Efficient PKI Design for Secure Communication and Collaboration in Space Networks

David Koisser[*], Albert Schwarzkopf[*], Ferdinand Brasser[*], Giacomo Da Broi[+]

[*]SANCTUARY Systems GmbH, [+]European Space Agency

Scalable Public Key Infrastructure for Large Constellation Secure Communications ESA Contract No. 4000143927/24/NL/RK

Structure of this Talk

- Motivation: Secure Communication at Scale
- The Role of PKI in Space Networks
- Challenges in PKI
- Our PKI Architecture
- Simulation-based Evaluation in Mega-Constellations
- Summary & Outlook

The Changing Landscape of Space Ops

Large constellations: hundreds to thousands of satellites, ground stations, relays

Diverse actors: commercial providers, new space nations, even academic missions

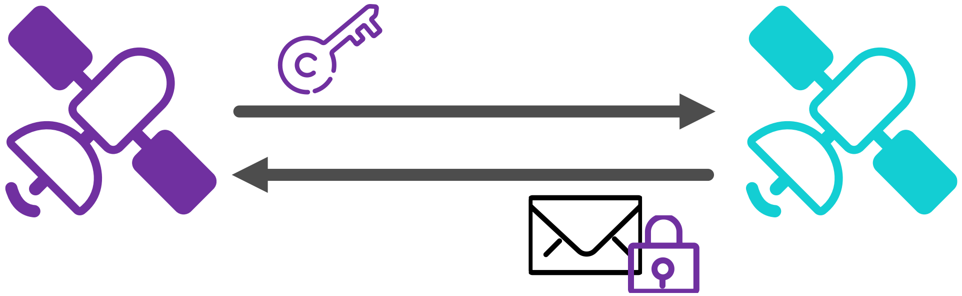
Service composability: AWS Ground Station, relay networks, Sat-as-a-Service

Mission Complexity: Complex, long-duration, multi-party missions (e.g., Artemis)

Sustainable Trust: Growing autonomy demands persistent and adaptable trust

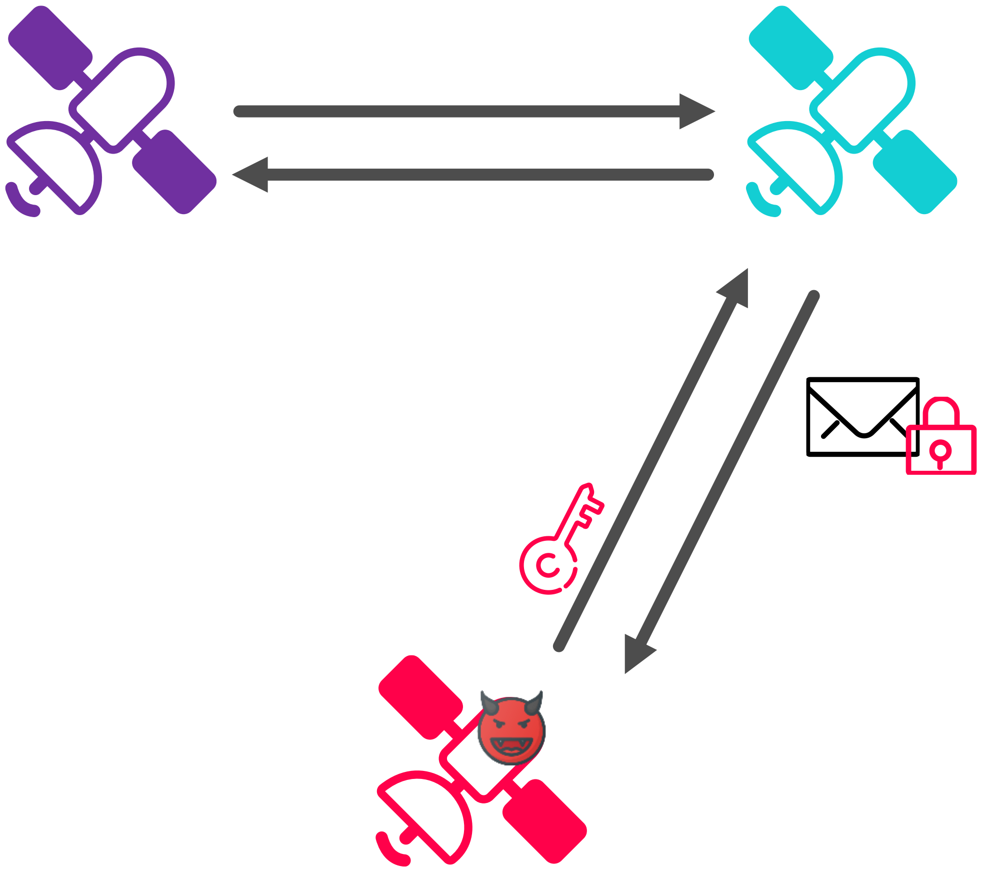
Scalable Secure Communication

- Asymmetric cryptography enables secure communication without pre-shared keys
  - Public keys can be shared openly over untrusted channels
- However, security relies on using the correct public key
  - Ensuring authenticity and integrity of public keys is essential
- Public Key Infrastructure (PKI) provides an internet-proven trust framework
  - Trusted authorities (CAs) endorse public keys via digital certificates



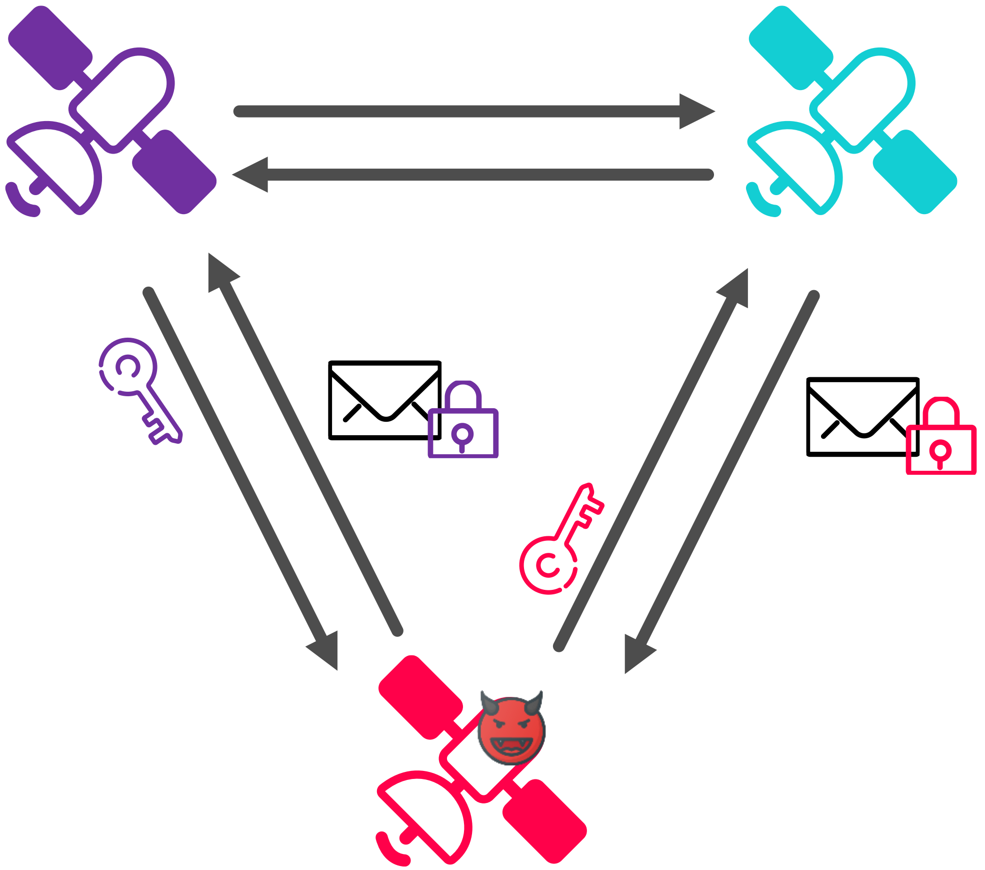
Scalable Secure Communication

- Asymmetric cryptography enables secure communication without pre-shared keys
  - Public keys can be shared openly over untrusted channels
- However, security relies on using the correct public key
  - Ensuring authenticity and integrity of public keys is essential
- Public Key Infrastructure (PKI) provides an internet-proven trust framework
  - Trusted authorities (CAs) endorse public keys via digital certificates



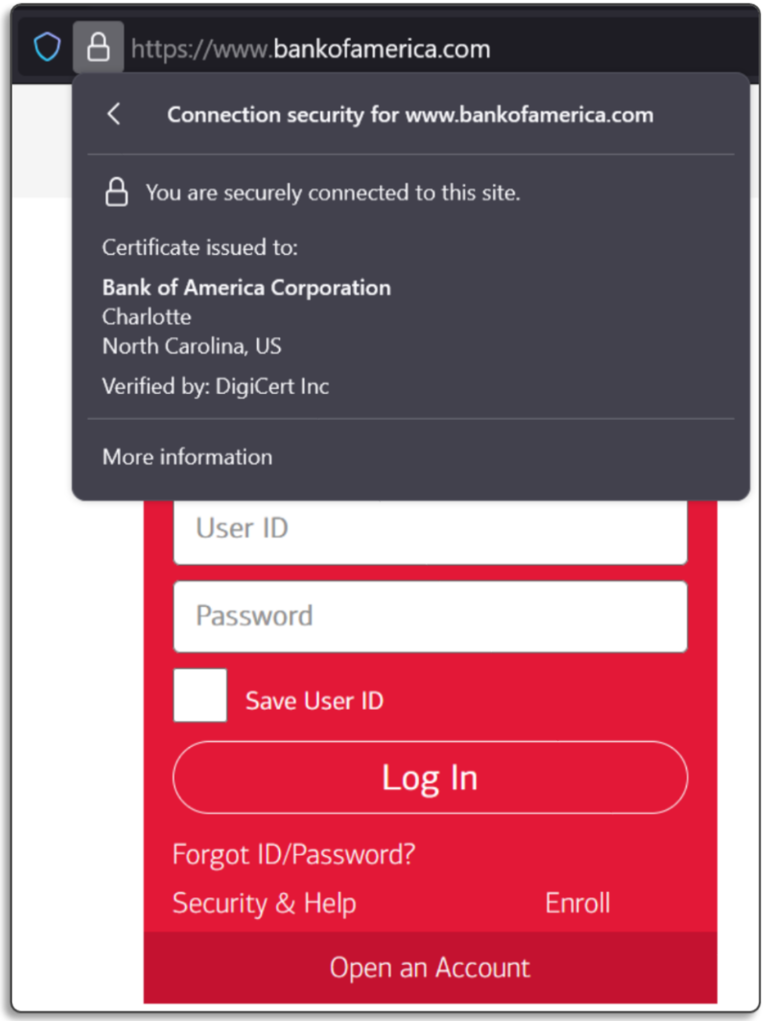
Scalable Secure Communication

- Asymmetric cryptography enables secure communication without pre-shared keys
  - Public keys can be shared openly over untrusted channels
- However, security relies on using the correct public key
  - Ensuring authenticity and integrity of public keys is essential
- Public Key Infrastructure (PKI) provides an internet-proven trust framework
  - Trusted authorities (CAs) endorse public keys via digital certificates



Scalable Secure Communication

- Asymmetric cryptography enables secure communication without pre-shared keys
  - Public keys can be shared openly over untrusted channels
- However, security relies on using the correct public key
  - Ensuring authenticity and integrity of public keys is essential
- Public Key Infrastructure (PKI) provides an internet-proven trust framework
  - Trusted authorities (CAs) endorse public keys via digital certificates



https://www.bankofamerica.com

Connection security for www.bankofamerica.com

You are securely connected to this site.

Certificate issued to:

Bank of America Corporation
Charlotte
North Carolina, US

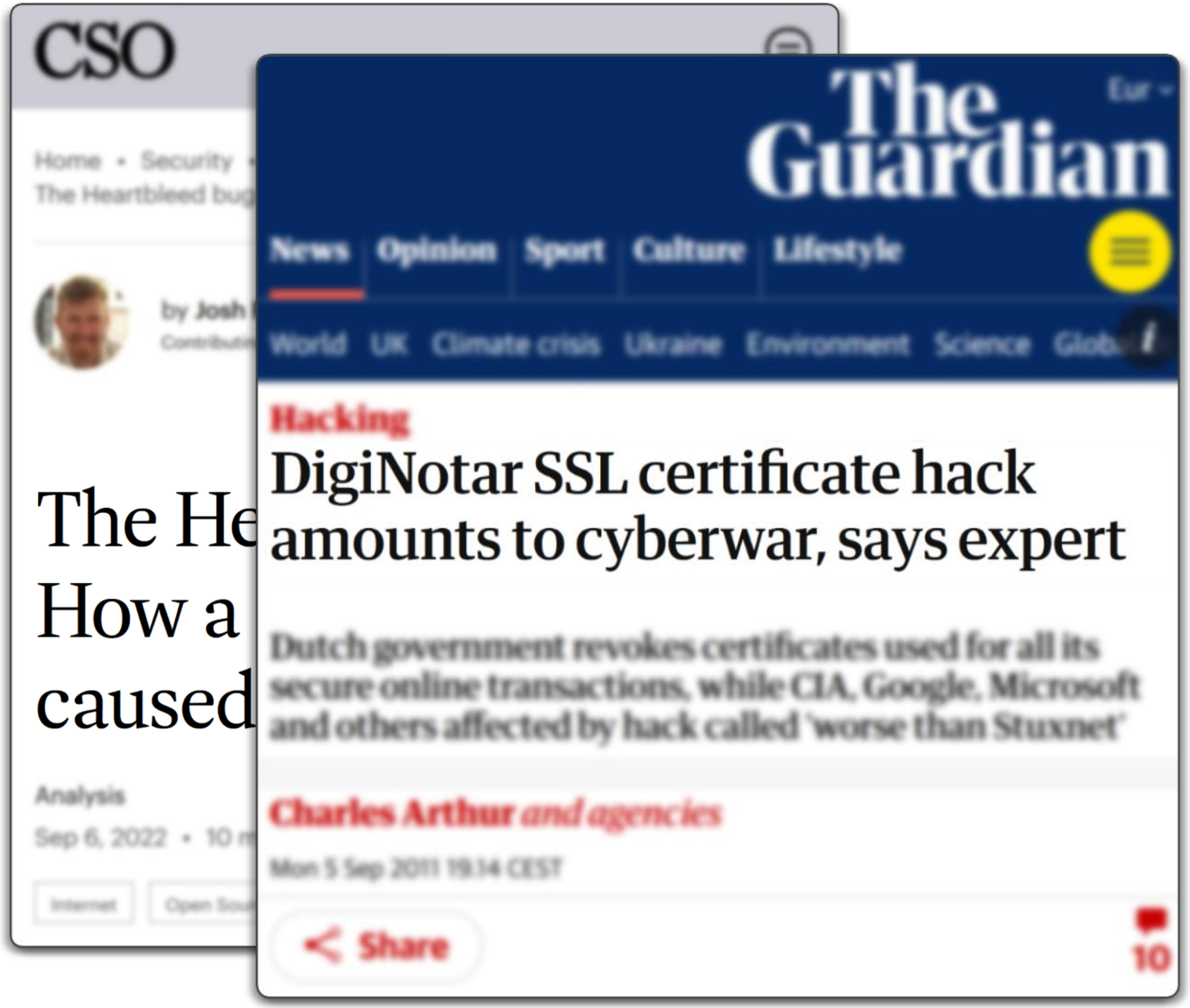
Verified by: DigiCert Inc

More information

1st Challenge: Loss of Trust

- Keys and certificates can become untrustworthy
  - Private key compromise (e.g., Heartbleed)
  - Certificate misuse or mis-issuance (e.g., DigiNotar)
  - Organizational or policy changes

- Revocation prevents ongoing misuse of untrustworthy identities
- Terrestrial PKI performs revocation checks on-demand or distribute large list at a high frequency



CSO

Home • Security •
The Heartbleed bug

by Josh
Contributor

The He
How a
caused

Analysis
Sep 6, 2022 • 10 m

Internet Open Sou

The Guardian

Eur

News Opinion Sport Culture Lifestyle

World UK Climate crisis Ukraine Environment Science Glob

Hacking

DigiNotar SSL certificate hack amounts to cyberwar, says expert

Dutch government revokes certificates used for all its secure online transactions, while CIA, Google, Microsoft and others affected by hack called 'worse than Stuxnet'

Charles Arthur *and agencies*

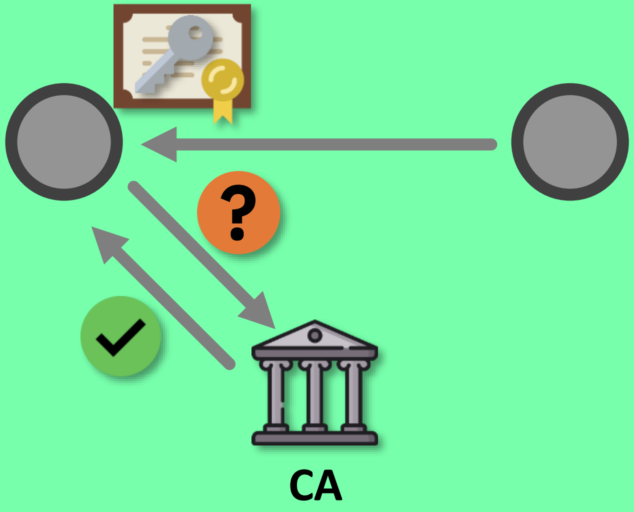
Mon 5 Sep 2011 19.14 CEST

Share

10

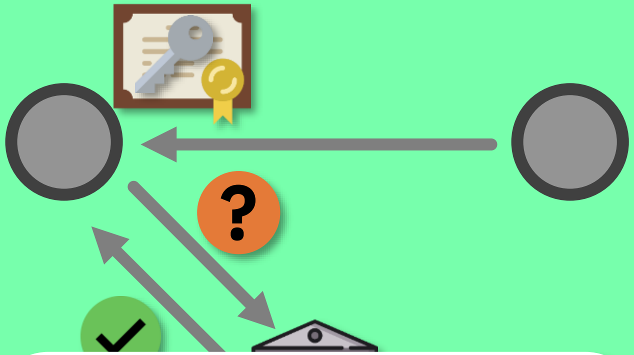
Existing Revocation Checks

Online Certificate Status Protocol
(i.e. on-demand check)



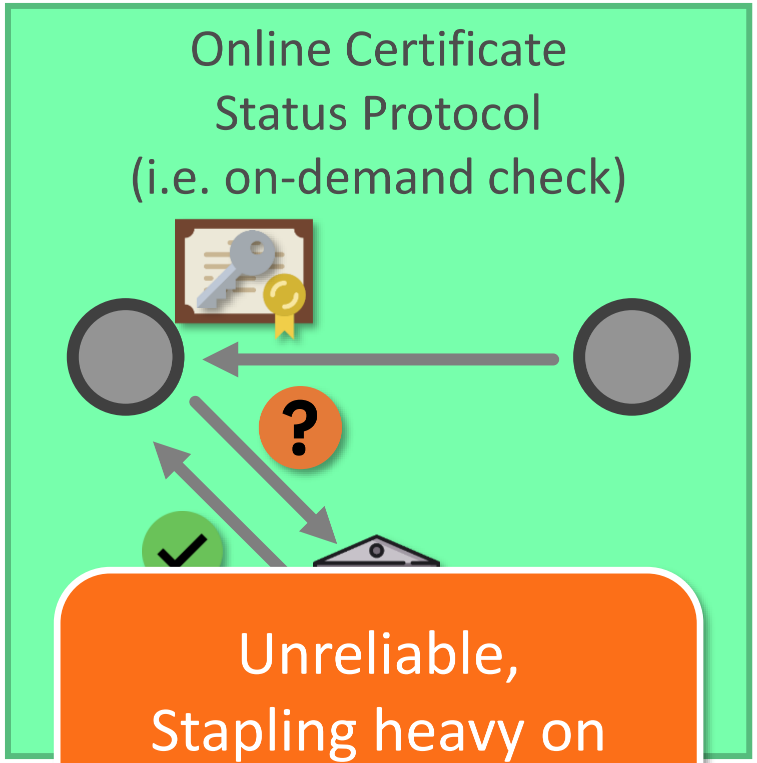
Existing Revocation Checks

Online Certificate Status Protocol (i.e. on-demand check)



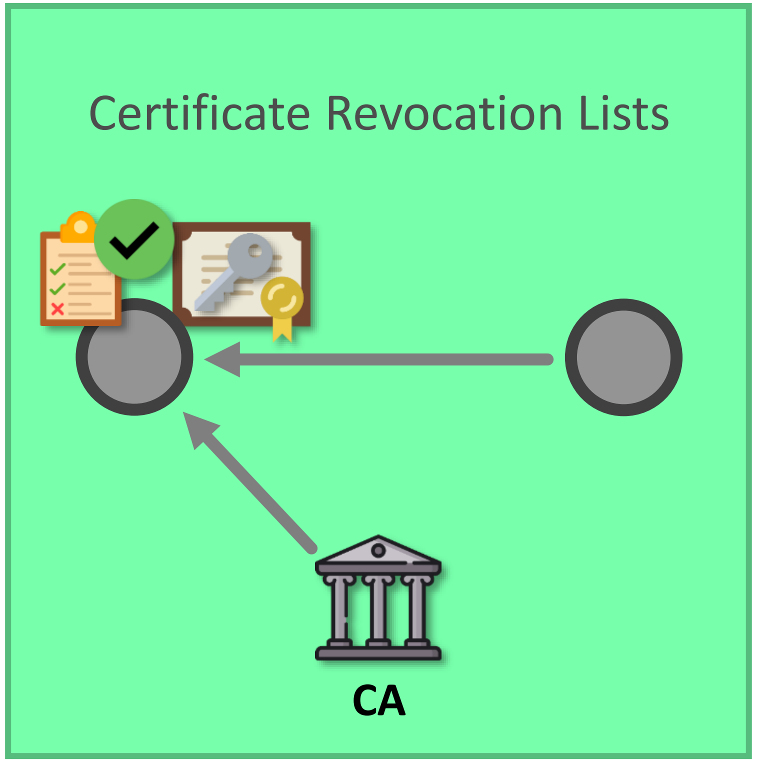
Unreliable, Stapling heavy on communication

Existing Revocation Checks



Online Certificate Status Protocol (i.e. on-demand check)

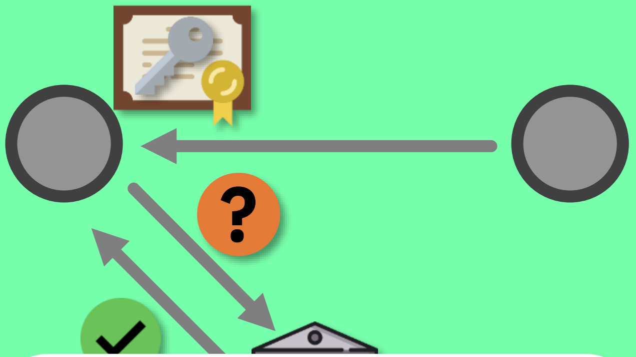
Unreliable,
Stapling heavy on
communication



Certificate Revocation Lists

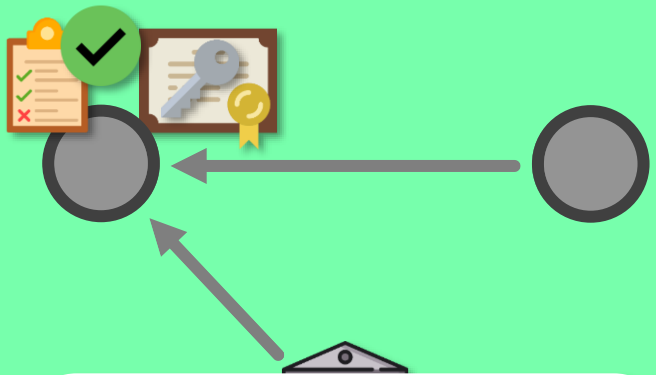
Existing Revocation Checks

Online Certificate Status Protocol (i.e. on-demand check)



Unreliable, Stapling heavy on communication

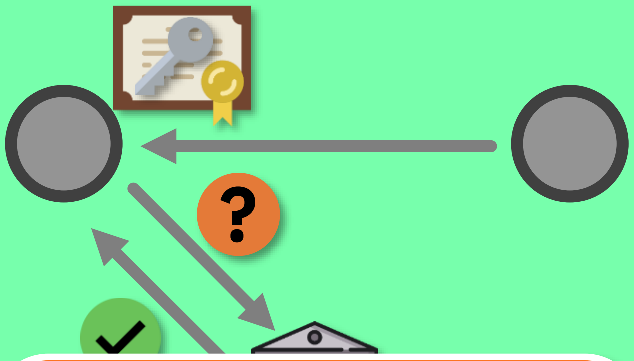
Certificate Revocation Lists



Heavy on storage and communication

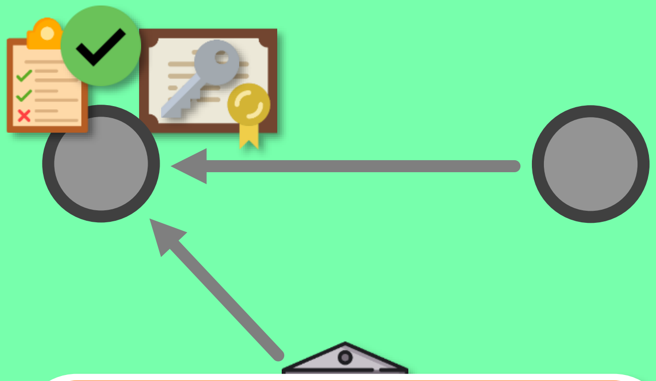
Existing Revocation Checks

Online Certificate Status Protocol (i.e. on-demand check)



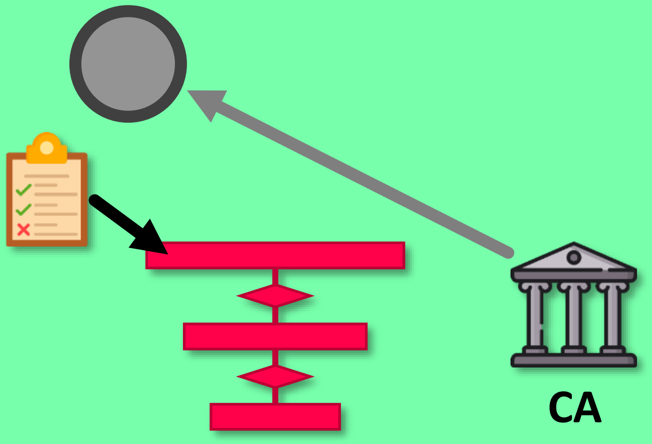
Unreliable, Stapling heavy on communication

Certificate Revocation Lists



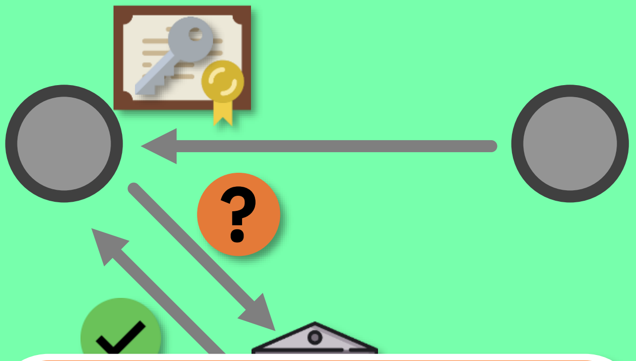
Heavy on storage and communication

Modern alternatives to Lists (e.g. CRLite, Let's Revoke)



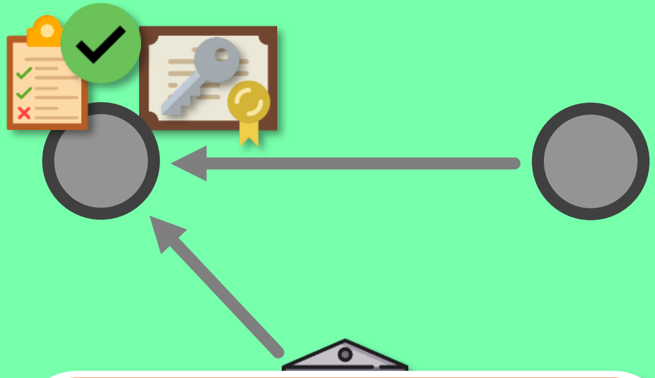
Existing Revocation Checks

Online Certificate
Status Protocol
(i.e. on-demand check)



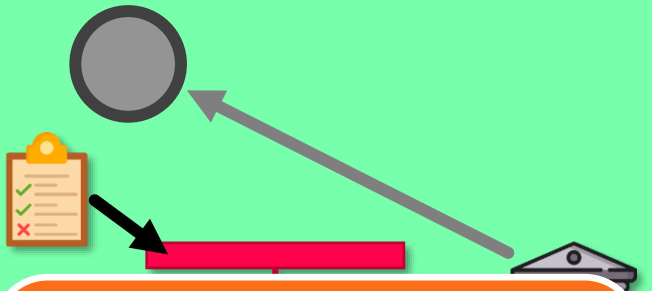
Unreliable,
Stapling heavy on
communication

Certificate Revocation Lists



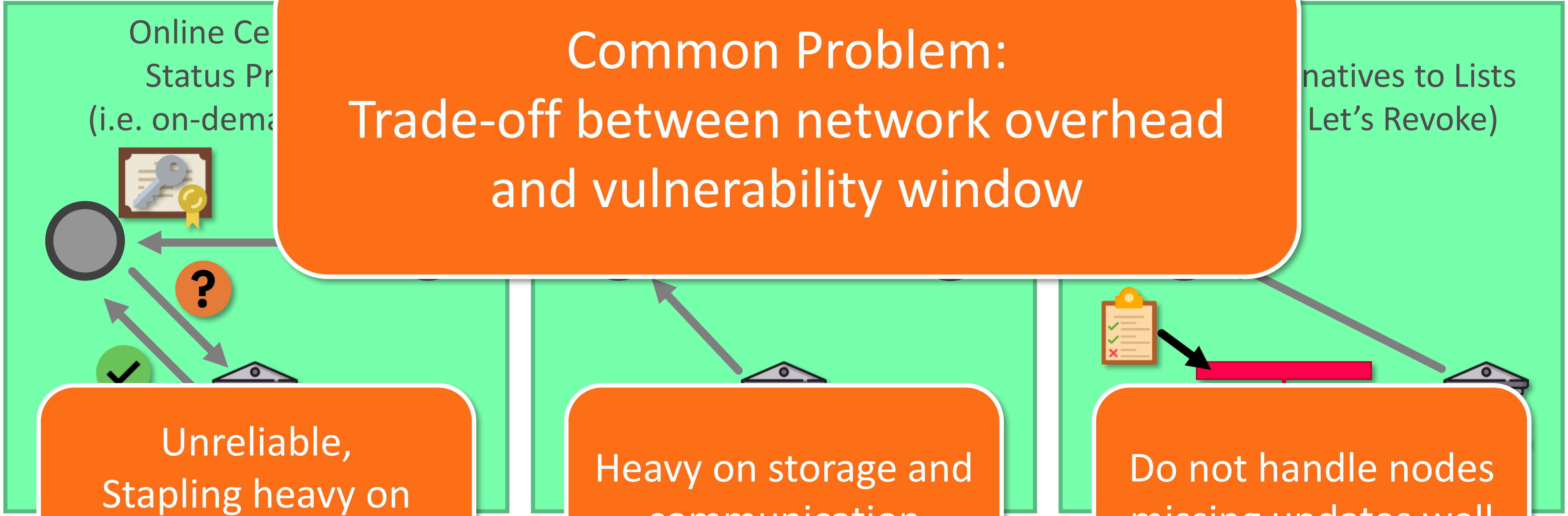
Heavy on storage and
communication

Modern alternatives to Lists
(e.g. CRLite, Let's Revoke)



Do not handle nodes
missing updates well

Existing Revocation Checks



Common Problem:
Trade-off between network overhead and vulnerability window

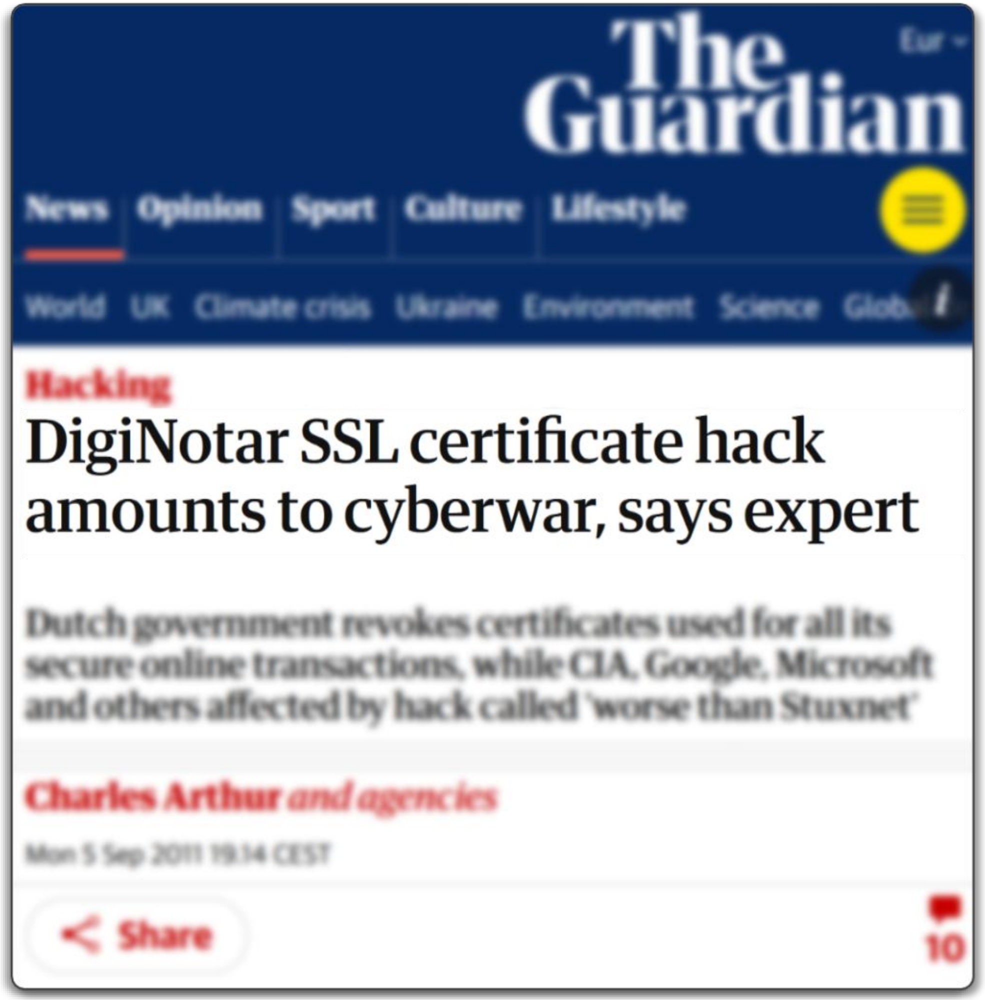
Unreliable,
Stapling heavy on communication

Heavy on storage and communication

Do not handle nodes missing updates well

2nd Challenge: Multi-Domain Trust

- PKI must work across independent, possibly conflicting authorities
- Past incidents show how one domain can compromise global trust
  - Revocation fails for compromised root CAs (e.g., DigiNotar)
  - Misbehaving authorities can impact the entire PKI (e.g., Rouge google.com certificates)
- Internet uses Certificate Transparency (CT): requires central logs and real-time access
  - Not suitable for space
- Bridge CAs and cross-signing do not solve the problem; they just shift the trust assumption



Hacking

DigiNotar SSL certificate hack amounts to cyberwar, says expert

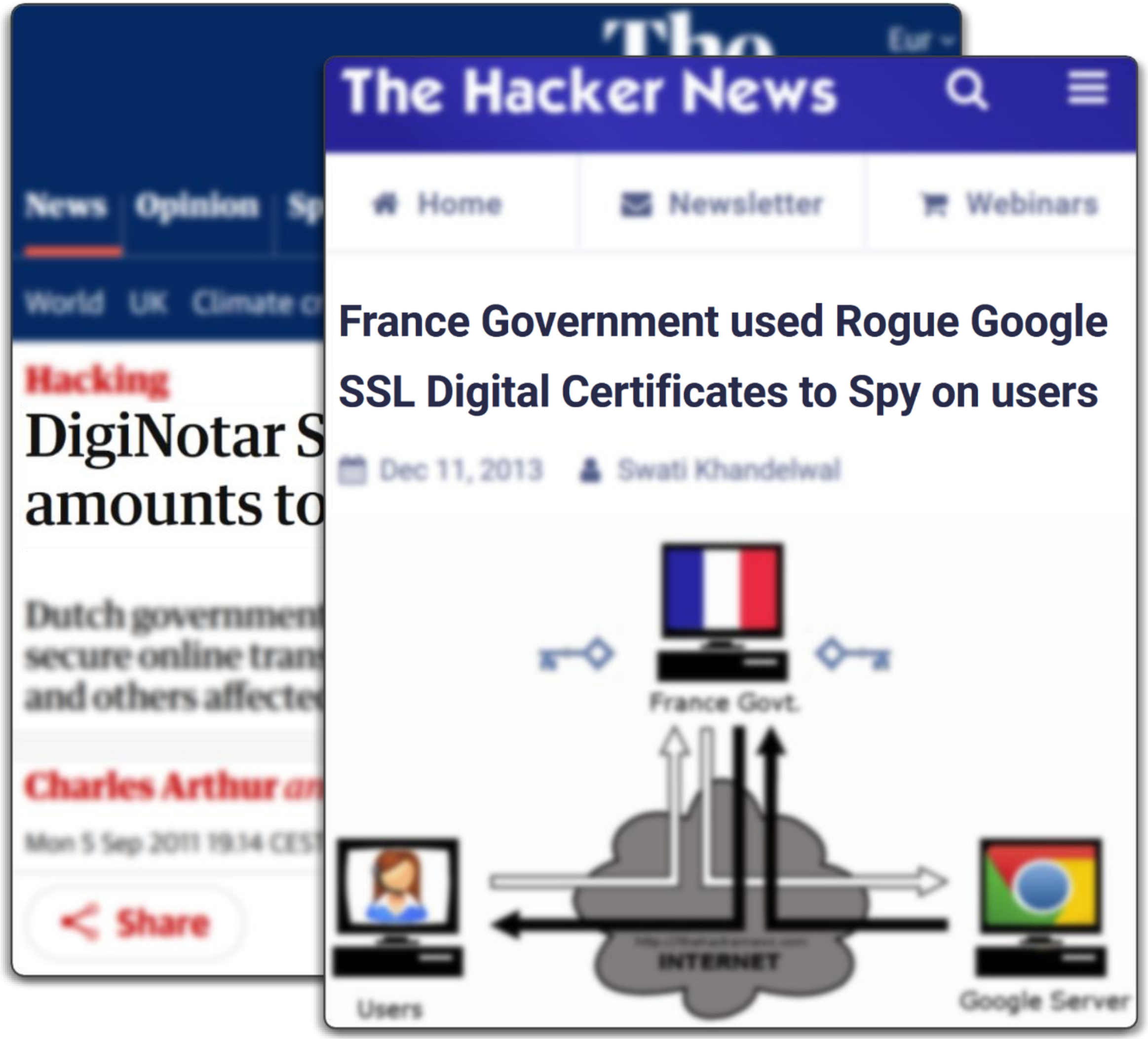
Dutch government revokes certificates used for all its secure online transactions, while CIA, Google, Microsoft and others affected by hack called 'worse than Stuxnet'

Charles Arthur *and agencies*

Mon 5 Sep 2011 19.14 CEST

2nd Challenge: Multi-Domain Trust

- PKI must work across independent, possibly conflicting authorities
- Past incidents show how one domain can compromise global trust
  - Revocation fails for compromised root CAs (e.g., DigiNotar)
  - Misbehaving authorities can impact the entire PKI (e.g., Rouge google.com certificates)
- Internet uses Certificate Transparency (CT): requires central logs and real-time access
  - Not suitable for space
- Bridge CAs and cross-signing do not solve the problem; they just shift the trust assumption



Hacking

DiginNotar S
amounts to

Dutch governmen
secure online tran
and others affecte

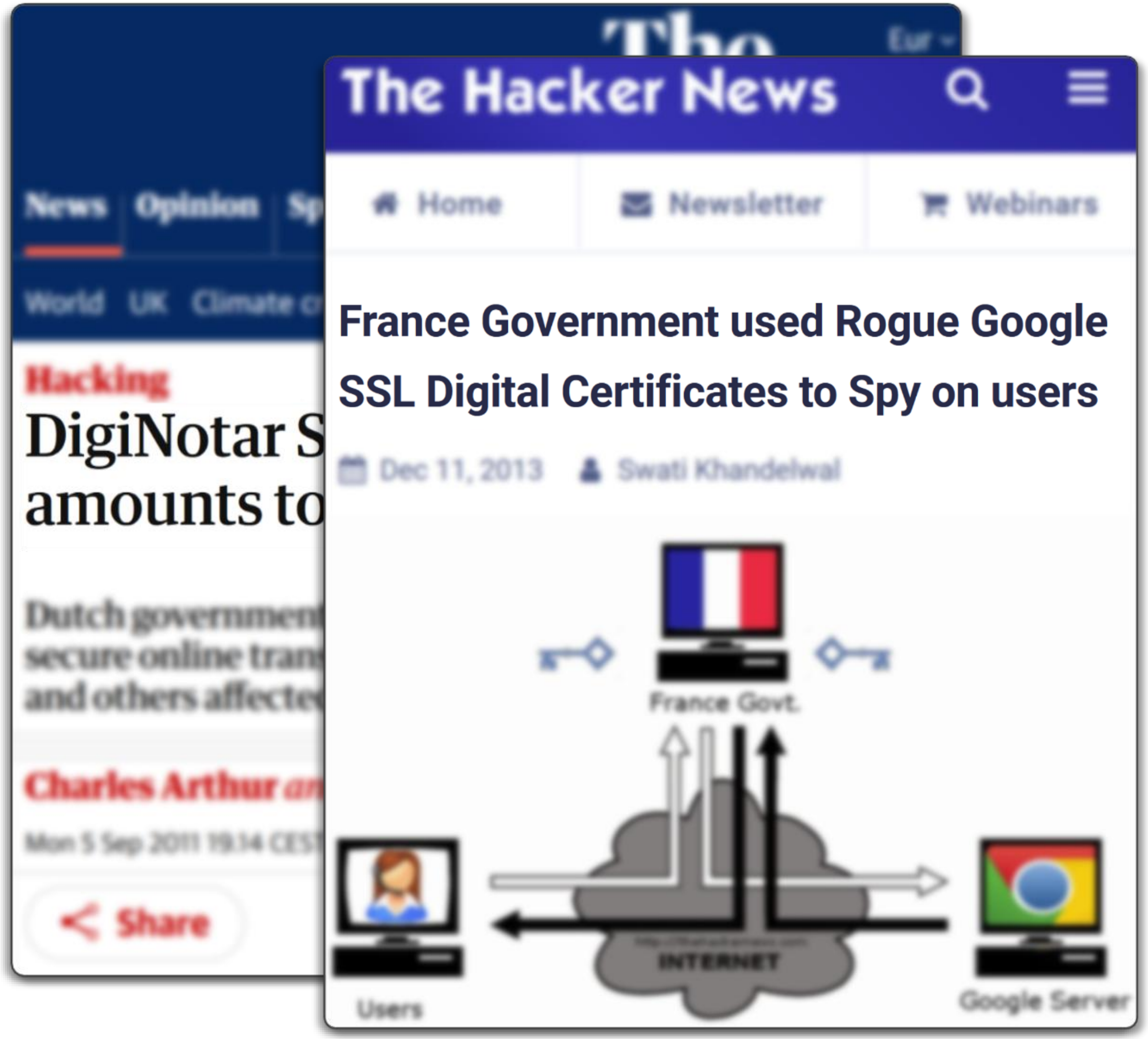
Charles Arthur an
Mon 5 Sep 2011 19.14 CEST

France Government used Rogue Google SSL Digital Certificates to Spy on users

Dec 11, 2013 Swati Khandelwal

2nd Challenge: Multi-Domain Trust

- PKI must work across independent, possibly conflicting authorities
- Past incidents show how one domain can compromise global trust
  - Revocation fails for compromised root CAs (e.g., DigiNotar)
  - Misbehaving authorities can impact the entire PKI (e.g., Rouge google.com certificates)
- Internet uses Certificate Transparency (CT): requires central logs and real-time access
  - Not suitable for space
- Bridge CAs and cross-signing do not solve the problem; they just shift the trust assumption



The

Eur

News | Opinion | Sp

World UK Climate c

Hacking

DigiNotar S
amounts to

Dutch governmen
secure online tran
and others affecte

Charles Arthur an

Mon 5 Sep 2011 19.14 CEST

Share

The Hacker News

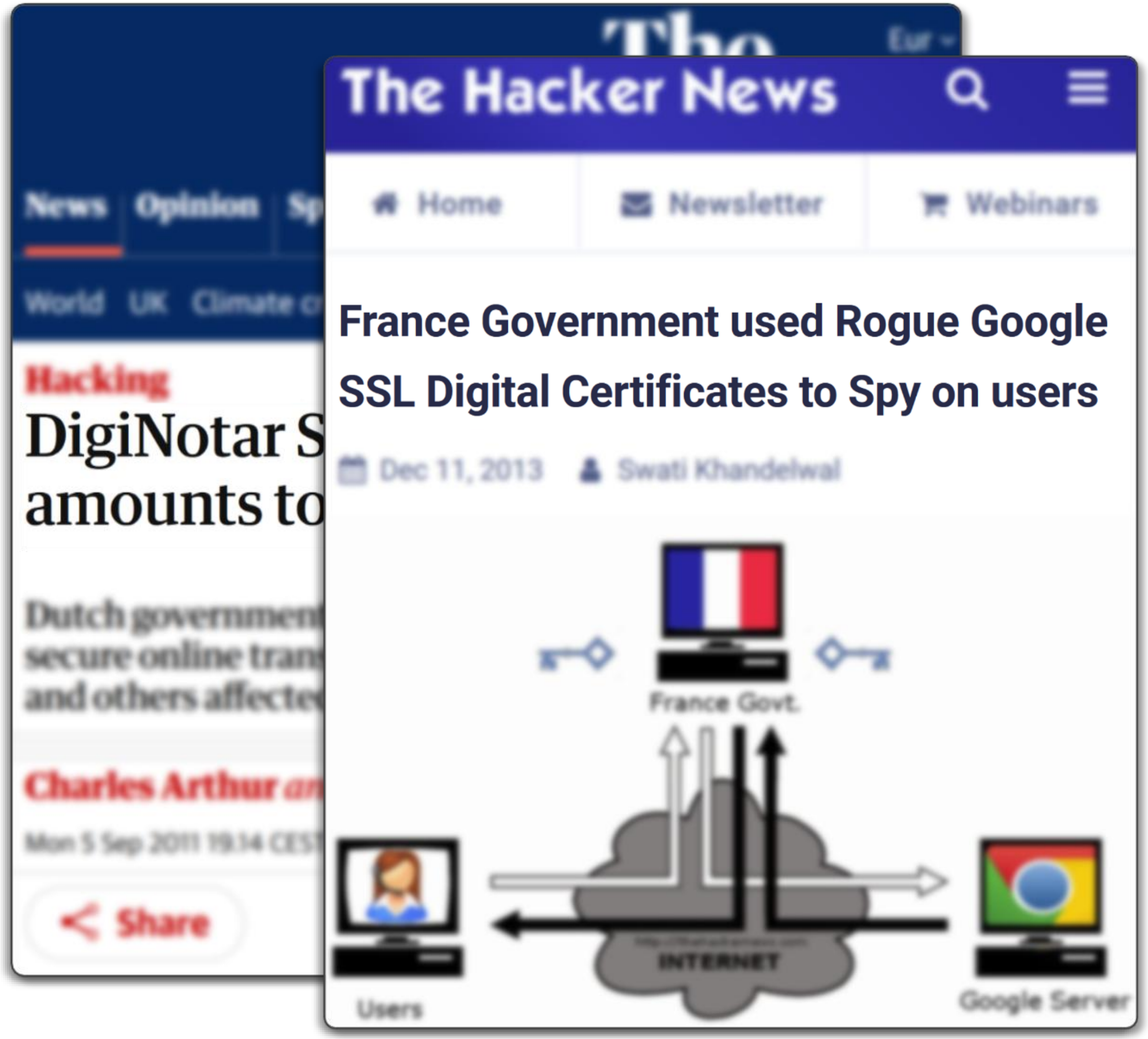
Home | Newsletter | Webinars

France Government used Rogue Google SSL Digital Certificates to Spy on users

Dec 11, 2013 Swati Khandelwal

2nd Challenge: Multi-Domain Trust

- PKI must work across independent, possibly conflicting authorities
- Past incidents show how one domain can compromise global trust
  - Revocation fails for compromised root CAs (e.g., DigiNotar)
  - Misbehaving authorities can impact the entire PKI (e.g., Rouge google.com certificates)
- Internet uses Certificate Transparency (CT): requires central logs and real-time access
  - Not suitable for space
- Bridge CAs and cross-signing do not solve the problem; they just shift the trust assumption



The

Eur

News | Opinion | Sp

World UK Climate c

Hacking

DigiNotar S
amounts to

Dutch governmen
secure online tran
and others affecte

Charles Arthur an

Mon 5 Sep 2011 19.14 CEST

Share

The Hacker News

Home | Newsletter | Webinars

France Government used Rogue Google SSL Digital Certificates to Spy on users

Dec 11, 2013 · Swati Khandelwal

Generic PKI for All Mission Profiles

Assumptions

- **Large-scale networks:**
  Thousands of nodes, global reach
- **Multi-party collaboration:**
  Heterogeneous operators and domains
- **Dynamic trust:**
  Changing partners, evolving roles
- **Extended lifetimes:**
  Spacecraft might operate for decades

Requirements

1. **Flexible trust model:**
   Cross-domain, sovereign, and evolving
2. **Fast & efficient revocation:**
   Delay-tolerant and scalable mechanisms
3. **Post-quantum readiness:**
   Long-term secure by design

sanctuary

Generic PKI for All Mission Profiles

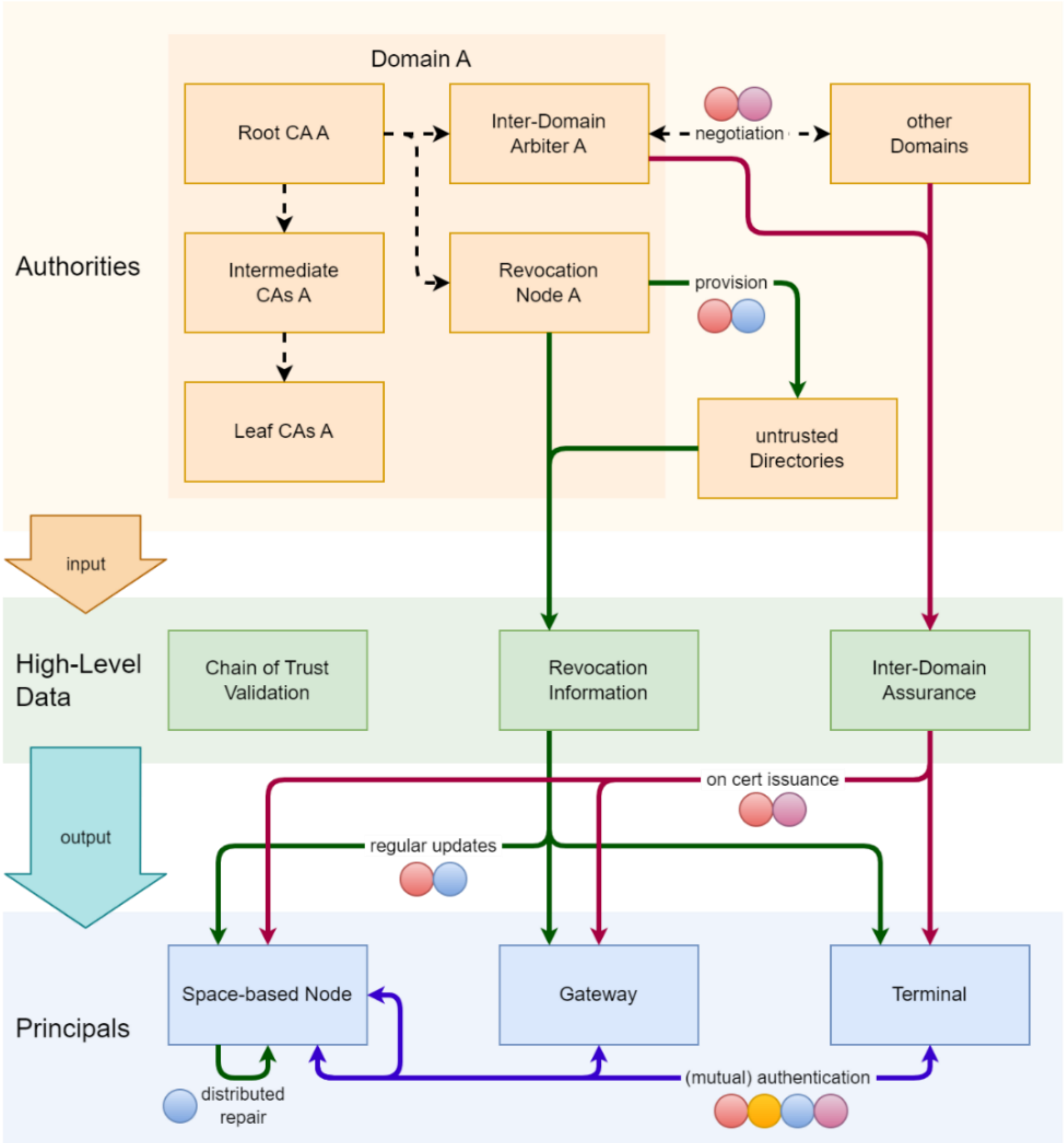
Assumptions

- **Large-scale networks:**
  Thousands of nodes, global reach
- **Multi-party collaboration:**
  Heterogeneous operators and domains
- **Dynamic trust:**
  Changing partners, evolving roles
- **Extended lifetimes:**
  Spacecraft might operate for decades

Requirements

1. **Flexible trust model:**
   Cross-domain, sovereign, and evolving
2. **Fast & efficient revocation:**
   Delay-tolerant and scalable mechanisms
3. **Post-quantum readiness:**
   Long-term secure by design

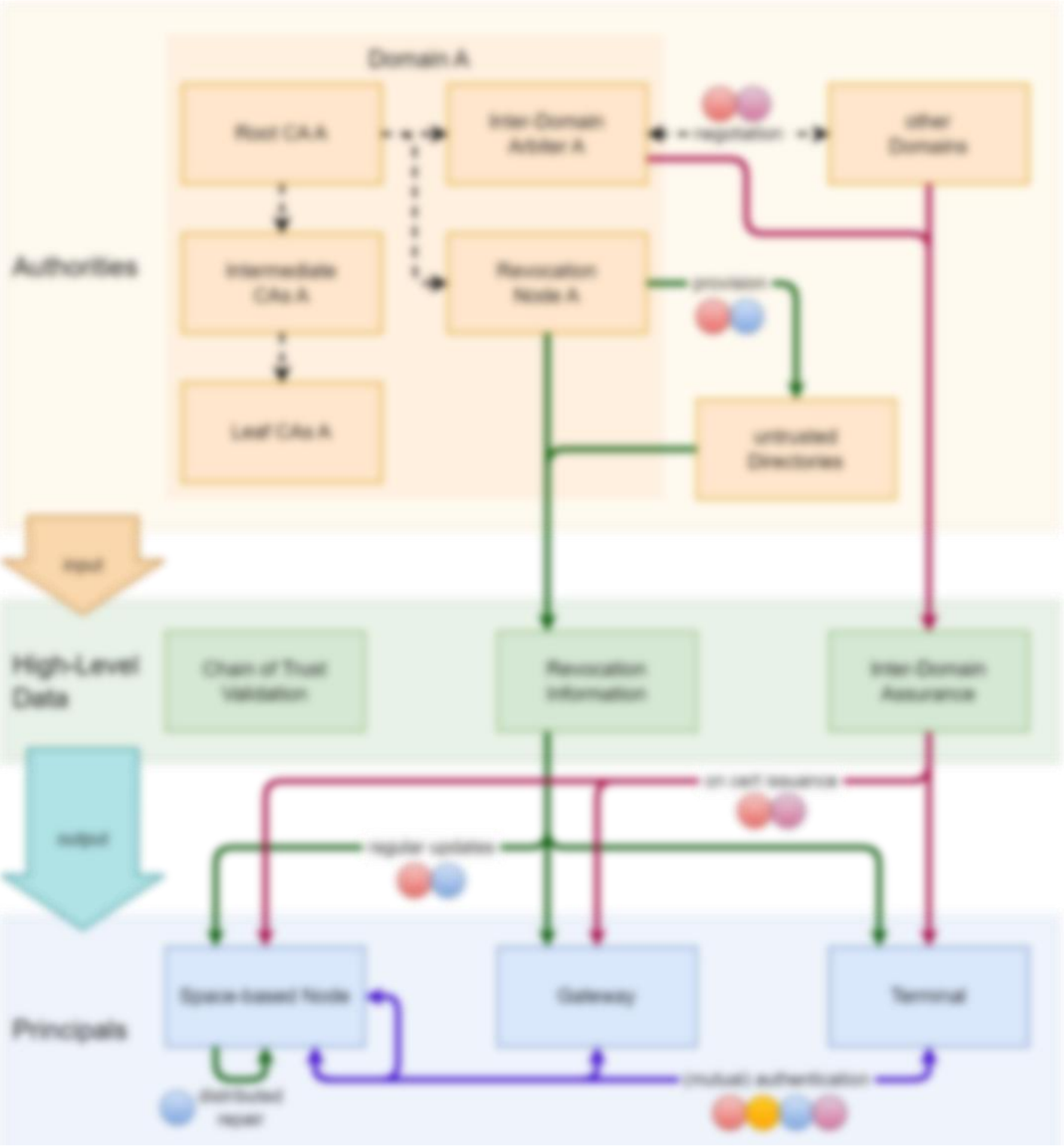
Our PKI Design



Our PKI Design

Core Components:

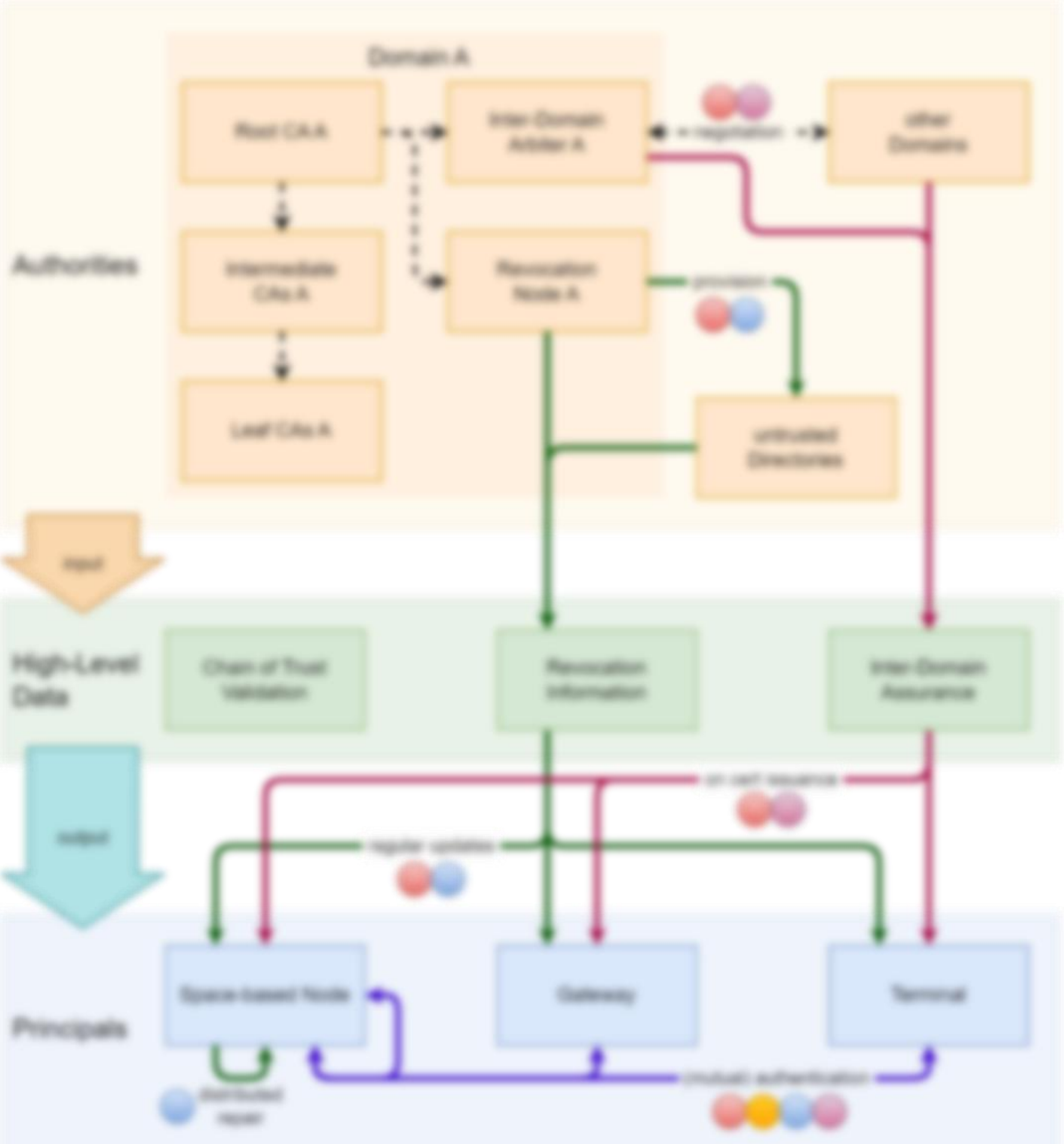
- **Multiple CAs:** Sovereign policy enforcement via offline validation, inspired by IETF’s Certificate Transparency



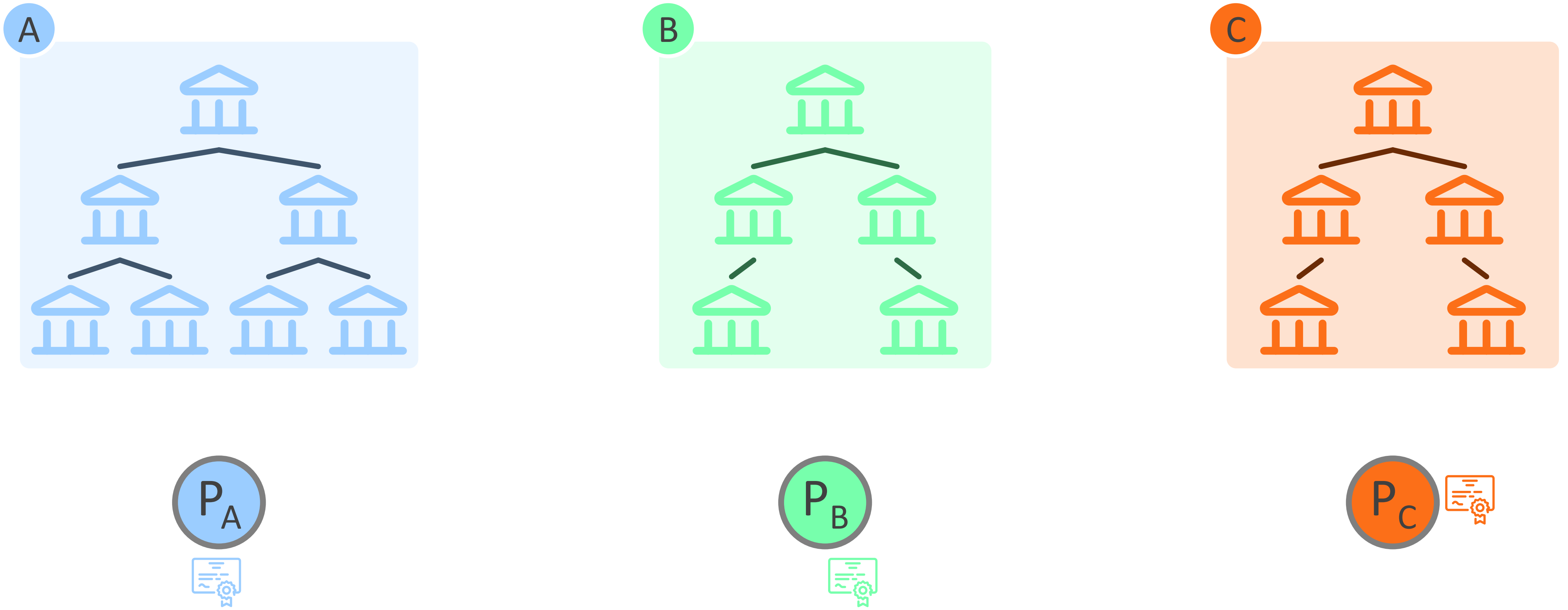
Our PKI Design

Core Components:

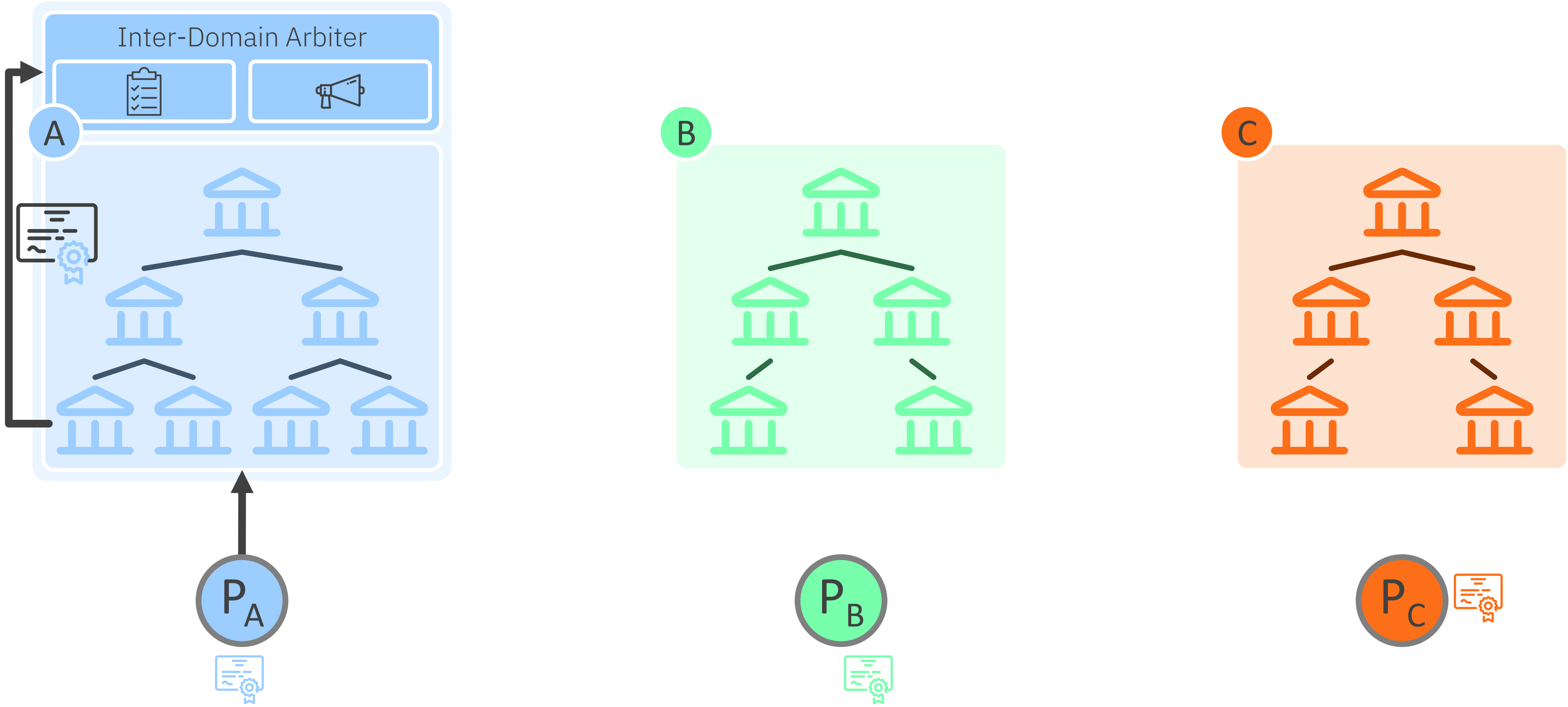
- **Multiple CAs:** Sovereign policy enforcement via offline validation, inspired by IETF’s Certificate Transparency
- **Revocation:** Combining efficient data structures and epidemic sat-2-sat propagation



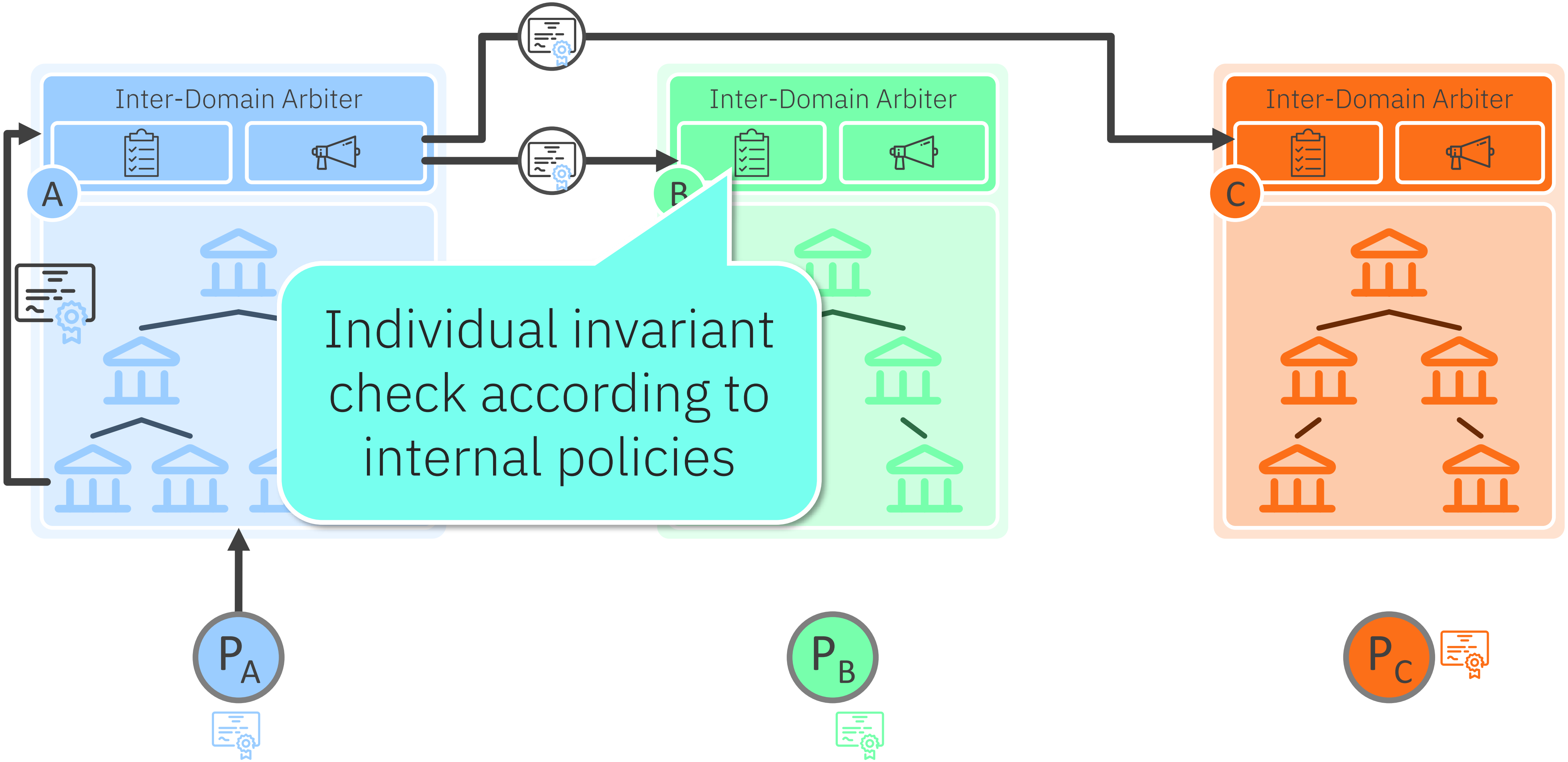
Scalable PKI: Domain Federation



Scalable PKI: Domain Federation

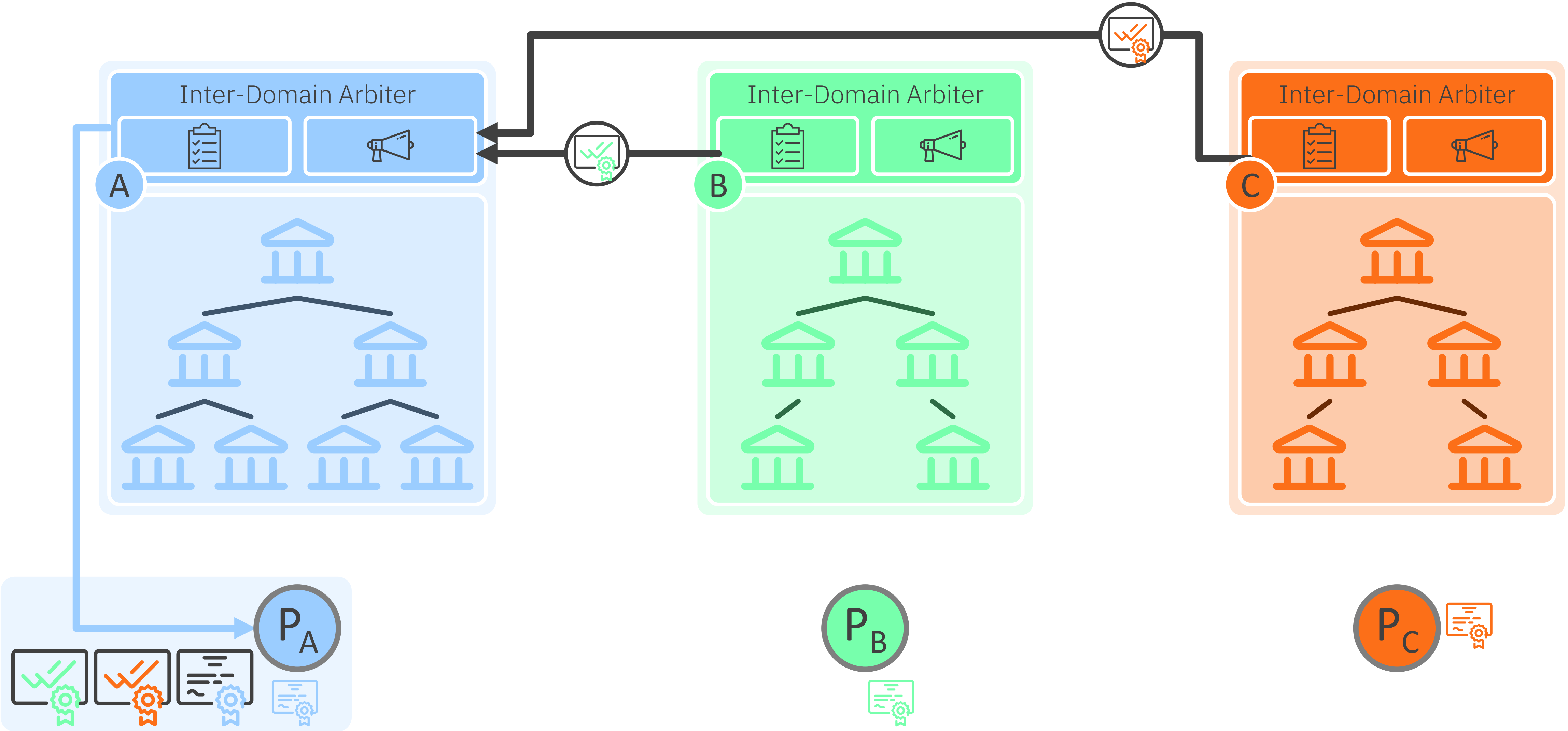


Scalable PKI: Domain Federation



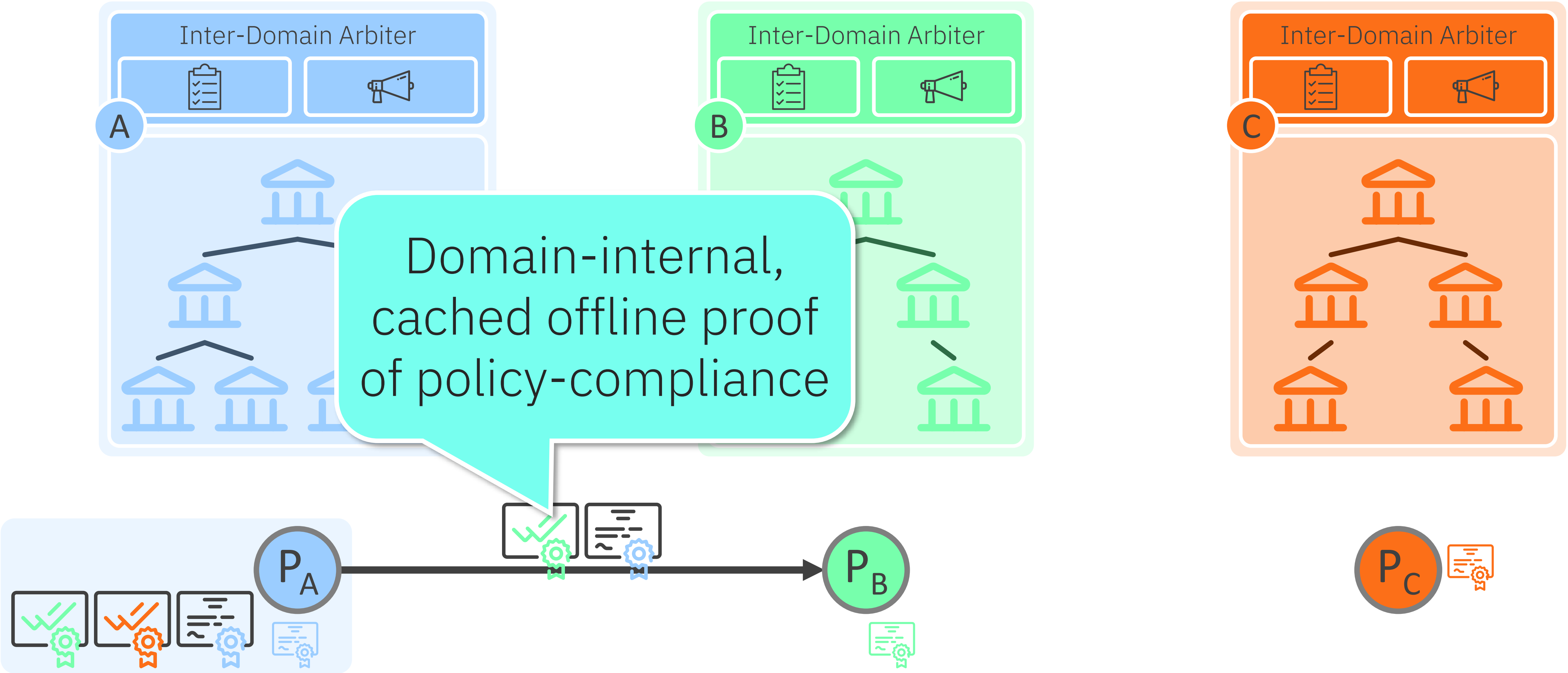
Individual invariant check according to internal policies

Scalable PKI: Domain Federation



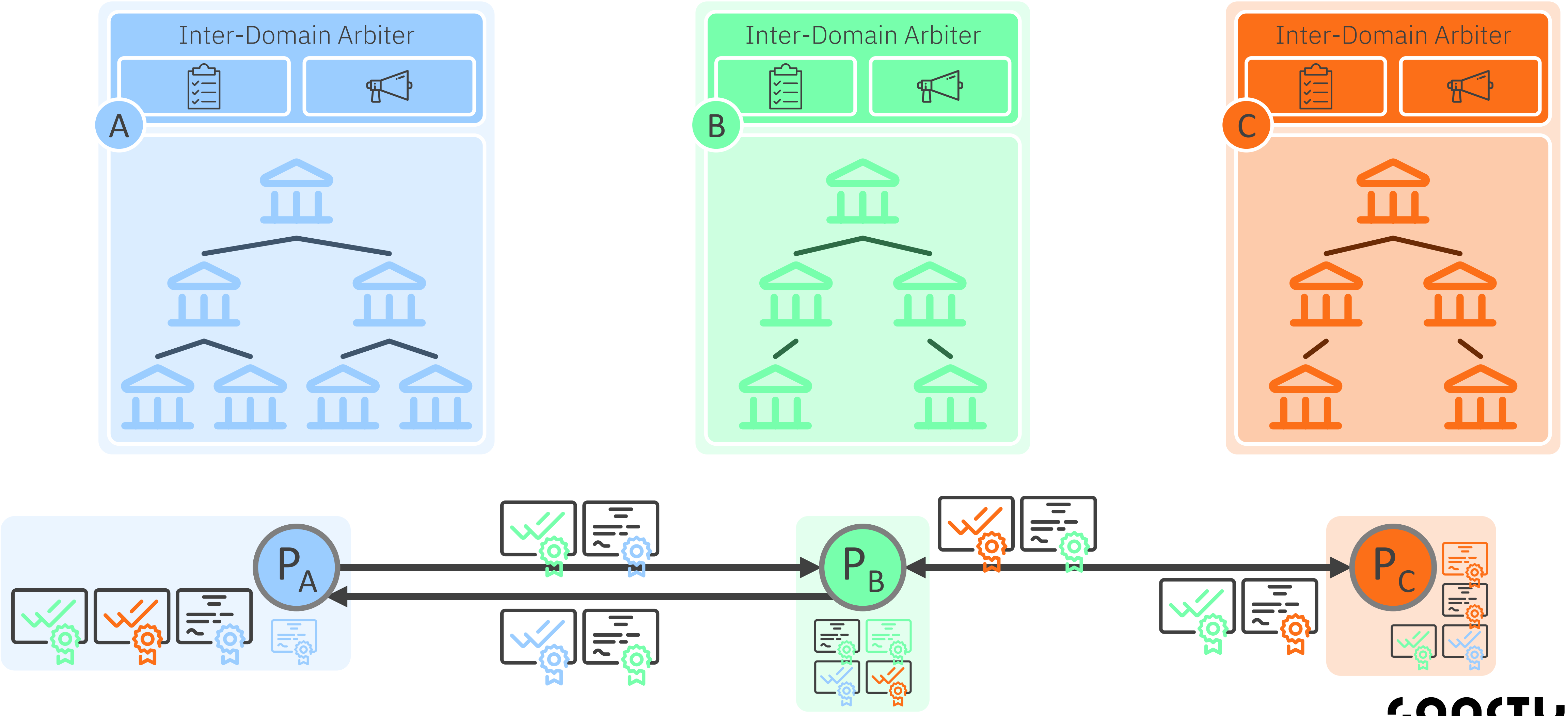
sanctuary

Scalable PKI: Domain Federation



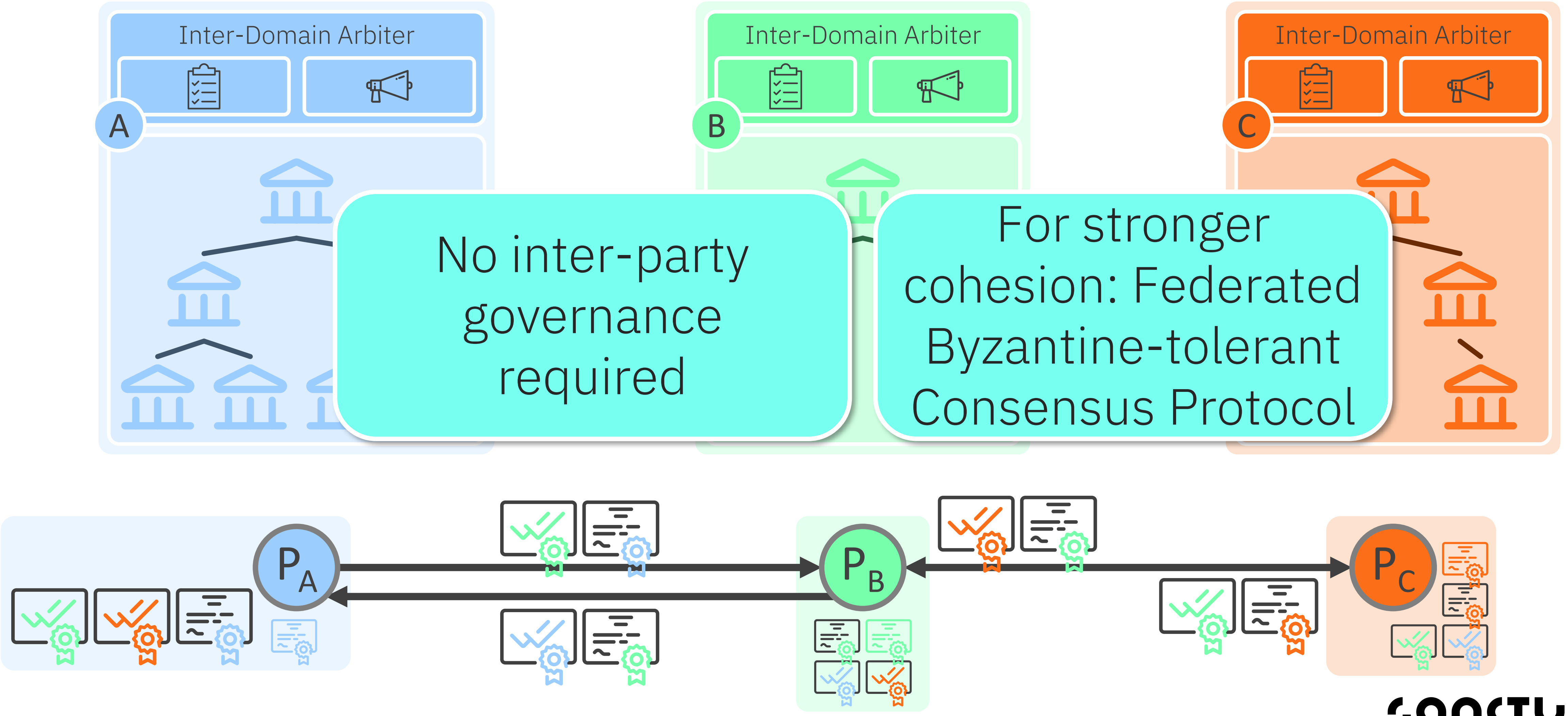
Domain-internal, cached offline proof of policy-compliance

Scalable PKI: Domain Federation



sanctuary

Scalable PKI: Domain Federation

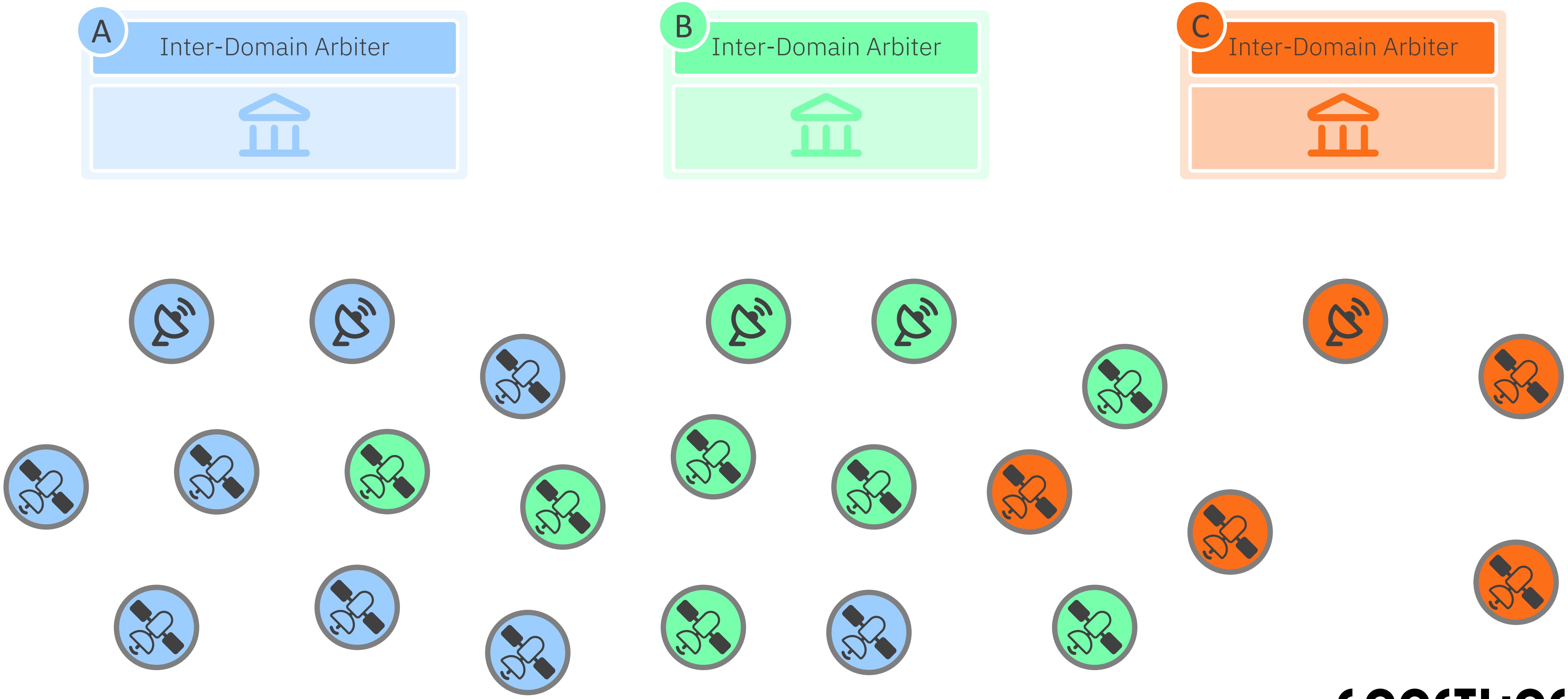


No inter-party governance required

For stronger cohesion: Federated Byzantine-tolerant Consensus Protocol

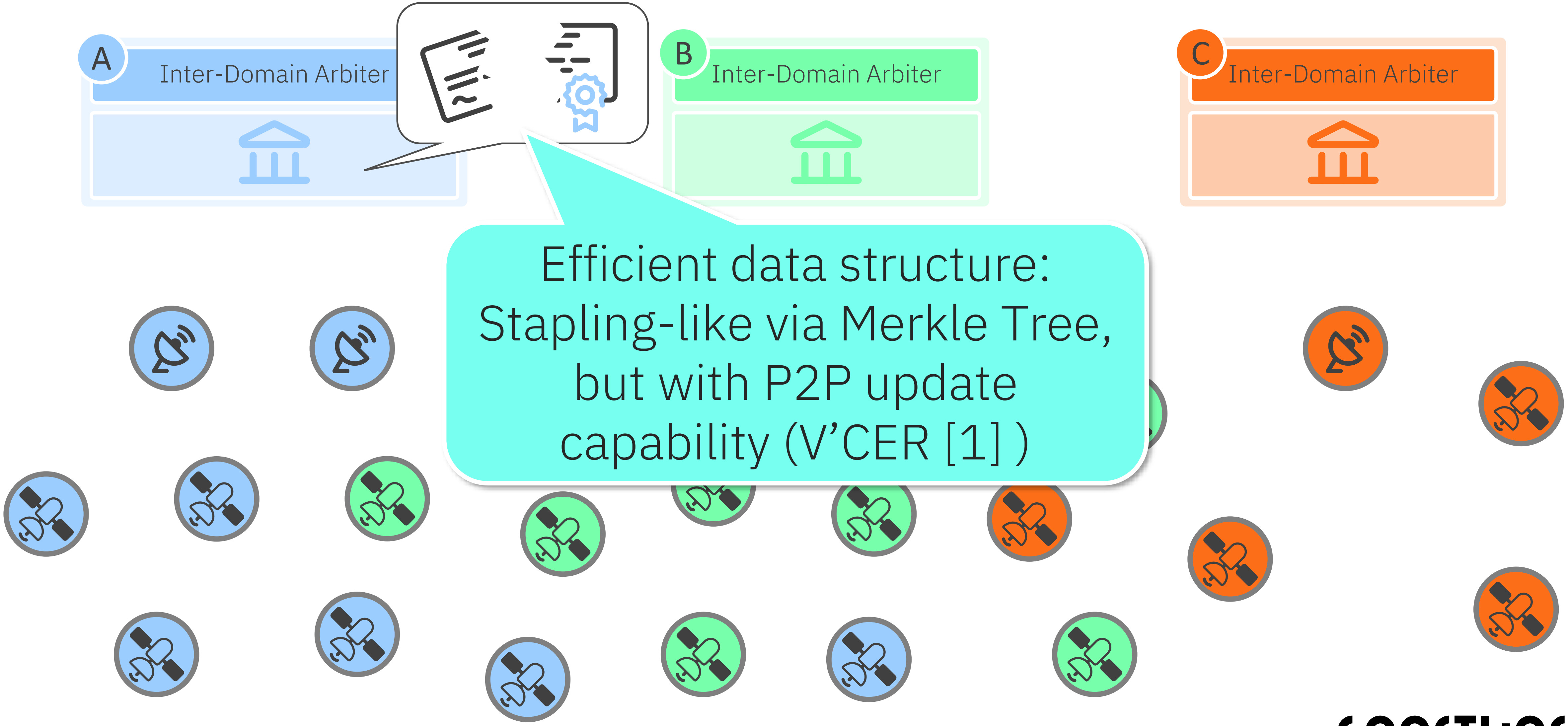
sanctuary

Scalable PKI: Epidemic Revocation



[1] “V’CER: Efficient Certificate Validation in Constrained Networks”, Koisser et al., USENIX Security 22

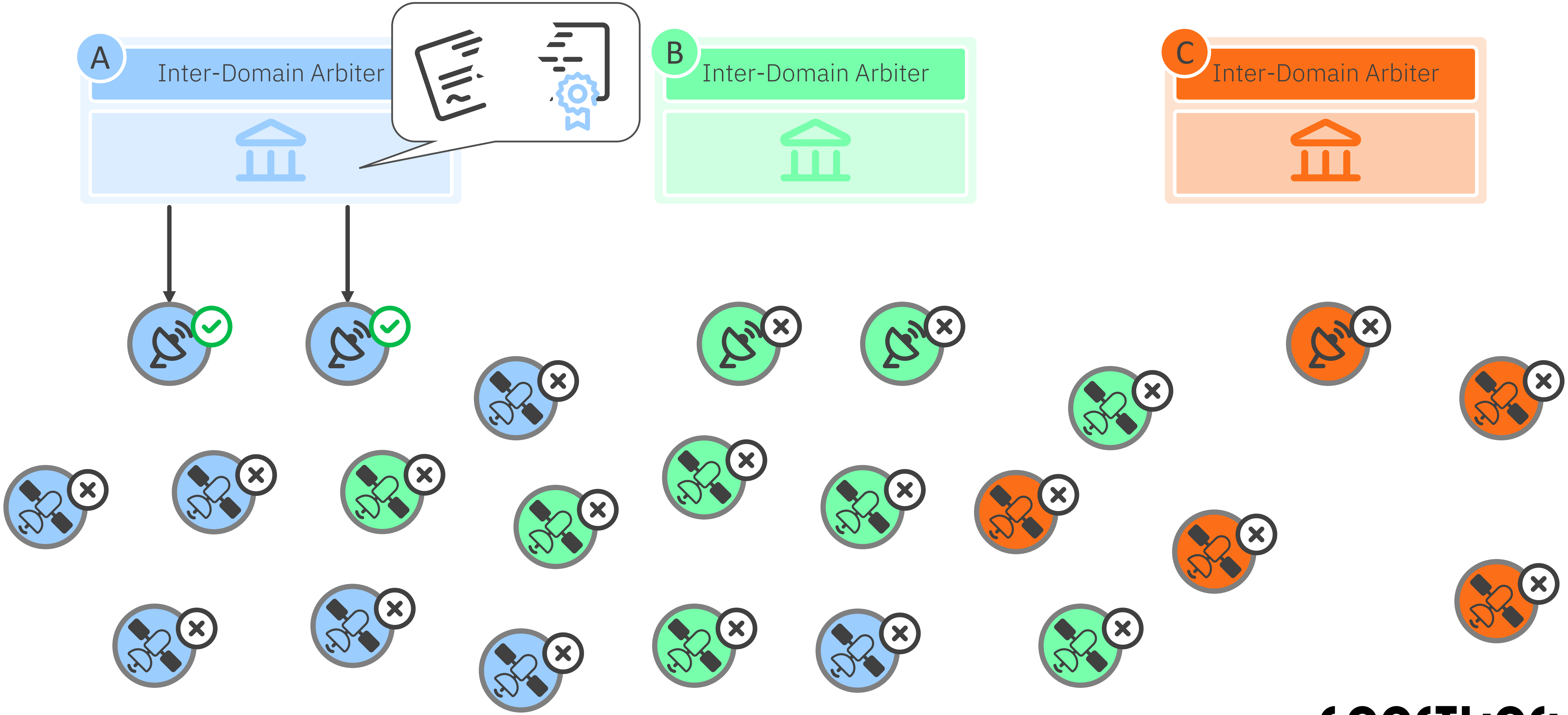
Scalable PKI: Epidemic Revocation



Efficient data structure:
Stapling-like via Merkle Tree,
but with P2P update
capability (V'CER [1])

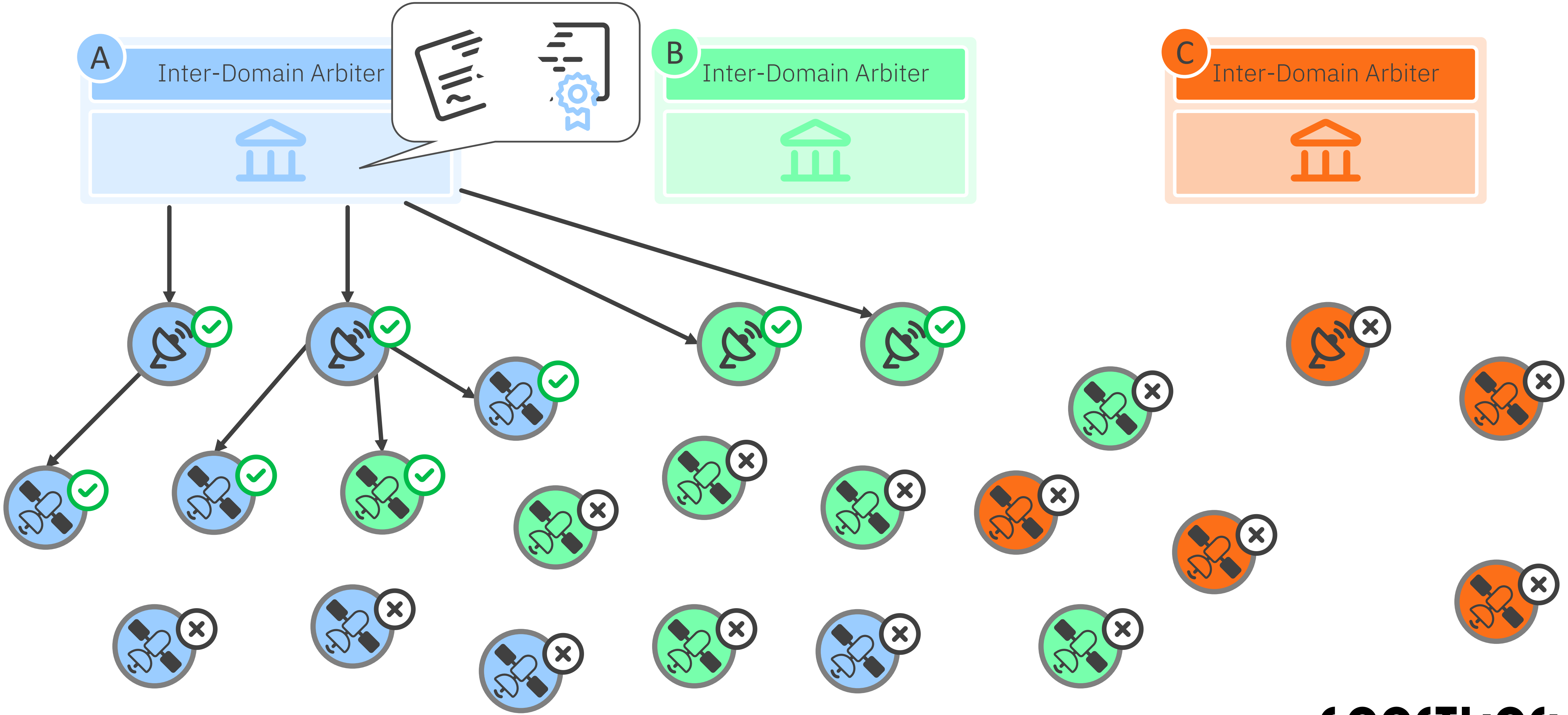
[1] "V'CER: Efficient Certificate Validation in Constrained Networks", Koisser et al., USENIX Security 22

Scalable PKI: Epidemic Revocation



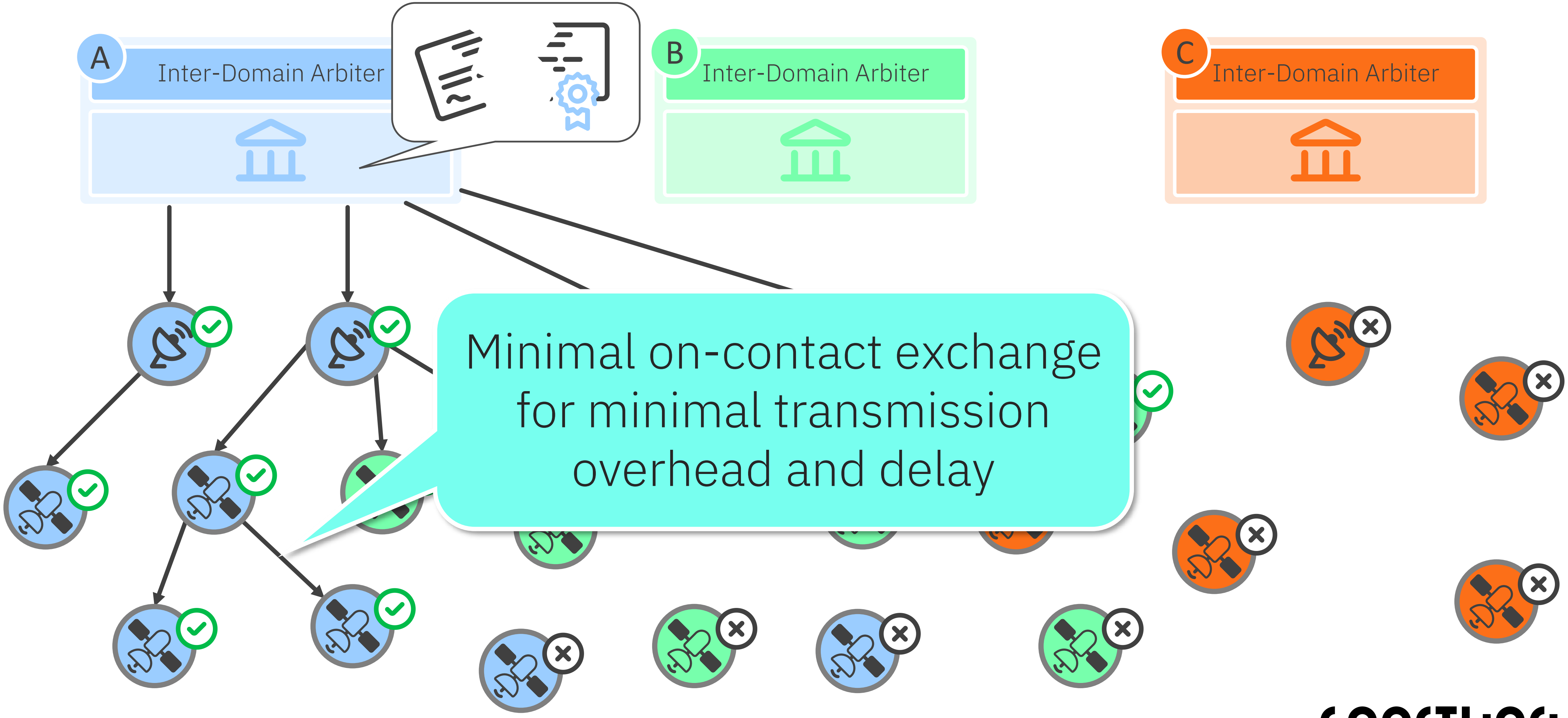
[1] “V’CER: Efficient Certificate Validation in Constrained Networks”, Koisser et al., USENIX Security 22

Scalable PKI: Epidemic Revocation



[1] “V’CER: Efficient Certificate Validation in Constrained Networks”, Koisser et al., USENIX Security 22

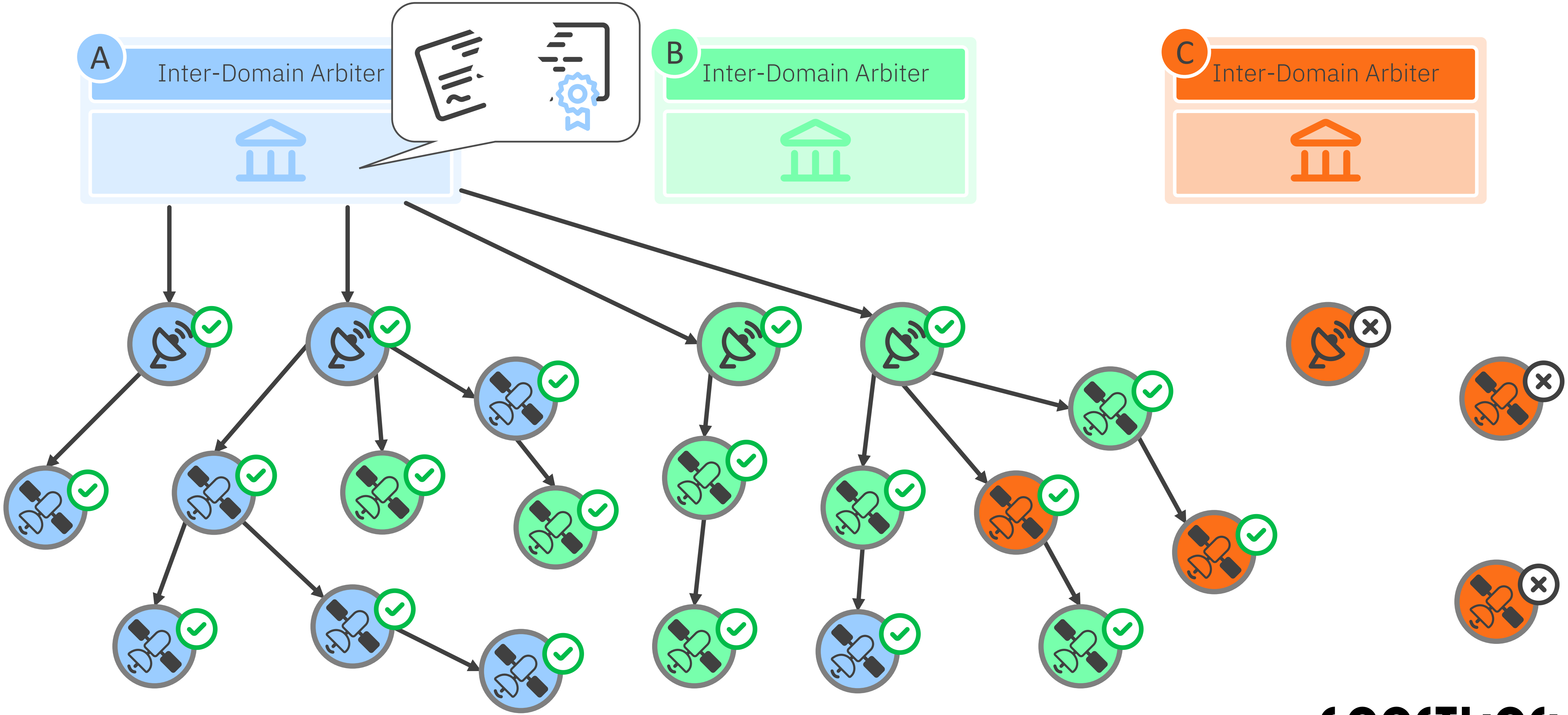
Scalable PKI: Epidemic Revocation



Minimal on-contact exchange for minimal transmission overhead and delay

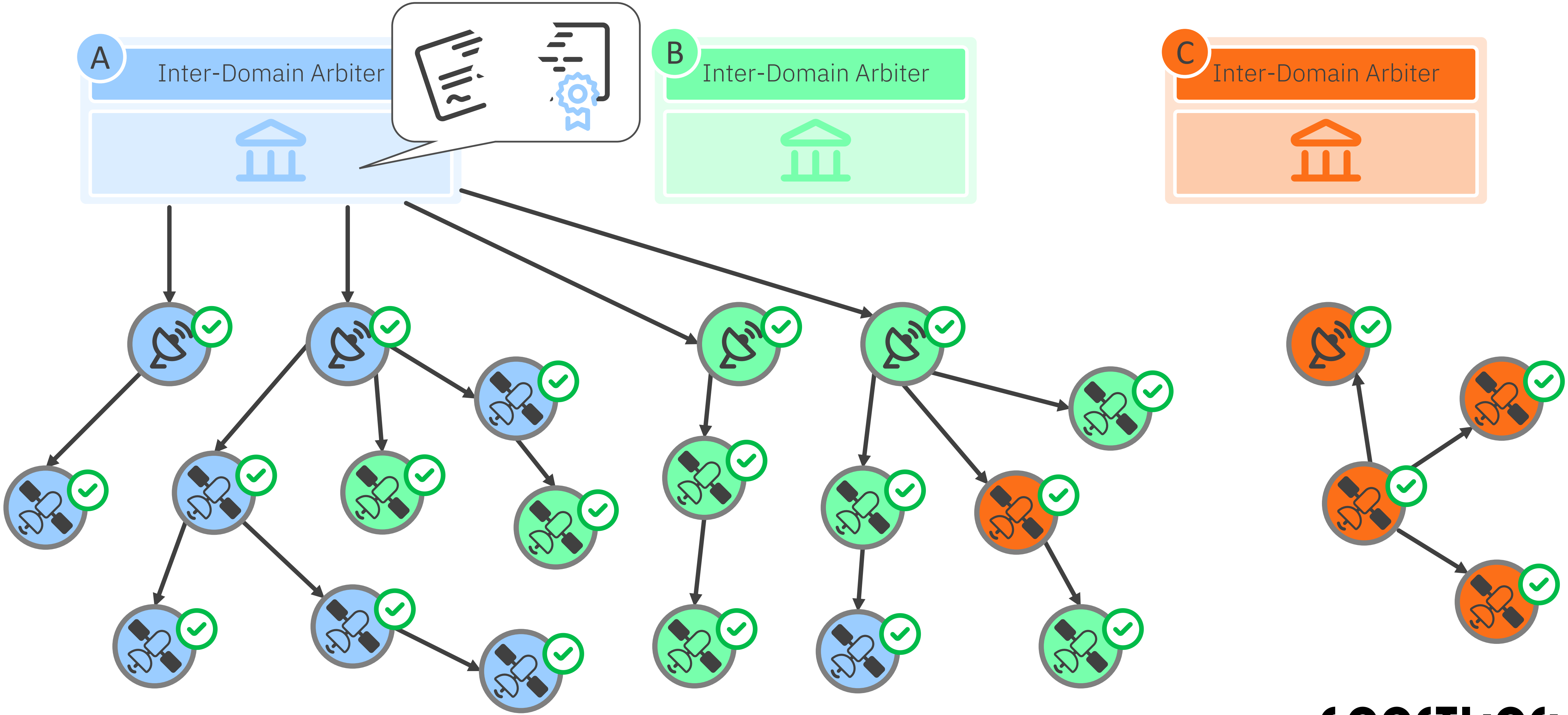
[1] “V’CER: Efficient Certificate Validation in Constrained Networks”, Koisser et al., USENIX Security 22

Scalable PKI: Epidemic Revocation



[1] “V’CER: Efficient Certificate Validation in Constrained Networks”, Koisser et al., USENIX Security 22

Scalable PKI: Epidemic Revocation



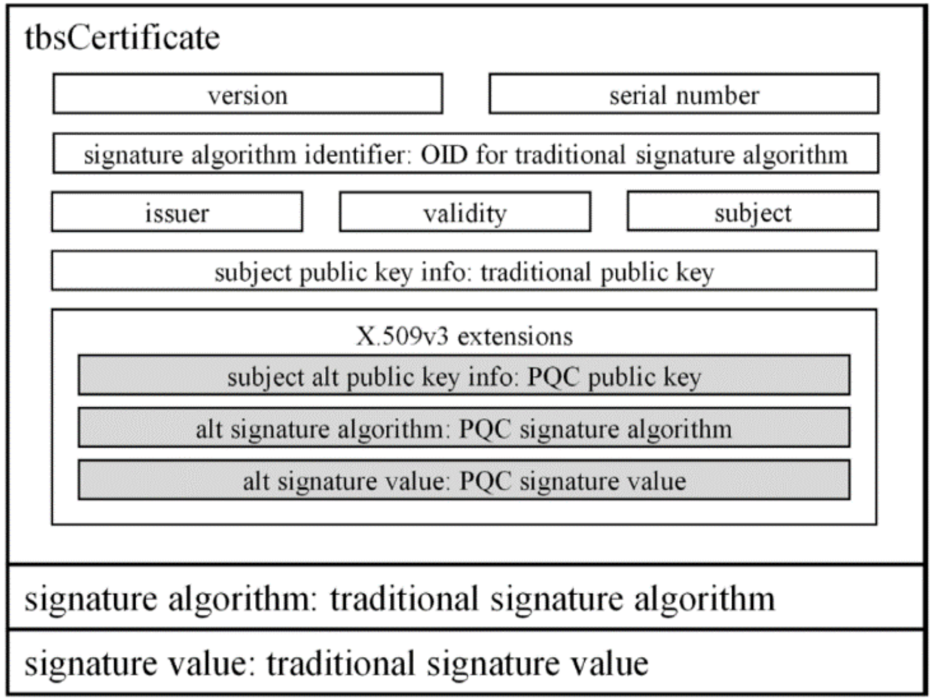
[1] “V’CER: Efficient Certificate Validation in Constrained Networks”, Koisser et al., USENIX Security 22

sanctuary

PQC via X.509 and TLS Extensions

- Hybrid Certificates
  - RFC 5280 [2]
  - ITU-T Recommendation
  - →Protects against quantum threat in transition phase

- Hybrid key exchange in TLS 1.3
  - draft-ietf-tls-hybrid-design-13 [3]
  - →Protects against store-now-decrypt-later adversary



tbsCertificate

version

serial number

signature algorithm identifier: OID for traditional signature algorithm

issuer

validity

subject

subject public key info: traditional public key

X.509v3 extensions

subject alt public key info: PQC public key

alt signature algorithm: PQC signature algorithm

alt signature value: PQC signature value

signature algorithm: traditional signature algorithm

signature value: traditional signature value

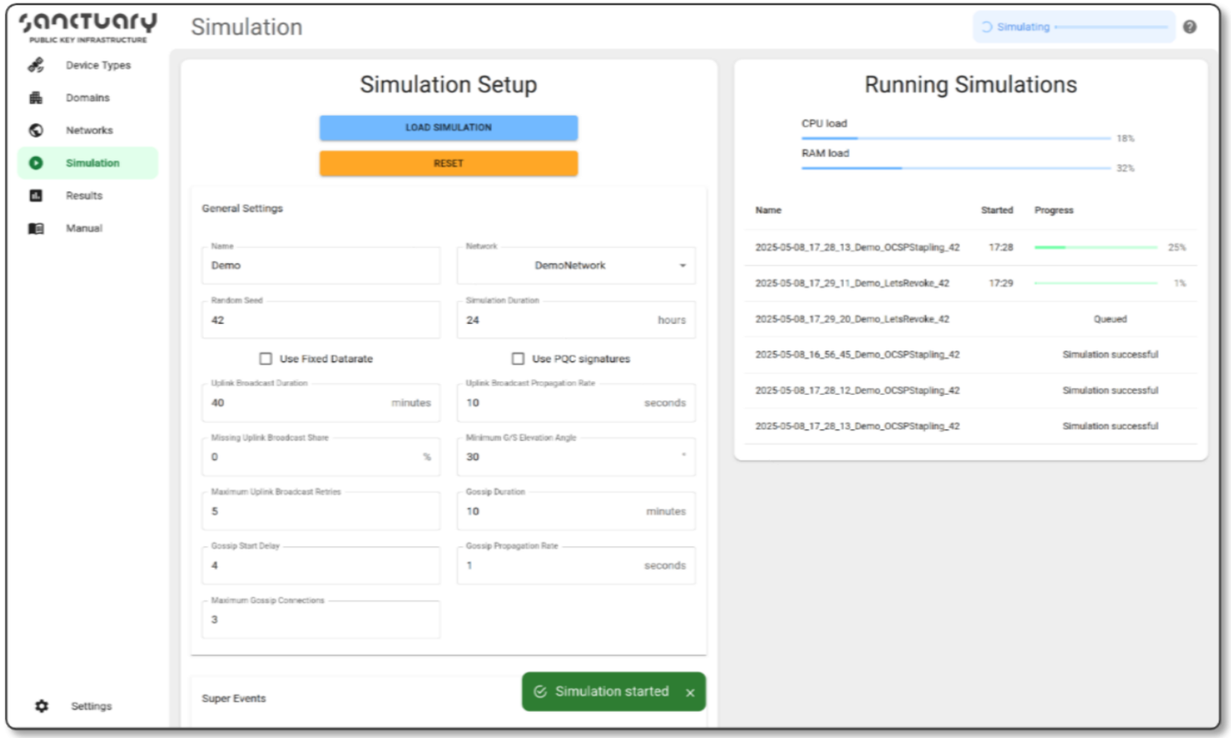
[2] https://datatracker.ietf.org/doc/html/rfc5280

[3] https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/13/

Simulation and Evaluation

PKI Simulation Framework

- Custom-built simulator for space-scale PKI evaluation
- Models certificate validation and revocation in dynamic topologies
- Realistic loss models for radio transmissions
- Supports comparison of revocation schemes (Lists, Staples, V’CER)
- Scales to thousands of nodes with realistic contact patterns
- Enables performance analysis under delay, disruption, and mobility



Simulation Setup

General Settings

Name: Demo

Network: DemoNetwork

Random Seed: 42

Simulation Duration: 24 hours

□ Use Fixed Datarate

□ Use PQC signatures

Uplink Broadcast Duration: 40 minutes

Uplink Broadcast Propagation Rate: 10 seconds

Missing Uplink Broadcast Share: 0 %

Minimum G/S Elevation Angle: 30 °

Maximum Uplink Broadcast Retries: 5

Gossip Duration: 10 minutes

Gossip Start Delay: 4

Gossip Propagation Rate: 1 seconds

Maximum Gossip Connections: 3

Super Events

Simulation started ×

Running Simulations

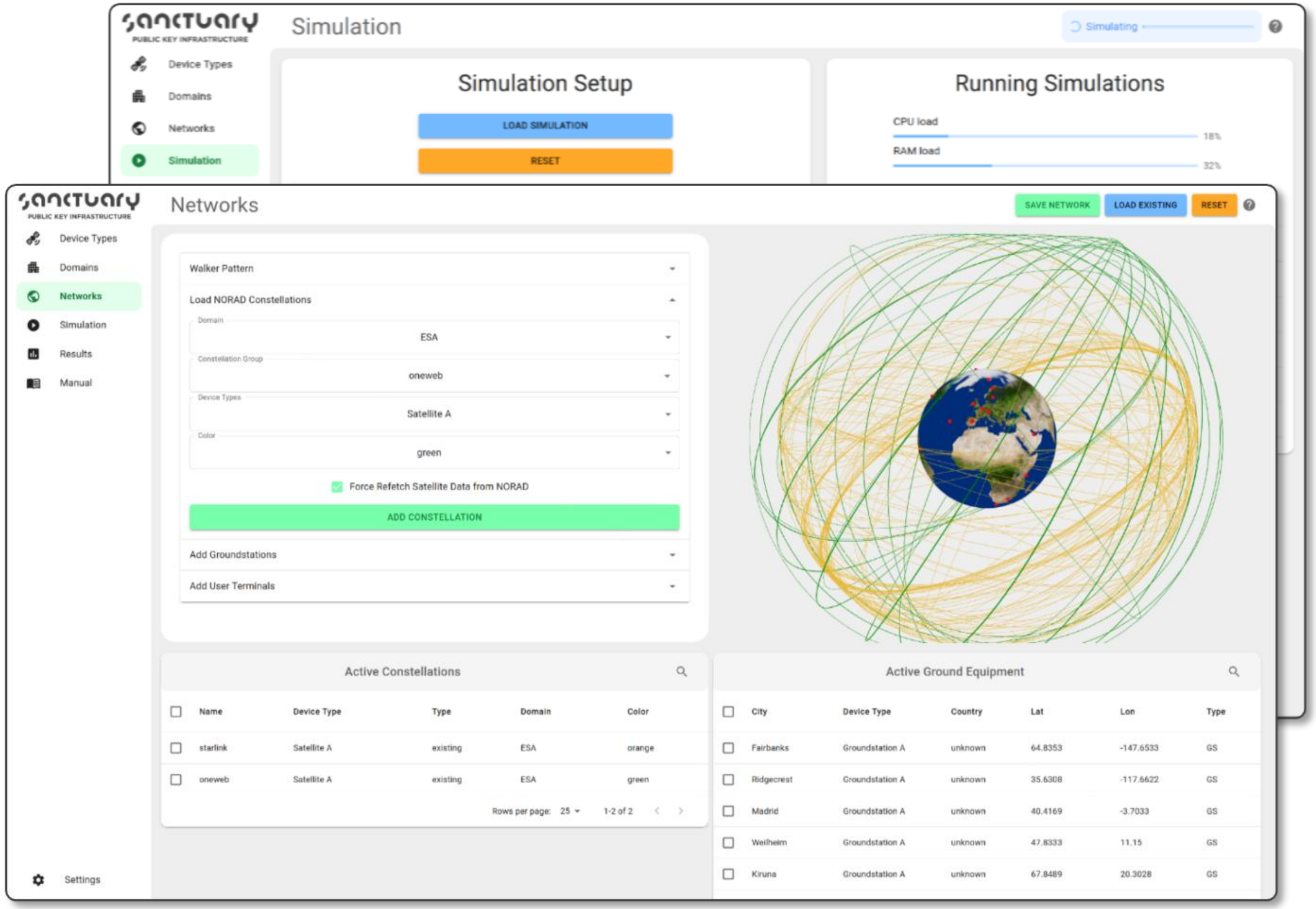
CPU load 18%

RAM load 32%

Name	Started	Progress
2025-05-08_17_28_13_Demo_OCSPStapling_42	17:28	25%
2025-05-08_17_29_11_Demo_LetsRevoke_42	17:29	1%
2025-05-08_17_29_20_Demo_LetsRevoke_42		Queued
2025-05-08_16_56_45_Demo_OCSPStapling_42		Simulation successful
2025-05-08_17_28_12_Demo_OCSPStapling_42		Simulation successful
2025-05-08_17_28_13_Demo_OCSPStapling_42		Simulation successful

PKI Simulation Framework

- Custom-built simulator for space-scale PKI evaluation
- Models certificate validation and revocation in dynamic topologies
- Realistic loss models for radio transmissions
- Supports comparison of revocation schemes (Lists, Staples, V'CER)
- Scales to thousands of nodes with realistic contact patterns
- Enables performance analysis under delay, disruption, and mobility



Domain: ESA

Constellation Group: oneweb

Device Types: Satellite A

Color: green

☑ Force Refetch Satellite Data from NORAD

Active Constellations

□	Name	Device Type	Type	Domain	Color
□	starlink	Satellite A	existing	ESA	orange
□	oneweb	Satellite A	existing	ESA	green

Rows per page: 25 1-2 of 2

Active Ground Equipment

□	City	Device Type	Country	Lat	Lon	Type
□	Fairbanks	Groundstation A	unknown	64.8353	-147.6533	GS
□	Ridgecrest	Groundstation A	unknown	35.6308	-117.6622	GS
□	Madrid	Groundstation A	unknown	40.4169	-3.7033	GS
□	Weilheim	Groundstation A	unknown	47.8333	11.15	GS
□	Kiruna	Groundstation A	unknown	67.8489	20.3028	GS

Evaluation Scenario

- Multi-Constellation Setting:
  - 5 Satellite Walker pattern Constellations
    - 3200 Satellites at ~600km (inspired by Amazon’s Project Kuiper)
    - 1300 Satellites at ~1000km (inspired by SSST’S Qianfan)
    - 700 Satellites at ~1200km, twice (inspired by Eutelsat’s OneWeb)
    - 300 Satellites at ~1200km (inspired by IRIS²)
  - Groundstation Network combining
    - ESA’s Estrack
    - AWS Ground Stations
- Simulation
  - 4 weeks of network operation
  - 28 revocations (on avg. ~1/day)

sanctuary

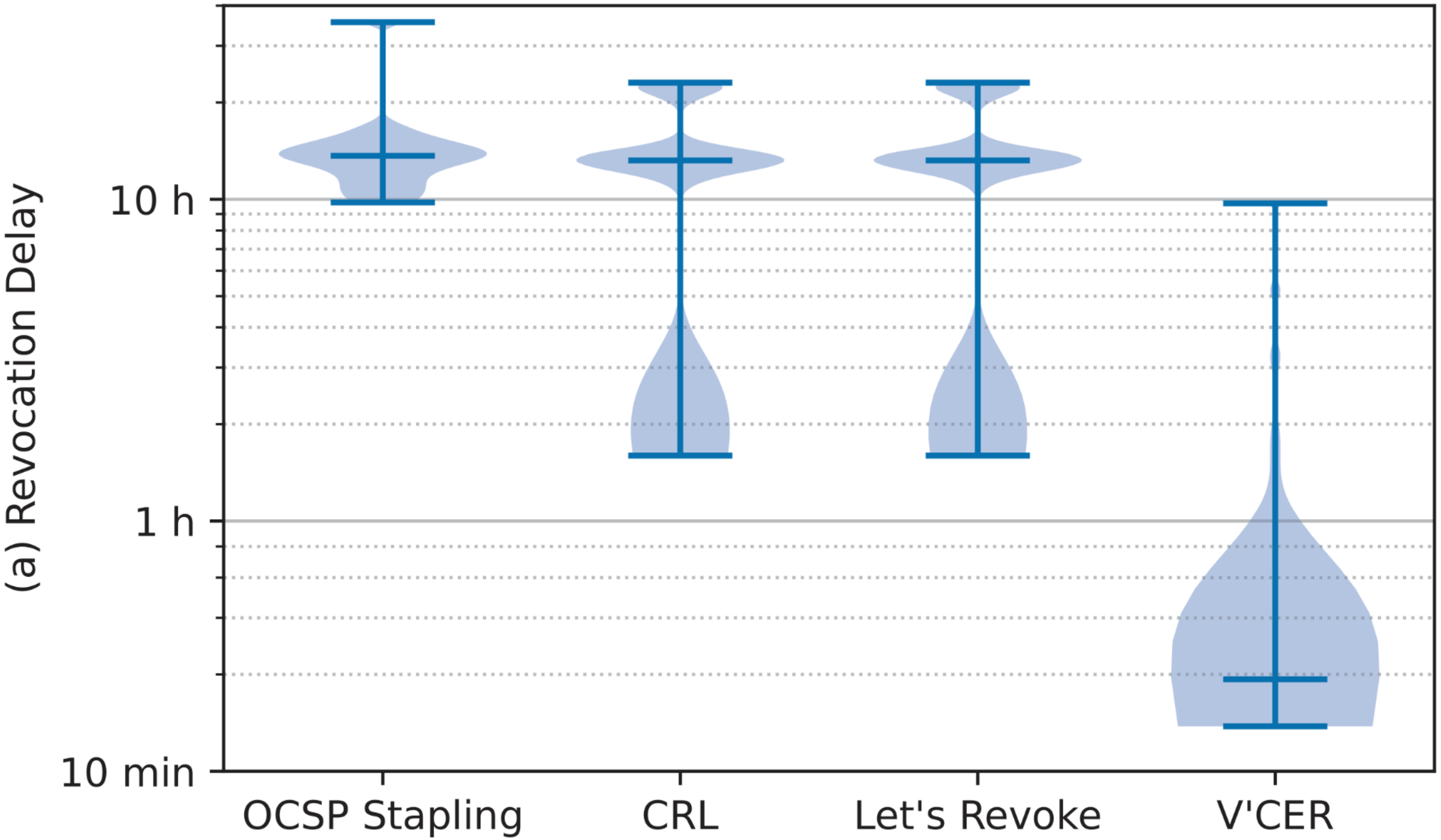
Evaluation Scenario

- Multi-Constellation Setting:
  - 5 Satellite Walker pattern Constellations
    - 3200 Satellites at ~600km (inspired by Amazon’s Project Kuiper)
    - 1300 Satellites at ~1000km (inspired by SSST’S Qianfan)
    - 700 Satellites at ~1200km, twice (inspired by Eutelsat’s OneWeb)
    - 300 Satellites at ~1200km (inspired by IRIS^2)
  - Groundstation Network combining
    - ESA’s Estrack
    - AWS Ground Stations
- Simulation
  - 4 weeks of network operation
  - 28 revocations (on avg. ~1/day)

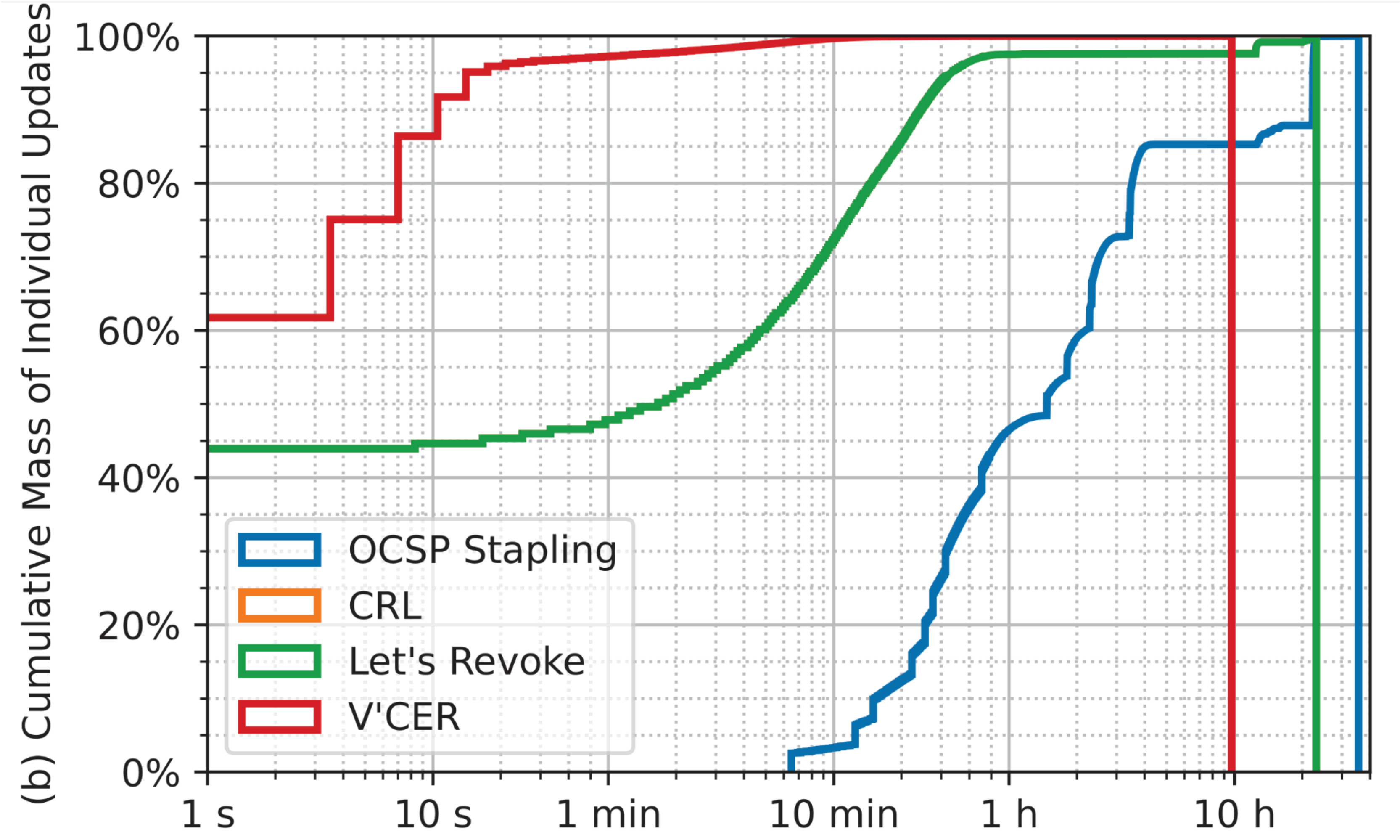
Evaluation Scenario

- Multi-Constellation Setting:
  - 5 Satellite Walker pattern Constellations
    - 3200 Satellites at ~600km (inspired by Amazon’s Project Kuiper)
    - 1300 Satellites at ~1000km (inspired by SSST’S Qianfan)
    - 700 Satellites at ~1200km, twice (inspired by Eutelsat’s OneWeb)
    - 300 Satellites at ~1200km (inspired by IRIS^2)
  - Groundstation Network combining
    - ESA’s Estrack
    - AWS Ground Stations
- Simulation
  - 4 weeks of network operation
  - 28 revocations (on avg. ~1/day)

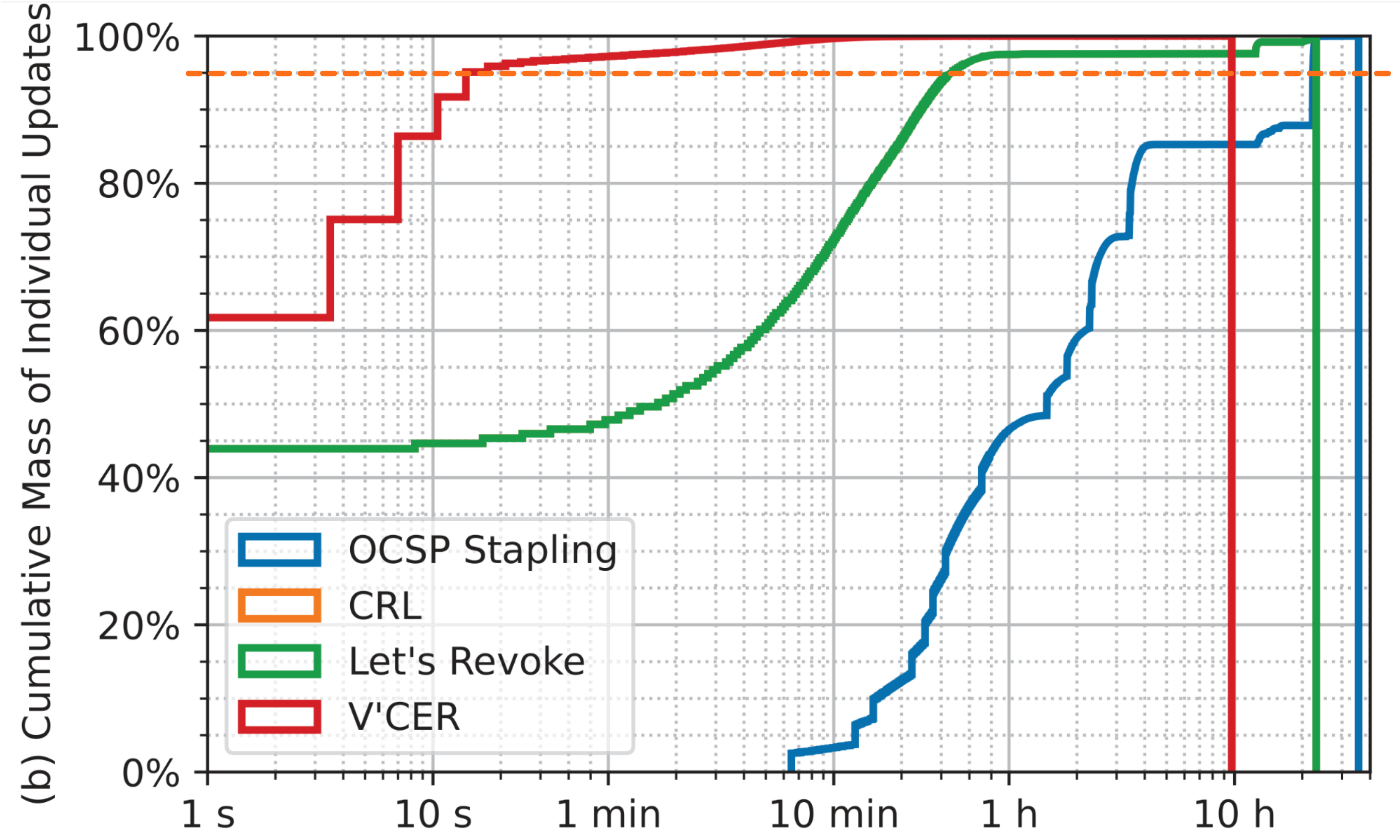
Revocation Delay



Revocation Update Distribution

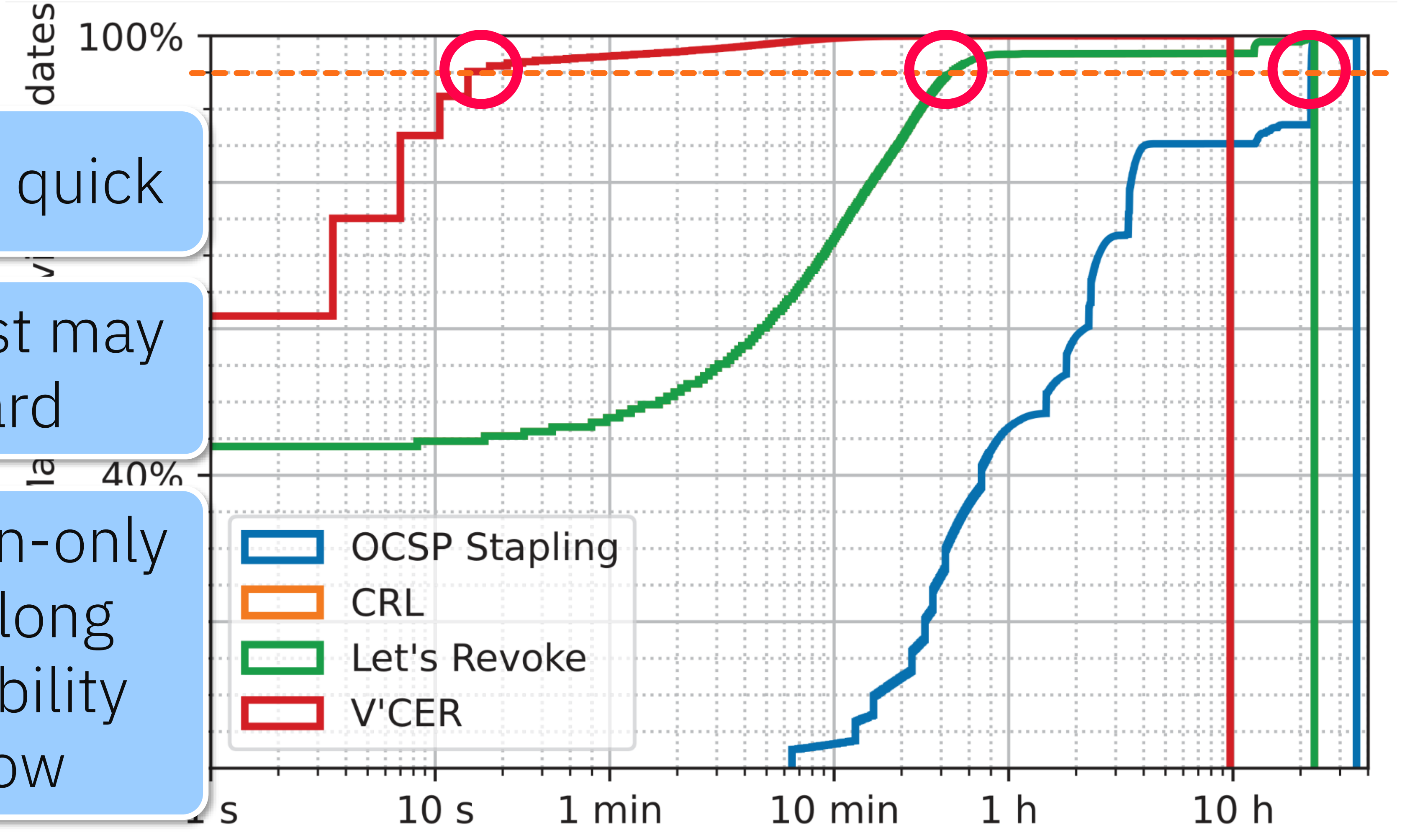


Revocation Update Distribution



95% of network is aware of revocation

Revocation Update Distribution



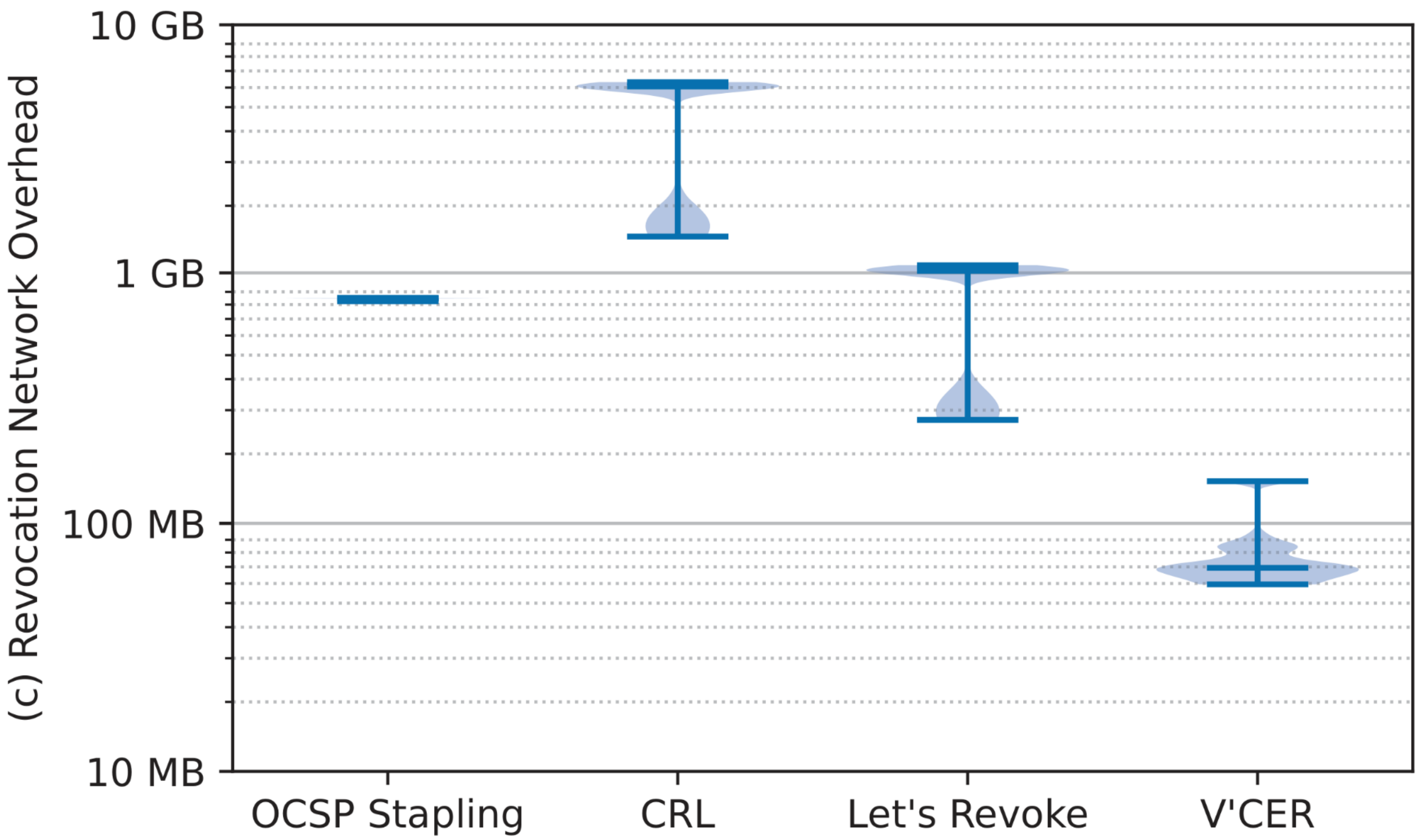
95% of network is aware of revocation

Gossip is quick

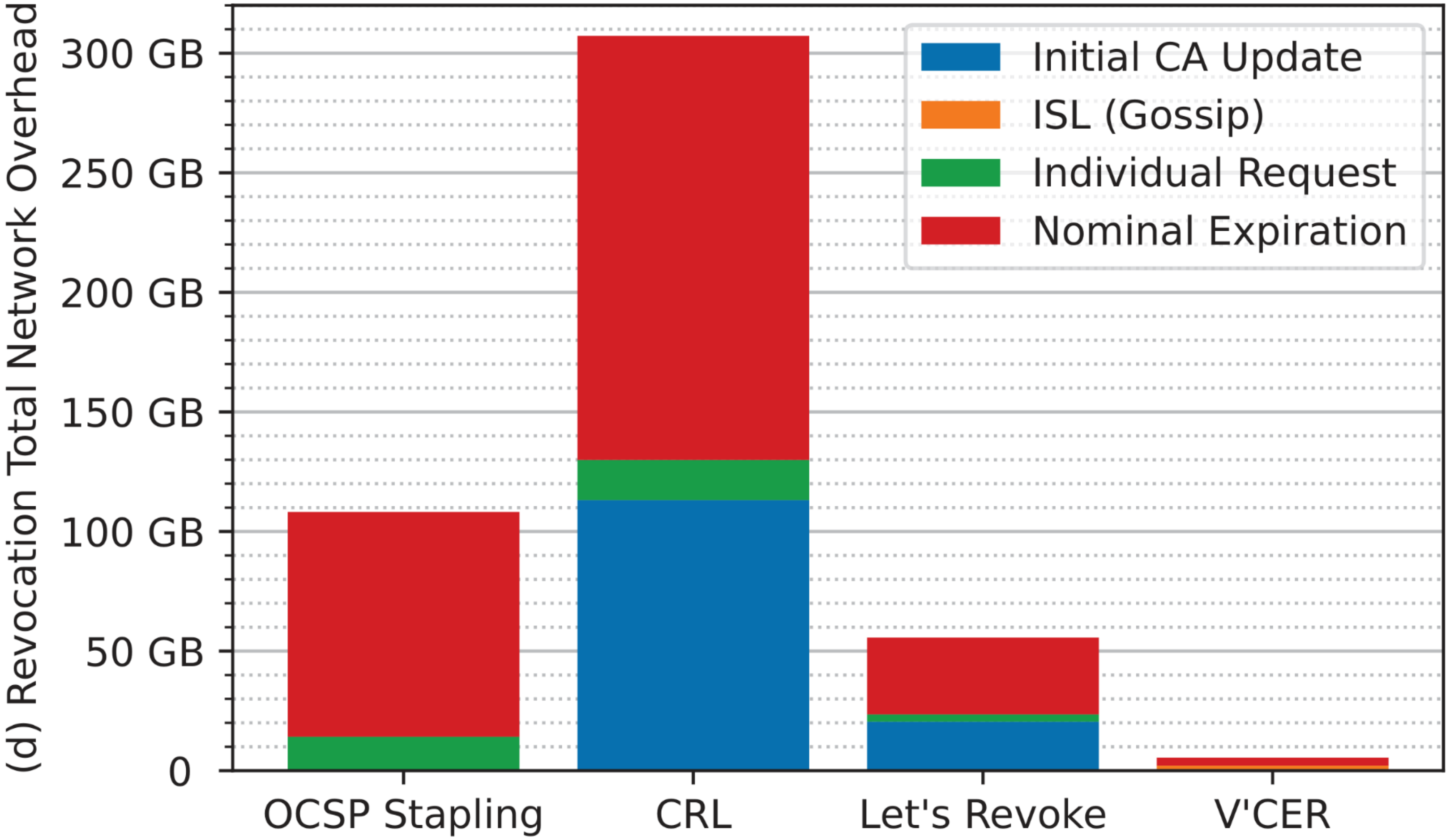
Broadcast may be hard

Expiration-only leaves long vulnerability window

Revocation Network Overhead

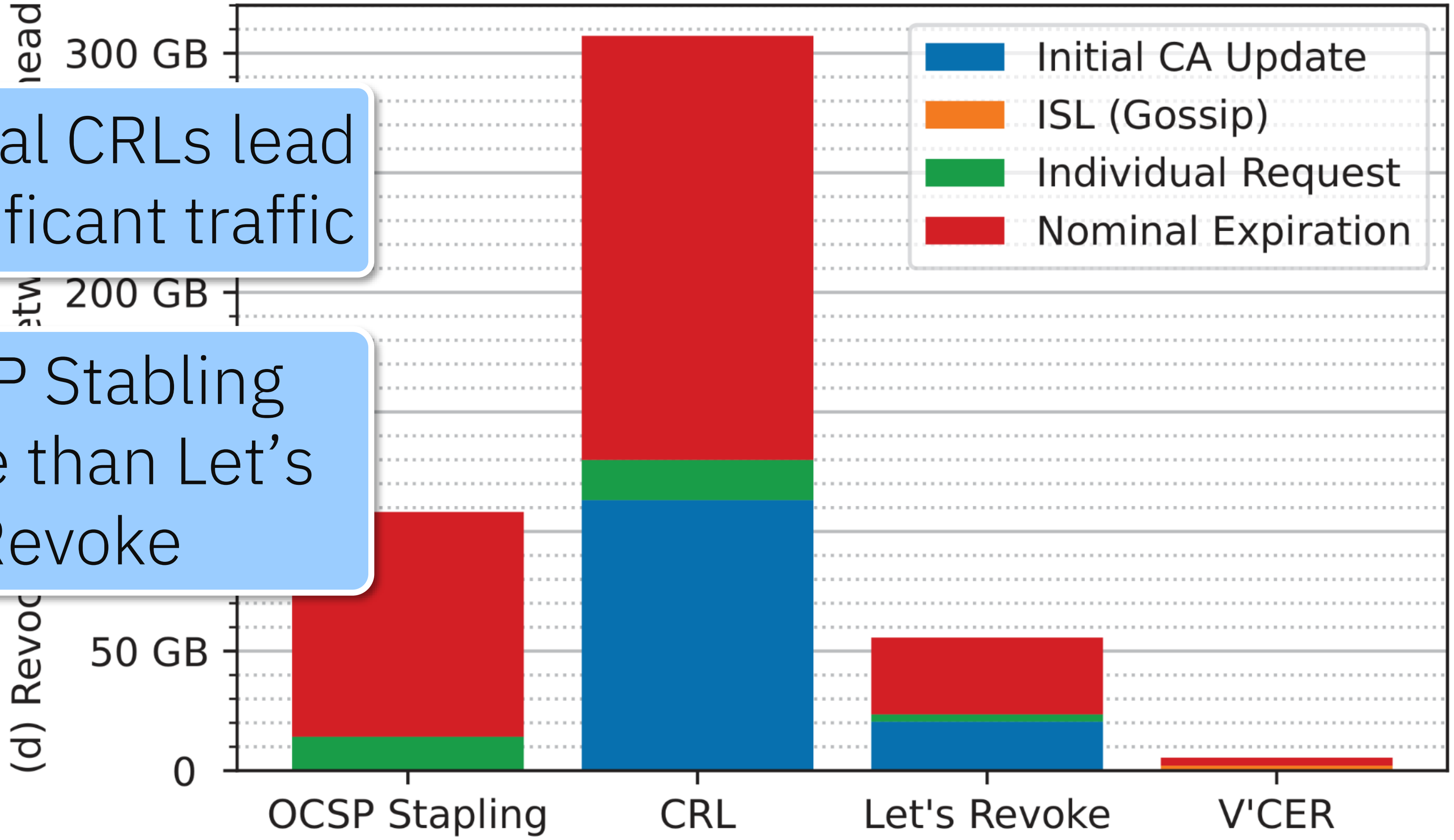


Accumulated Network Overheads



sanctuary

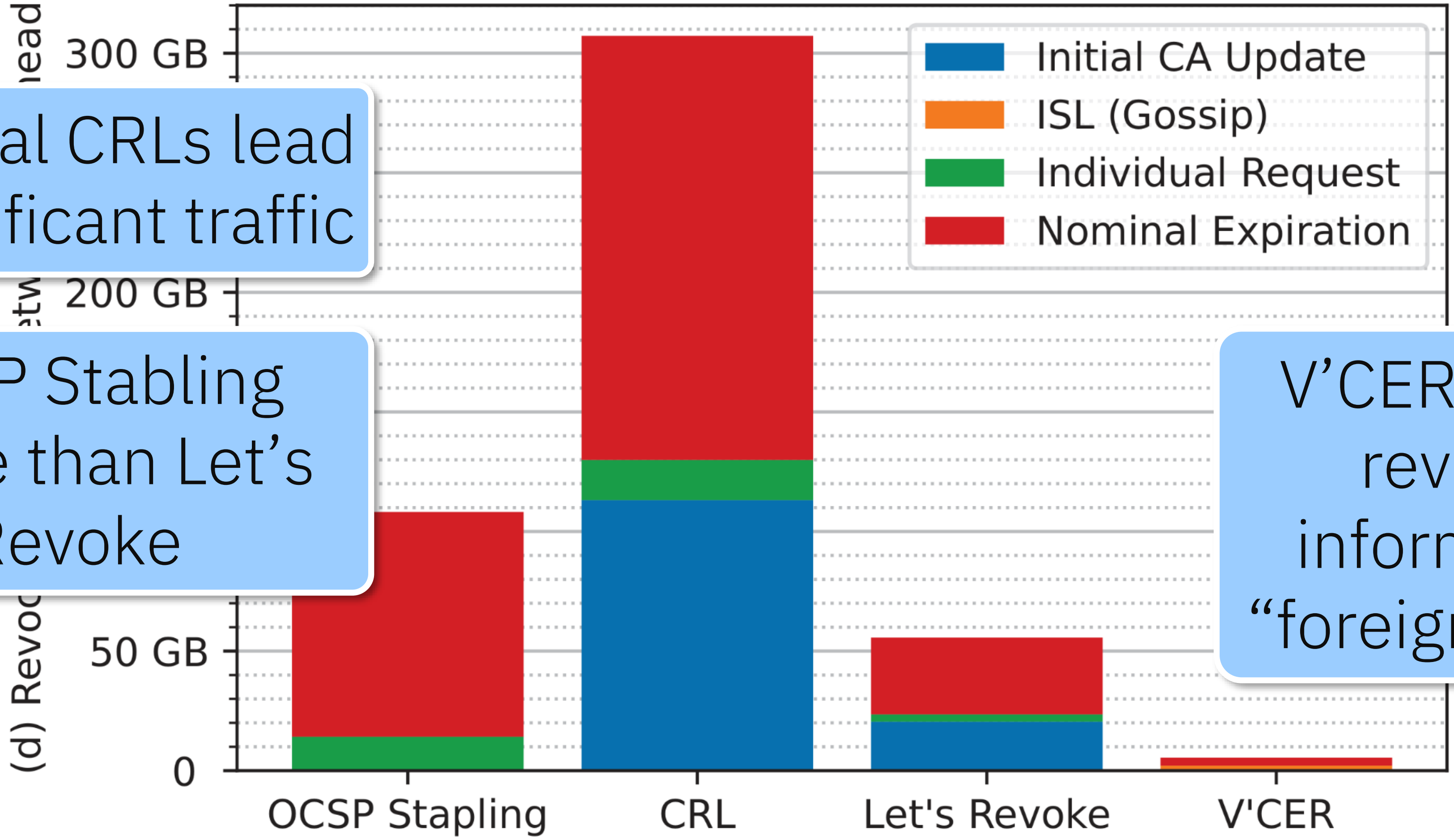
Accumulated Network Overheads



Classical CRLs lead to significant traffic

OCSP Stabling worse than Let’s Revoke

Accumulated Network Overheads



Classical CRLs lead to significant traffic

OCSP Stabling worse than Let’s Revoke

V’CER: compact revocation information for “foreign” domains

Conclusion & Outlook

- Flexible governance via internal policy checks
- Fast but efficient revocation enforcement (minimal vulnerability window)
- PQC-readiness via hybrid certificates and future-proof key exchange

- Advance the PKI Design to a commercial solution
- Selected for in-orbit demonstration on CyberCUBE mission

Conclusion & Outlook

- Flexible governance via internal policy checks
- Fast but efficient revocation enforcement (minimal vulnerability window)
- PQC-readiness via hybrid certificates and future-proof key exchange

- Advance the PKI Design to a commercial solution
- Selected for in-orbit demonstration on CyberCUBE mission

Q & A

sanctuary

✉ info@sanctuary.dev

🌐 www.sanctuary.dev

Security Designs

Fuzzing

Attestation

IP Protection

Secure Boot

Public Key Infrastructures

SBOM

CVE Scanning

Real-time Hypervisor

OT Asset Management

Arm TrustZone

TPM

Zero Trust Concepts

sanctuary

SANCTUARY Systems GmbH

🏢 Robert-Bosch-Str. 7, D-64293 Darmstadt

✉ info@sanctuary.dev

🌐 www.sanctuary.dev

in www.linkedin.com/company/sanctuary-dev/

Security Designs

Fuzzing

Attestation

IP Protection

Secure Boot

Public Key Infrastructures

SBOM

CVE Scanning

Real-time Hypervisor

OT Asset Management

Arm TrustZone

TPM

Zero Trust Concepts