

DANE, why we need it

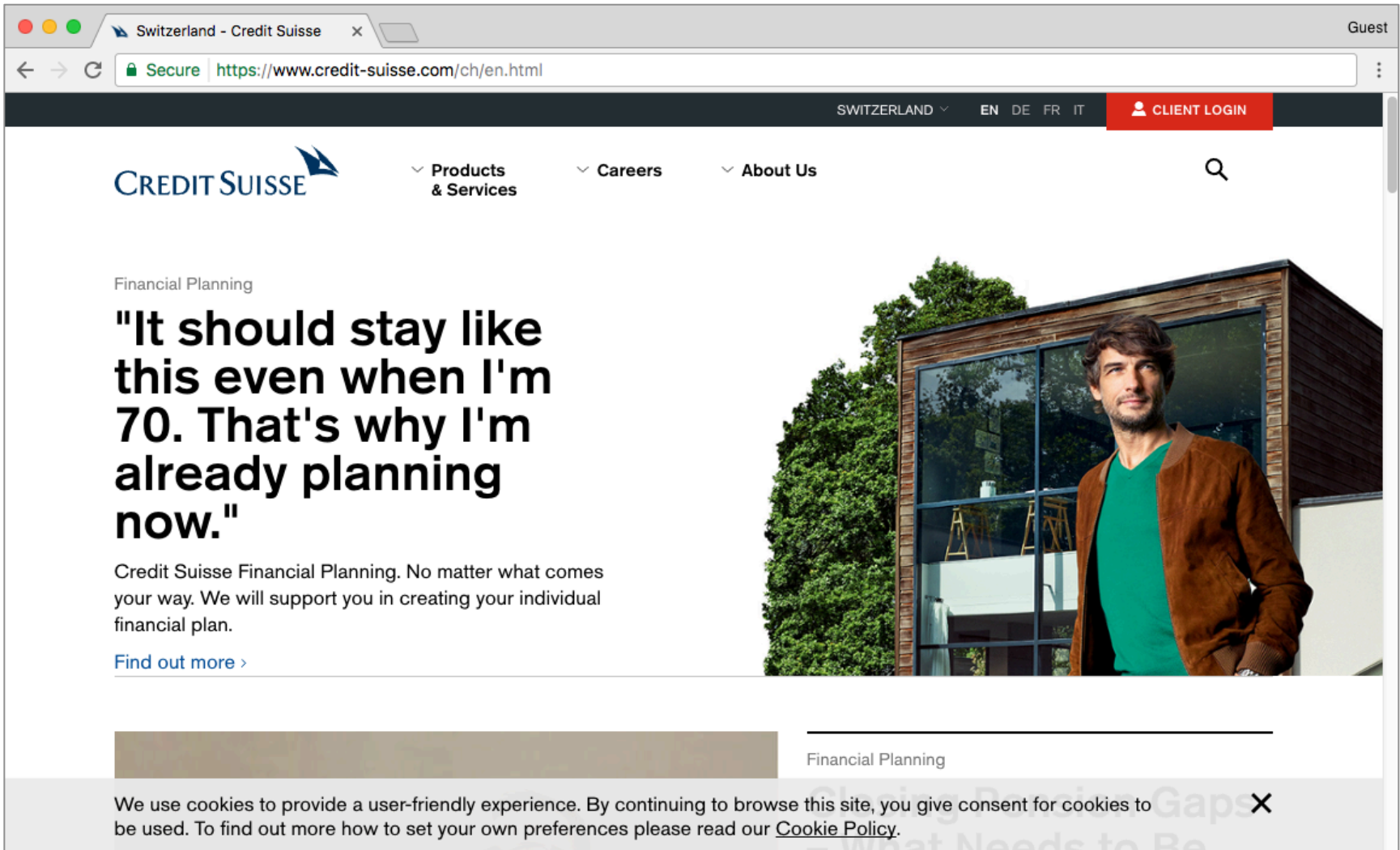


SWITCH

Daniel Stirnimann
daniel.stirnimann@switch.ch

Bern, 29. March 2017

Why do we trust this website?



The screenshot shows a web browser window with the URL <https://www.credit-suisse.com/ch/en.html>. The page features the Credit Suisse logo and navigation menus for Products & Services, Careers, and About Us. A search icon is also present. The main content area displays a financial planning advertisement with the headline "It should stay like this even when I'm 70. That's why I'm already planning now." and a photograph of a man in a brown jacket standing in front of a modern building. Below the headline, there is a sub-headline "Financial Planning" and a paragraph of text: "Credit Suisse Financial Planning. No matter what comes your way. We will support you in creating your individual financial plan." A link "Find out more >" is provided. At the bottom of the page, there is a cookie consent banner that reads: "We use cookies to provide a user-friendly experience. By continuing to browse this site, you give consent for cookies to be used. To find out more how to set your own preferences please read our [Cookie Policy](#)." A close button (X) is visible on the right side of the banner.

Switzerland - Credit Suisse x Guest

Secure <https://www.credit-suisse.com/ch/en.html>

SWITZERLAND EN DE FR IT CLIENT LOGIN

CREDIT SUISSE

Products & Services Careers About Us

Financial Planning

"It should stay like this even when I'm 70. That's why I'm already planning now."

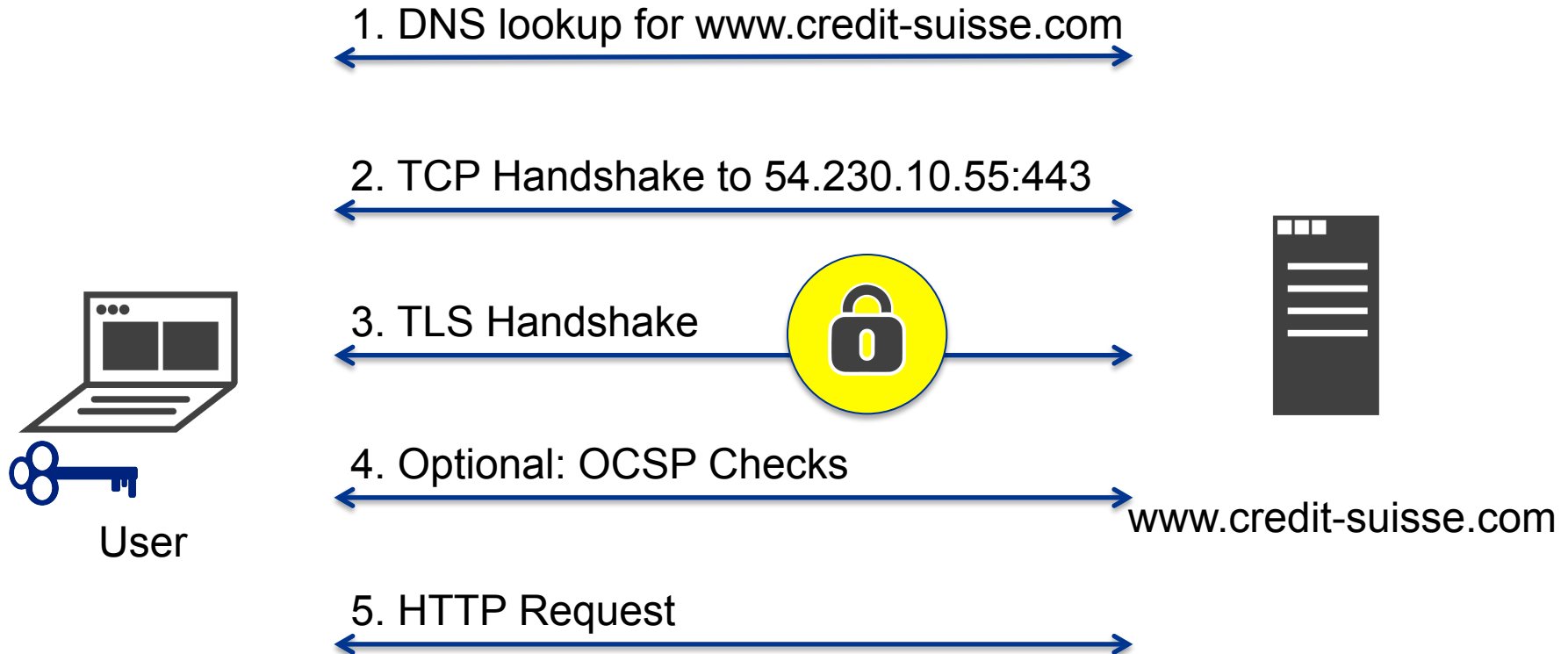
Credit Suisse Financial Planning. No matter what comes your way. We will support you in creating your individual financial plan.

[Find out more >](#)

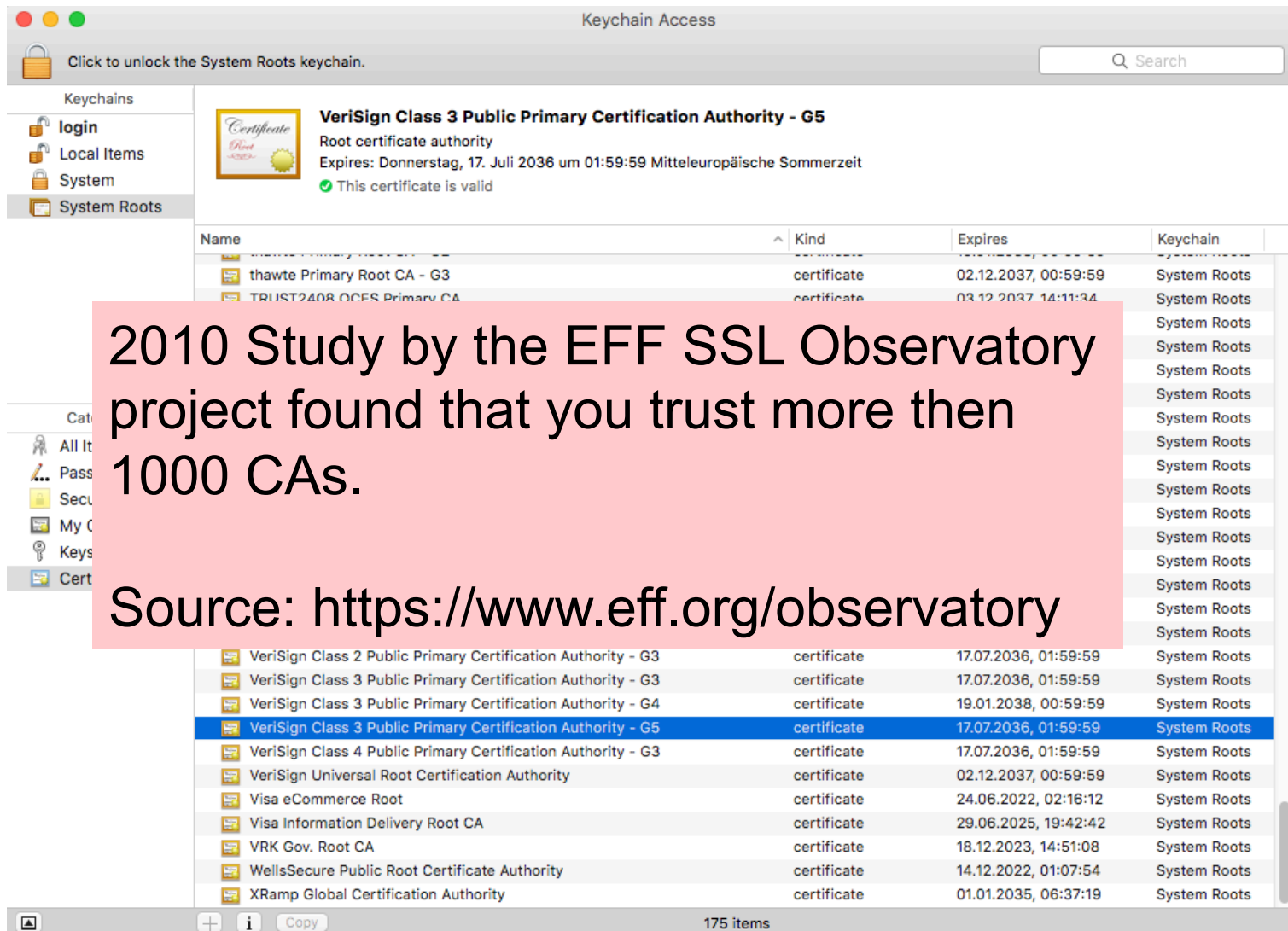
Financial Planning

We use cookies to provide a user-friendly experience. By continuing to browse this site, you give consent for cookies to be used. To find out more how to set your own preferences please read our [Cookie Policy](#). X

Why do we trust this website?



Local Trust Store



Keychain Access

Click to unlock the System Roots keychain.

Search

Keychains

- login
- Local Items
- System
- System Roots

VeriSign Class 3 Public Primary Certification Authority - G5

Root certificate authority

Expires: Donnerstag, 17. Juli 2036 um 01:59:59 Mitteleuropäische Sommerzeit

✓ This certificate is valid

Name	Kind	Expires	Keychain
thawte Primary Root CA - G3	certificate	02.12.2037, 00:59:59	System Roots
TRUST2408 OCES Primary CA	certificate	03.12.2037, 14:11:34	System Roots
VeriSign Class 2 Public Primary Certification Authority - G3	certificate	17.07.2036, 01:59:59	System Roots
VeriSign Class 3 Public Primary Certification Authority - G3	certificate	17.07.2036, 01:59:59	System Roots
VeriSign Class 3 Public Primary Certification Authority - G4	certificate	19.01.2038, 00:59:59	System Roots
VeriSign Class 3 Public Primary Certification Authority - G5	certificate	17.07.2036, 01:59:59	System Roots
VeriSign Class 4 Public Primary Certification Authority - G3	certificate	17.07.2036, 01:59:59	System Roots
VeriSign Universal Root Certification Authority	certificate	02.12.2037, 00:59:59	System Roots
Visa eCommerce Root	certificate	24.06.2022, 02:16:12	System Roots
Visa Information Delivery Root CA	certificate	29.06.2025, 19:42:42	System Roots
VRK Gov. Root CA	certificate	18.12.2023, 14:51:08	System Roots
WellsSecure Public Root Certificate Authority	certificate	14.12.2022, 01:07:54	System Roots
XRamp Global Certification Authority	certificate	01.01.2035, 06:37:19	System Roots

2010 Study by the EFF SSL Observatory project found that you trust more than 1000 CAs.

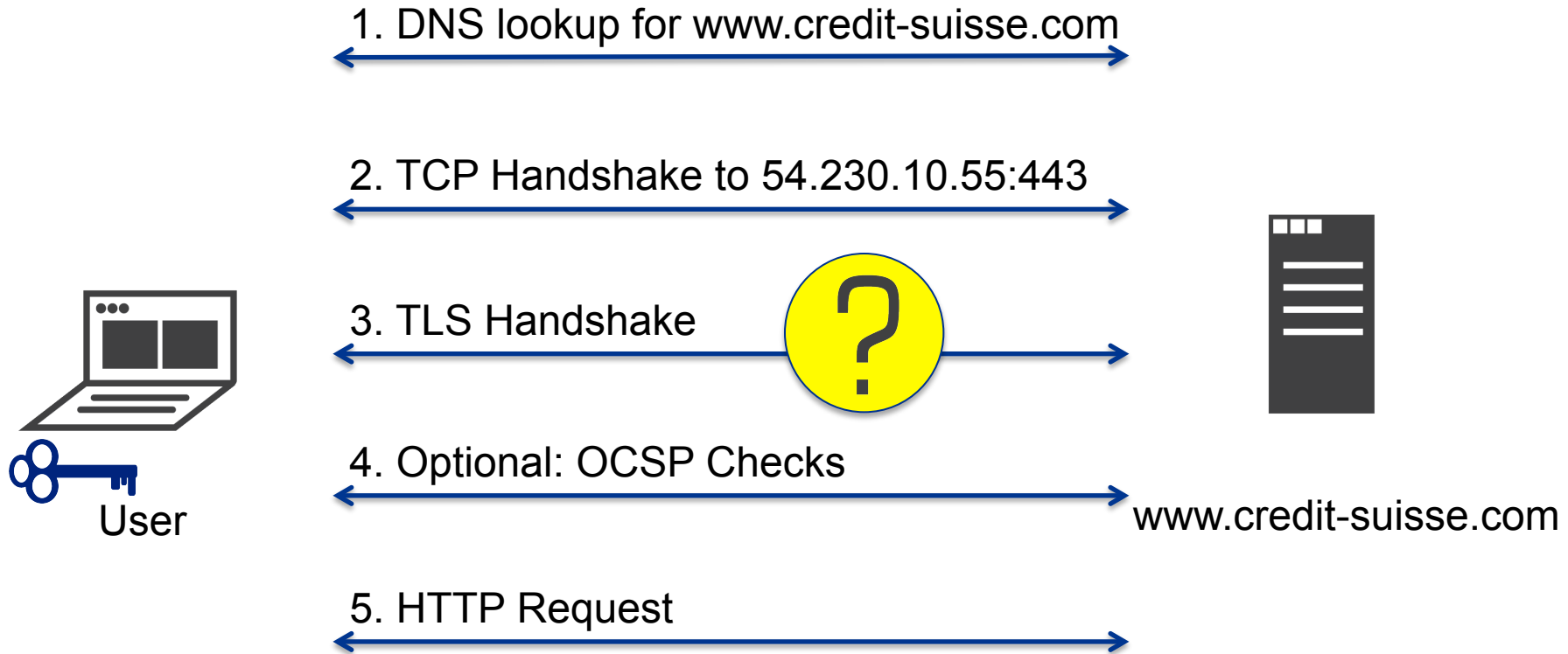
Source: <https://www.eff.org/observatory>

175 items

Broken CA Model

- Any CA can issue certificates for any domain (weakest link)
- CAs have been compromised in the past
- CAs have issued wrong or unauthorized certificates
 - <https://sslmate.com/certspotter/failures>
 - <https://arstechnica.com/security/2017/01/already-on-probation-symantec-issues-more-illegit-https-certificates/>
- Domain Validated (DV) certificates are entirely automated
 - Risk of vulnerability in the API
 - A temporary compromise of DNS, email or web can lead to long-term fraudulent certificate
 - CA validated domain ownership over insecure channels such as unauthenticated DNS, insecure HTTP and email

Recap: Why do we trust this website?



DEMO



Solutions 1/2

- DNS Certification Authority Authorization (CAA) RR (RFC 6844)
 - Over insecure unauthenticated DNS! CAA does not mandate DNSSEC (only recommend it)
 - Helps prevent mis-issuance. Does not prevent usage.
 - CAB Forum has decided to make CAA checking mandatory
- Certificate Transparency (certificate-transparency.org)
 - Search and Monitor:
 - <https://sslmate.com/certspotter/>
 - <https://crt.sh/>
 - Puts burden on every domain owner to monitor and internally verify every issued certificate. Does help for big companies.
 - Does not prevent mis-issuance. Does not prevent usage. Helps detecting misuse.
 - Note: web browsers will mandate CT logs in the future in order to accept CA issued certificate

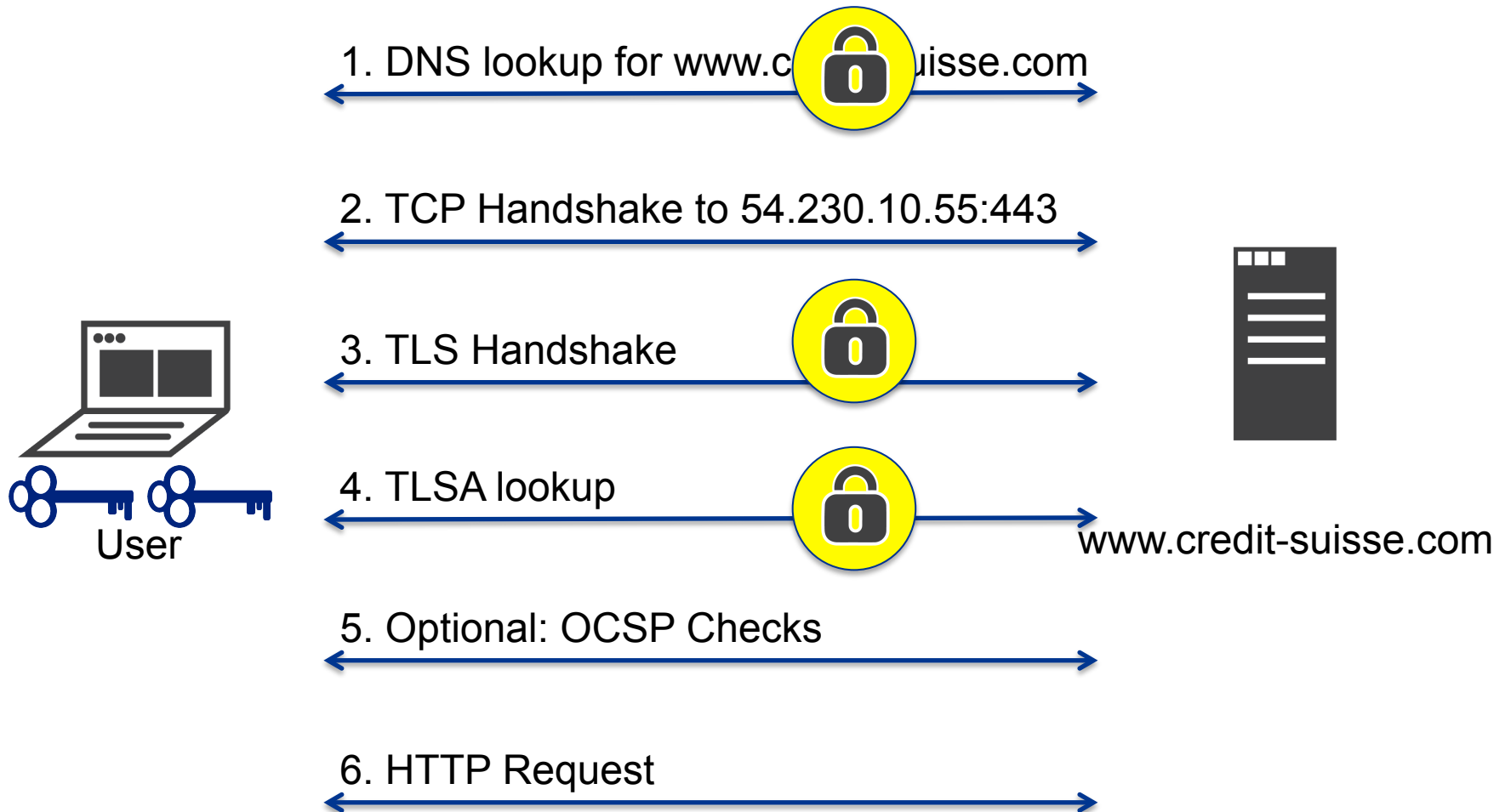
Solutions 2/2

- Using the DNS to associated domain name public key certificates with domain name (RFC 6698, RFC 7671)
 - Mandates authenticated (secure) DNS -> DNSSEC

DANE TLSA specifies a protocol for publishing TLS server certificate associations via DNSSEC

With DANE:

Why do we trust this website?



TLSA Resource Record

Example:

```
_25._tcp.mail.example.com.
( 3FE246A84879
  6B6E7CA8E29
```

- Certificate validity does not apply
- Certificate CN/SNI has no effect
- Only TLSA record is relevant

Cert Usage Field:

- 0: PKIX-TA } Replaces signed certificate by PKI in
trust stores
- 1: PKIX-EE }
- 2: DANE-TA } Use DANE only (e.g. non-public internal CA)
- 3: DANE-EE } Use DANE only (only option if self-signed)

TLSA Resource Record

Example:

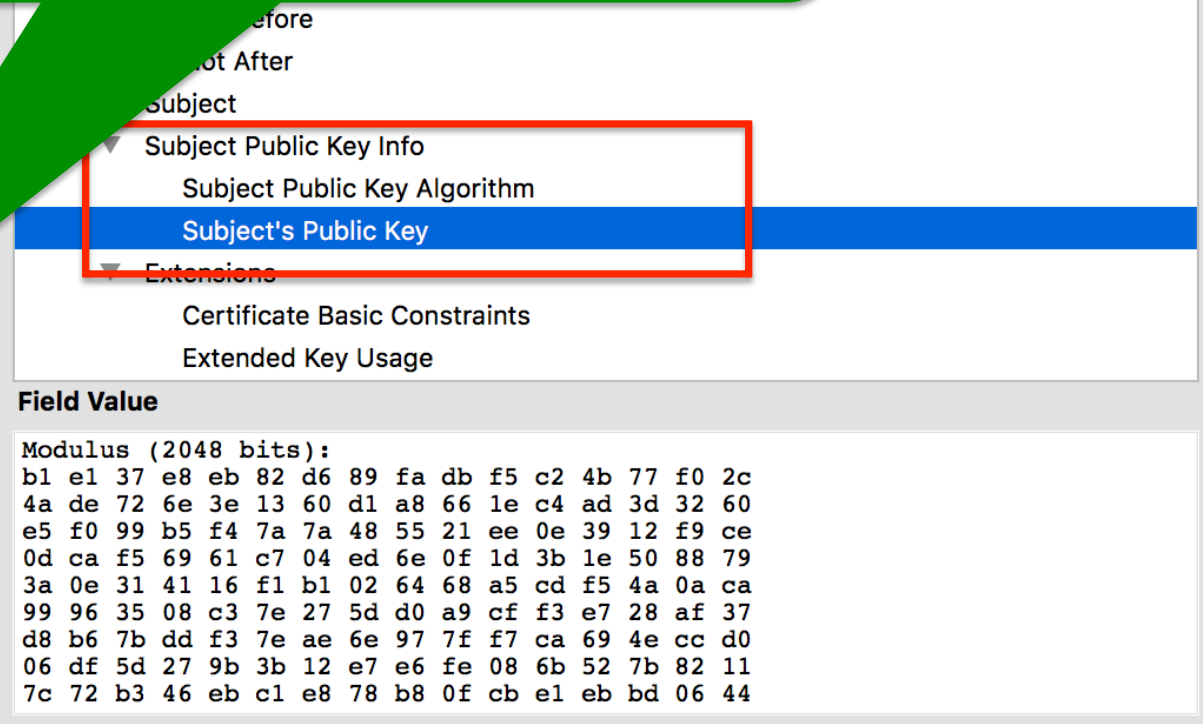
_25._tcp.mail.example.com
 (3FE246A8E2
 6B6E7CA8E2)

Recommended:

- TLSA RR needs no change across renewal of cert if same private key is used

Selector Field:

- 0: Full certificate
- 1: SubjectPublicKey



Before
Not After
Subject
Subject Public Key Info
Subject Public Key Algorithm
Subject's Public Key
Extensions
Certificate Basic Constraints
Extended Key Usage

Field Value

Modulus (2048 bits):
 b1 e1 37 e8 eb 82 d6 89 fa db f5 c2 4b 77 f0 2c
 4a de 72 6e 3e 13 60 d1 a8 66 1e c4 ad 3d 32 60
 e5 f0 99 b5 f4 7a 7a 48 55 21 ee 0e 39 12 f9 ce
 0d ca f5 69 61 c7 04 ed 6e 0f 1d 3b 1e 50 88 79
 3a 0e 31 41 16 f1 b1 02 64 68 a5 cd f5 4a 0a ca
 99 96 35 08 c3 7e 27 5d d0 a9 cf f3 e7 28 af 37
 d8 b6 7b dd f3 7e ae 6e 97 7f f7 ca 69 4e cc d0
 06 df 5d 27 9b 3b 12 e7 e6 fe 08 6b 52 7b 82 11
 7c 72 b3 46 eb c1 e8 78 b8 0f cb e1 eb bd 06 44

TLSA Resource Record

Example:

```
_25._tcp.mail.example.com. IN TLSA 3 1 1  
  ( 3FE246A848798236DD2AB78D39F0651D  
    6B6E7CA8E2984012EB0A2E1AC8A87B72 )
```

Matching Type Field:

- 0: Full } Size issue
- 1: SHA2-256 } Must be supported by all DANE clients
- 2: SHA2-512 } Not recommended

TLSA Survey .CH

Zones with TLSA Records: 614

Zones with TLSA Records for MX: 611

Zones with TLSA Records for Web: 611

Found TLSA Usage Strings: 676

TLSA usage strings 1 0 0: 360

TLSA usage strings 2 0 0: 316

TLSA usage strings 3 0 0: 60

TLSA usage strings 1 0 1: 30

TLSA usage strings 2 0 1: 24

TLSA usage strings 3 0 1: 12

TLSA usage strings 3 1 0: 12

TLSA usage strings 3 1 1: 676

TLSA usage strings 3 0 1: 360



govcert.ch
antiphishing.ch
abuse.ch
gmx.ch
posteo.ch
open.ch
switch.ch

...just one Problem

- No web browsers supports DANE out of the box
 - You need a plug-in such as www.dnssec-validator.cz
- Reasons:
 - additional DNS lookups on every connection
 - Non-validating resolvers
 - broken middle-boxes (firewalls)
- This is about to change:
 - draft-shore-tls-dnssec-chain-extension
 - https://bugzilla.mozilla.org/show_bug.cgi?id=672600

DANE for Mail just works

- No usage issues:
 - Typically has a static local resolver (no unexpected middlebox)
 - Latency of an additional DNS lookup is no problem
- DANE for mail provides:
 - Authenticated encrypted connection between SMTP servers
 - Prevents STARTTLS “downgrade” attacks
- It’s in use by some big mail providers
- It’s required by the BSI “Richtlinie für sicherer E-Mail-Transport”

Home Work

- Turn on DNSSEC validation on your local resolver
 - Guidelines for BIND, unbound, Windows DNS:
<https://www.surf.nl/en/knowledge-base/2012/white-paper-deploying-dnssec.html>
- DNSSEC sign your zone
- Strongly consider enabling DANE for mail
- Plan for using DANE for the web 😊

Questions?