ETH zürich
Network Security Group

PRINCETON
UNIVERSITY

F-PKI: Enabling Innovation and Trust Flexibility in the HTTPS Public-Key Infrastructure

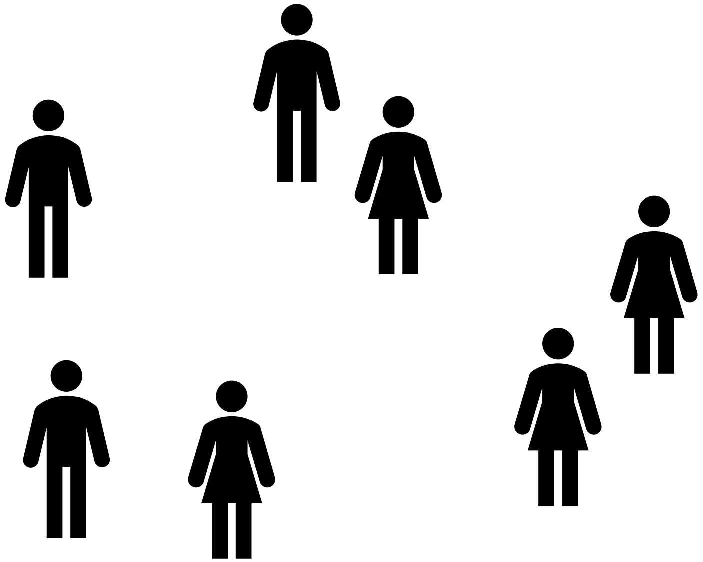
Laurent Chuat[*], **Cyrill Krähenbühl[*]**, Prateek Mittal[†], Adrian Perrig[*]
[*]ETH Zürich, [†]Princeton University

Web PKI

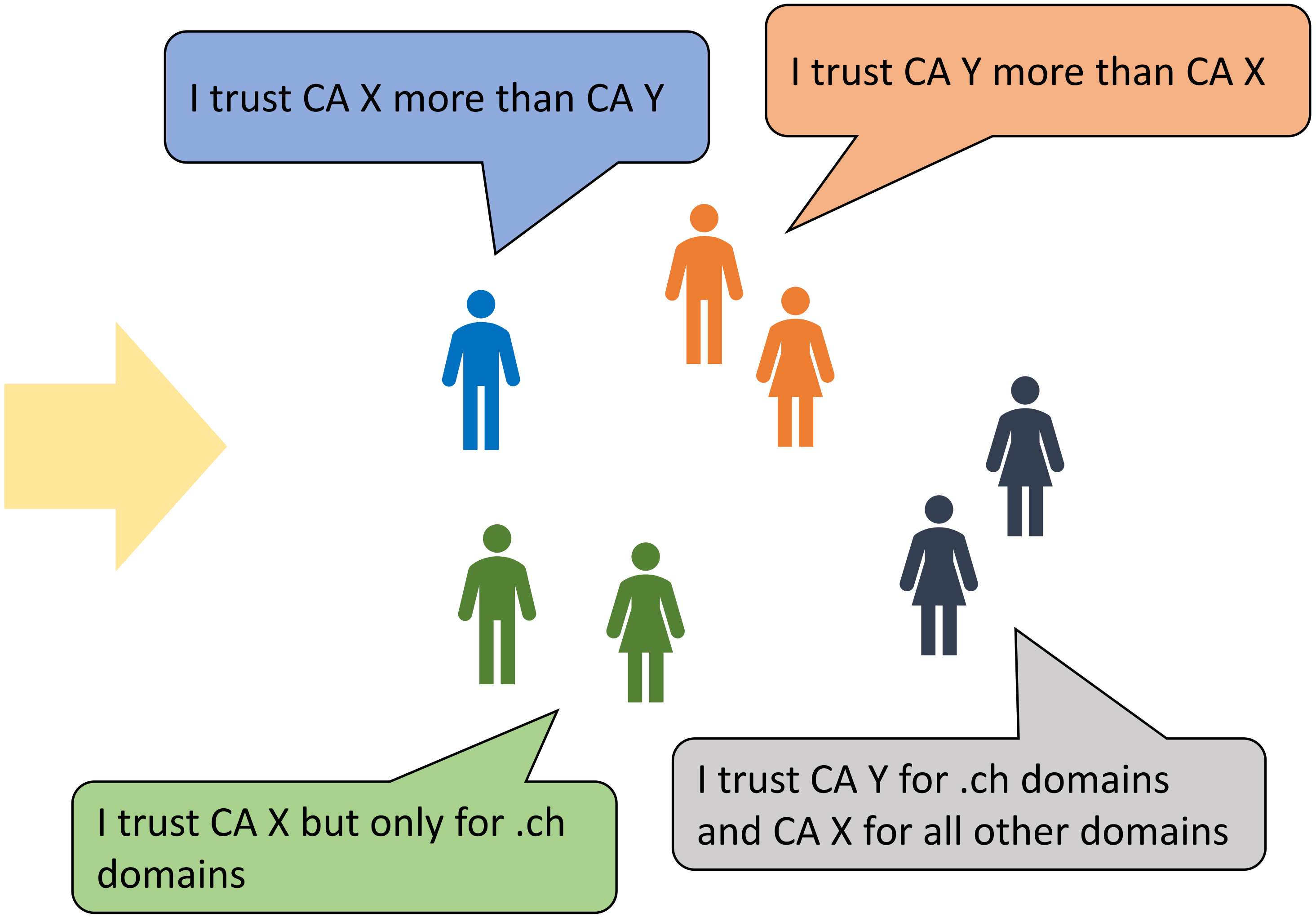
- Essential building block for security on the Internet
- Basis of TLS, HTTPS, DoH, DoT, …
- Myriad of improvements and extensions
  - OCSP (stapling)
  - Certificate Transparency
  - ACME
  - …

Web PKI is Too Rigid

Equal Trust placed into a **fixed** set of CAs



Heterogeneous global society requires more **flexibility**!



I trust CA X more than CA Y

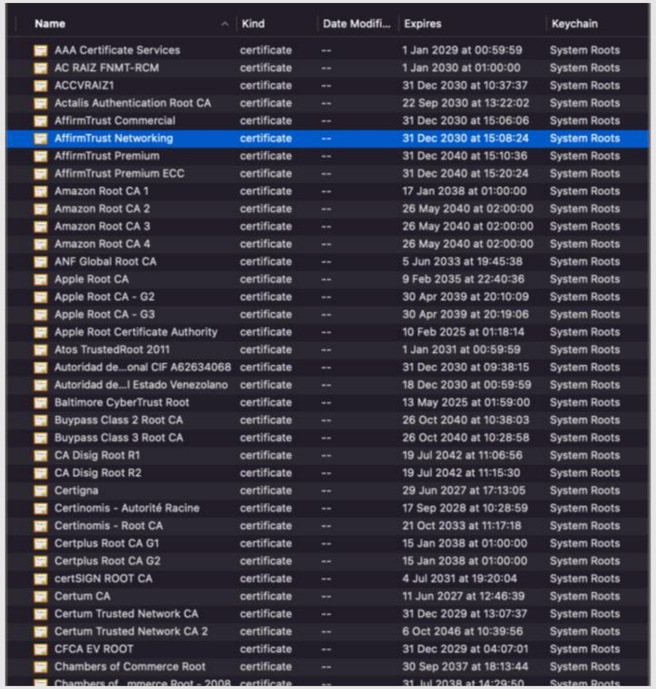
I trust CA Y more than CA X

I trust CA X but only for .ch domains

I trust CA Y for .ch domains and CA X for all other domains

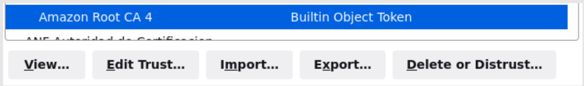
Problems in the Web PKI

Weakest Link Security



Name	Kind	Date Modifi...	Expires	Keychain
AAA Certificate Services	certificate	--	1 Jan 2029 at 00:59:59	System Roots
AC RAIZ FNMT-RCM	certificate	--	1 Jan 2030 at 01:00:00	System Roots
ACCVRAIZ1	certificate	--	31 Dec 2030 at 10:37:37	System Roots
Actalis Authentication Root CA	certificate	--	22 Sep 2030 at 13:22:02	System Roots
AffirmTrust Commercial	certificate	--	31 Dec 2030 at 15:06:06	System Roots
AffirmTrust Networking	certificate	--	31 Dec 2030 at 15:08:24	System Roots
AffirmTrust Premium	certificate	--	31 Dec 2040 at 15:10:36	System Roots
AffirmTrust Premium ECC	certificate	--	31 Dec 2040 at 15:20:24	System Roots
Amazon Root CA 1	certificate	--	17 Jan 2038 at 01:00:00	System Roots
Amazon Root CA 2	certificate	--	26 May 2040 at 02:00:00	System Roots
Amazon Root CA 3	certificate	--	26 May 2040 at 02:00:00	System Roots
Amazon Root CA 4	certificate	--	26 May 2040 at 02:00:00	System Roots
ANF Global Root CA	certificate	--	5 Jun 2033 at 19:45:38	System Roots
Apple Root CA	certificate	--	9 Feb 2035 at 22:40:36	System Roots
Apple Root CA - G2	certificate	--	30 Apr 2039 at 20:10:09	System Roots
Apple Root CA - G3	certificate	--	30 Apr 2039 at 20:19:06	System Roots
Apple Root Certificate Authority	certificate	--	10 Feb 2025 at 01:18:14	System Roots
Atos TrustedRoot 2011	certificate	--	1 Jan 2031 at 00:59:59	System Roots
Autoridad de...onal CIF A62634068	certificate	--	31 Dec 2030 at 09:38:15	System Roots
Autoridad de...l Estado Venezolano	certificate	--	18 Dec 2030 at 00:59:59	System Roots
Baltimore CyberTrust Root	certificate	--	13 May 2025 at 01:59:00	System Roots
Buypass Class 2 Root CA	certificate	--	26 Oct 2040 at 10:38:03	System Roots
Buypass Class 3 Root CA	certificate	--	26 Oct 2040 at 10:28:58	System Roots
CA Disig Root R1	certificate	--	19 Jul 2042 at 11:06:56	System Roots
CA Disig Root R2	certificate	--	19 Jul 2042 at 11:15:30	System Roots
Certigna	certificate	--	29 Jun 2027 at 17:13:05	System Roots
Certinomis - Autorité Racine	certificate	--	17 Sep 2028 at 10:28:59	System Roots
Certinomis - Root CA	certificate	--	21 Oct 2033 at 11:17:18	System Roots
Certplus Root CA G1	certificate	--	15 Jan 2038 at 01:00:00	System Roots
Certplus Root CA G2	certificate	--	15 Jan 2038 at 01:00:00	System Roots
certSIGN ROOT CA	certificate	--	4 Jul 2031 at 19:20:04	System Roots
Certum CA	certificate	--	11 Jun 2027 at 12:46:39	System Roots
Certum Trusted Network CA	certificate	--	31 Dec 2029 at 13:07:37	System Roots
Certum Trusted Network CA 2	certificate	--	6 Oct 2046 at 10:39:56	System Roots
CFCA EV ROOT	certificate	--	31 Dec 2029 at 04:07:01	System Roots
Chambers of Commerce Root	certificate	--	30 Sep 2037 at 18:13:44	System Roots
Chambers of...mmerce Root - 2008	certificate	--	31 Jul 2038 at 14:29:50	System Roots

No Trust Flexibility



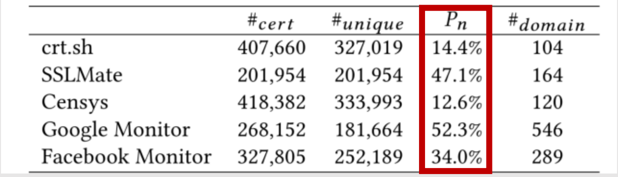
Amazon Root CA 4 Builtin Object Token

Limited Control for Domain Owners

Censys

crt.sh

sslmate



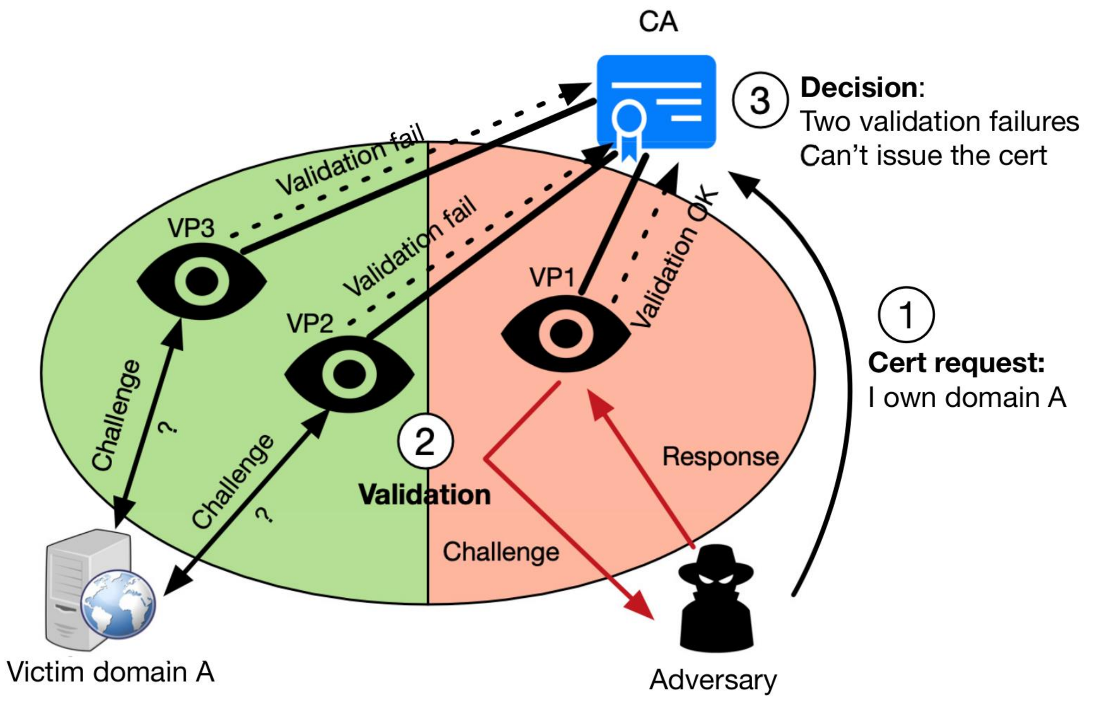
	$\#_{cert}$	$\#_{unique}$	P_n	$\#_{domain}$
crt.sh	407,660	327,019	14.4%	104
SSLMate	201,954	201,954	47.1%	164
Censys	418,382	333,993	12.6%	120
Google Monitor	268,152	181,664	52.3%	546
Facebook Monitor	327,805	252,189	34.0%	289

"Certificate Transparency in the Wild", Li et al., CCS '19

Lack of Innovation

Lack of Innovation

- **All** CAs must implement a new security measure
  - Lack of incentives to be the first one to innovate!
- Trust root changes cause collateral damage
  - Removal of CAs leads to unavailable (secure) websites

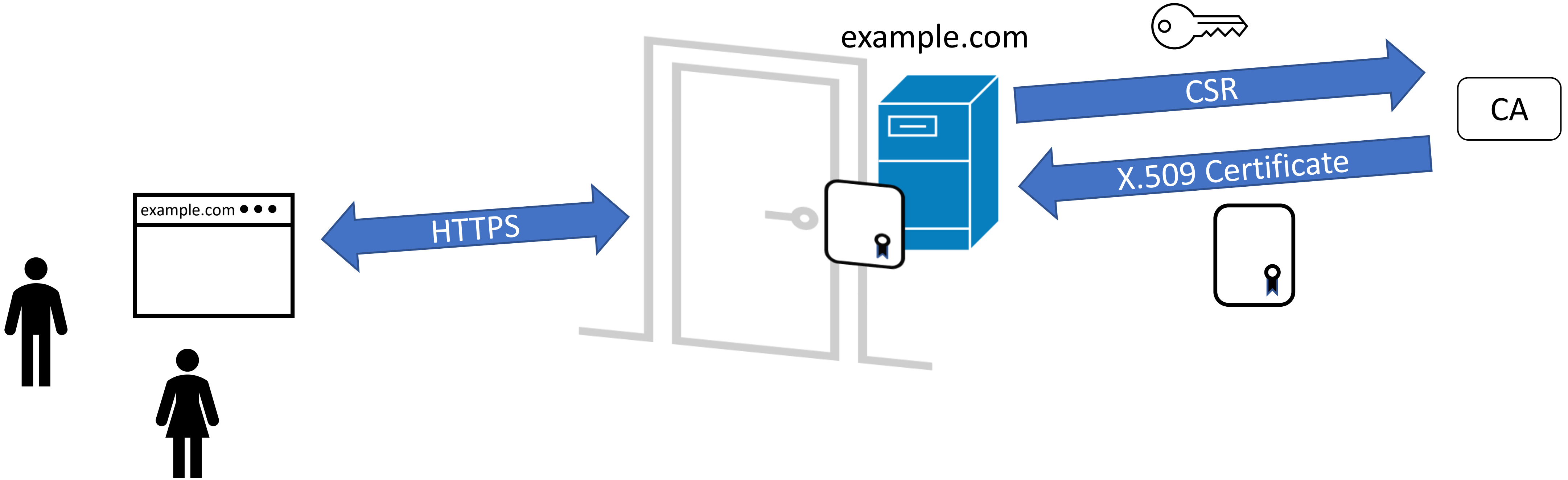


"Experiences Deploying Multi-Vantage-Point Domain Validation at Let's Encrypt", Birge-Lee et al., USENIX Security '21

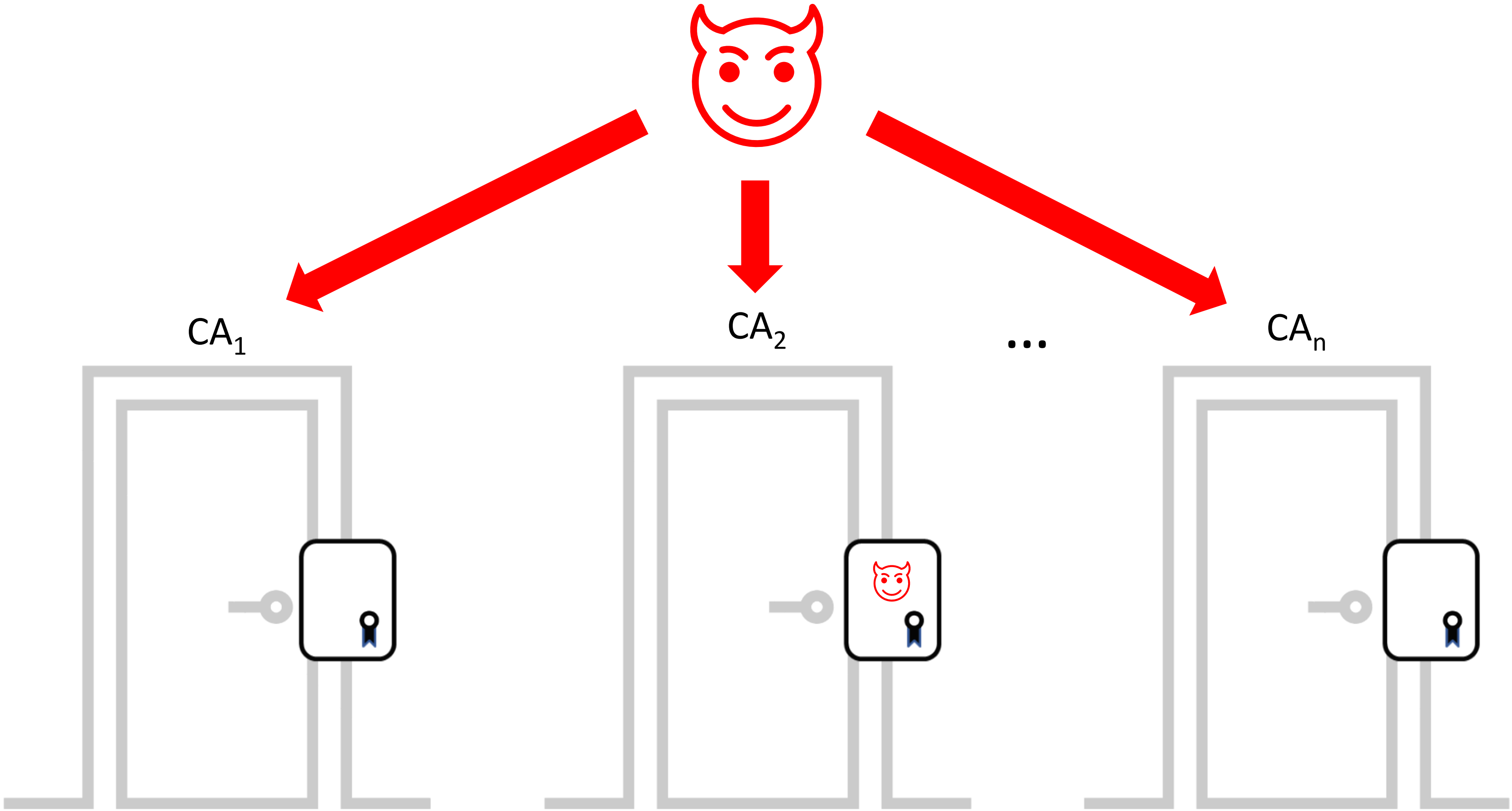
Flexible PKI (F-PKI)

- Fix for weakest link security in Web PKI
- Flexible notion of trust
- Increased control over certificates for domain owners
- Incremental deployability
- No server-side modifications in HTTPS
- Leverages existing CT infrastructure

Web PKI

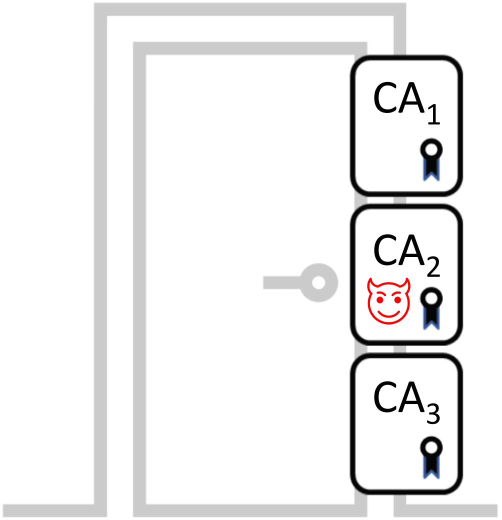


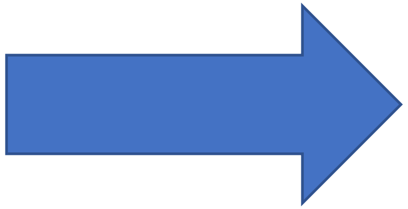
Web PKI: Weakest Link Security



Fix Weakest Link Security

Validate certificates from all CAs ⇒ detect misbehaving CA



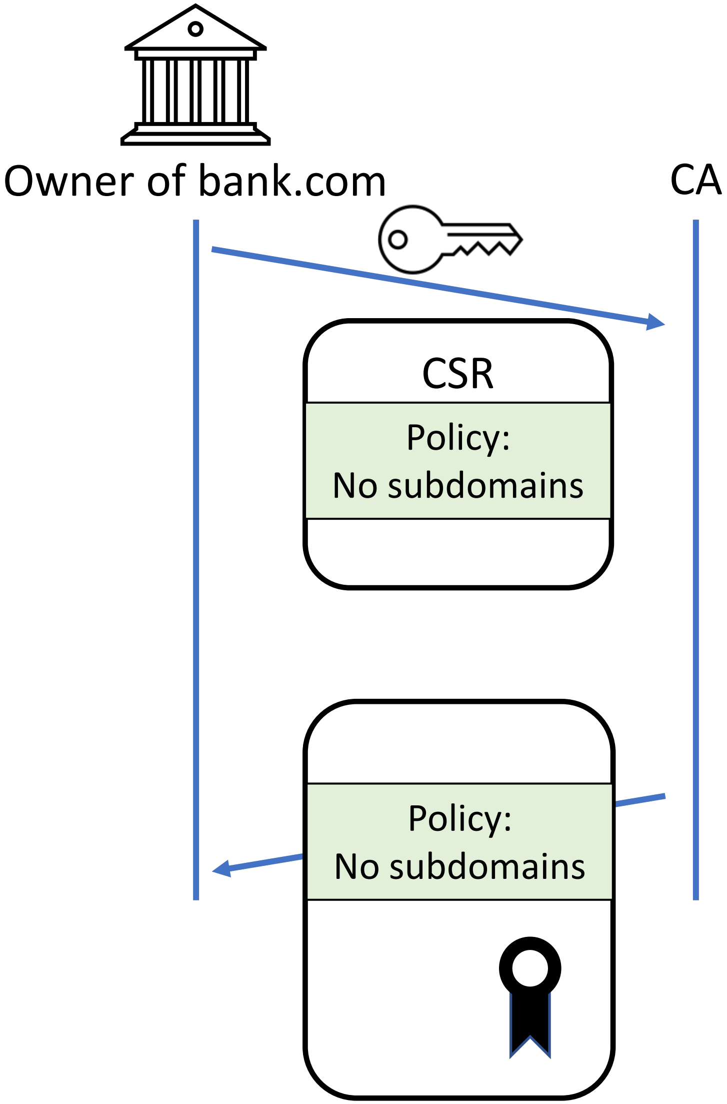


1. How do we fetch all certificates?
2. What are conflicting certificates?
   - Different public keys?
   - Different Issuers?

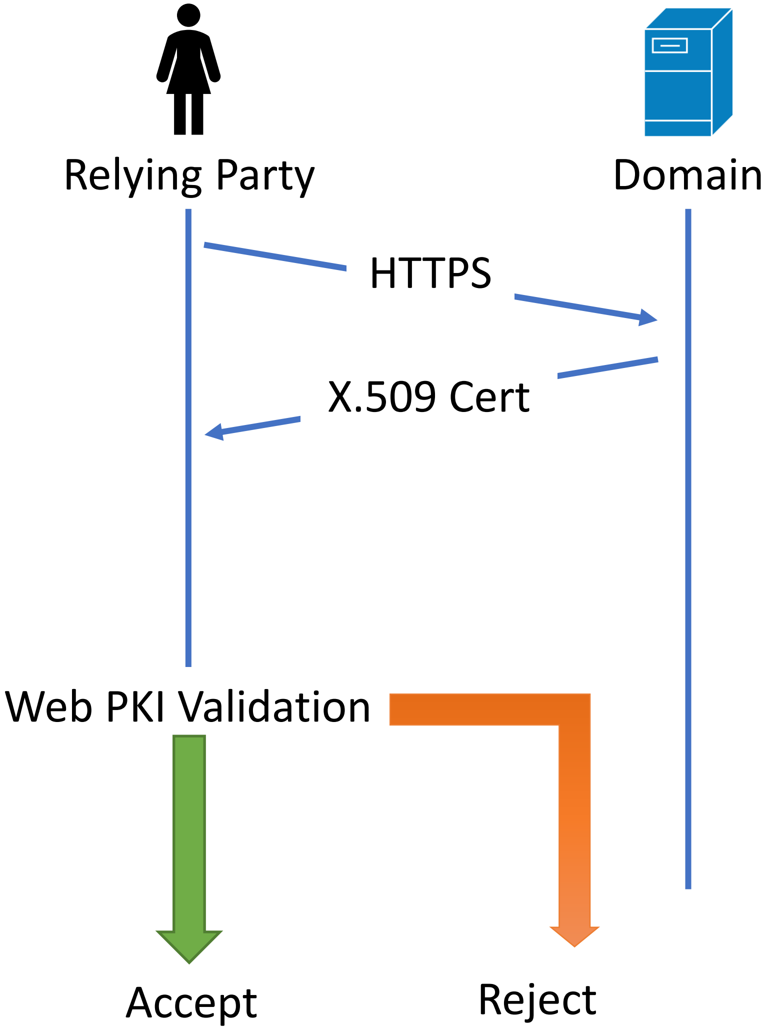
Domain Owner Defines Conflicts

F-PKI Policies:

- Allowed Issuers
- Allowed Subdomains
- Allow Wildcards
- Maximum Lifetime
- …



Web PKI Validation



Relying Party

Domain

HTTPS

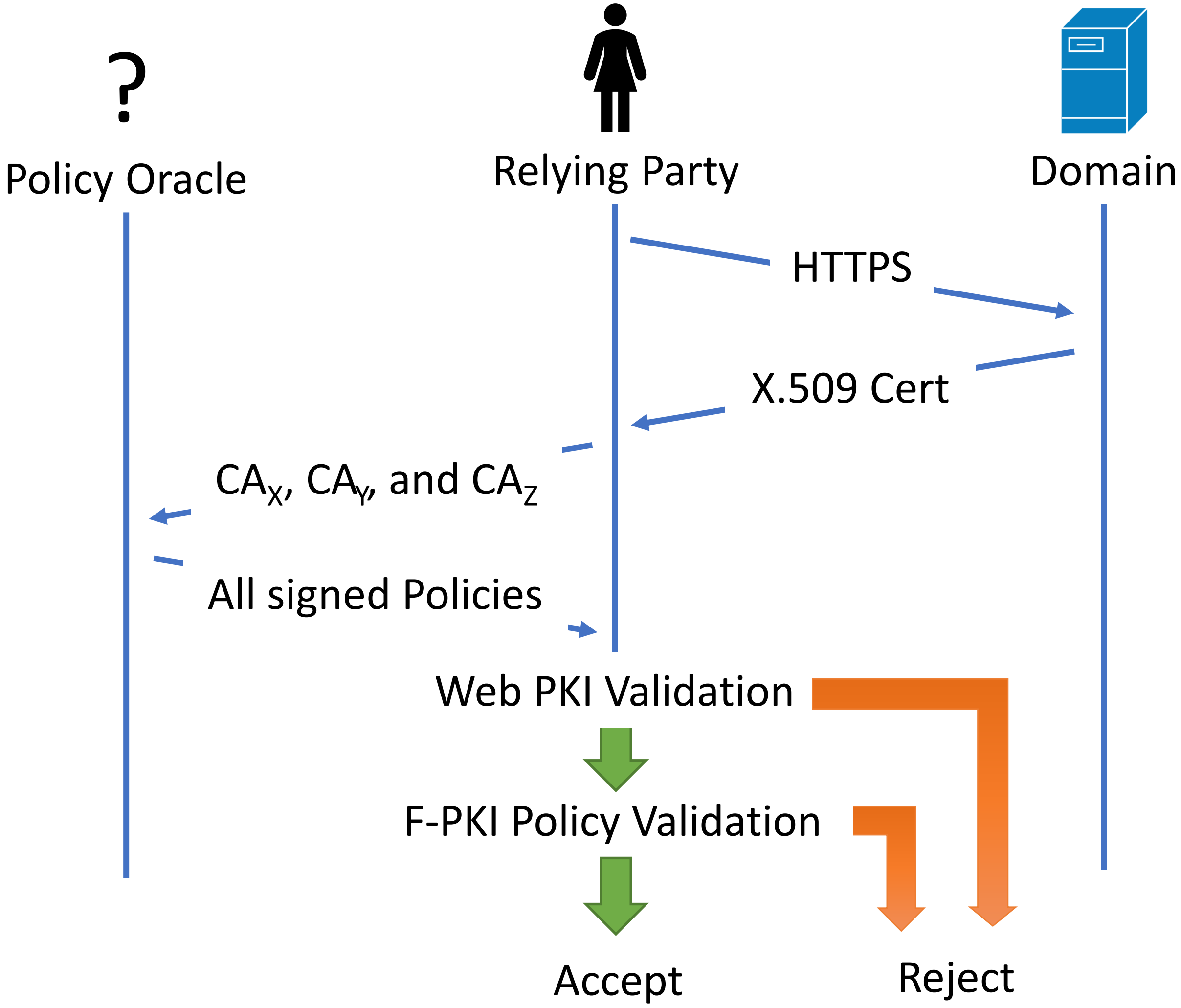
X.509 Cert

Web PKI Validation

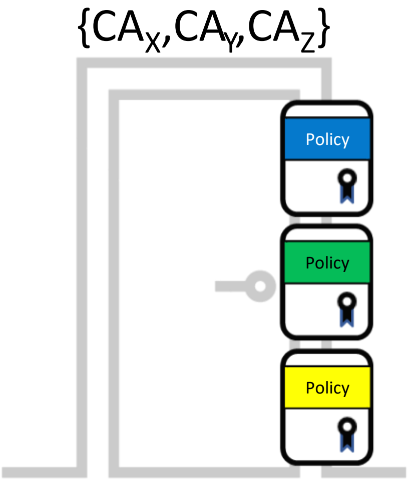
Accept

Reject

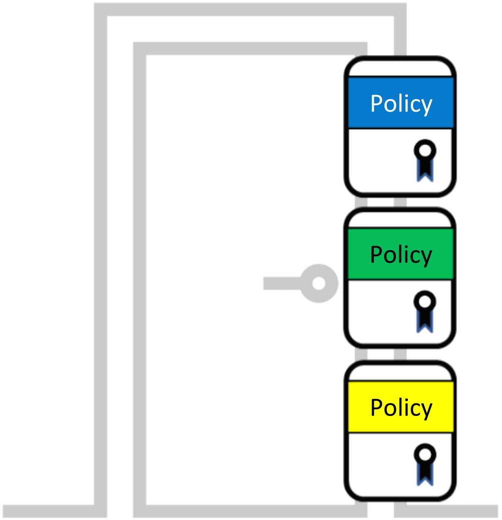
F-PKI Validation



Policies signed by the CAs CA$_X$, CA$_Y$, and CA$_Z$ are considered, i.e., these CAs are said to be "highly trusted"



Use Strongest Possible Policy



Policies:

Final Policy

- Allowed Issuers (intersection)

  $CA_1,CA_2 \cap CA_1,CA_2 \cap CA_2,CA_3 = \{CA_2\}$

- Allowed Subdomains (intersection)

  {a-z}.example.com ∩ * ∩ b.example.com = b.example.com

- Allow Wildcards (logical conjunction)

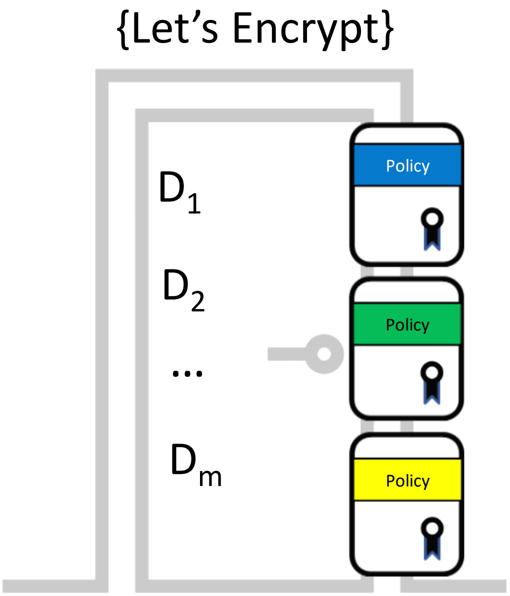
  Allow ∧ - ∧ Disallow = Disallow

- Maximum Lifetime (minimum)

  min(10 years , 1 year , 3 months) = 3 months

Enable Trust Flexibility

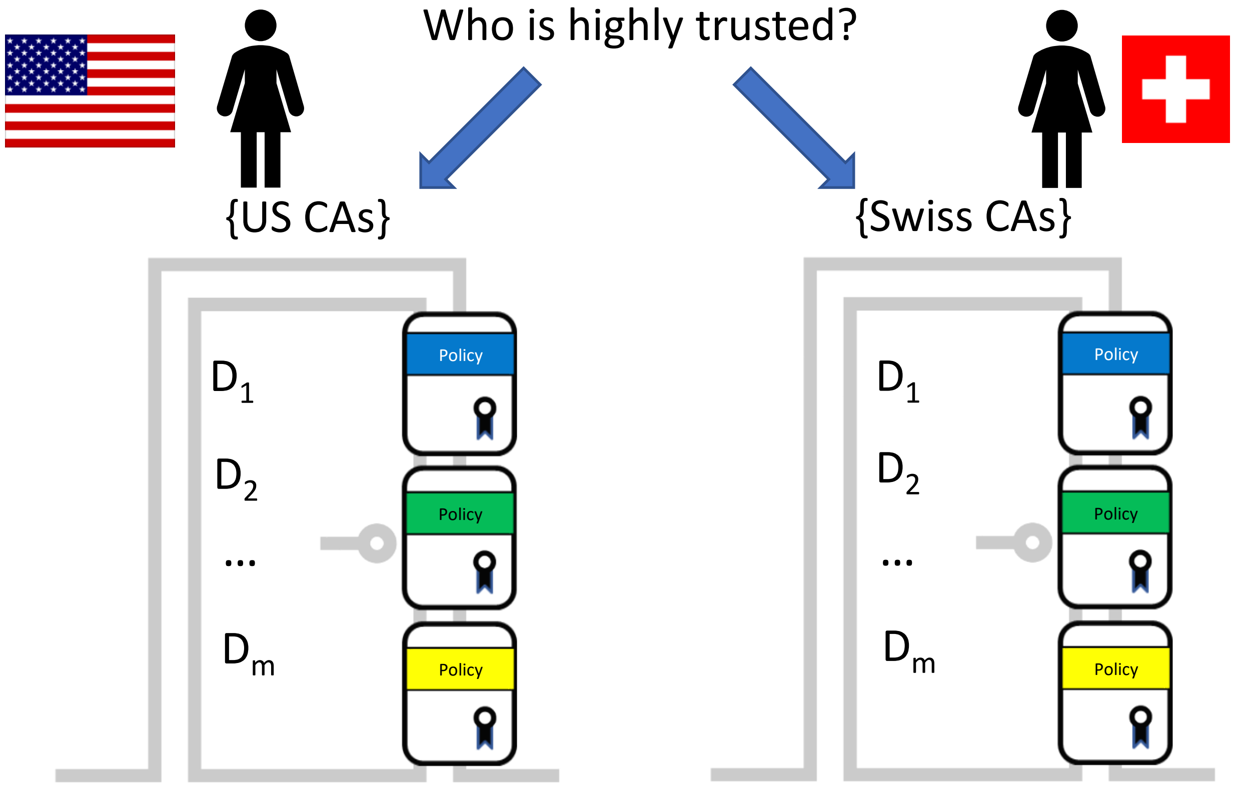
Highly trust CAs using multi-vantage point ACME 👍



User-Dependent Trust

Highly trust CAs using multi-vantage point ACME 👍

Highly trust CAs located in my own country

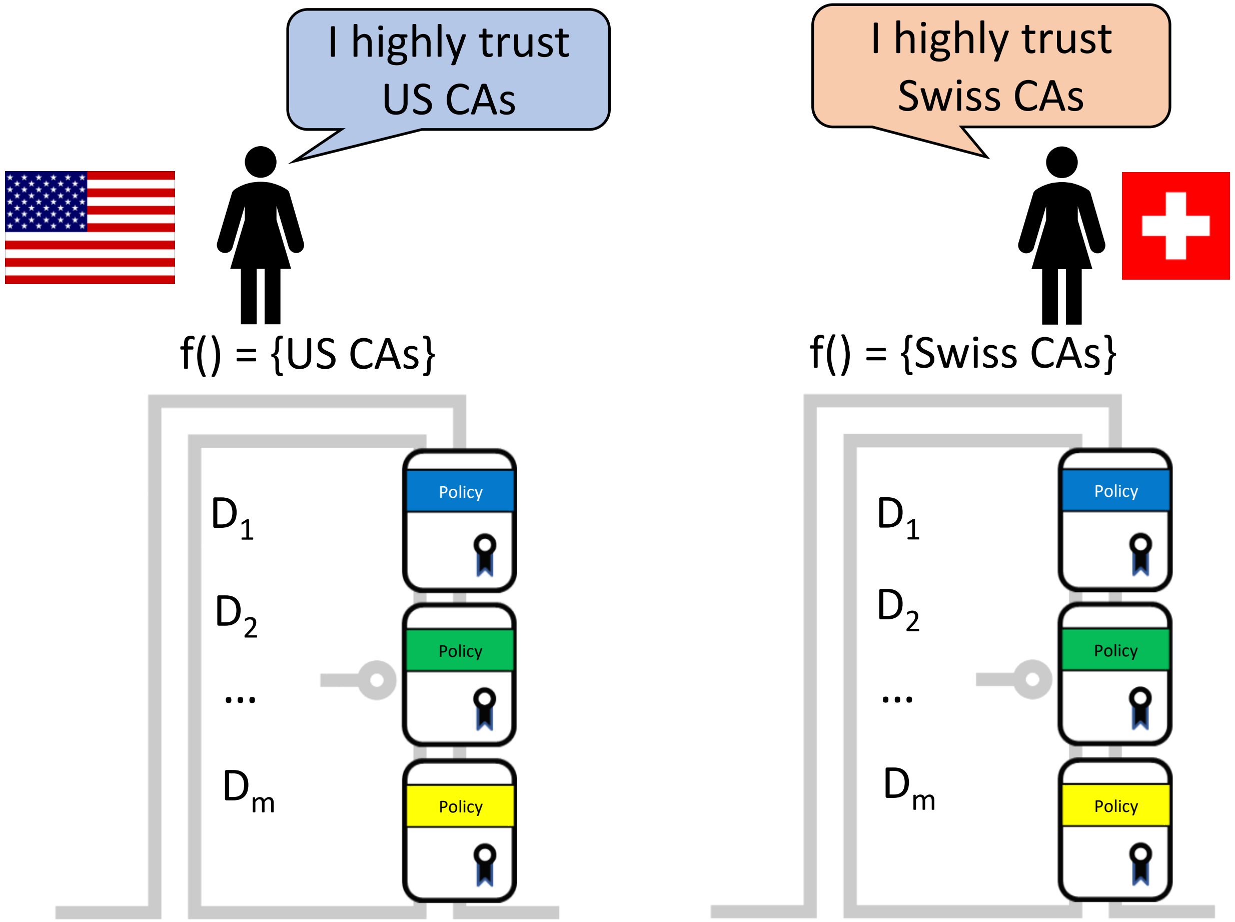


Who is highly trusted?

User-Dependent Trust

Highly trust CAs using multi-vantage point ACME 👍

Highly trust CAs located in my own country 👍



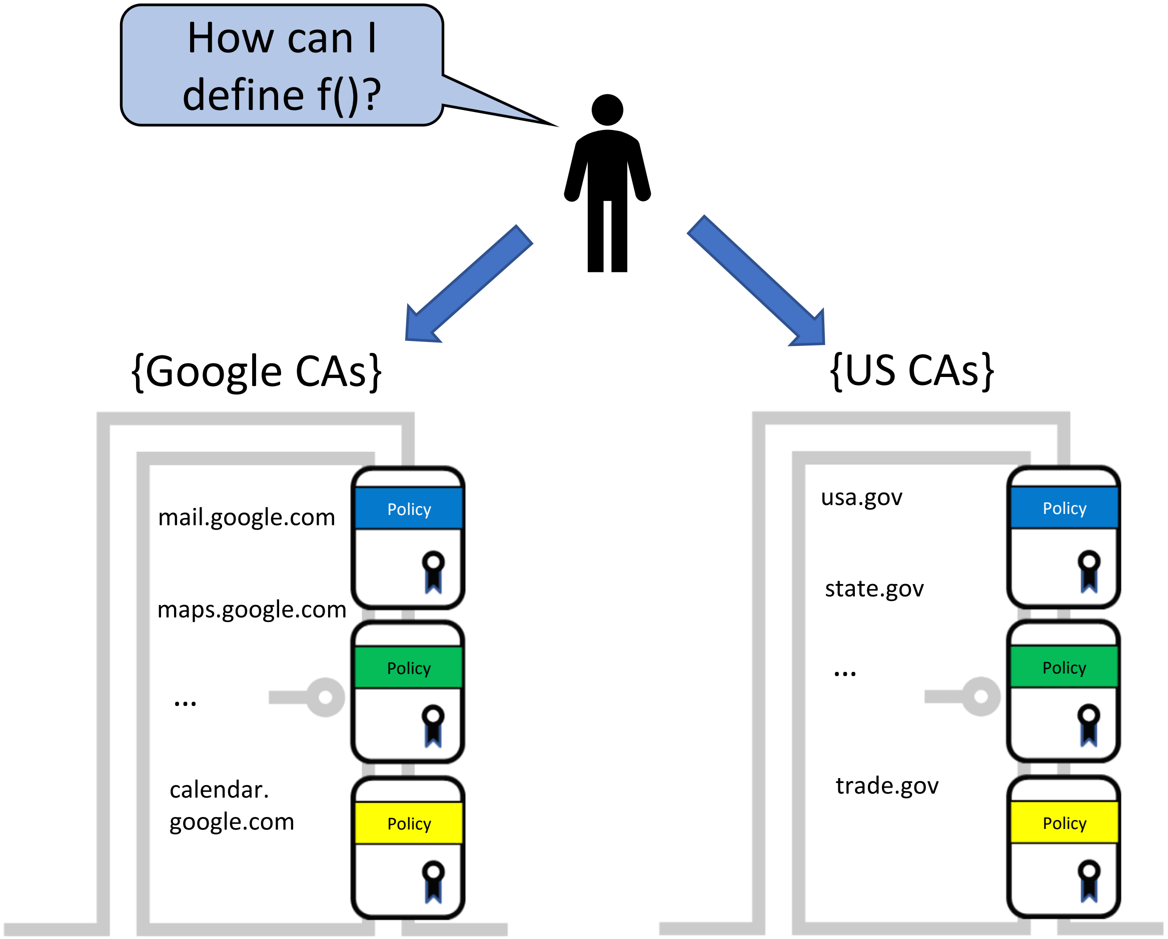
Domain-Dependent Trust

Highly trust CAs using multi-vantage point ACME 👍

Highly trust CAs located in my own country 👍

Highly trust Google CAs for google.com subdomains

Highly trust US CAs for .gov Domains



How can I define f()?

{Google CAs}

mail.google.com

maps.google.com

…

calendar.
google.com

{US CAs}

usa.gov

state.gov

…

trade.gov

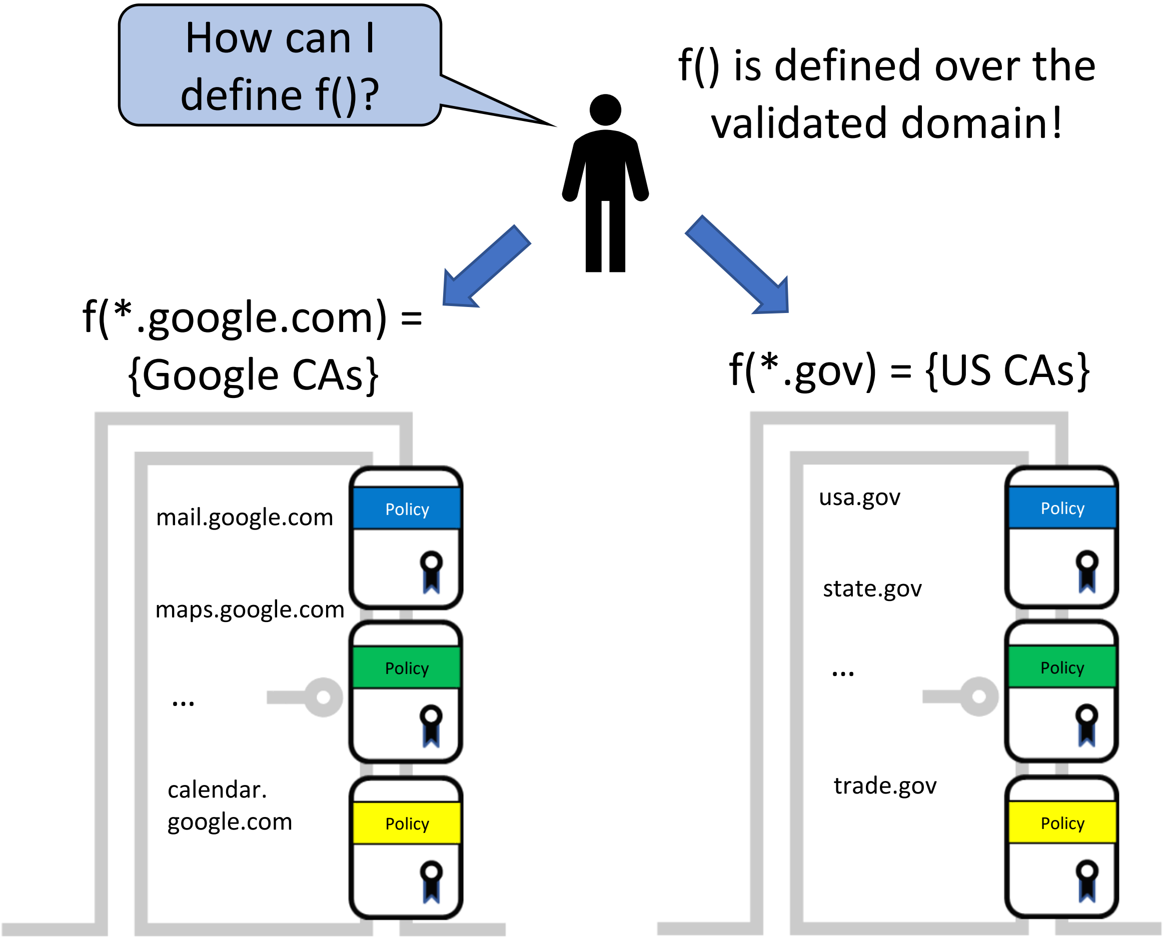
Domain-Dependent Trust

Highly trust CAs using multi-vantage point ACME 👍

Highly trust CAs located in my own country 👍

Highly trust Google CAs for google.com subdomains 👍

Highly trust US CAs for .gov Domains 👍



How can I define f()?

f() is defined over the validated domain!

f(*.google.com) = {Google CAs}

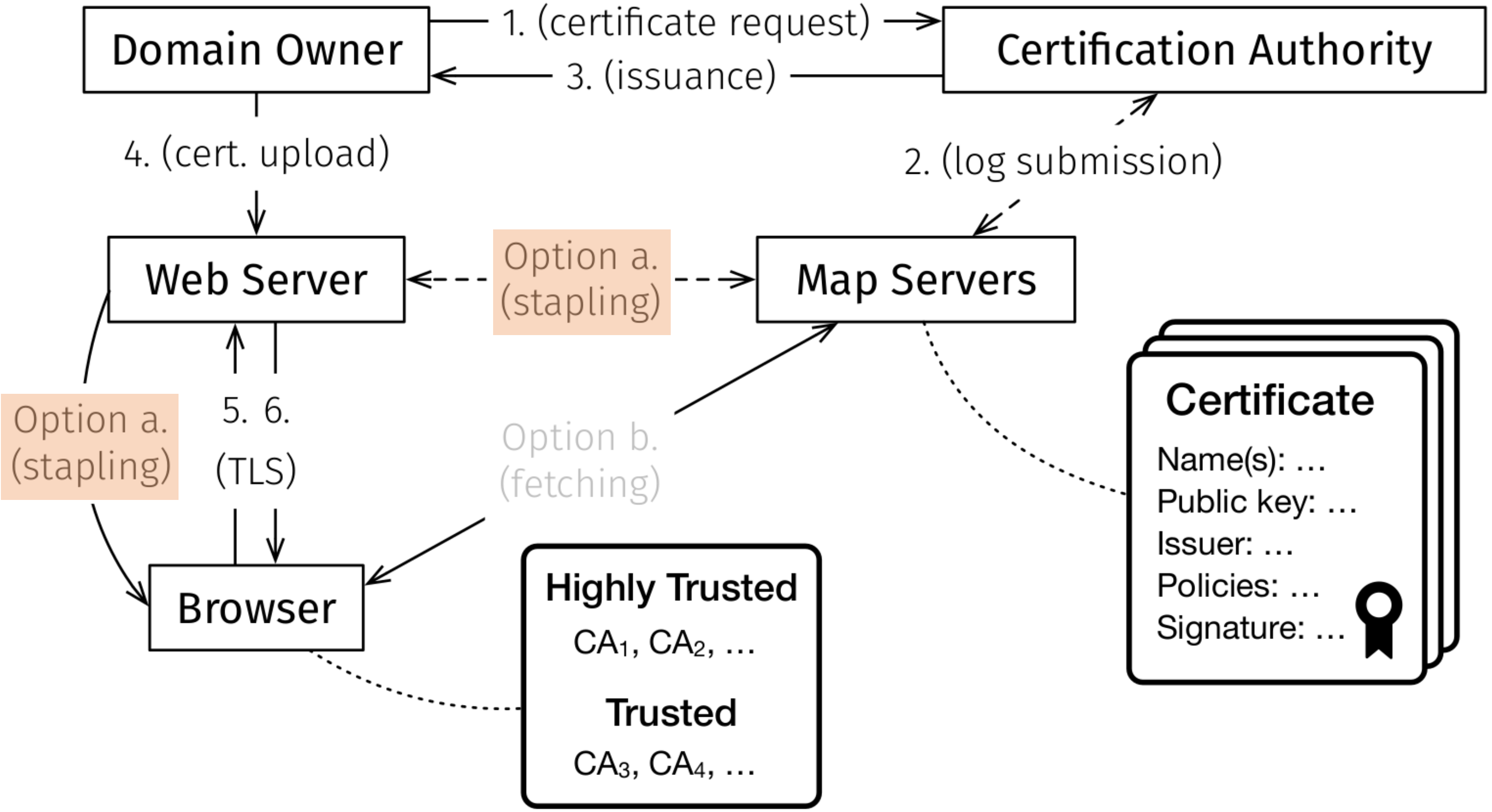
f(*.gov) = {US CAs}

What is our Policy Oracle?

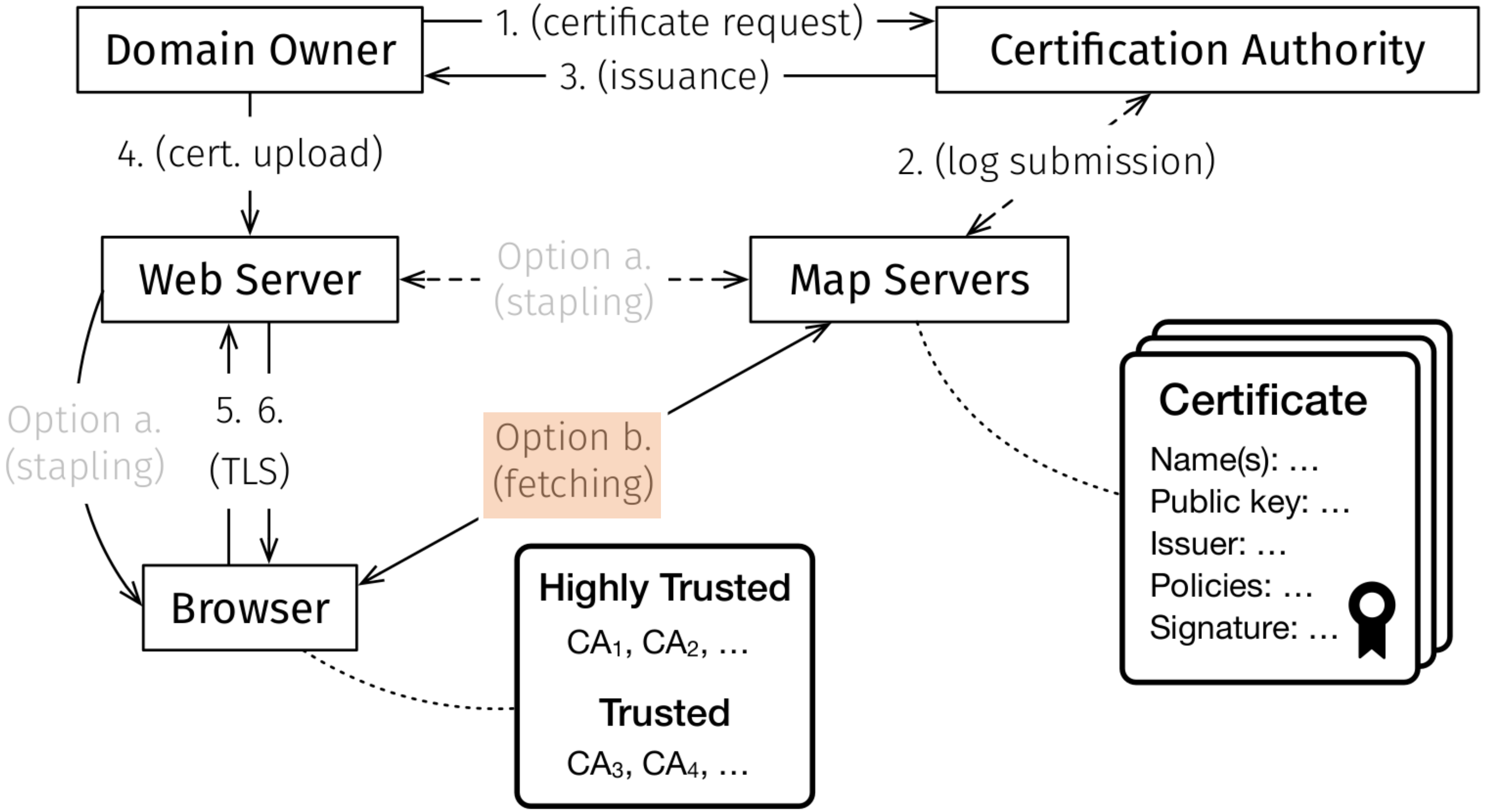
Map Servers!

- Fetches certificates from CT log servers
- Provides mapping from domain to all existing certificates
- Uses a sparse MHT to store certificates and verify correct operation
- Provides cryptographic proof of the (non-)existence of a certain domain to certificate set mapping

Certificate and Proof Retrieval

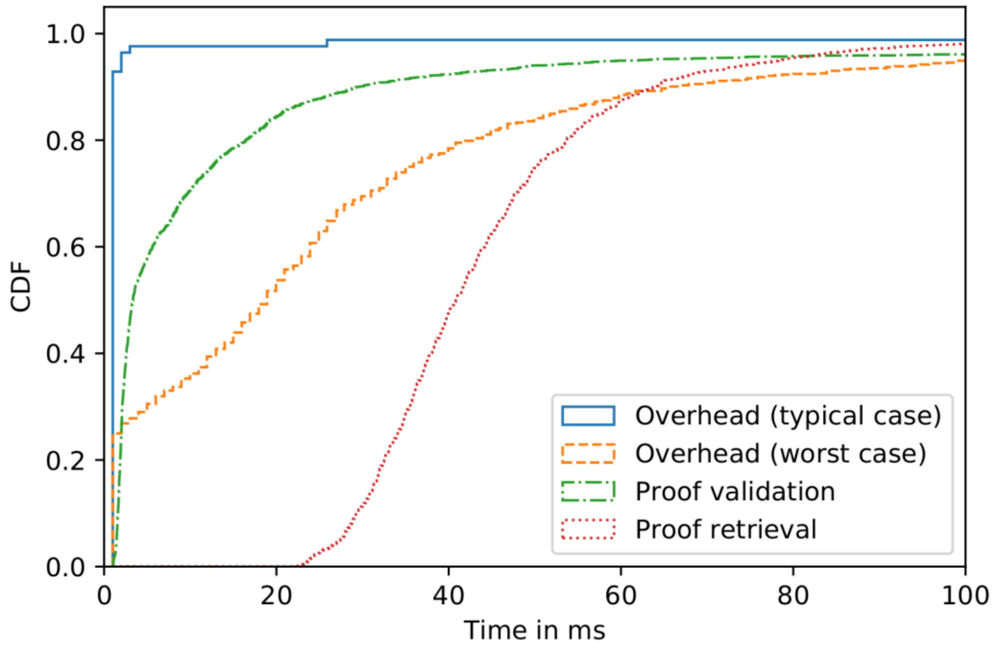


Certificate and Proof Retrieval

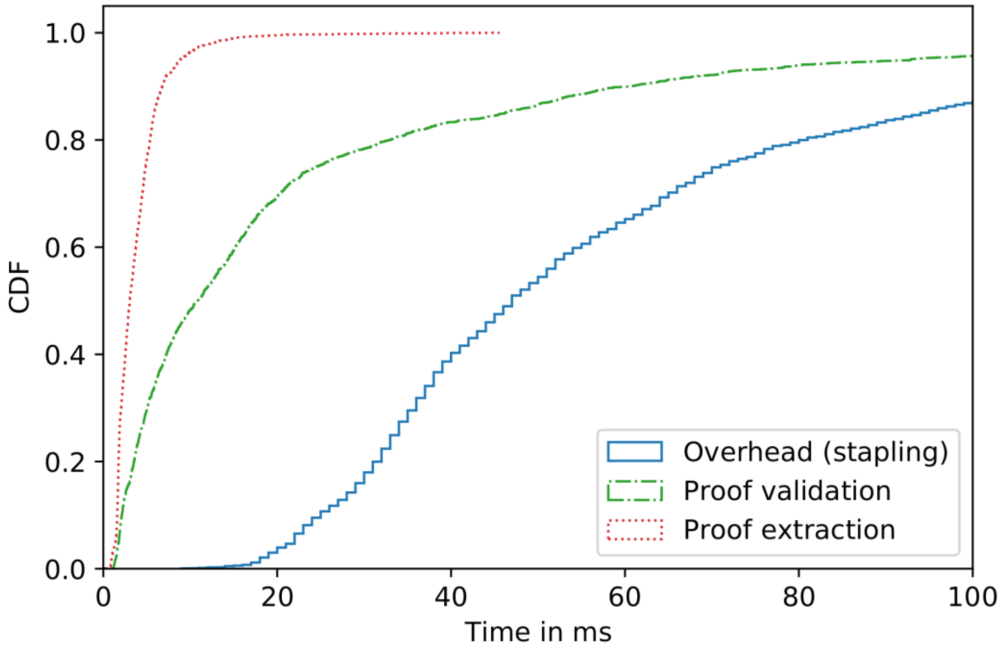


Certificate and Proof Retrieval

DNS



Stapling



Conclusion

- F-PKI enables innovation and trust flexibility in the Web PKI
- F-PKI extends CT and is incrementally deployable
- Working proof-of-concept implementation

Thank you for your attention!

Cyrill Krähenbühl
Network Security Group
ETH Zürich
cyrill.kraehenbuehl@inf.ethz.ch