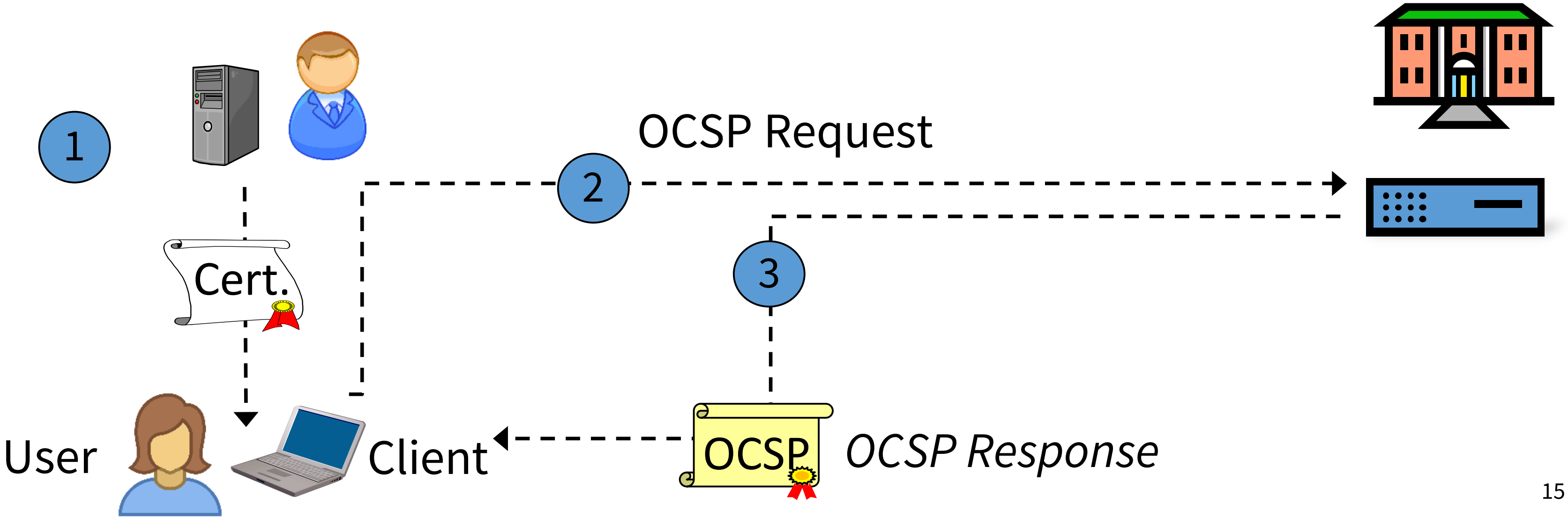
- What happens if certificate owner wants to invalidate a certificate (e.g. lost or stolen private key)?
  - Contact certificate authority
  - CA marks certificate as revoked
- How can the recipient of the certificate know of this revocation?
  - Certificate Revocation List (CRL)
  - Online Certificate Status Protocol (OCSP)

Certificate Revocation List (CRL)

- Server/CA offers the list of revoked certificate for download
- Example (uio.no):
  - `http://crl3.digicert.com/TERENASSLCA3.crl`
  - `http://crl4.digicert.com/TERENASSLCA3.crl`
- Problems?
  - Download CRL for every TLS connection → additional delay
  - Download CRL in certain intervals → is CRL still up to date?
  - How often is the CRL updated at the CLR endpoint?
  - CRL can become very large → additional traffic / load
  - What is the browser supposed to do when the CRL endpoint is not accessible?
  - CRL is neither integrity protected nor authentic → attacker can inject an empty list

Online Certificate Status Protocol (OCSP)

- Interactive protocol to validate if the certificate is still valid
- Example (uio.no):
  - http://ocsp.digicert.com
- Client sends a request to the CA containing the serial number
- CA sends a responds which is digitally signed

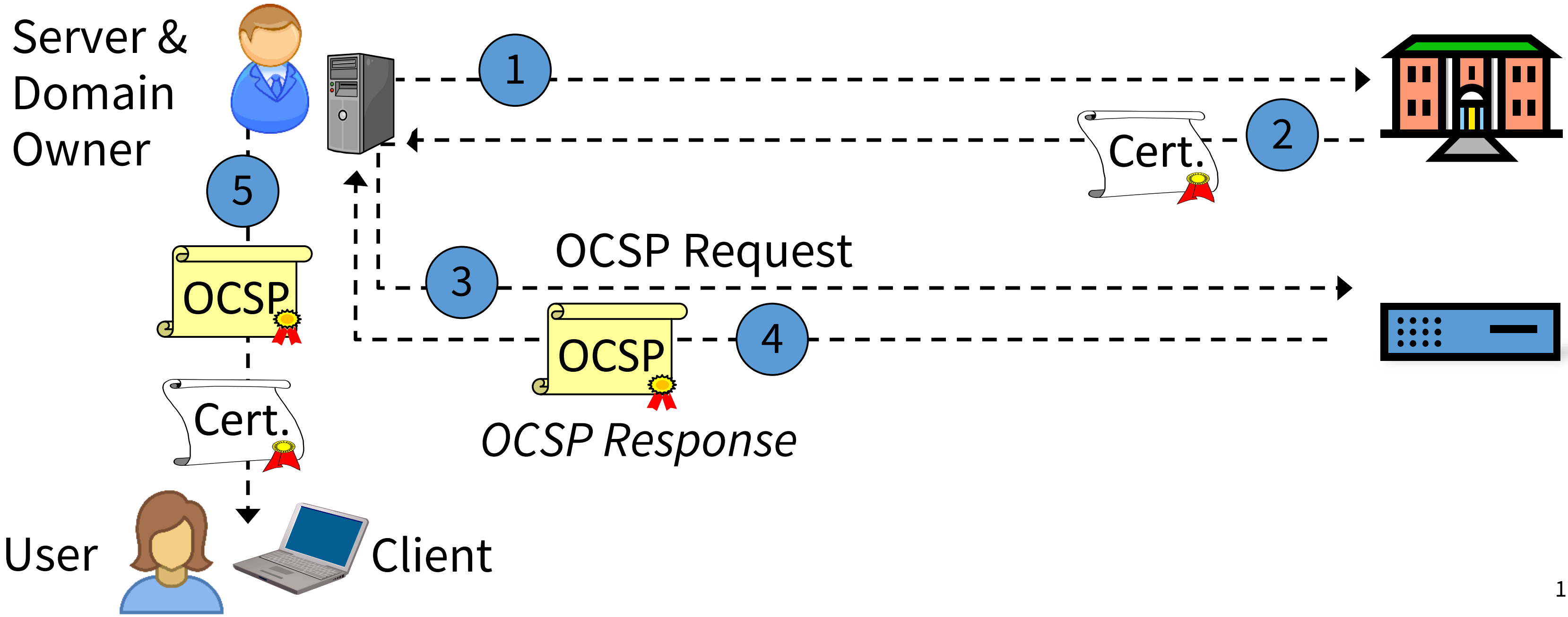


Online Certificate Status Protocol (OCSP)

- Advantages compared to CRL?
  - Allows (theoretically) realtime access to certificate status
  - Reduced traffic
- Problems remaining?
  - Often implemented at the CA using a CRL
  - Delay in TLS connection setup
  - Attacker can block access to the OCSP endpoint
  - What is the browser supposed to do when the OCSP endpoint is not accessible?
- New problems?
  - CA learns which (HTTPS) Web pages have been accessed by the client

OCSP stapling

- Extension of the TLS protocol
- OCSP Certificate is **not** requested by the client at the CA
- Server request OCSP Certificate at the CA and send it during the TLS handshake to the client

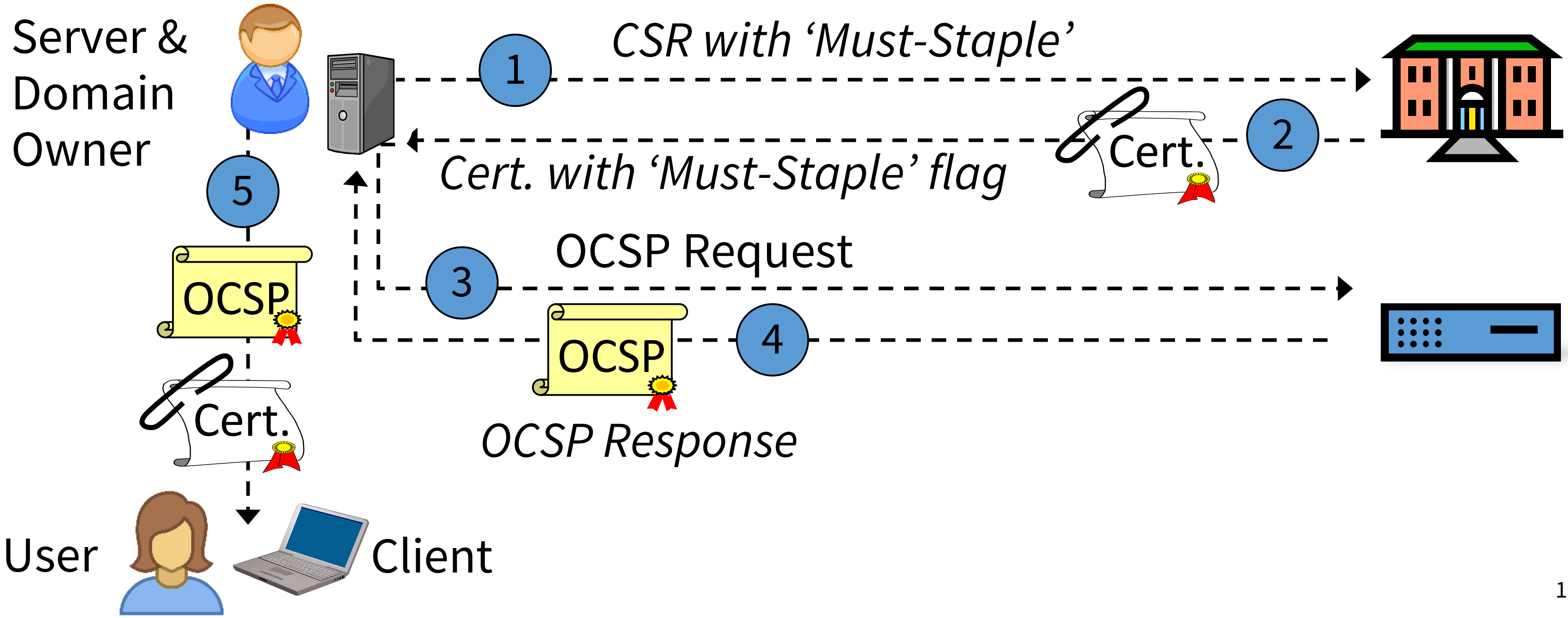


OCSP stapling

- Advantages compared to OCSP?
  - Client does not contact the CA → no privacy issue
- Problems remaining?
  - Attacker („owner“ of private key for the compromised certificate) can deliver the certificate without the OCSP status

OCSP “Must-Staple”

- The certificate is issued with a flag indicating a mandatory OCSP status response

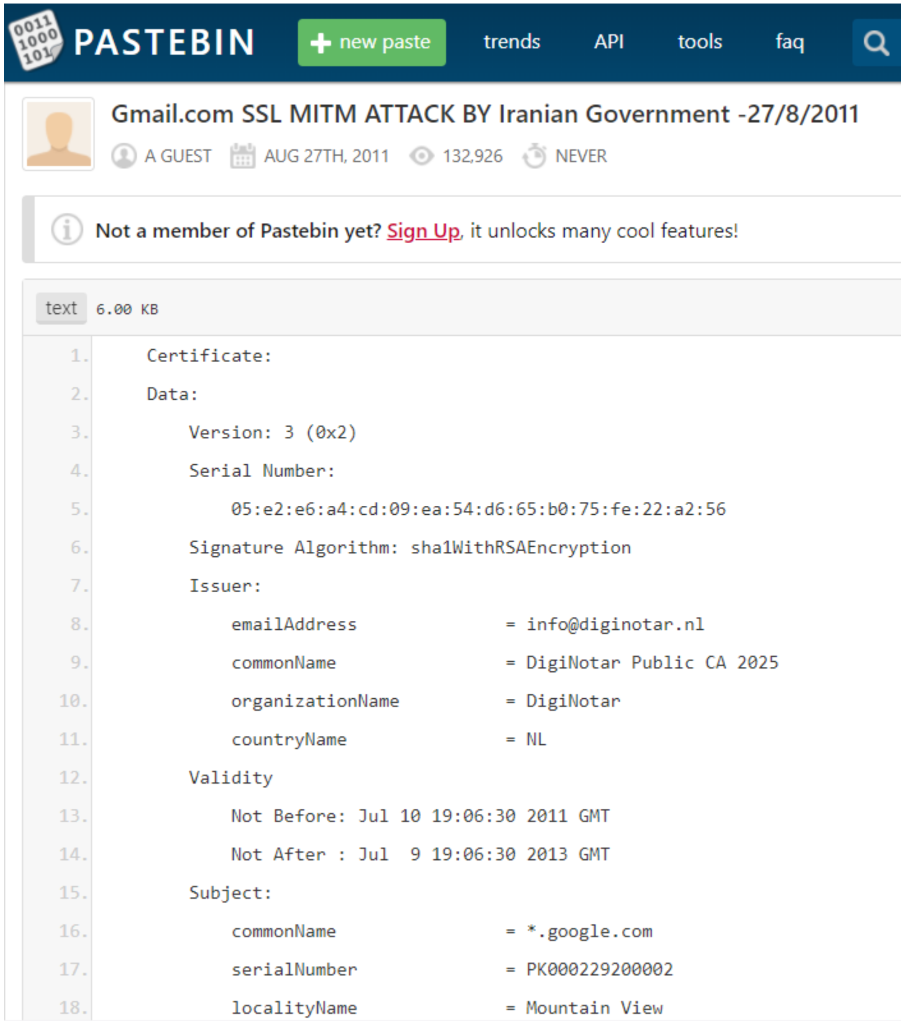


OCSP “Must-Staple”

- Advantages compared to OCSP stapling?
  - Client detects a missing OCSP status
- Problems remaining?
  - What is the browser supposed to do when the OCSP status is missing?
  - Insufficient implementation support (client, server, network tools)
  - Not used by any major Web site

Compromised Certificate Authority

- CA DigiNotar was hacked in 2011
- A number of illegitimate certificates (e.g. *.google.com) were created by the intruders



Gmail.com SSL MITM ATTACK BY Iranian Government -27/8/2011

A GUEST AUG 27TH, 2011 132,926 NEVER

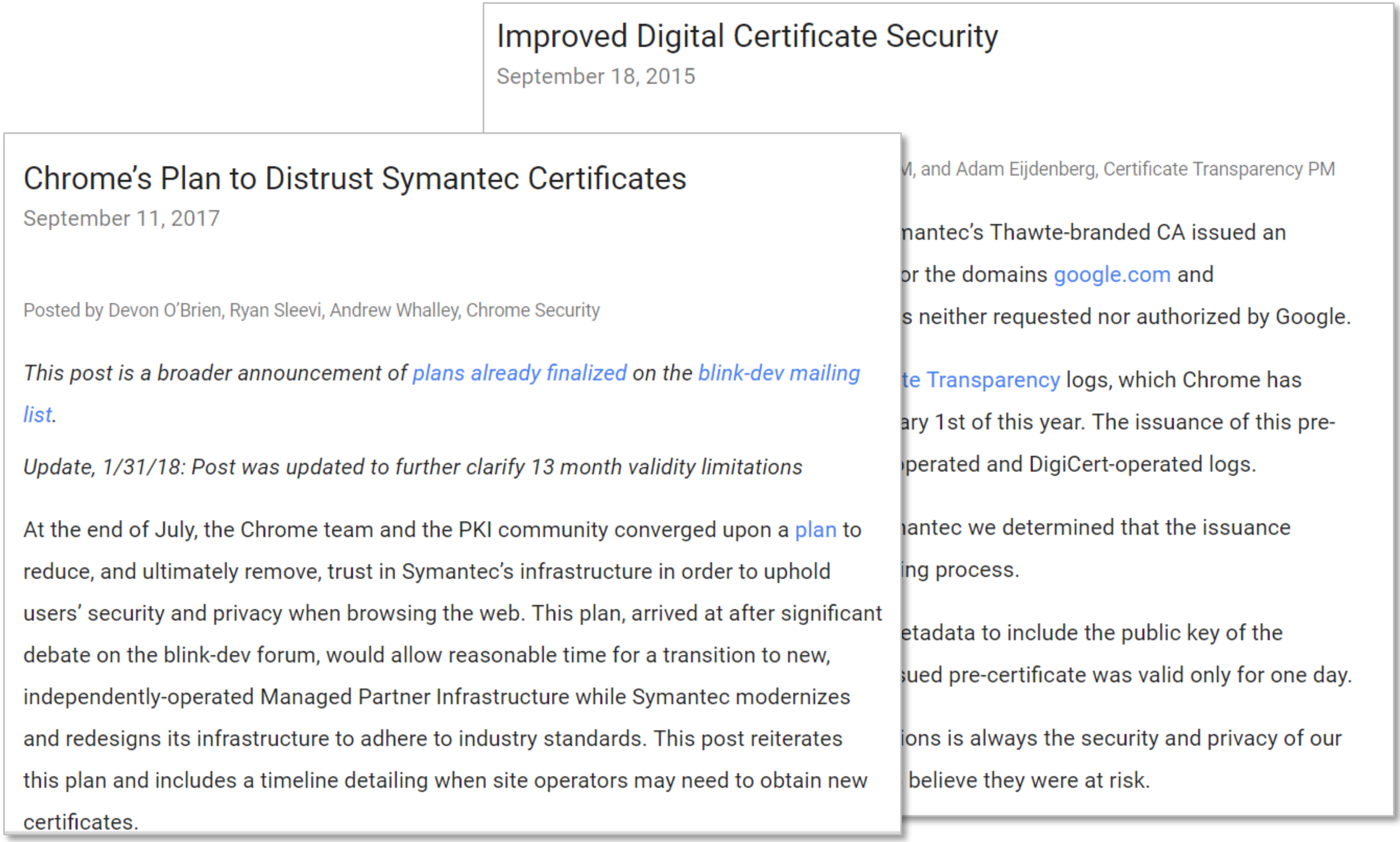
Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

text 6.00 KB

```
Certificate:
Data:
    Version: 3 (0x2)
    Serial Number:
        05:e2:e6:a4:cd:09:ea:54:d6:65:b0:75:fe:22:a2:56
    Signature Algorithm: sha1WithRSAEncryption
    Issuer:
        emailAddress              = info@diginotar.nl
        commonName                = DigiNotar Public CA 2025
        organizationName          = DigiNotar
        countryName               = NL
    Validity
        Not Before: Jul 10 19:06:30 2011 GMT
        Not After : Jul  9 19:06:30 2013 GMT
    Subject:
        commonName                = *.google.com
        serialNumber              = PK000229200002
        localityName              = Mountain View
```

Source: https://pastebin.com/ff7Yg663

Sloppy Certificate Authority



Improved Digital Certificate Security

September 18, 2015

M, and Adam Eijdenberg, Certificate Transparency PM

nantec's Thawte-branded CA issued an
or the domains google.com and
s neither requested nor authorized by Google.

te Transparency logs, which Chrome has
ary 1st of this year. The issuance of this pre-
perated and DigiCert-operated logs.

nantec we determined that the issuance
ing process.

etadata to include the public key of the
sued pre-certificate was valid only for one day.

ions is always the security and privacy of our
believe they were at risk.

Chrome's Plan to Distrust Symantec Certificates

September 11, 2017

Posted by Devon O'Brien, Ryan Sleevi, Andrew Whalley, Chrome Security

This post is a broader announcement of plans already finalized on the blink-dev mailing list.

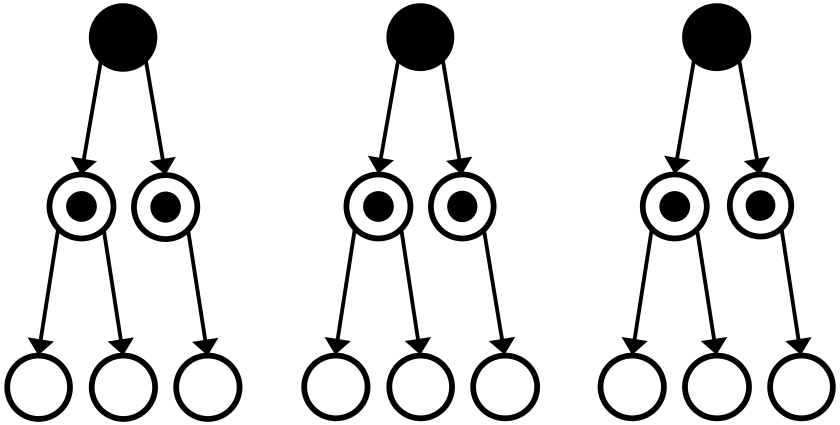
Update, 1/31/18: Post was updated to further clarify 13 month validity limitations

At the end of July, the Chrome team and the PKI community converged upon a plan to reduce, and ultimately remove, trust in Symantec's infrastructure in order to uphold users' security and privacy when browsing the web. This plan, arrived at after significant debate on the blink-dev forum, would allow reasonable time for a transition to new, independently-operated Managed Partner Infrastructure while Symantec modernizes and redesigns its infrastructure to adhere to industry standards. This post reiterates this plan and includes a timeline detailing when site operators may need to obtain new certificates.

Source: https://security.googleblog.com/2015/09/improved-digital-certificate-security.html
https://security.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html#

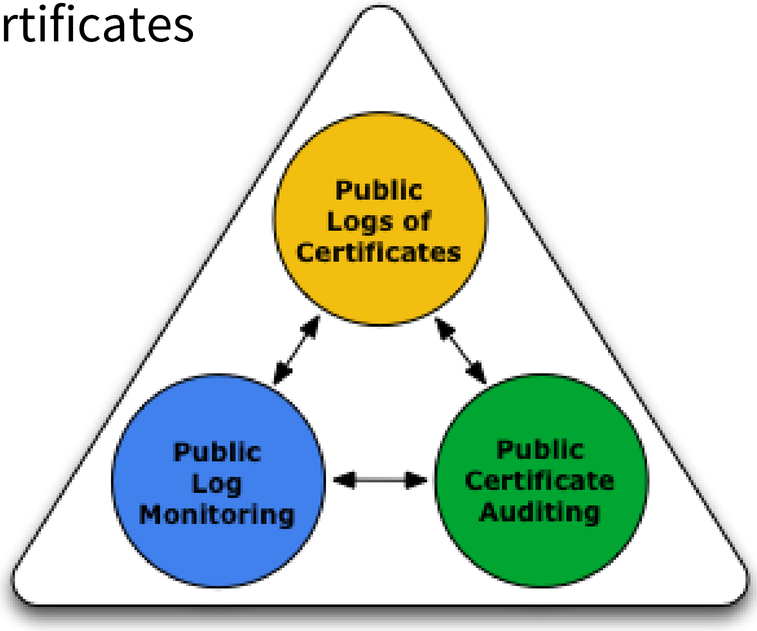
Compromised/Sloppy Certificate Authority

- HTTP Public Key Pinning (HPKP)
- DNS-based Authentication of Named Entities (DANE)
- DNS Certification Authority Authorization (CAA)
- Certificate Transparency (CT)



Certificate Transparency (CT)

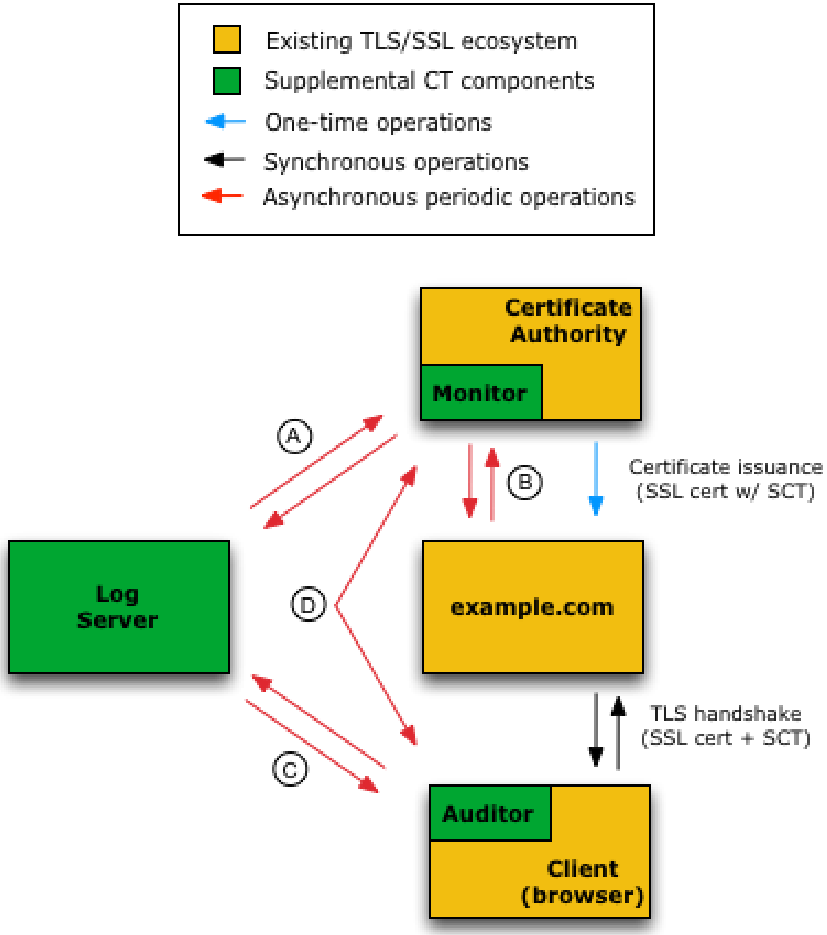
- Idea:
  - All issued certificates are logged into a public append-only log (typically by the issuing CA)
  - These logs can be monitored and audited by CAs, domain owners and clients
  - Mistakenly or maliciously issued certificates can be detected



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

Certificate Transparency

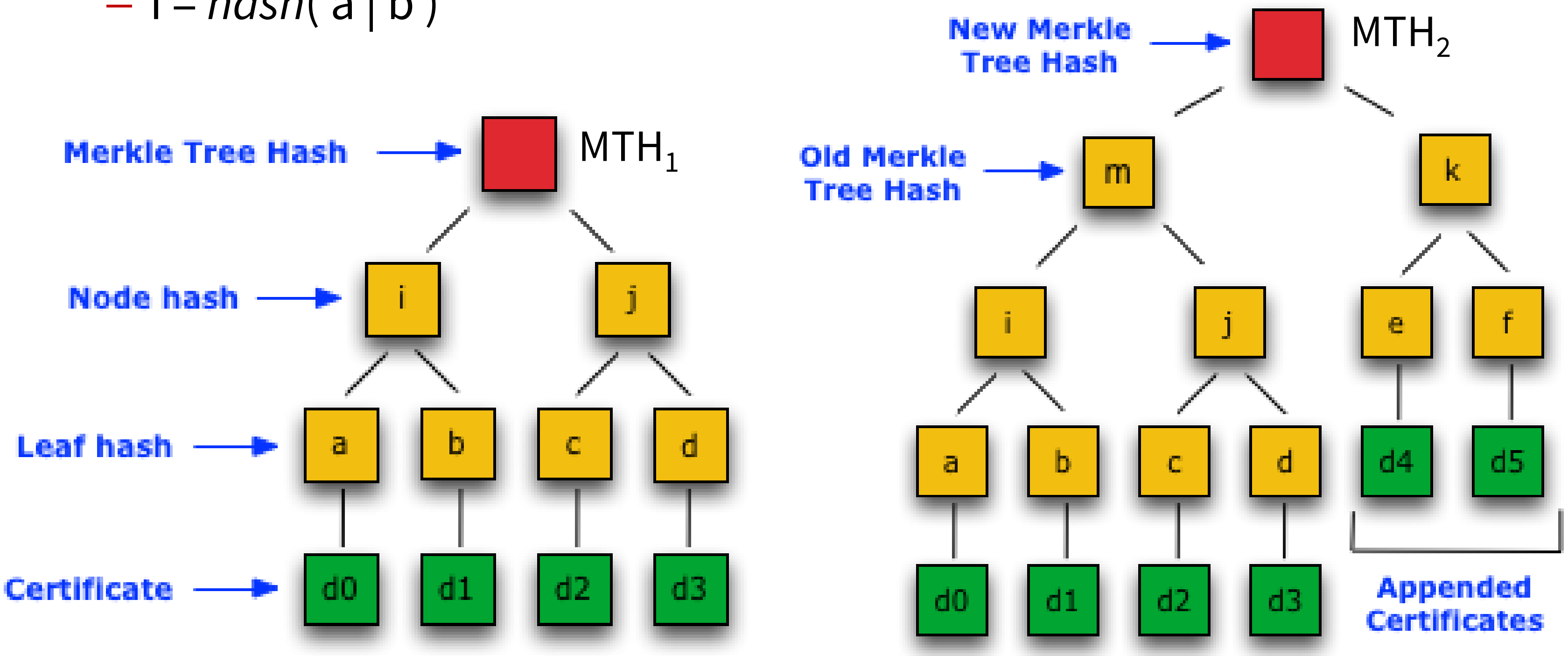
- Sample system configuration
  - A. Monitor watch logs for suspicious certificates
  - B. Certificate owner request logs for their domain
  - C. Auditors verify correct log behaviour
  - D. Monitors and auditor exchange information about logs


🟨 Existing TLS/SSL ecosystem
🟩 Supplemental CT components
← One-time operations
← Synchronous operations
← Asynchronous periodic operations
Certificate Authority
Monitor
A
B
Certificate issuance (SSL cert w/ SCT)
Log Server
D
example.com
TLS handshake (SSL cert + SCT)
C
Auditor
Client (browser)

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

Certificate Transparency

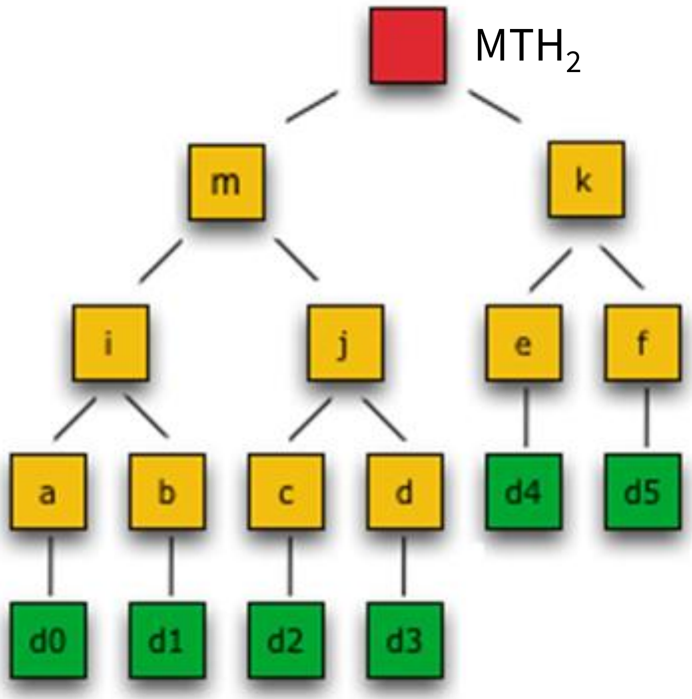
- Certificates are stored at logs in a Merkle tree: every node contains the hash value of its children, e.g.:
  - i = *hash*(a | b)

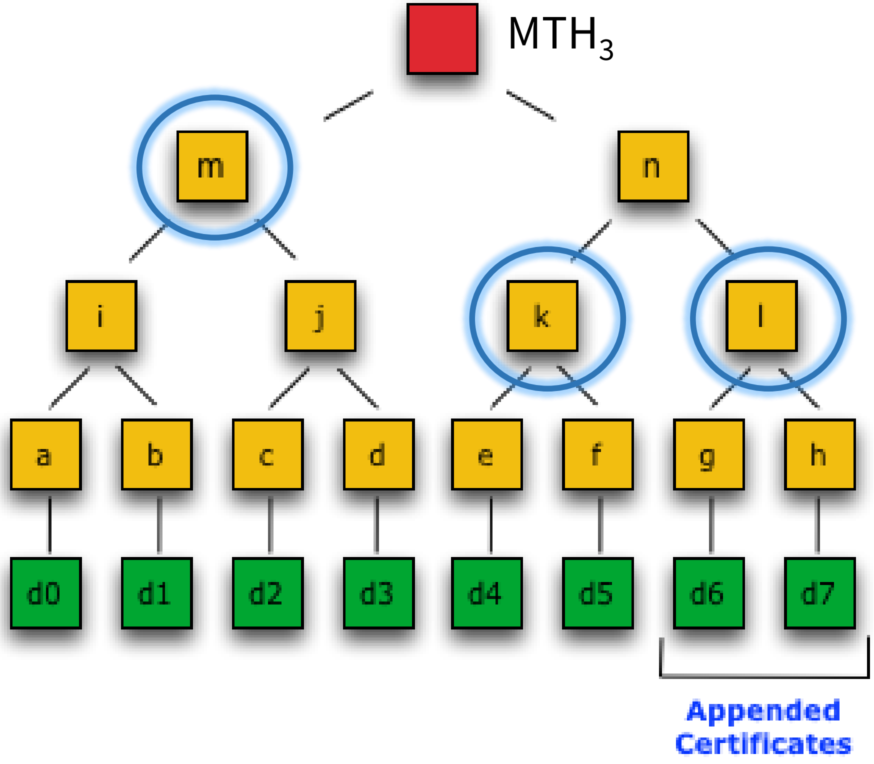


Source: https://www.certificate-transparency.org/

Certificate Transparency

- Consistency proof

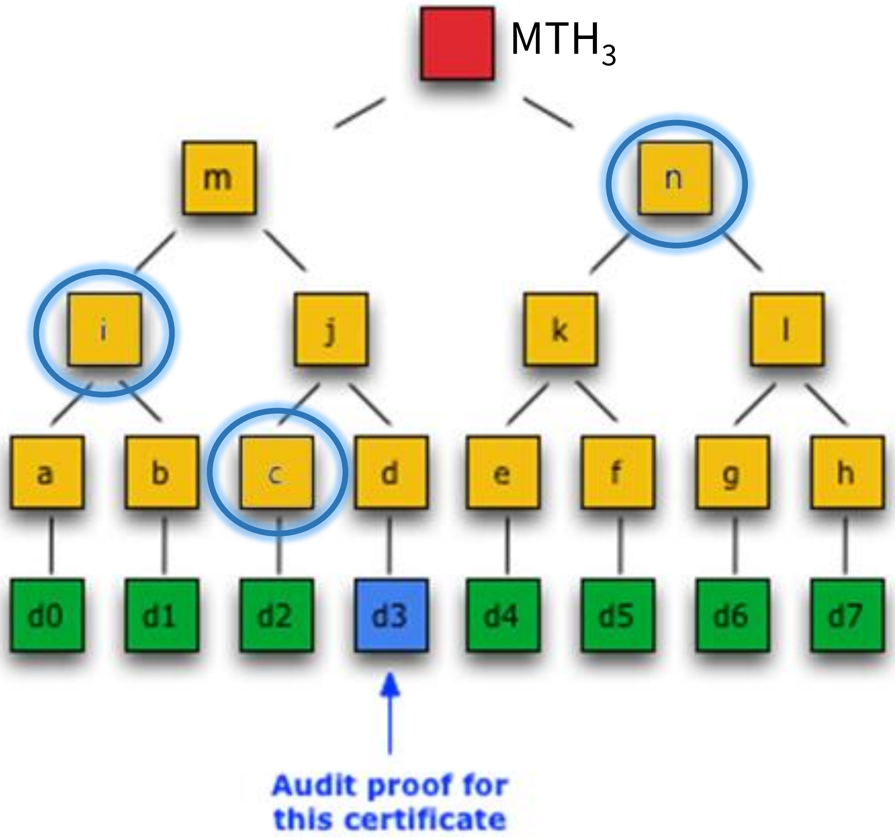




Source: https://www.certificate-transparency.org/

Certificate Transparency

- Merkle audit proof
  - Auditor wants proof that d3 is in the log
  - Auditor already knows MTH_3
  - Log sends hashes c, i, n
  - Auditor can calculate d, j, m and MTH_3^*
  - Auditor checks if $MTH_3^* = MTH_3$



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

Certificate Transparency

- Advantages:
  - If one log is not available, other logs can be requested
  - Simple overview of all issued certificates
  - Fast detection of misissued certificated and sloppy/rogue CAs
- Disadvantages:
  - No mechanism for revocation of misissued certificates
  - Logs might become large and slow
  - If the client access a log, the log might learn the users access pattern
  - If the client finds a missing certificate it is supposed to publish the log misbehavior → user's privacy of the user at risk

Summary

- Certificates are essential for TLS and for a “more secure Web”
- A single unreliable or untrustworthy certificate authority can endanger the whole Web PKI
- Still, no secure and practical solution is available
- Certificate transparency is the current candidate favored by the browser vendors
- However: some problems remain unsolved (e.g. revocation)
- Current research:
  - Certificate revocation for CT logs
  - Efficient log implementation
  - Privacy conserving log management

References

- J. Gustafsson, G. Overier, M. Arlitt, and N. Carlsson, “A First Look at the CT Landscape: Certificate Transparency Logs in Practice,” in *Passive and Active Measurement*, 2017, pp. 87–99.
- Google, “Certificate Transparency,” 2018. [Online]. Available: https://www.certificate-transparency.org/. [Accessed: 22-Feb-2018].
- S. Eskandarian, E. Messeri, J. Bonneau, and D. Boneh, “Certificate Transparency with Privacy,” *Proceedings on Privacy Enhancing Technologies*, vol. 2017, no. 4, pp. 329–344, 2017.
- K. Borgolte, T. Fiebig, S. Hao, C. Kruegel, and G. Vigna, “Cloud Strife: Mitigating the Security Risks of Domain-Validated Certificates,” in *Proc. Internet Society Symposium on Network and Distributed System Security (NDSS)*, 2018.
- “Dell Computers Contain CA Root Certificate Vulnerability.” [Online]. Available: https://www.us-cert.gov/ncas/current-activity/2015/11/24/Dell-Computers-Contain-CA-Root-Certifcate-Vulnerability. [Accessed: 25-Feb-2018].
- L. Sjöström and C. Nykvist, *How Certificate Transparency Impact the Performance*. 2017.
- C. Jackson, A. Barth, and J. Hodges, “HTTP Strict Transport Security (HSTS),” 2012. [Online]. Available: https://tools.ietf.org/html/rfc6797. [Accessed: 23-Feb-2018].
- Nettrack, “SSL Issuer Popularity,” *NetTrack - Anonymous Web Statistics*, 2018. [Online]. Available: https://nettrack.info//ssl_certificate_issuers.html. [Accessed: 22-Feb-2018].
- H. Böck, “The Problem with OCSP Stapling and Must Staple and why Certificate Revocation is still broken - Hanno’s blog,” 2017. [Online]. Available: https://blog.hboeck.de/archives/886-The-Problem-with-OCSP-Stapling-and-Must-Staple-and-why-Certificate-Revocation-is-still-broken.html. [Accessed: 22-Feb-2018].
- Google, “Transparency Report,” 2018. [Online]. Available: https://transparencyreport.google.com/. [Accessed: 22-Feb-2018].
- D. Eastlake, “Transport Layer Security (TLS) Extensions: Extension Definitions,” 2011. [Online]. Available: https://tools.ietf.org/html/rfc6066. [Accessed: 23-Feb-2018].
- S. Galperin, S. Santesson, M. Myers, A. Malpani, and C. Adams, “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP,” 2013. [Online]. Available: https://tools.ietf.org/html/rfc6960. [Accessed: 23-Feb-2018].
- P. Hallam-Baker, “X.509v3 Transport Layer Security (TLS) Feature Extension,” 2015. [Online]. Available: https://tools.ietf.org/html/rfc7633. [Accessed: 23-Feb-2018].
- R. Dahlberg, T. Pulls, and R. Peeters, “Efficient Sparse Merkle Trees,” in *Secure IT Systems*, 2016, pp. 199–215.