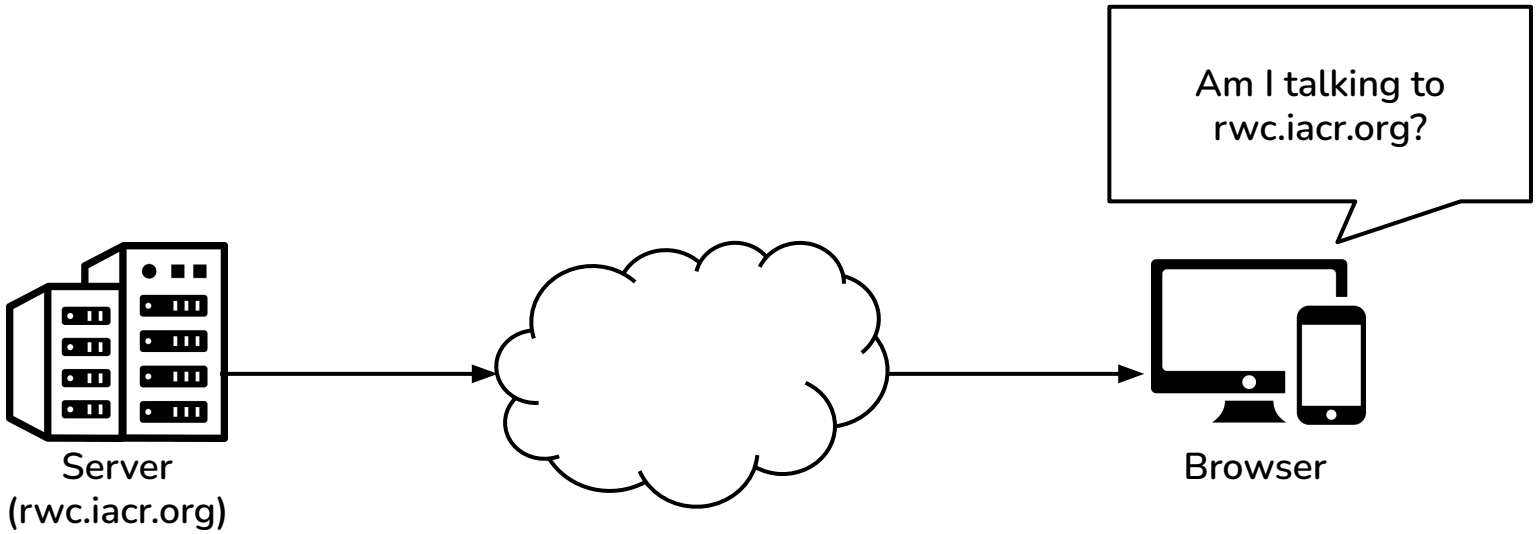
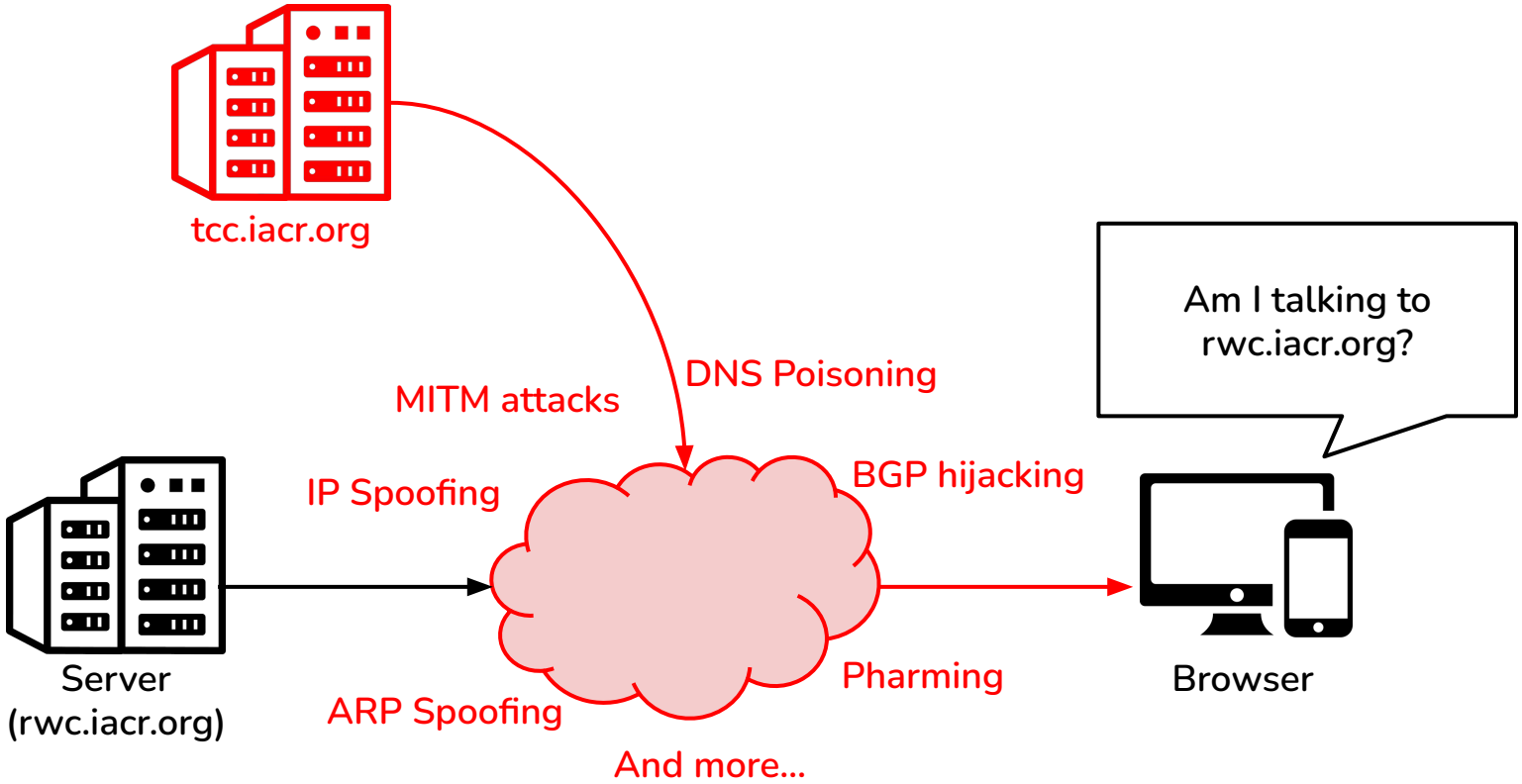
NOPE: Strengthening Domain Authentication with Succinct Proofs

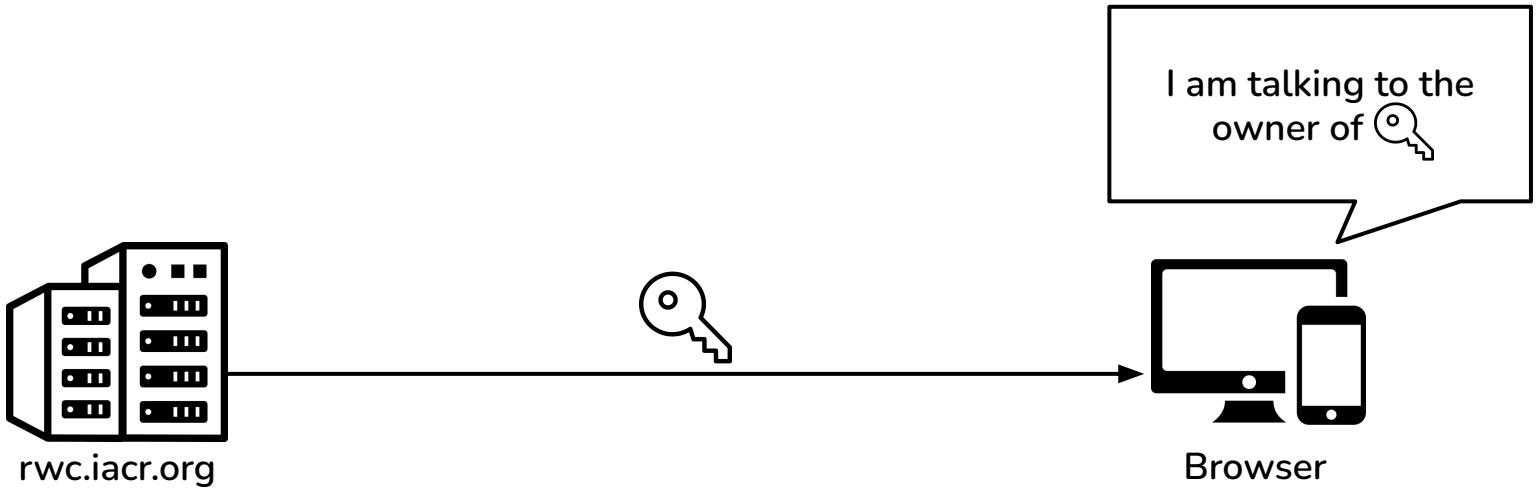
Zachary DeStefano, Jeff J. Ma,
Joseph Bonneau, and Michael Walfish

Appeared at SOSP 2024

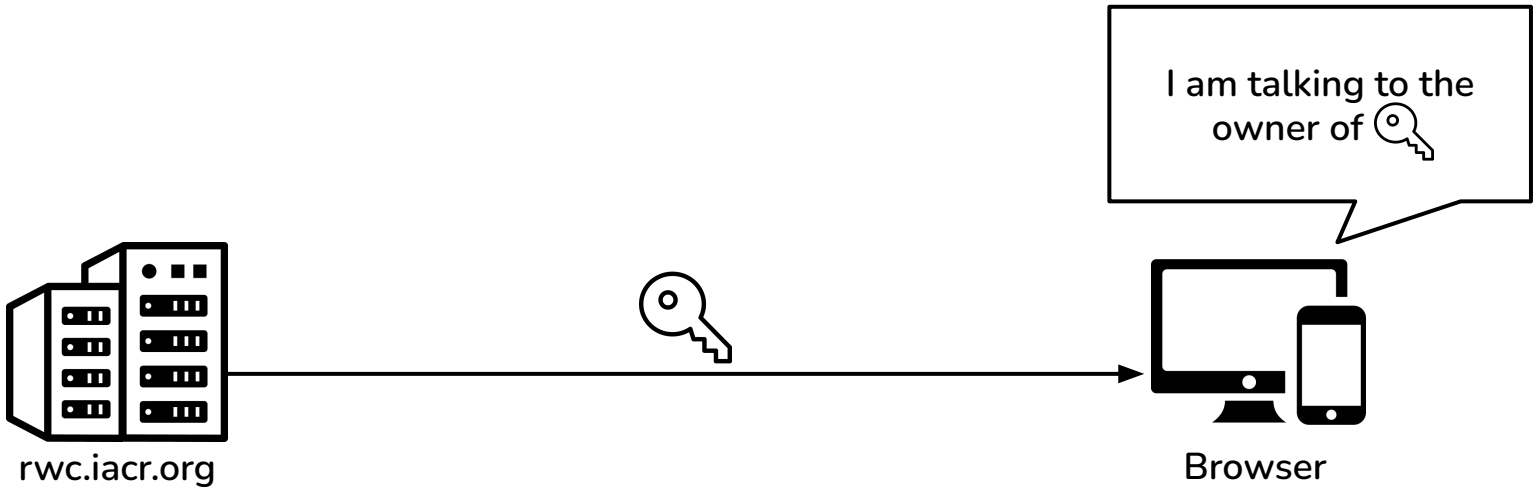

Am I talking to
rwc.iacr.org?
Server
(rwc.iacr.org)
Browser


tcc.iacr.org
DNS Poisoning
MITM attacks
IP Spoofing
BGP hijacking
Am I talking to rwc.iacr.org?
Server (rwc.iacr.org)
Pharming
ARP Spoofing
Browser
And more...

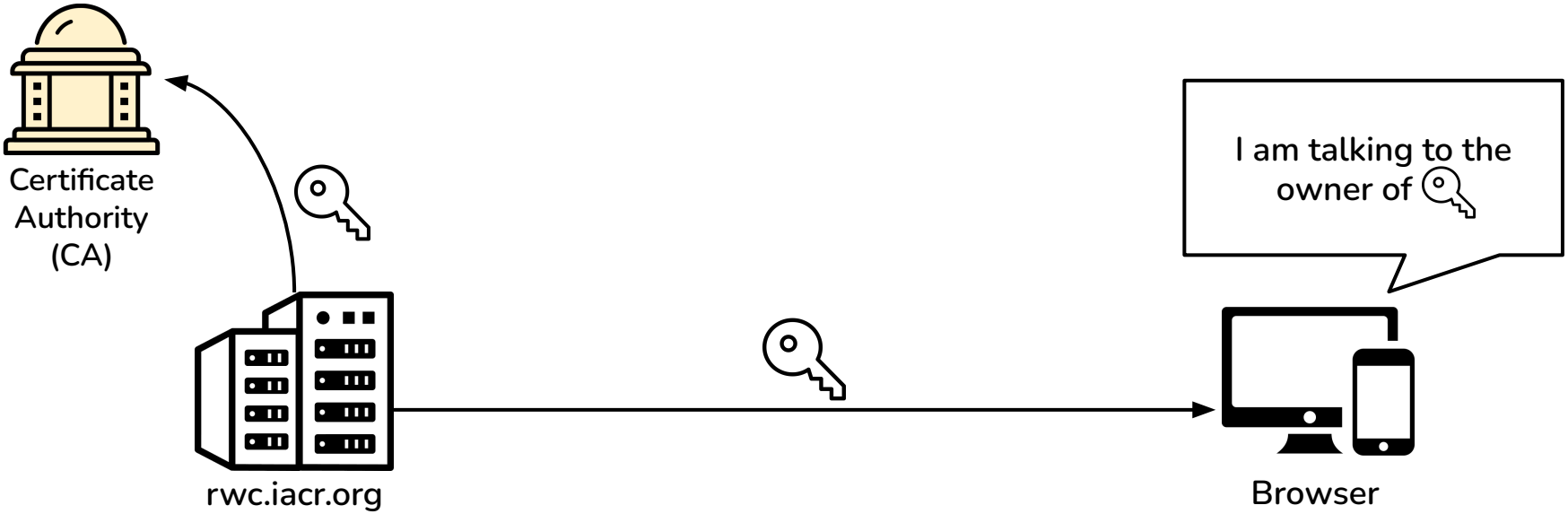
Authentication relies on TLS



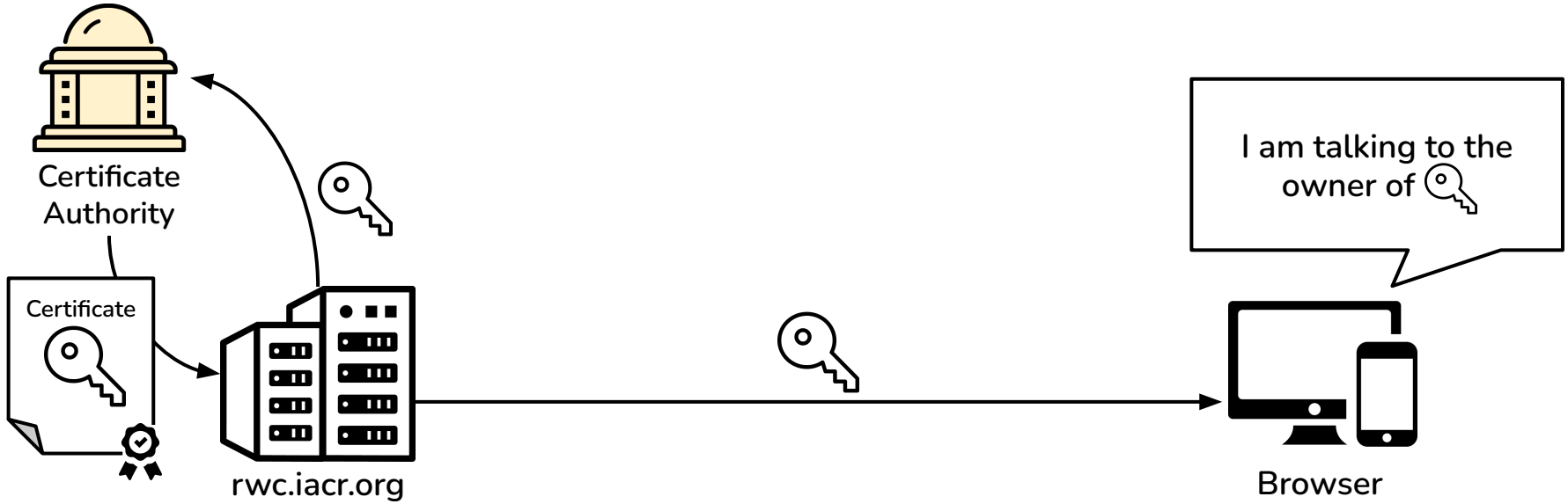
Authentication relies on TLS – partially



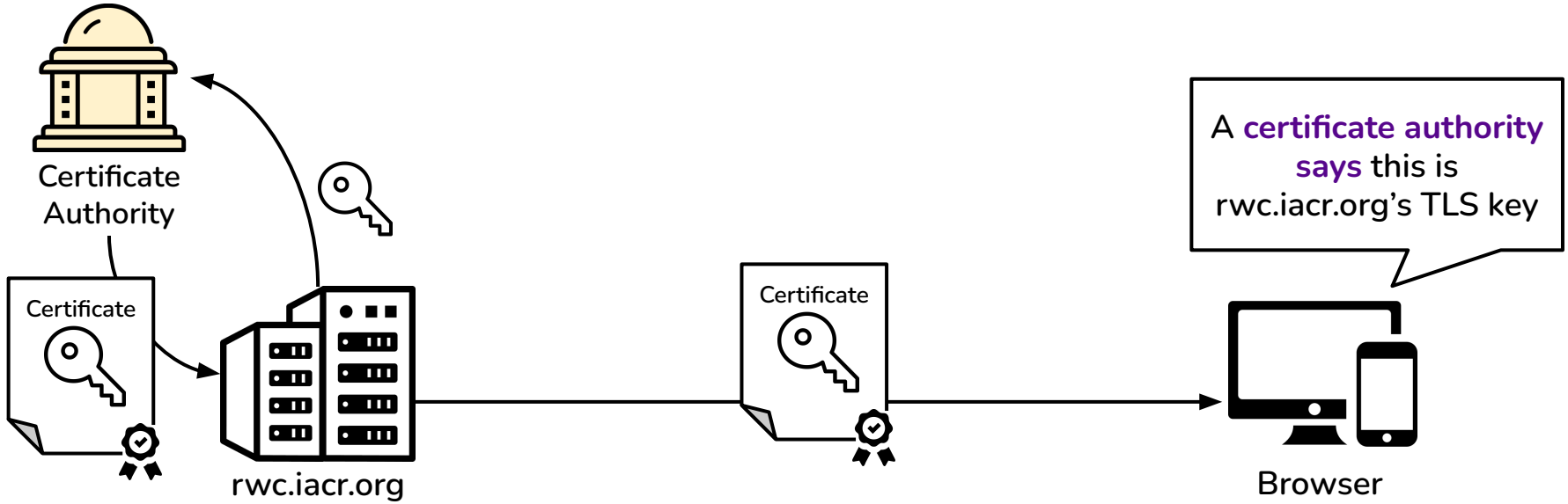
Authentication also relies on CAs



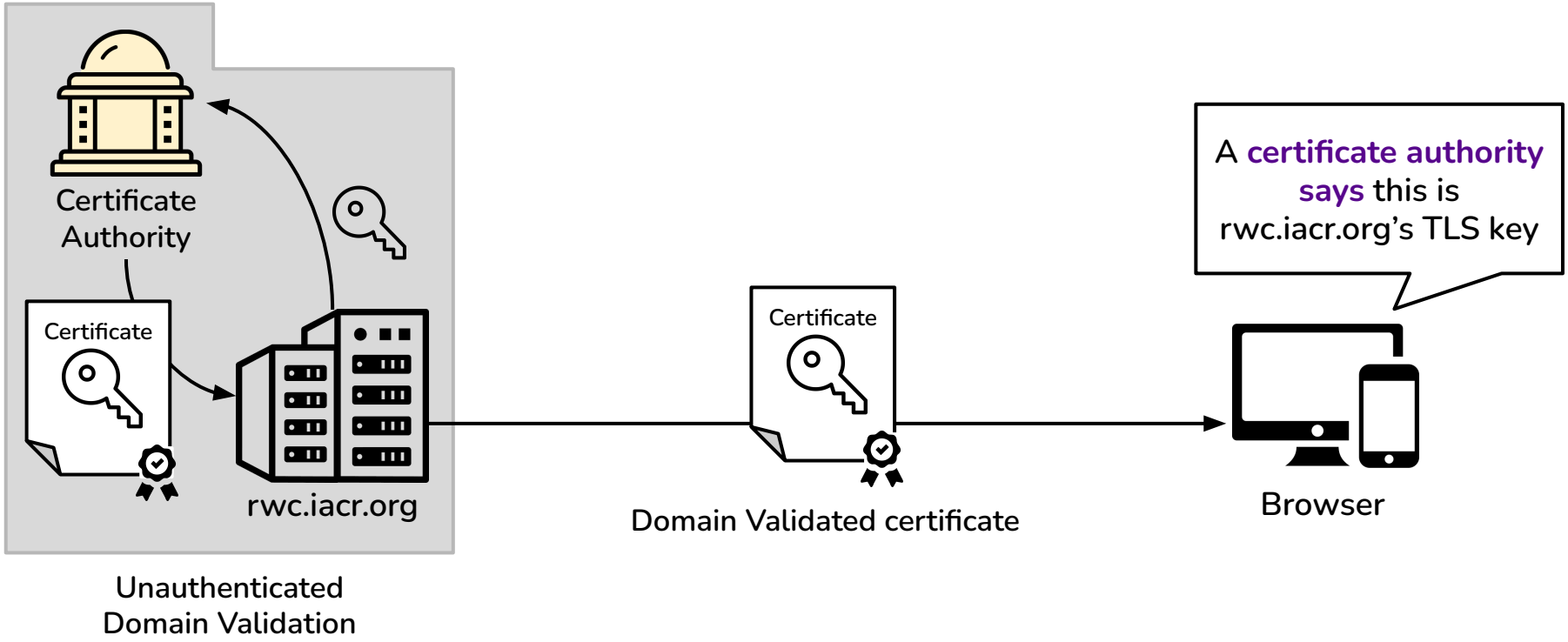
Authentication also relies on CAs

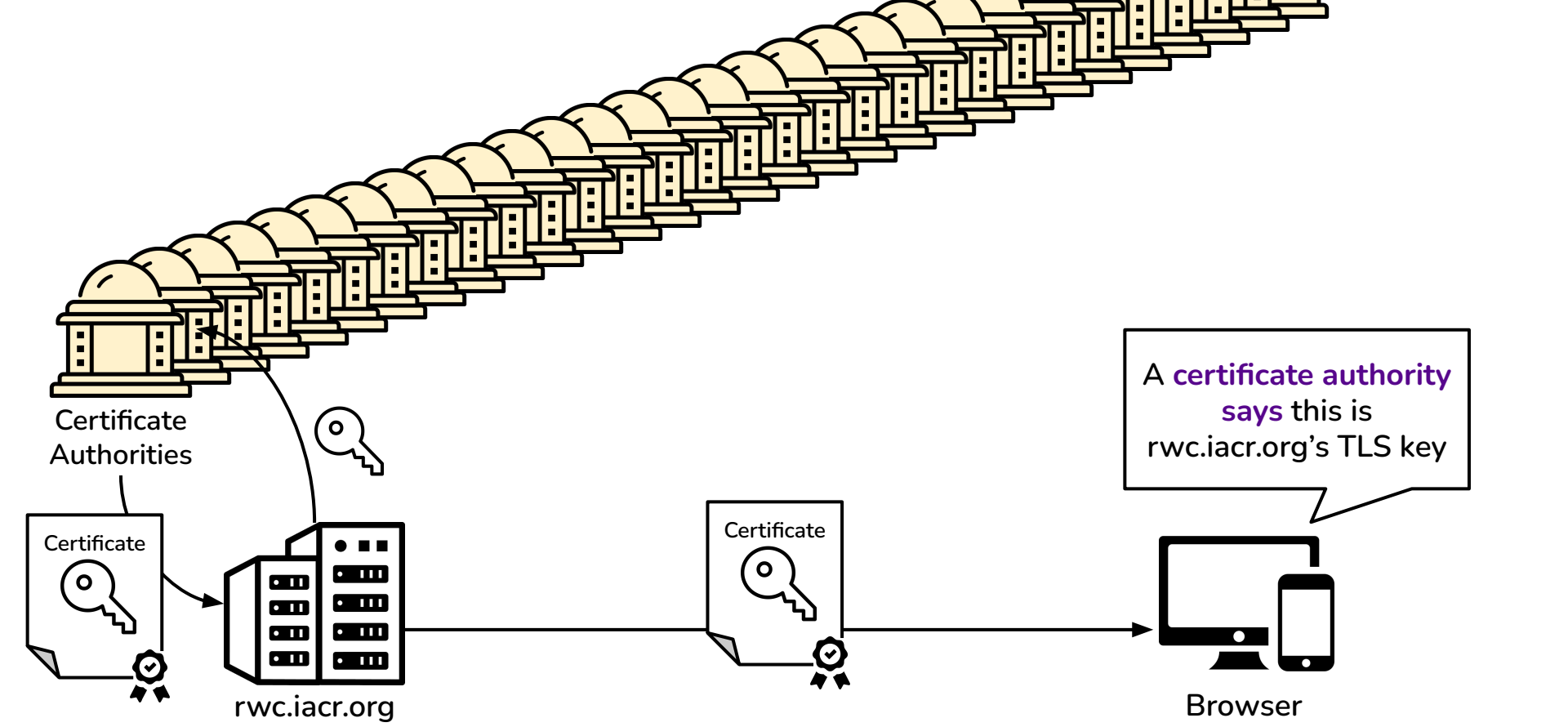


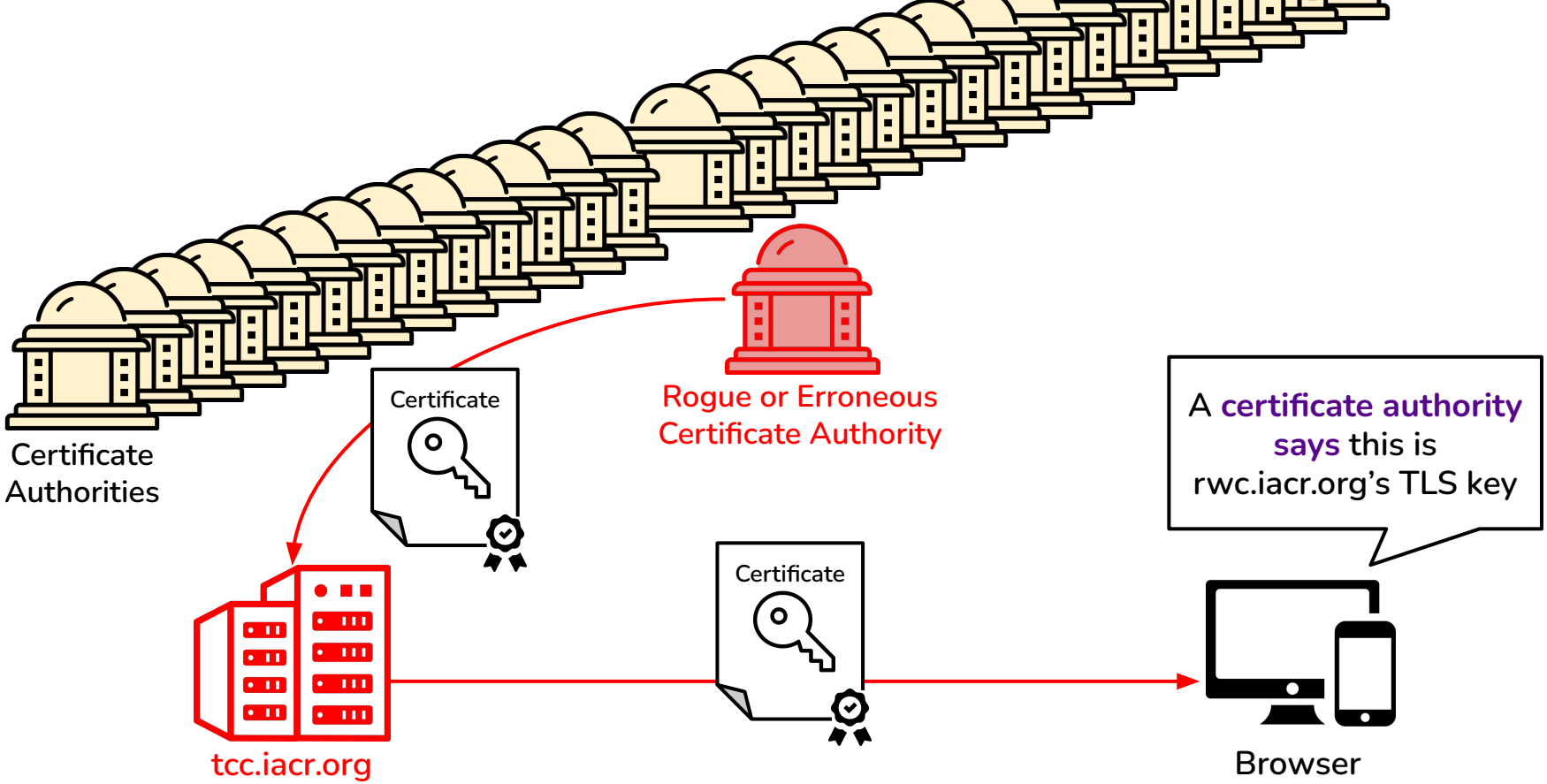
Authentication also relies on CAs



Authentication also relies on CAs




Certificate Authorities
Certificate
rwc.iacr.org
Certificate
A certificate authority says this is rwc.iacr.org's TLS key
Browser


Certificate Authorities
Rogue or Erroneous Certificate Authority
Certificate
Certificate
A certificate authority says this is rwc.iacr.org's TLS key
tcc.iacr.org
Browser

2008 - Thawte

Mike Zusman registers the email address sslcertificates@live.com and uses it to obtain a rogue SSL certificate from Thawte for Microsoft's live.com.

2009 - Null prefix attack

Moxie Marlinspike gets a certificate from ipsCA for a DNS name containing a null character. Although ipsCA correctly validates the DNS name as belonging to Moxie's domain, the null character tricks some clients into thinking the certificate belongs to www.paypal.com, enabling impersonation of PayPal.

2011 - TurkTrust

TurkTrust accidentally issues two intermediate CA certificates to subscribers. These intermediate certificates can be used to forge certificates for any domain on the Internet. Sixteen months later, one of them is used to forge a certificate for google.com.

Using BGP to Acquire Bogus TLS Certificates

Henry Birge-Lee[1], Yixin Sun[1], Annie Edmundson[1], Jennifer Rexford[1], and Prateek Mittal[1]
{birgelee, yixins, annee, jrex, pmittal}@princeton.edu

[1]Princeton University

2014 - NICCA

The National Informatics Centre (NIC) of India, a subordinate CA of the Indian Controller of Certifying Authorities (India CCA), issues rogue certificates for Google and Yahoo domains. NIC claims that their issuance process was compromised and that only four certificates were misissued. However, Google is aware of misissued certificates not reported by NIC, so it can only be assumed that the scope of the breach is unknown.

2016 - StartCom

Thijs Alkemade discovers that StartCom's brand new automated issuance API suffers from numerous flaws, including flaws that had previously been discovered and fixed by other CAs, that would allow attackers to obtain certificates for domains they don't control.

A Post Mortem on the Iranian DigiNotar Attack

SEPTEMBER 13, 2011

by Eva Galperin, Seth Schoen and Peter Eckersley

More facts have recently come to light about the compromise of the DigiNotar Certificate Authority, which appears to have enabled Iranian hackers to launch successful man-in-the-middle attacks against hundreds of thousands of Internet users inside and outside of Iran.

Mitigating the Hetzner/Linode XMPP.ru MitM interception incident

(If you just want some recommendations for what to do, skip down to the Recommendations section below.)

Today, the operator of jabber.ru and xmpp.ru reported that their service had been successfully subject to a man-in-the-middle attack via a combination of

- their hosting providers, Hetzner and Linode, intercepting traffic to their machines; and
- the unauthorized issuance of a Domain Validation certificate for their service by an attacker.

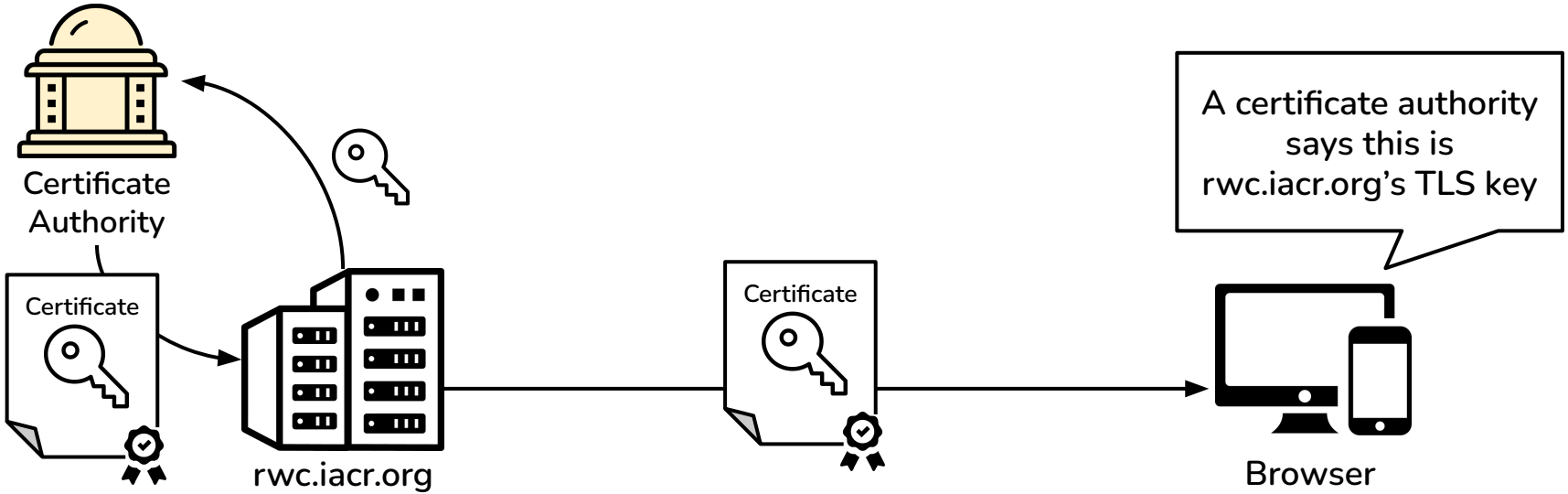
Keeping Positive – Obtaining Arbitrary Wildcard SSL Certificates from Comodo via Dangling Markup Injection

December 2, 2015

Duplicate Signature Key Selection Attack in Let's Encrypt

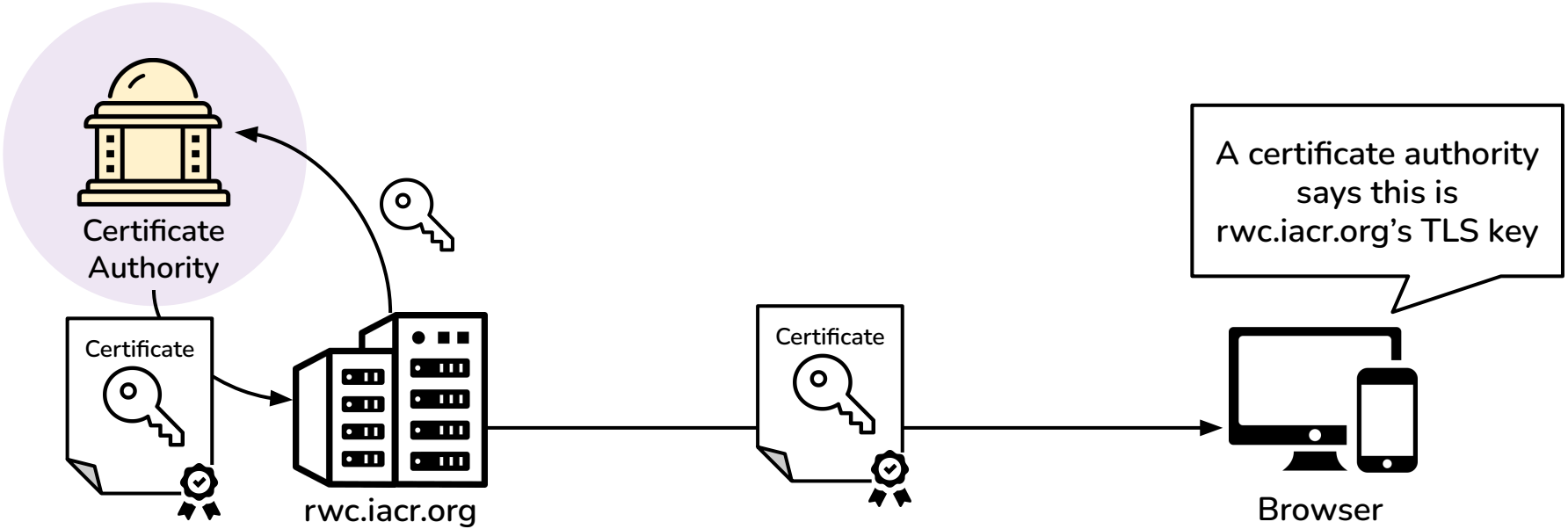
Existing proposals require modifying infrastructure

or are purely reactive.



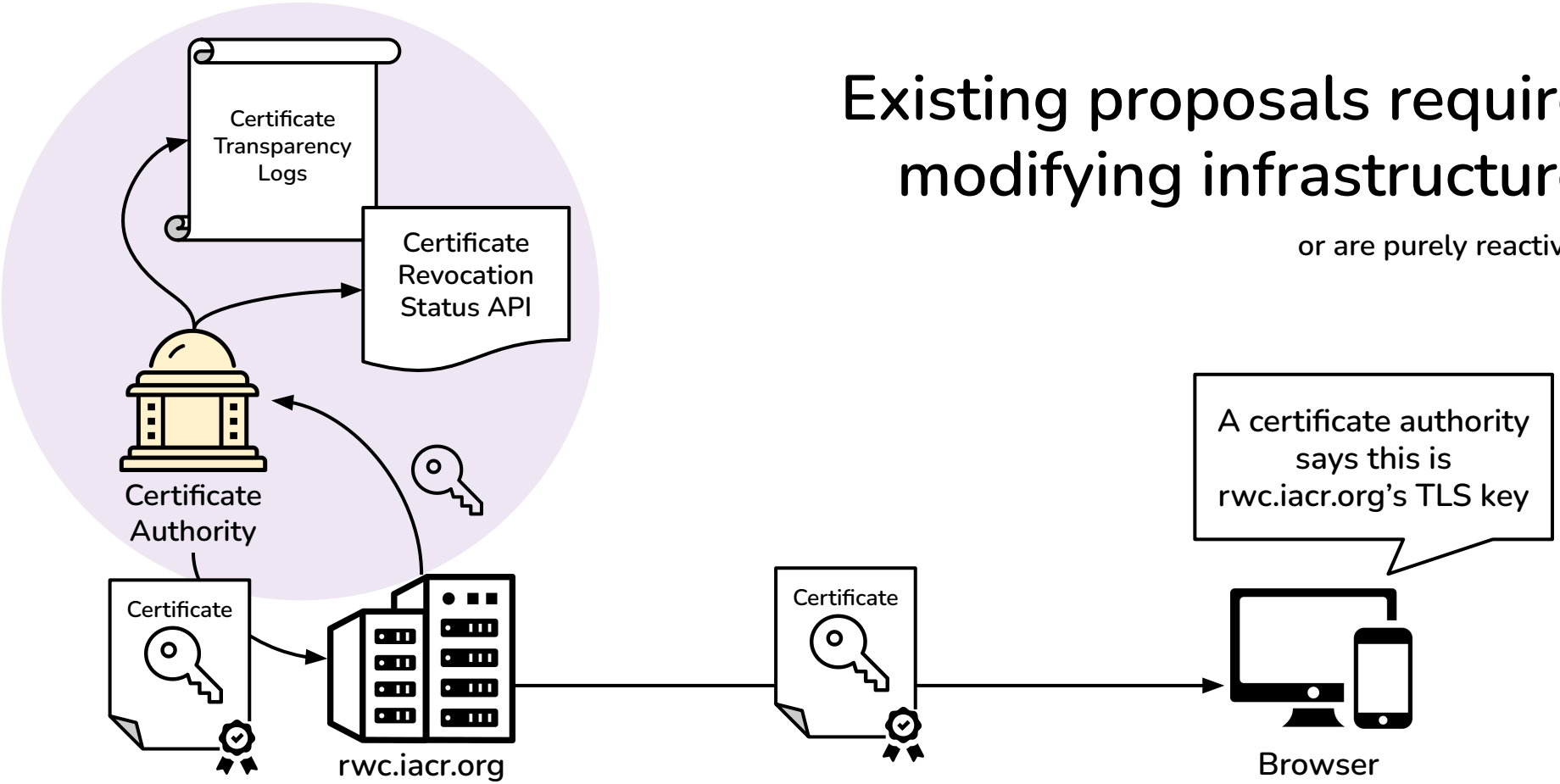
Existing proposals require modifying infrastructure

or are purely reactive.

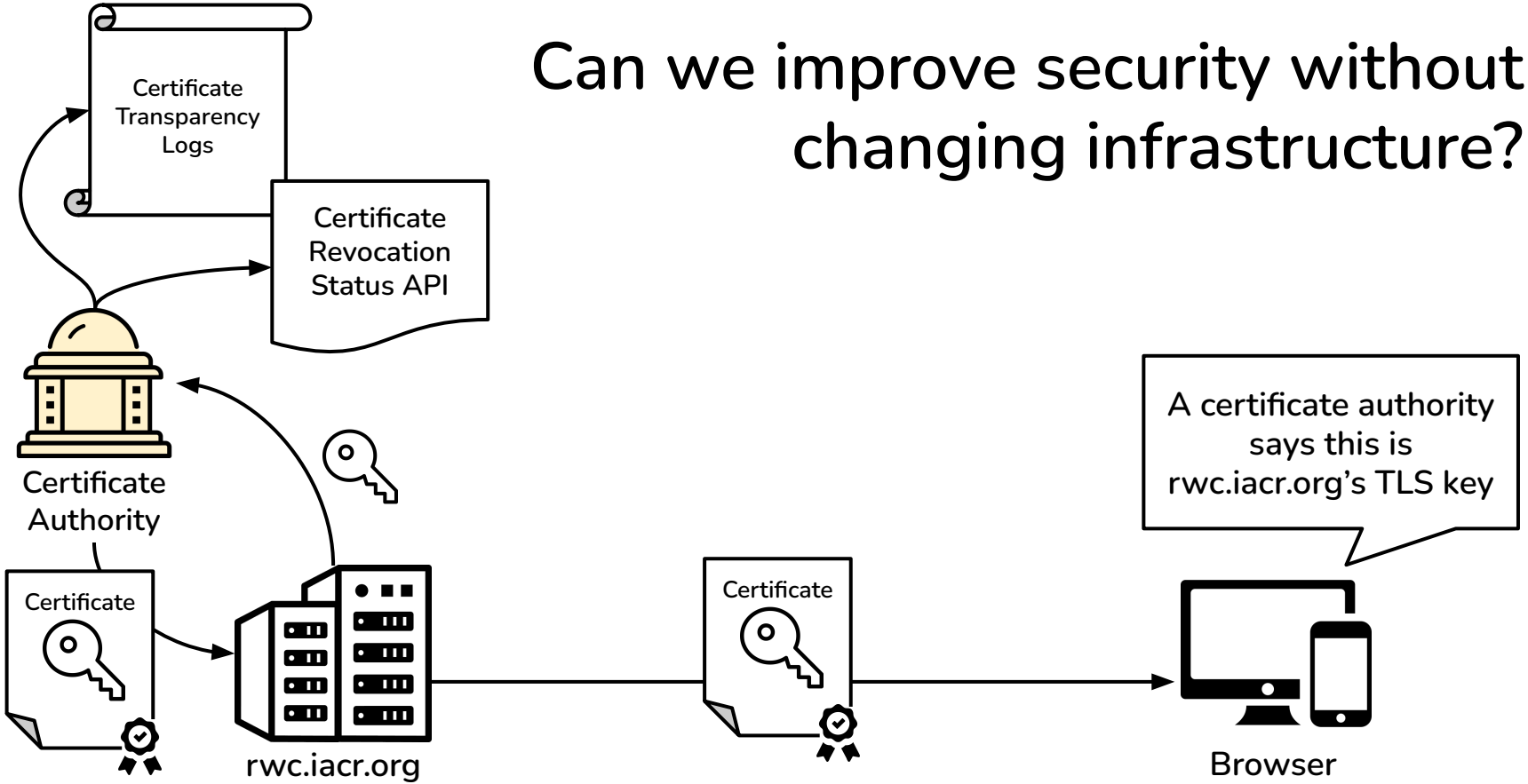


Existing proposals require modifying infrastructure

or are purely reactive.



Can we improve security without changing infrastructure?

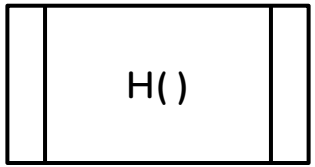


Key tool: succinct proofs

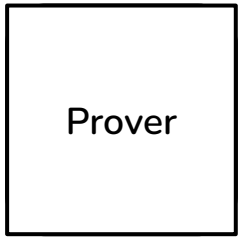
(probabilistic proofs, zero-knowledge proofs, SNARKs, SNARGs, PCPs)

Key tool: succinct proofs

(probabilistic proofs, zero-knowledge proofs, SNARKs, SNARGs, PCPs)

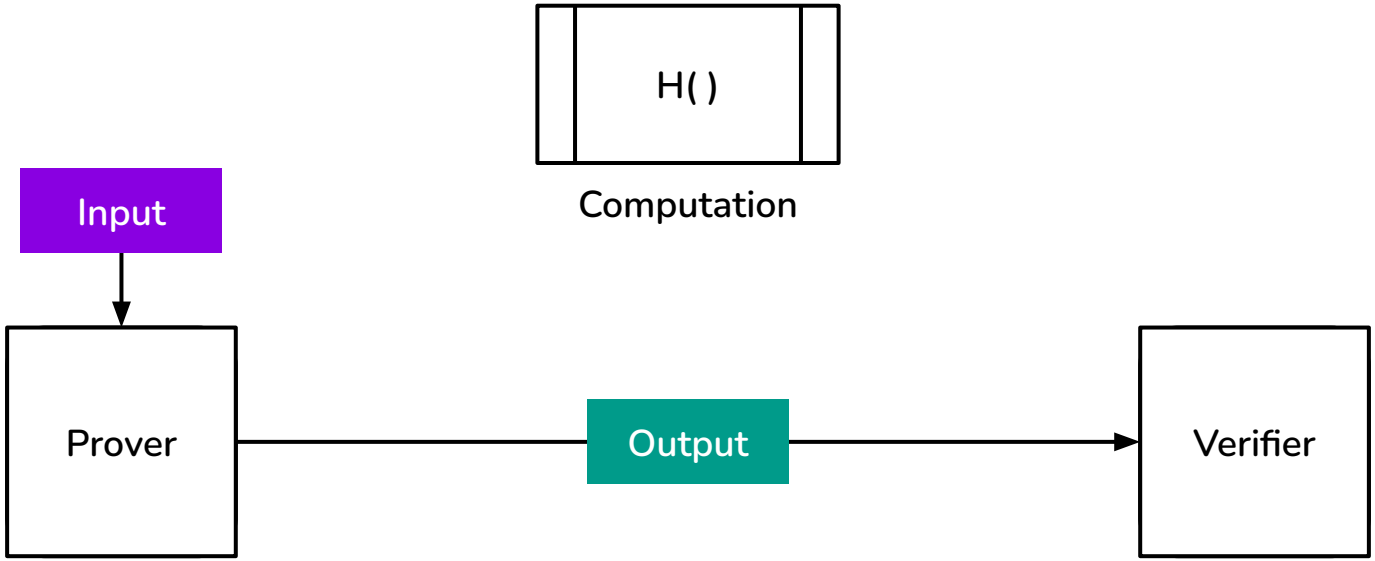


Computation



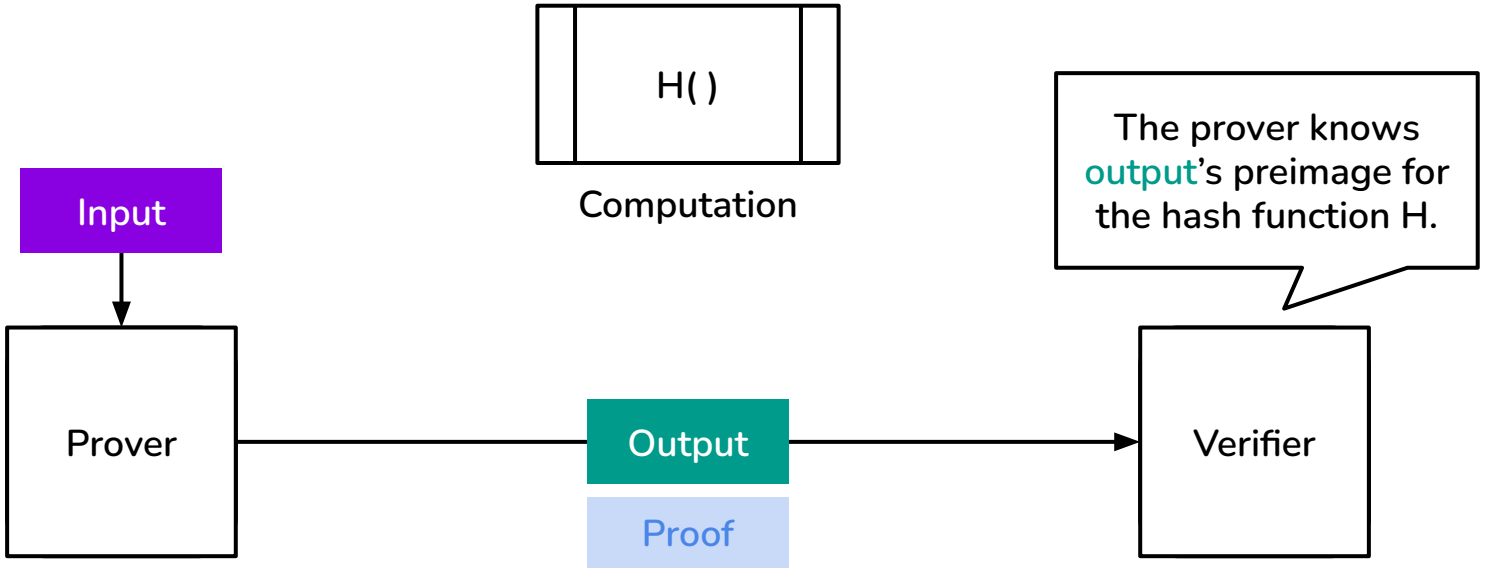
Key tool: succinct proofs

(probabilistic proofs, zero-knowledge proofs, SNARKs, SNARGs, PCPs)



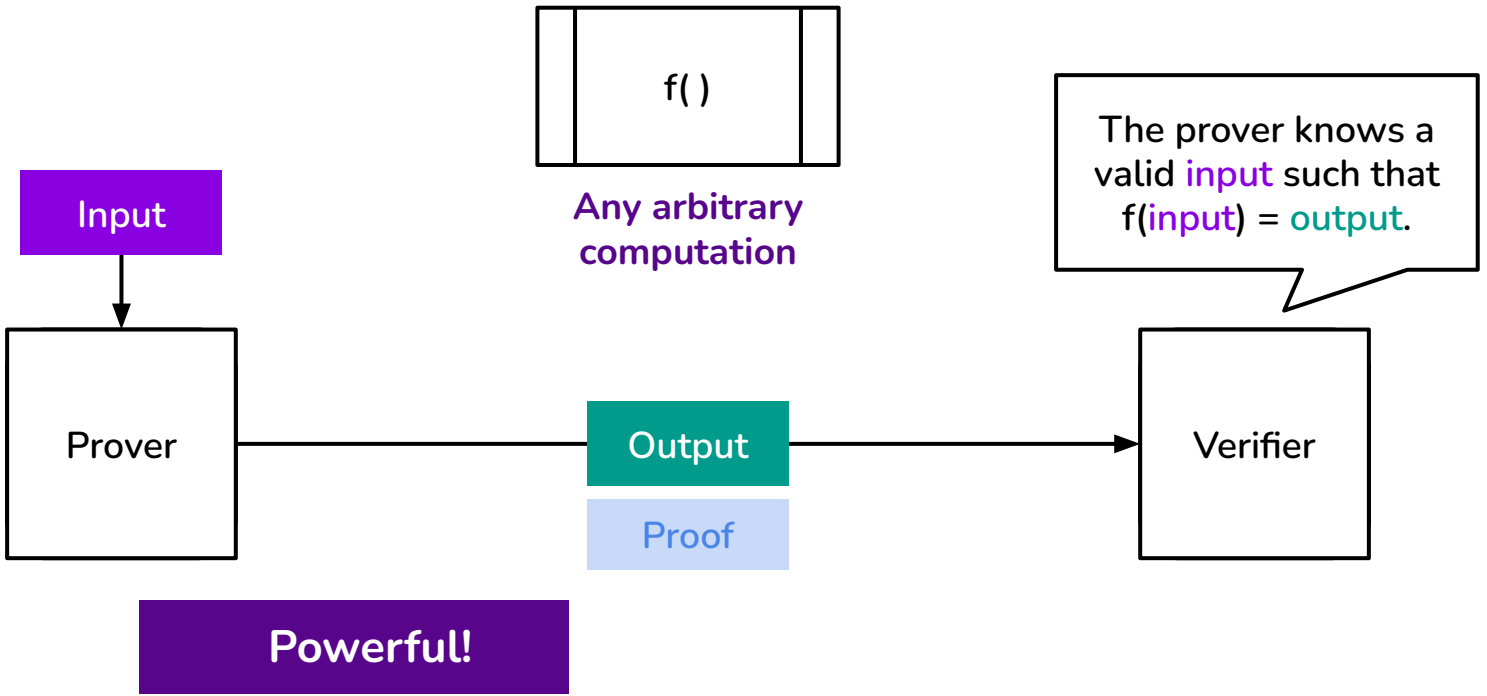
Key tool: succinct proofs

(probabilistic proofs, zero-knowledge proofs, SNARKs, SNARGs, PCPs)



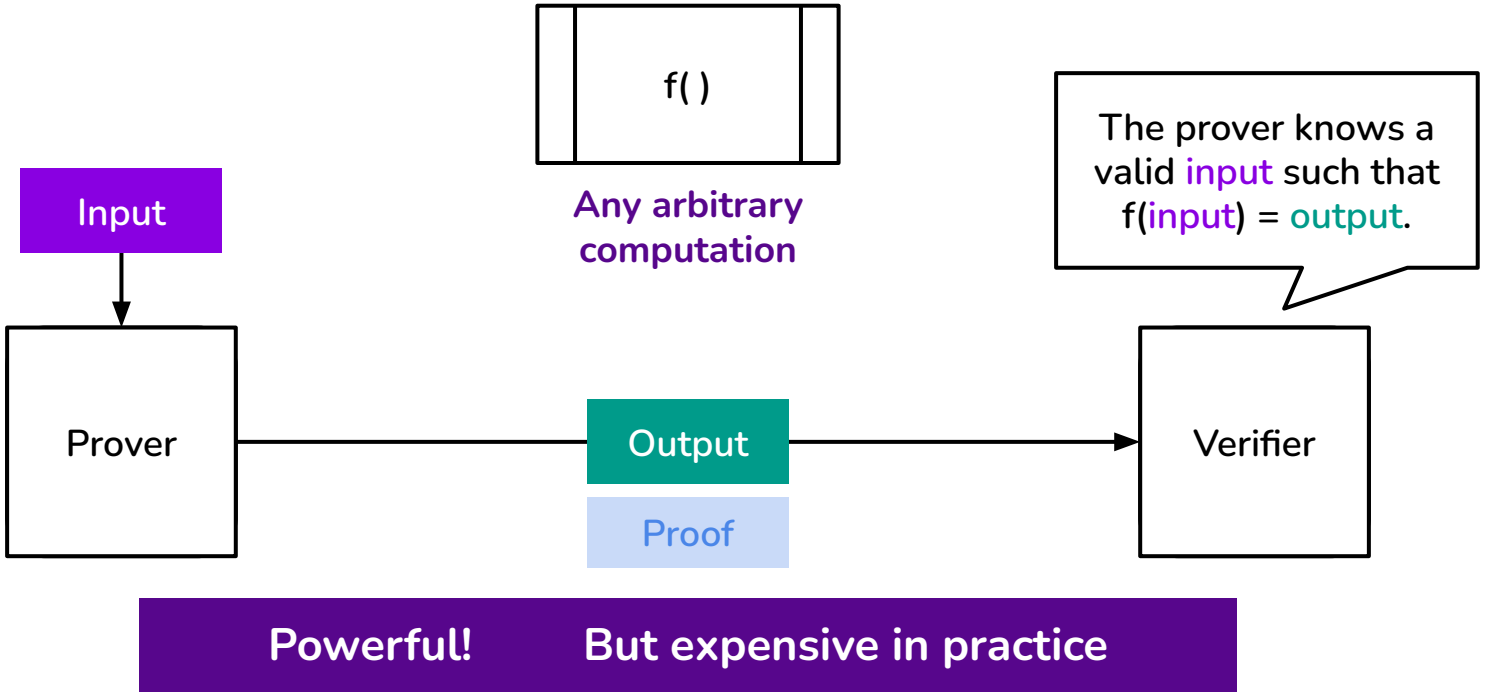
Key tool: succinct proofs

(probabilistic proofs, zero-knowledge proofs, SNARKs, SNARGs, PCPs)

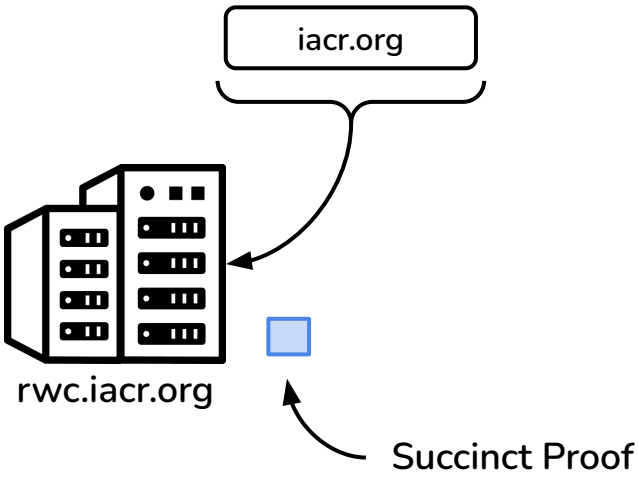


Key tool: succinct proofs

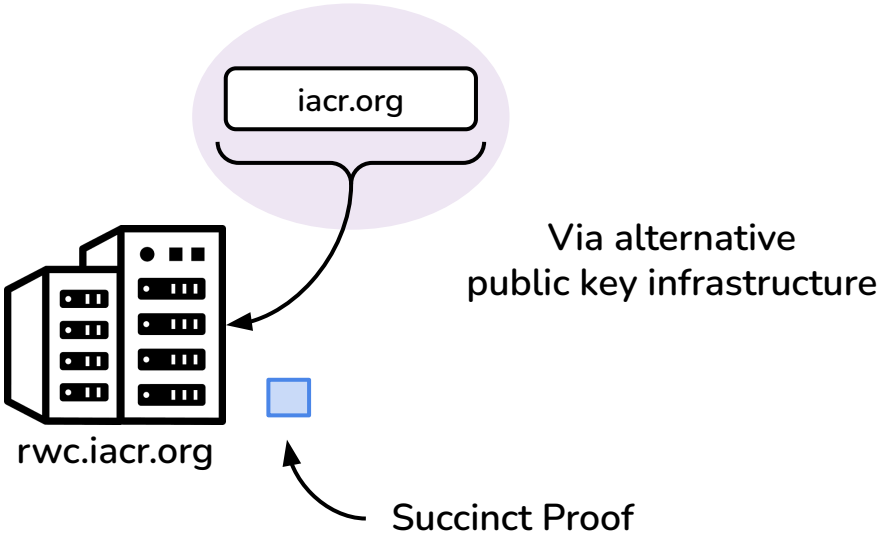
(probabilistic proofs, zero-knowledge proofs, SNARKs, SNARGs, PCPs)



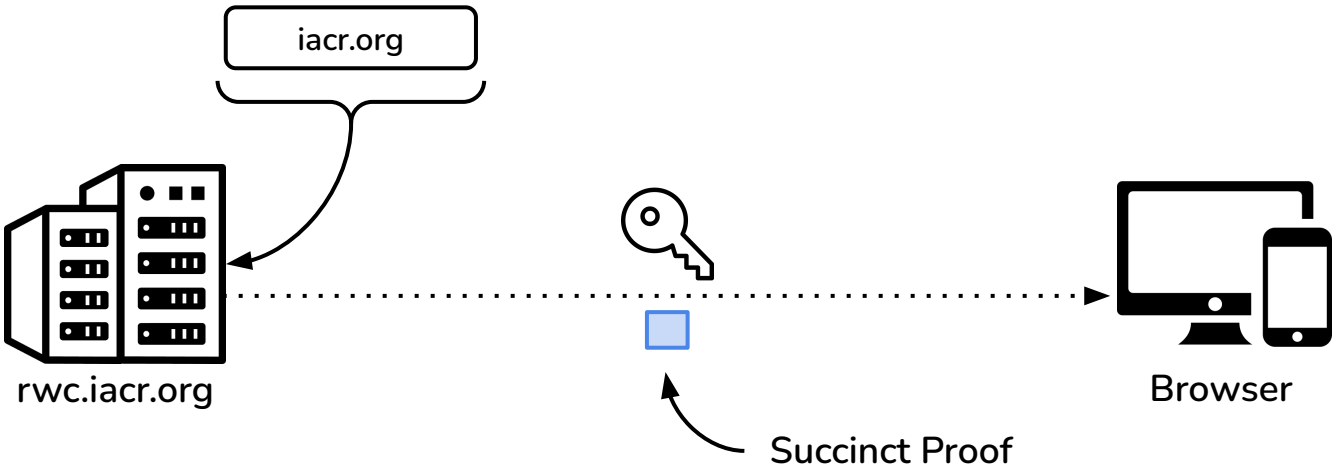
Our work, NOPE, in a nutshell



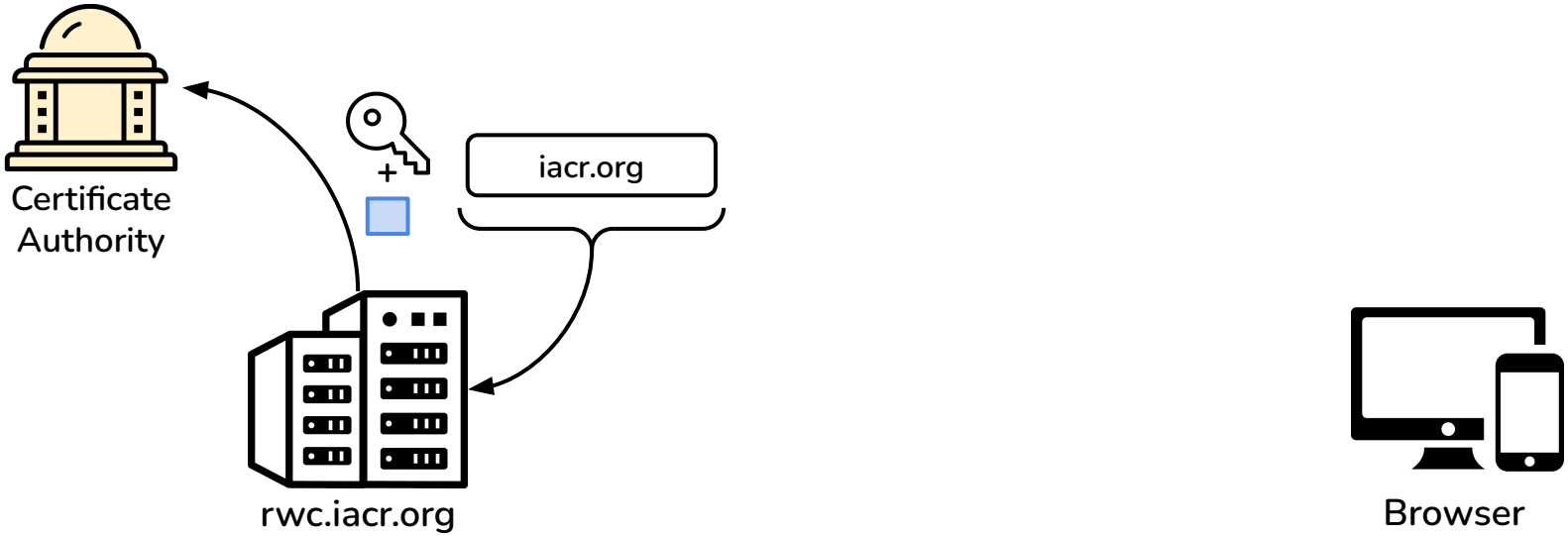
Our work, NOPE, in a nutshell



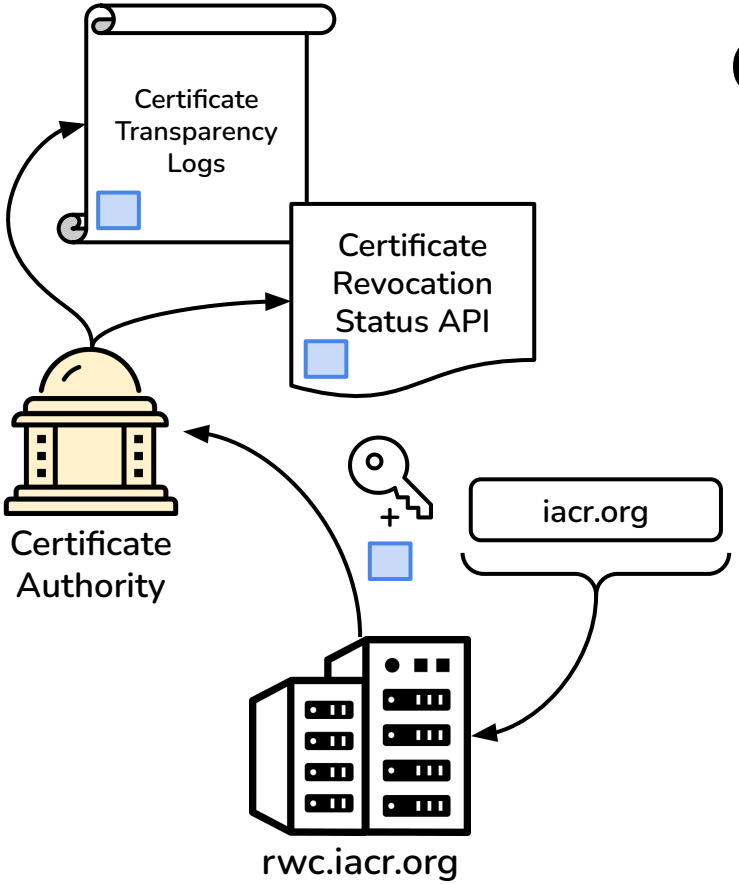
Our work, NOPE, in a nutshell

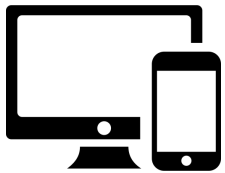


Our work, NOPE, in a nutshell

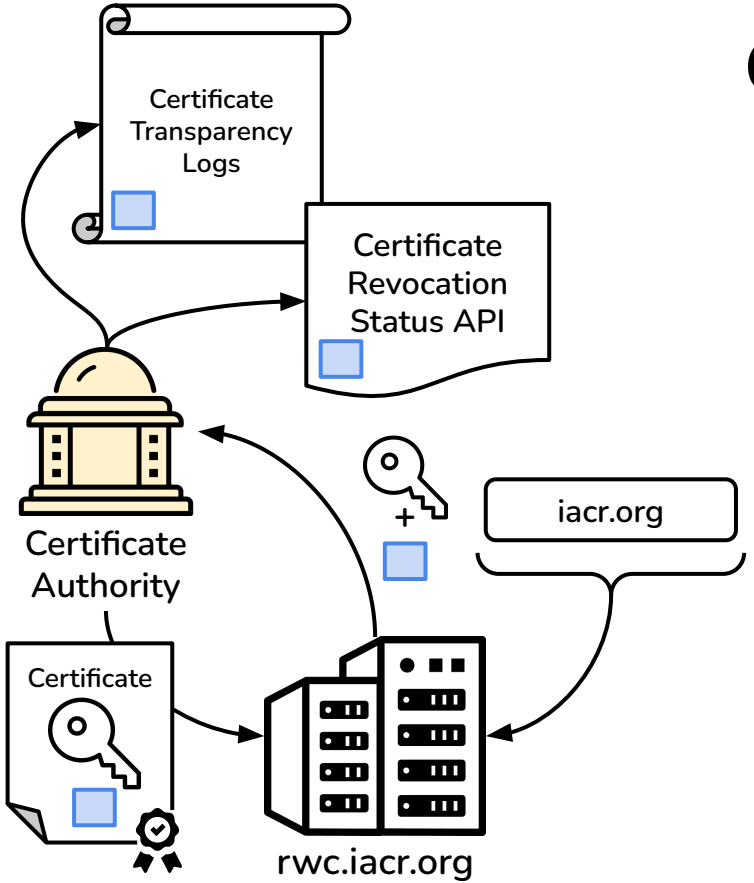


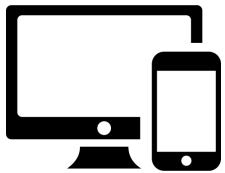
Our work, NOPE, in a nutshell



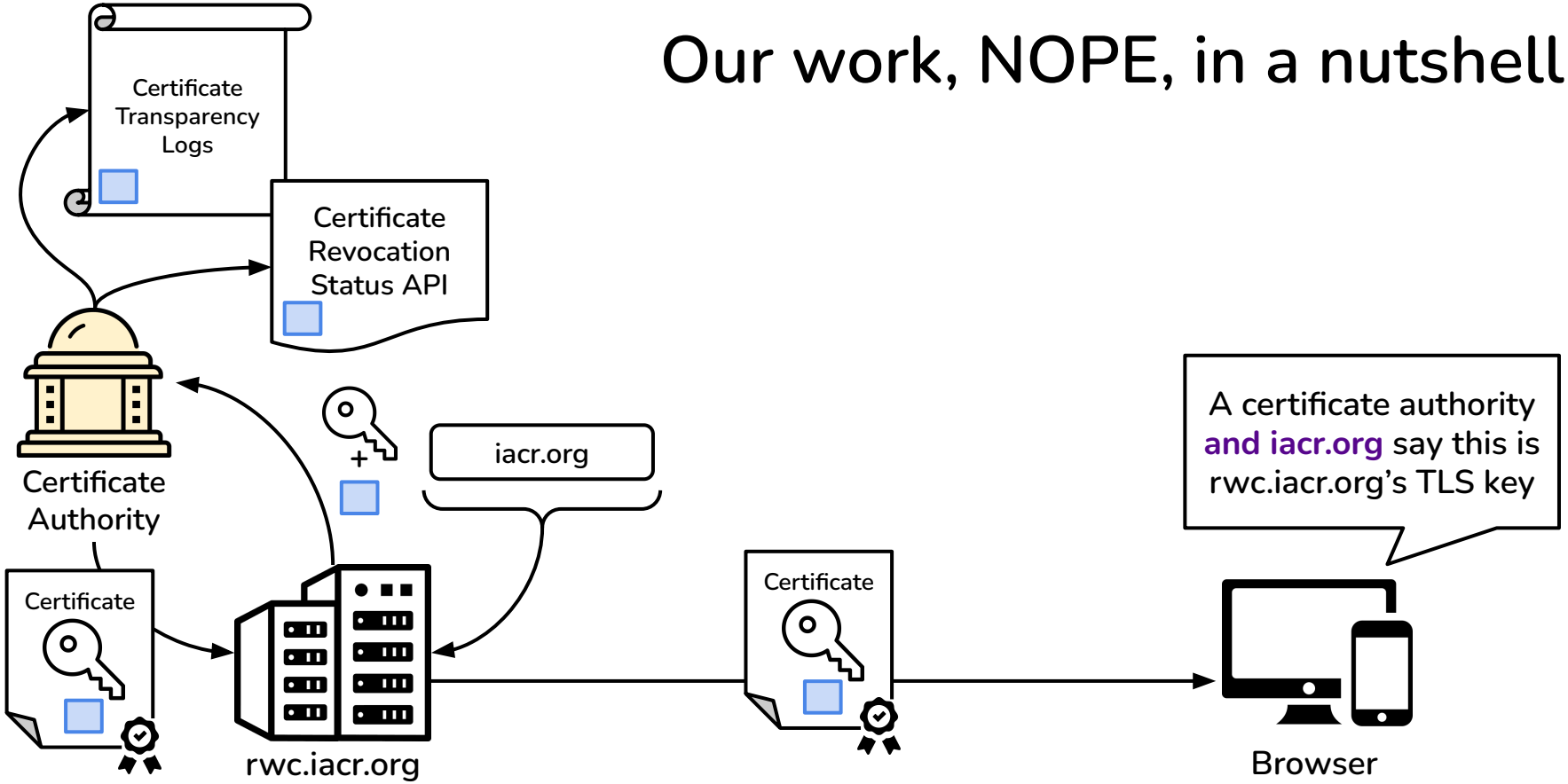


Our work, NOPE, in a nutshell





Our work, NOPE, in a nutshell



Welcome to NOPE

NOPE is a research project focused on improving server authentication by reducing dependence on certification authorities

Instead of solely relying on CAs, NOPE introduces a new method that uses succinct proofs, such as zero-knowledge proof
public key to a domain.

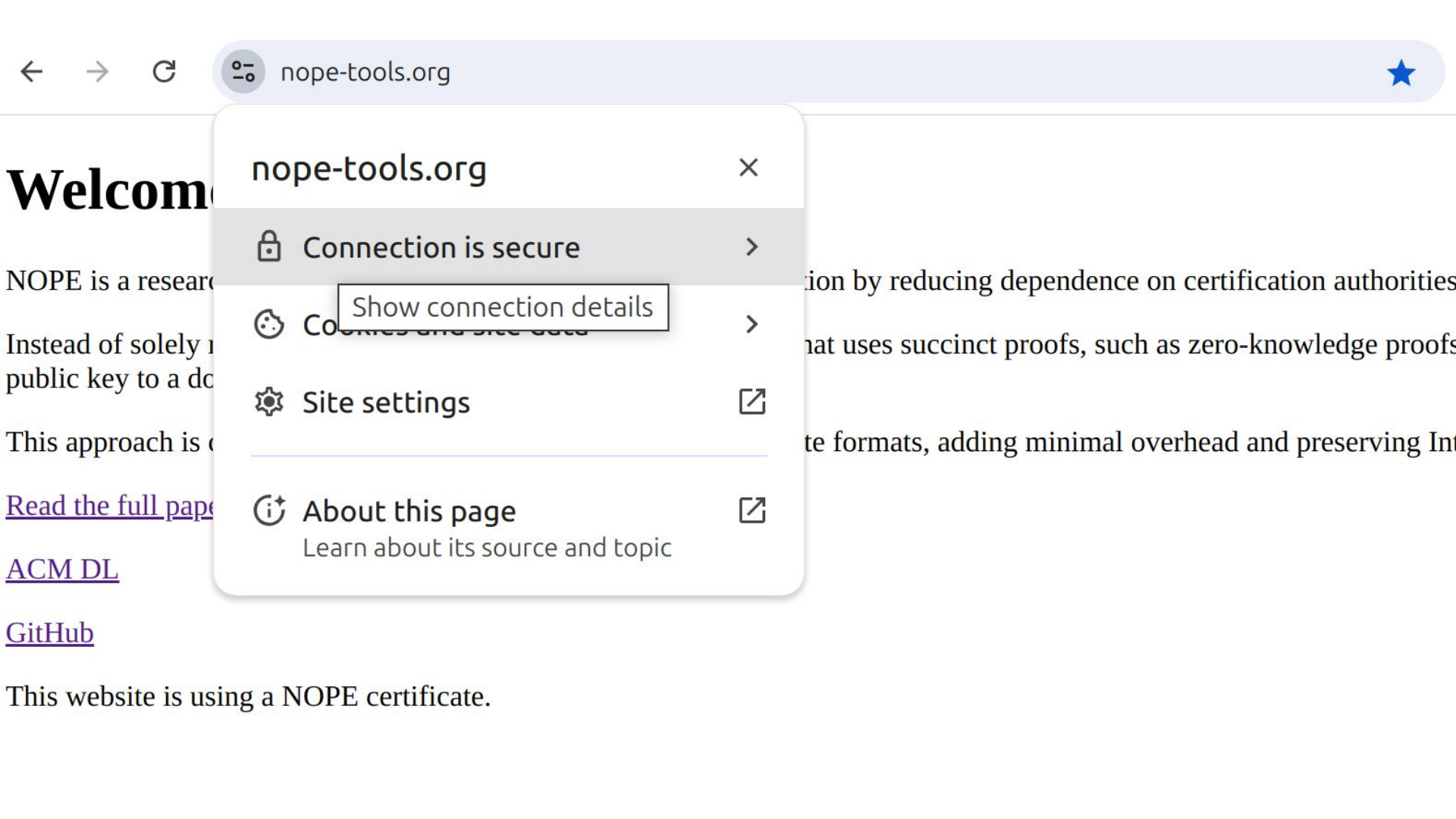
This approach is compatible with existing TLS servers and certificate formats, adding minimal overhead and preserving In

Read the full paper here.

ACM DL

GitHub

This website is using a NOPE certificate.



Welcom

NOPE is a researc ion by reducing dependence on certification authorities

Instead of solely r at uses succinct proofs, such as zero-knowledge proofs public key to a dc

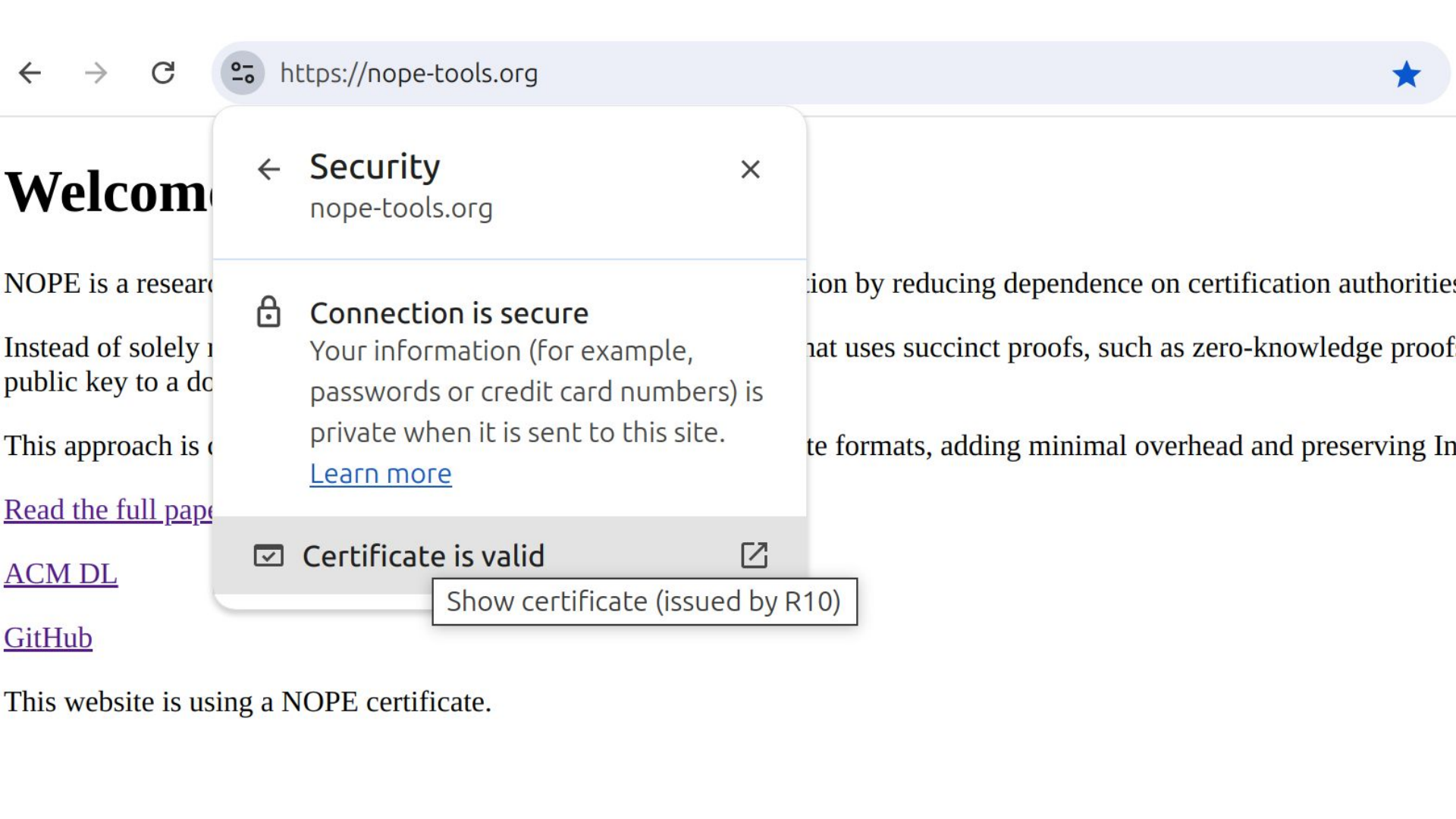
This approach is c te formats, adding minimal overhead and preserving Int

Read the full pape

ACM DL

GitHub

This website is using a NOPE certificate.



Welcom

NOPE is a researc ion by reducing dependence on certification authorities

Instead of solely r hat uses succinct proofs, such as zero-knowledge proof public key to a dc

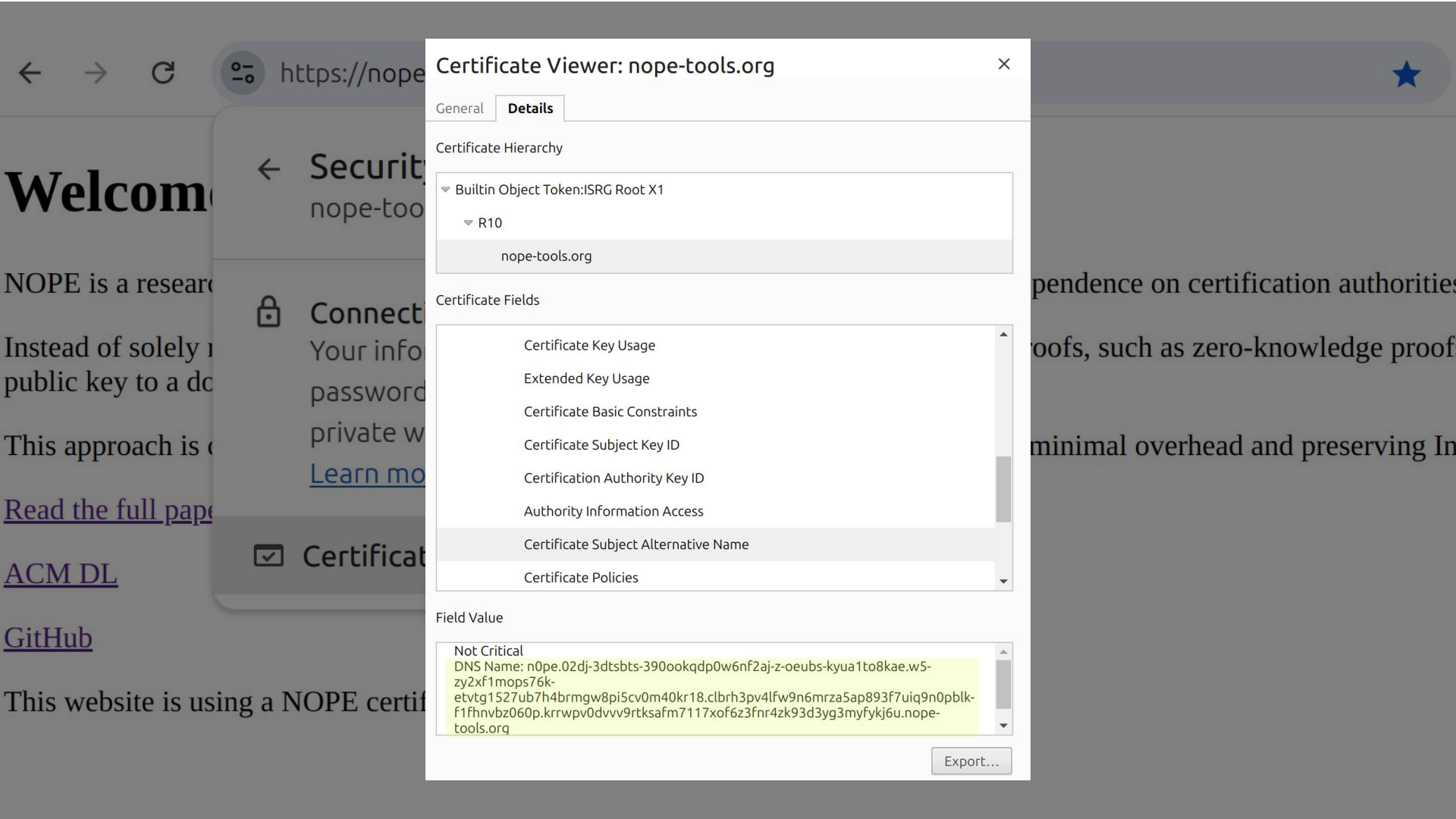
This approach is c te formats, adding minimal overhead and preserving In

Read the full pape

ACM DL

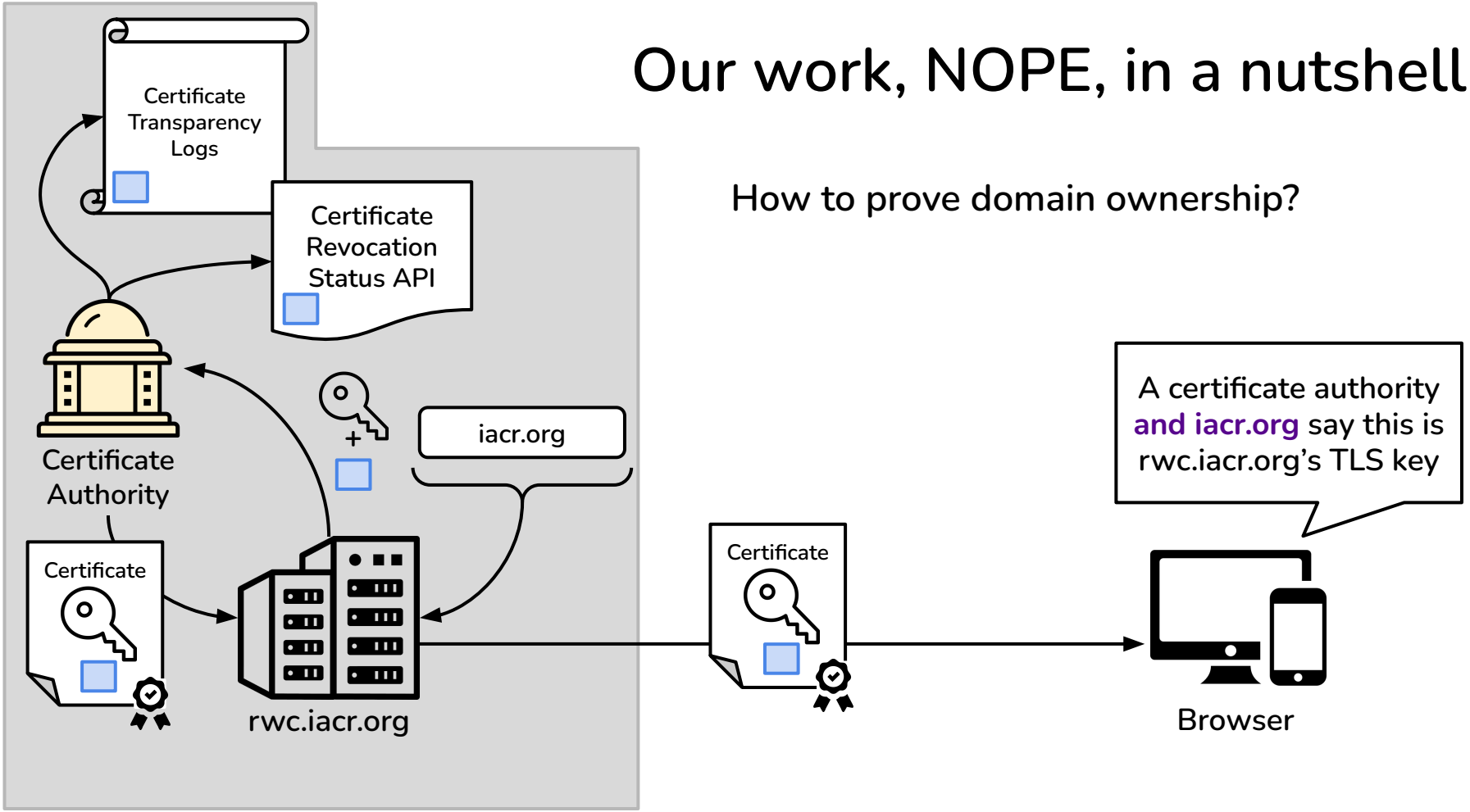
GitHub

This website is using a NOPE certificate.


Certificate Viewer: nope-tools.org
General
Details
Certificate Hierarchy
Builtin Object Token:ISRG Root X1
R10
nope-tools.org
Certificate Fields
Certificate Key Usage
Extended Key Usage
Certificate Basic Constraints
Certificate Subject Key ID
Certification Authority Key ID
Authority Information Access
Certificate Subject Alternative Name
Certificate Policies
Field Value
Not Critical
DNS Name: n0pe.02dj-3dtsbts-390ookqdp0w6nf2aj-z-oeubs-kyua1to8kae.w5-zy2xf1mops76k-etvtg1527ub7h4brmgw8pi5cv0m40kr18.clbrh3pv4lfw9n6mrza5ap893f7uiq9n0pblk-f1fhnvbz060p.krrwpv0dvvv9rtksafm7117xof6z3fnr4zk93d3yg3myfykj6u.nope-tools.org
Export...

Our work, NOPE, in a nutshell

How to prove domain ownership?



There is a lesser used PKI, DNSSEC

There is a **lesser used** PKI, DNSSEC

Common objections

DNSSEC is used by fewer than 7% of all domains!

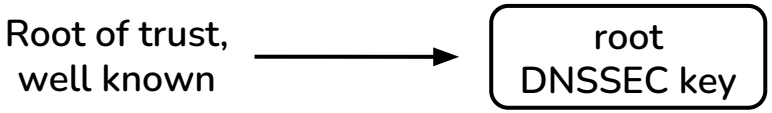
DNSSEC includes signatures with insecure schemes and parameters!

DNSSEC transport and validation is unreliable!

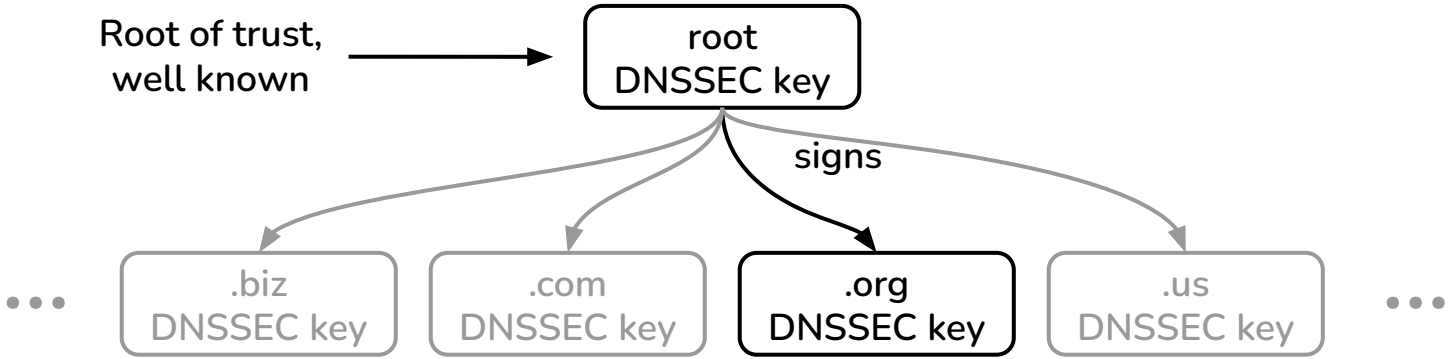
There is a **lesser used** PKI, DNSSEC

Common objections	Yes, however...
DNSSEC is used by fewer than 7% of all domains!	A domain owner can deploy DNSSEC for their own domain.
DNSSEC includes signatures with insecure schemes and parameters!	This was the case a decade ago, but not anymore.
DNSSEC transport and validation is unreliable!	NOPE does not require transporting DNSSEC records to clients.

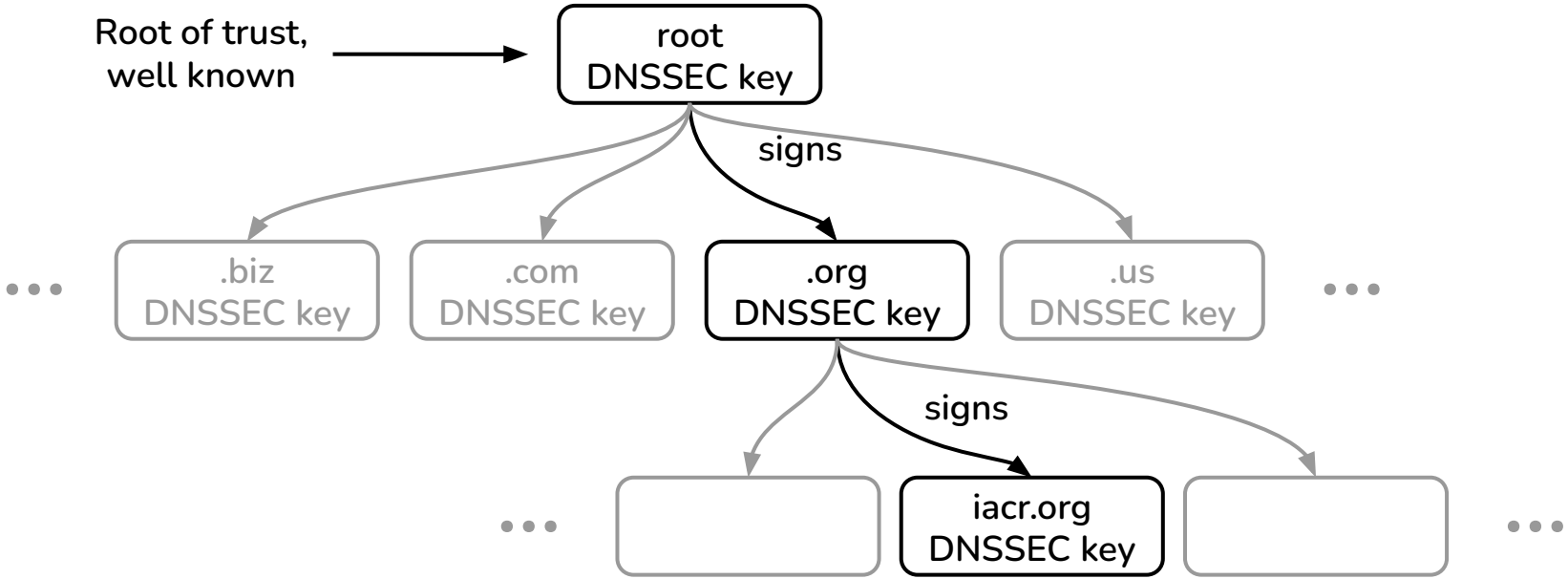
DNSSEC from 30,000 feet



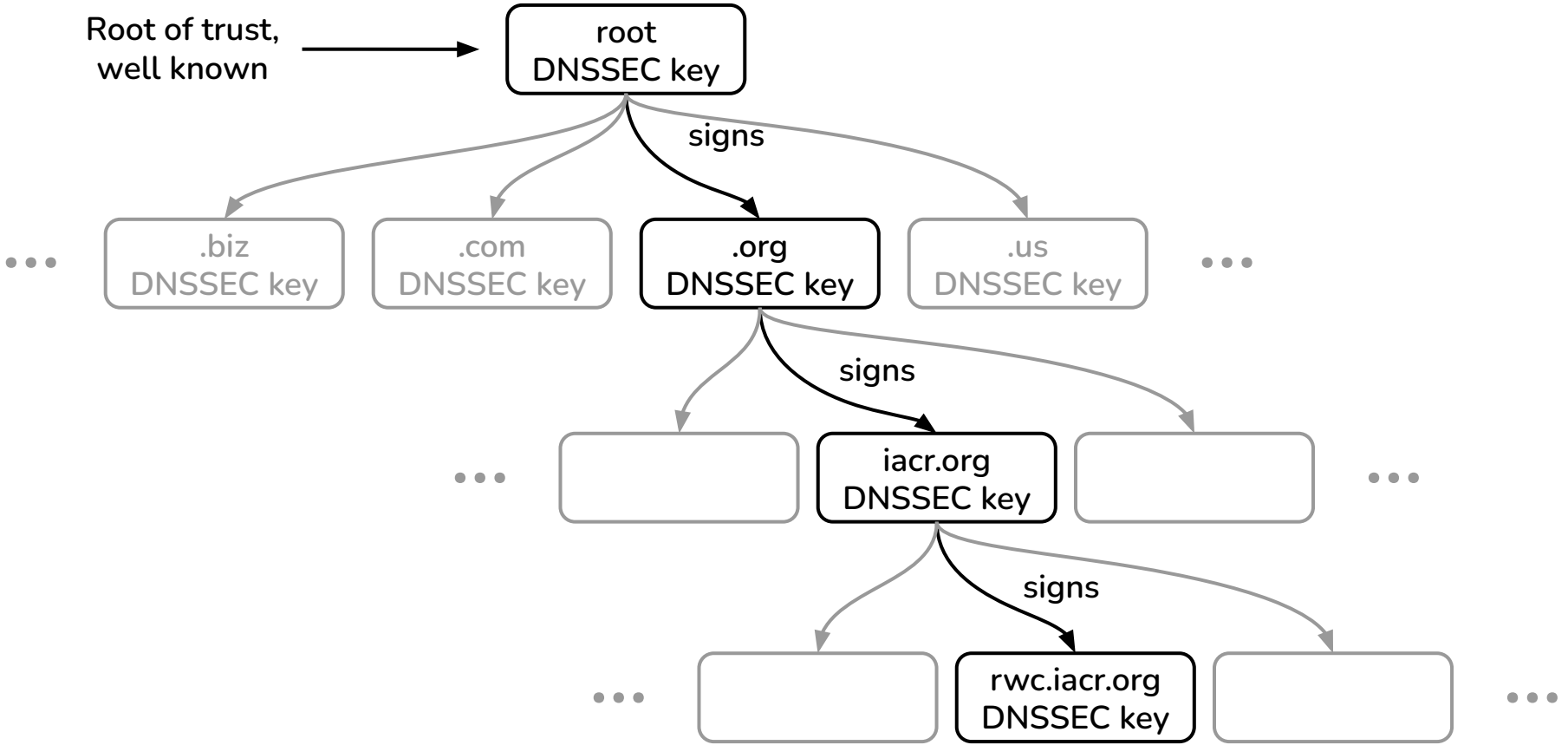
DNSSEC from 30,000 feet



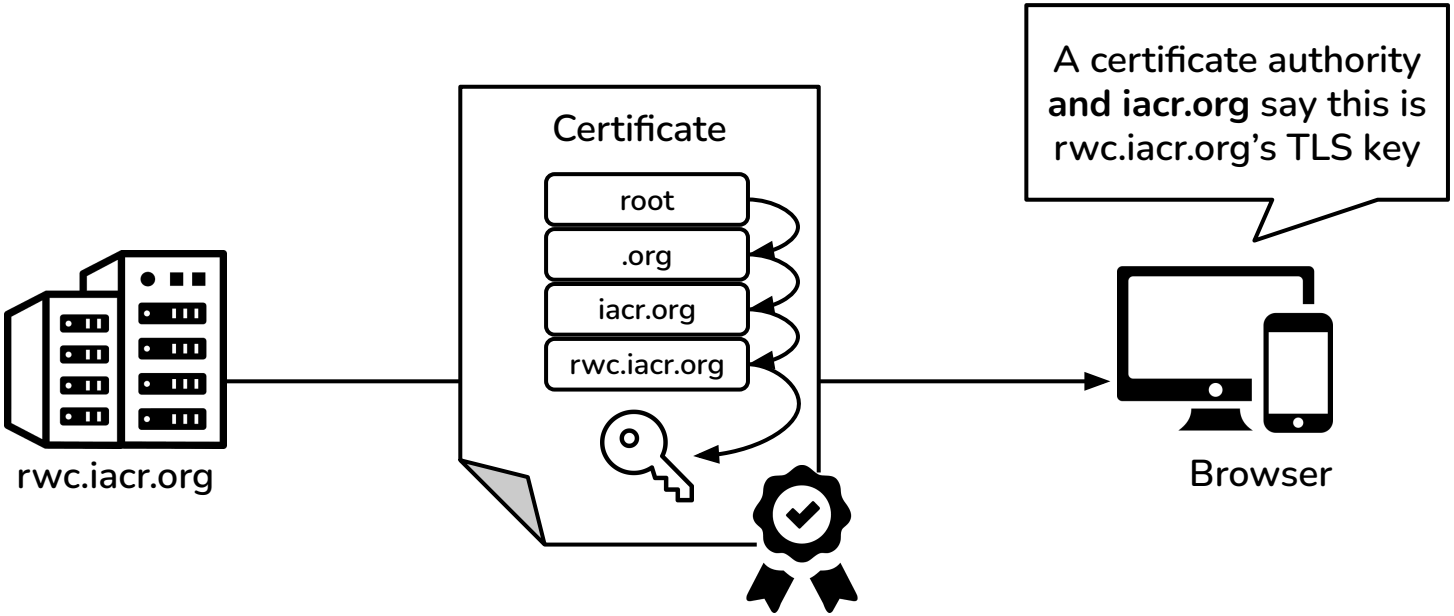
DNSSEC from 30,000 feet



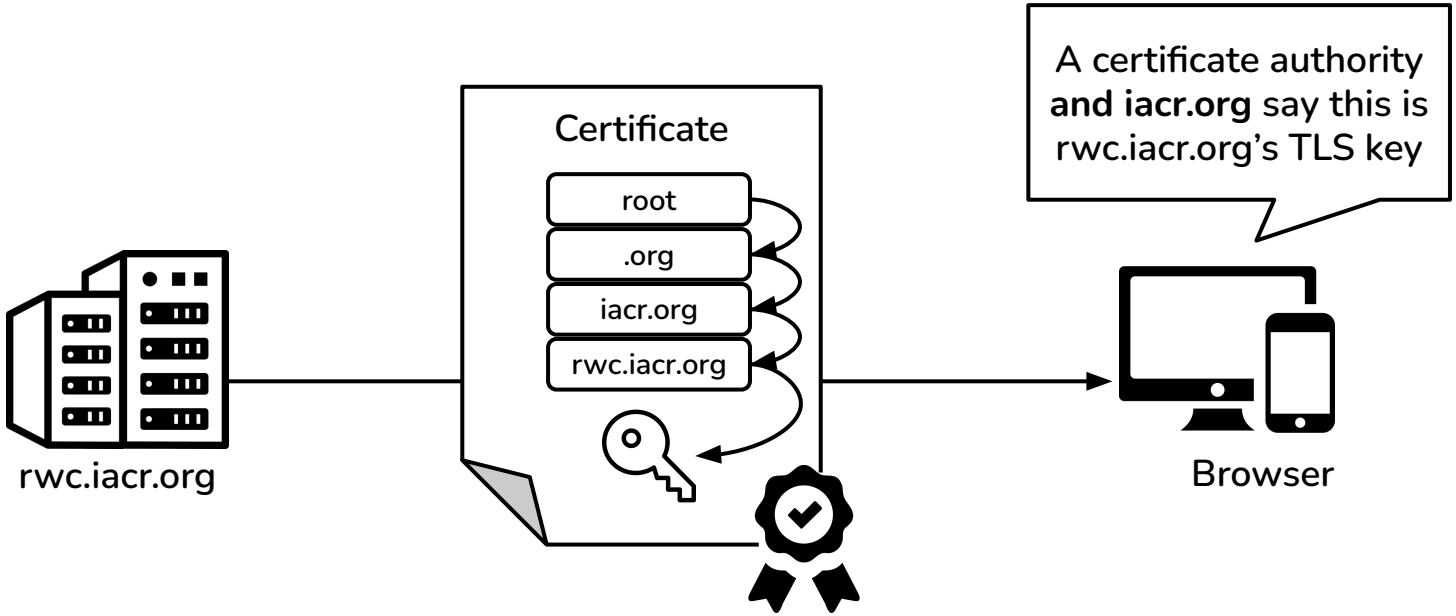
DNSSEC from 30,000 feet



First attempt at building NOPE: use a DNSSEC chain as the proof

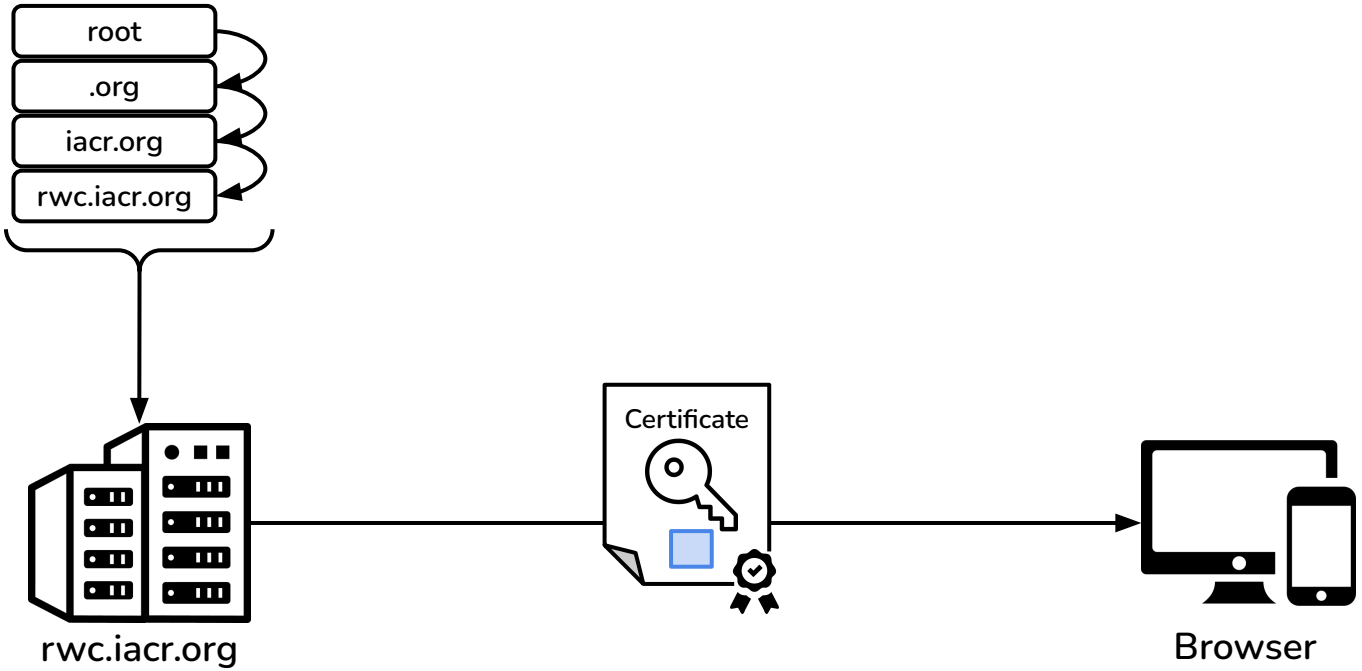


First attempt at building NOPE: use a DNSSEC chain as the proof

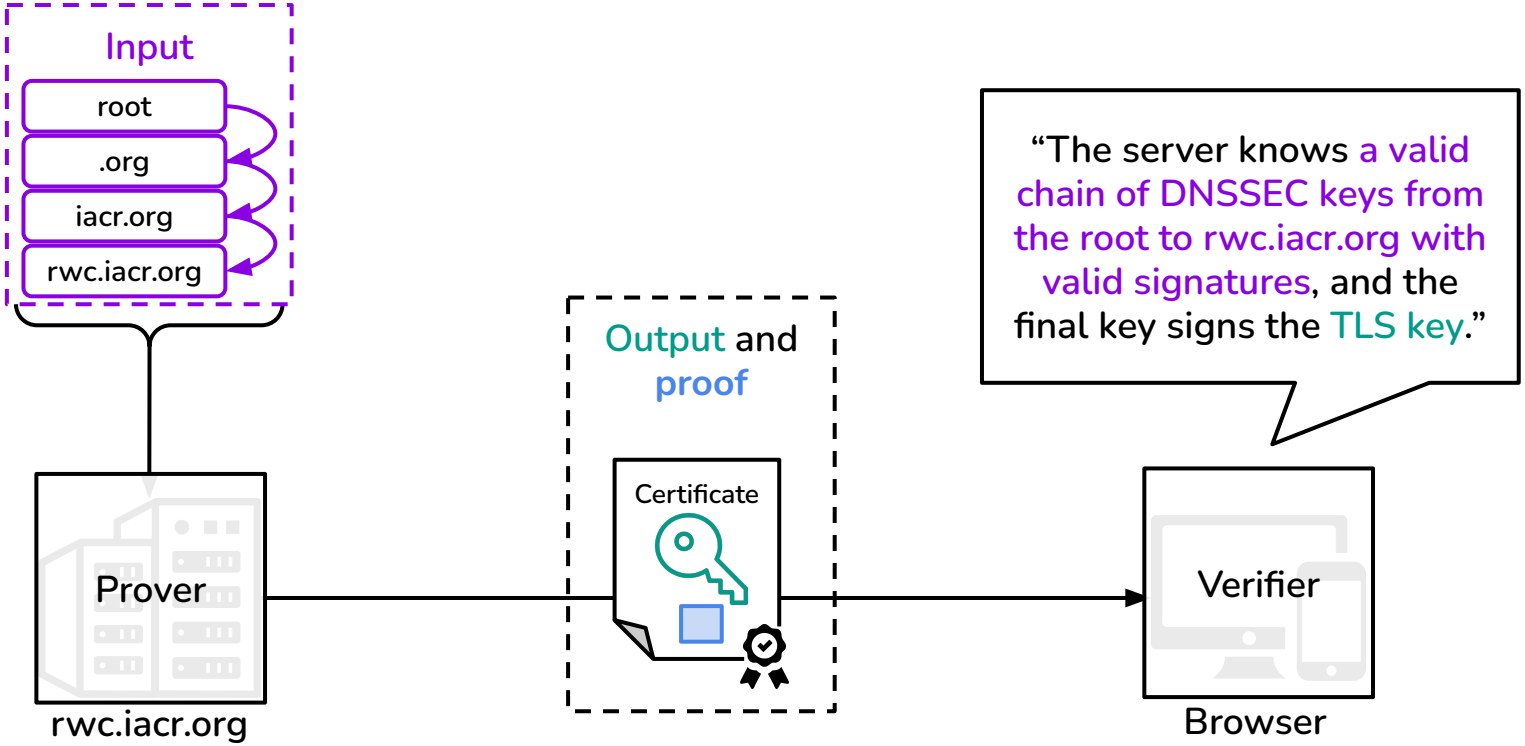


Including a DNSSEC chain in a certificate requires modifying infrastructure

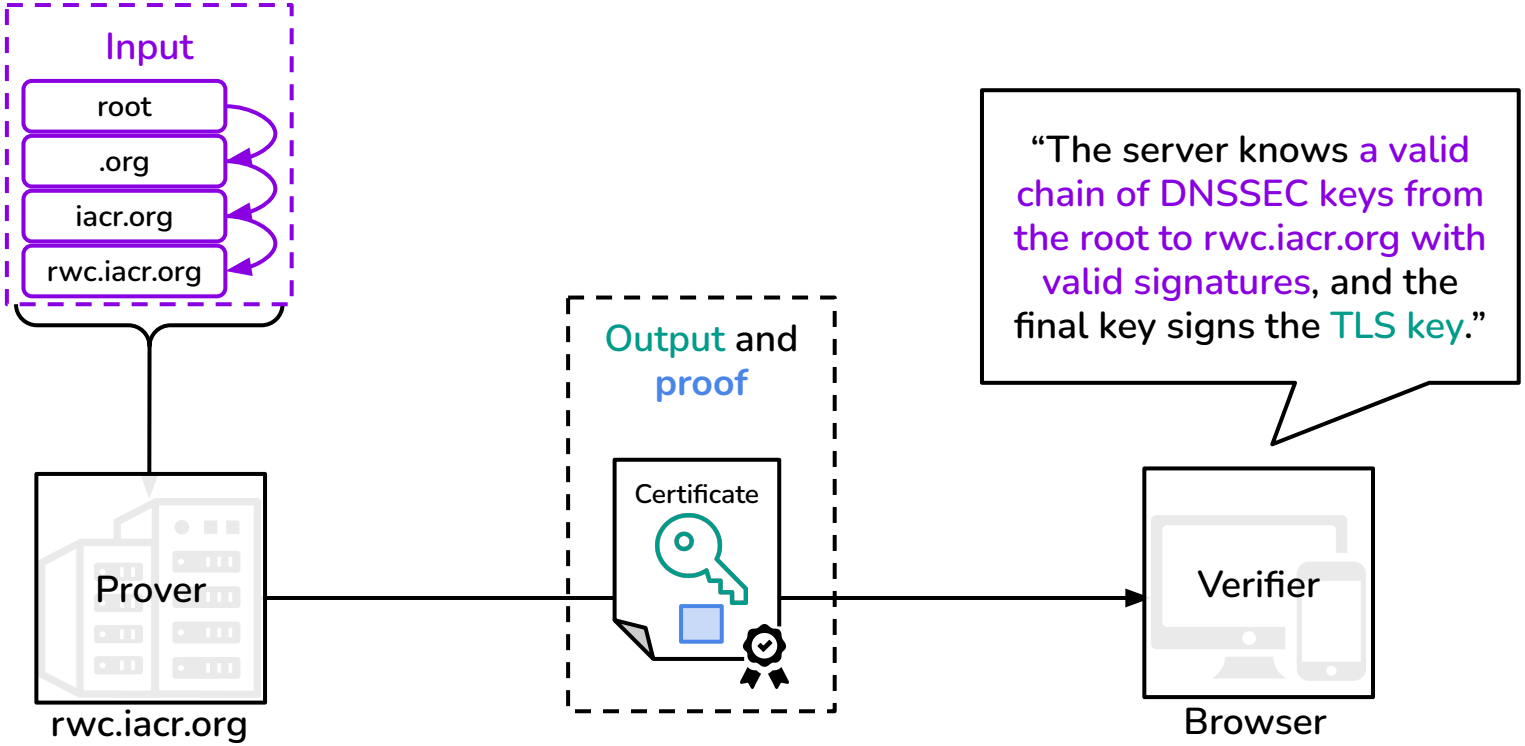
Idea: prove the existence of the full DNSSEC chain



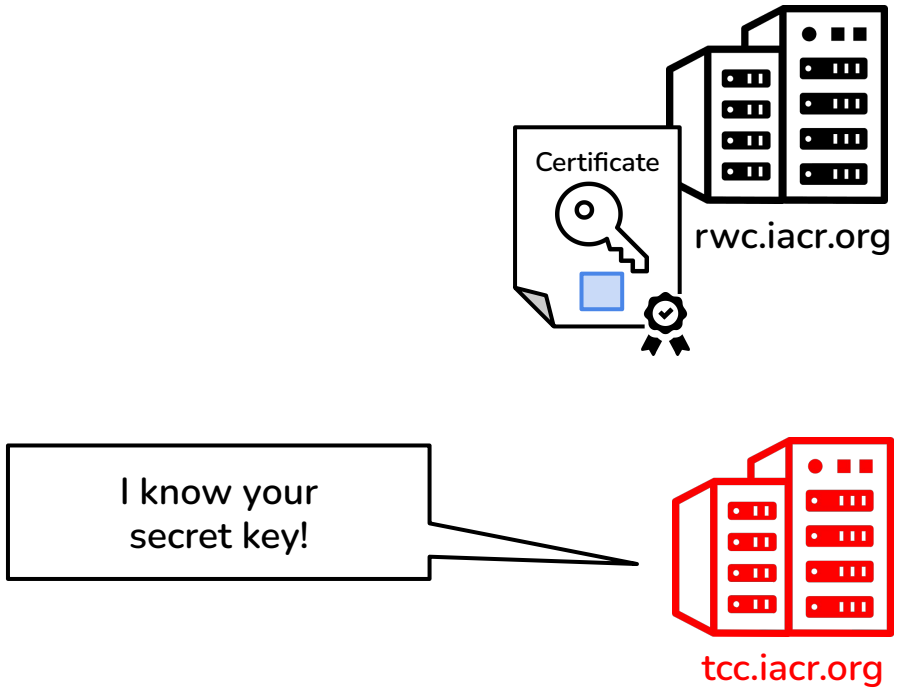
Idea: prove the existence of the full DNSSEC chain

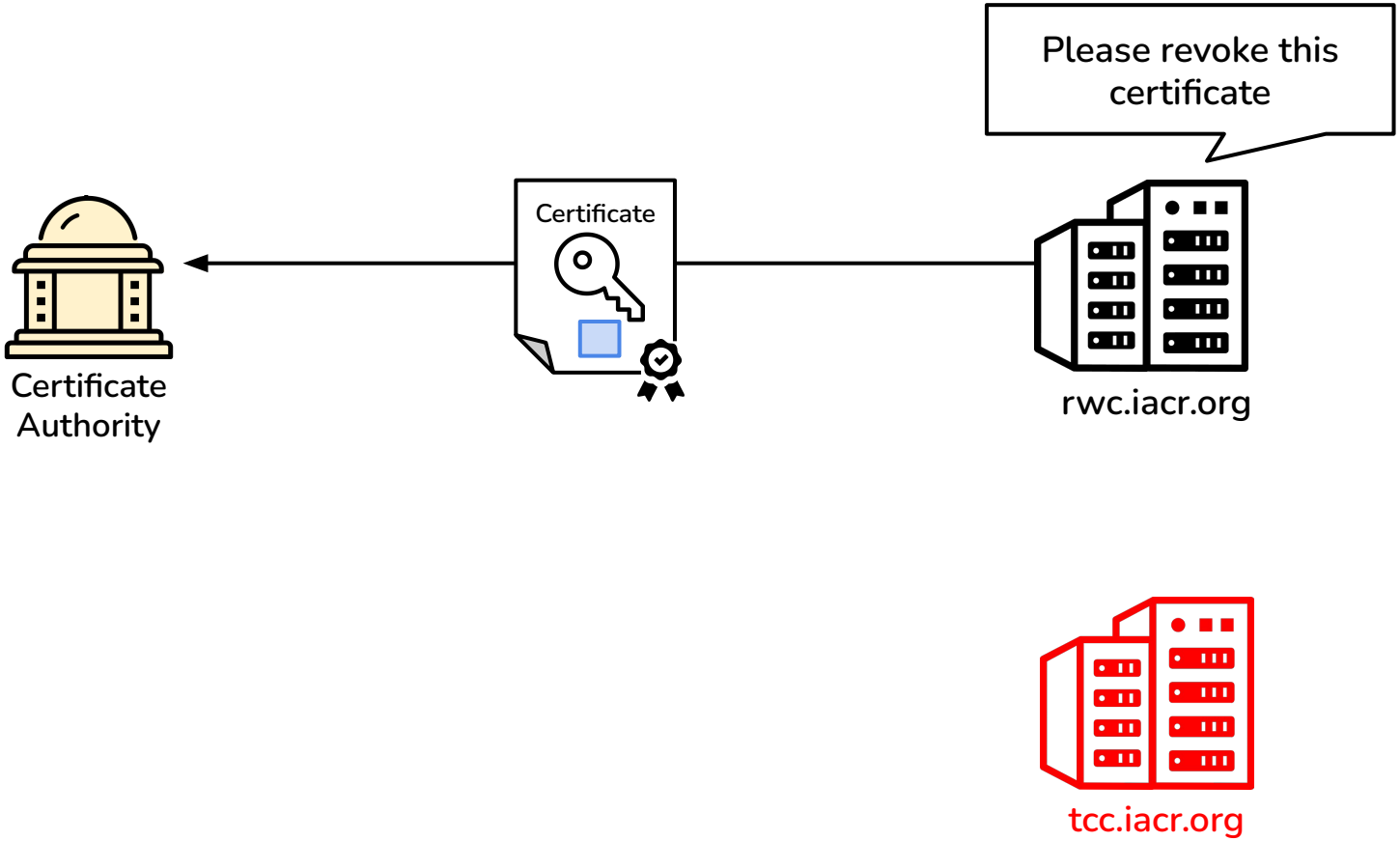


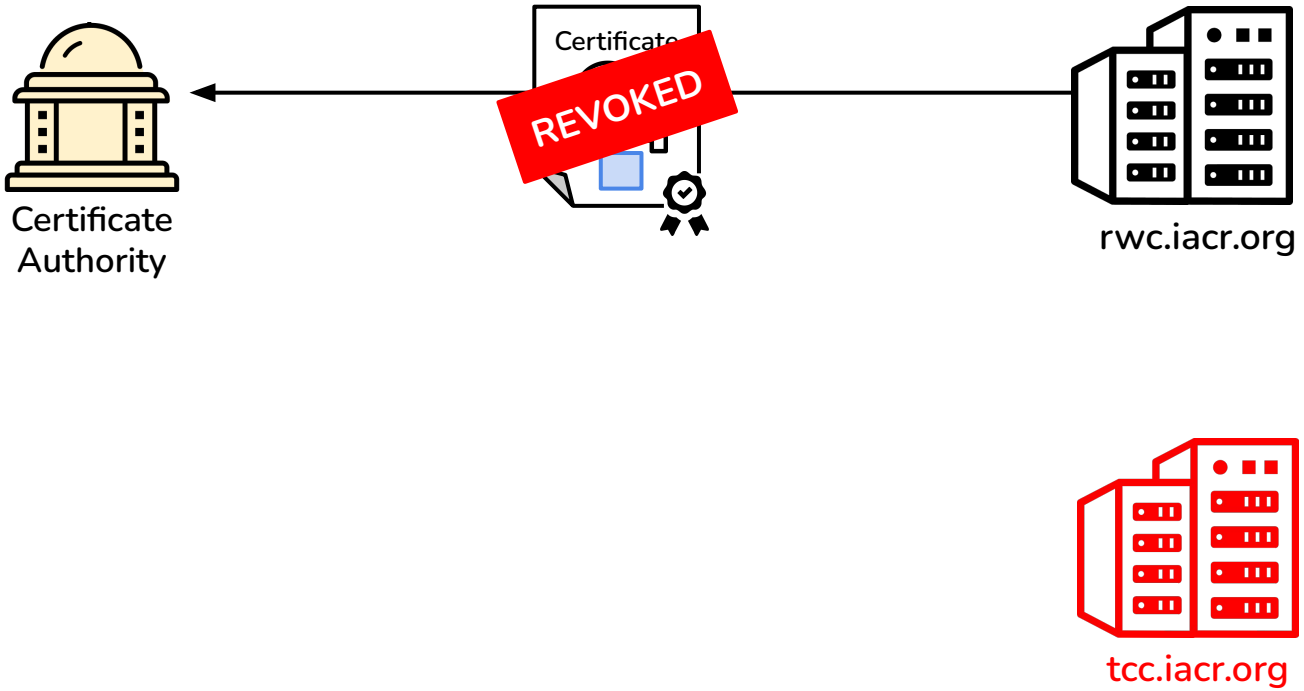
Idea: prove the existence of the full DNSSEC chain

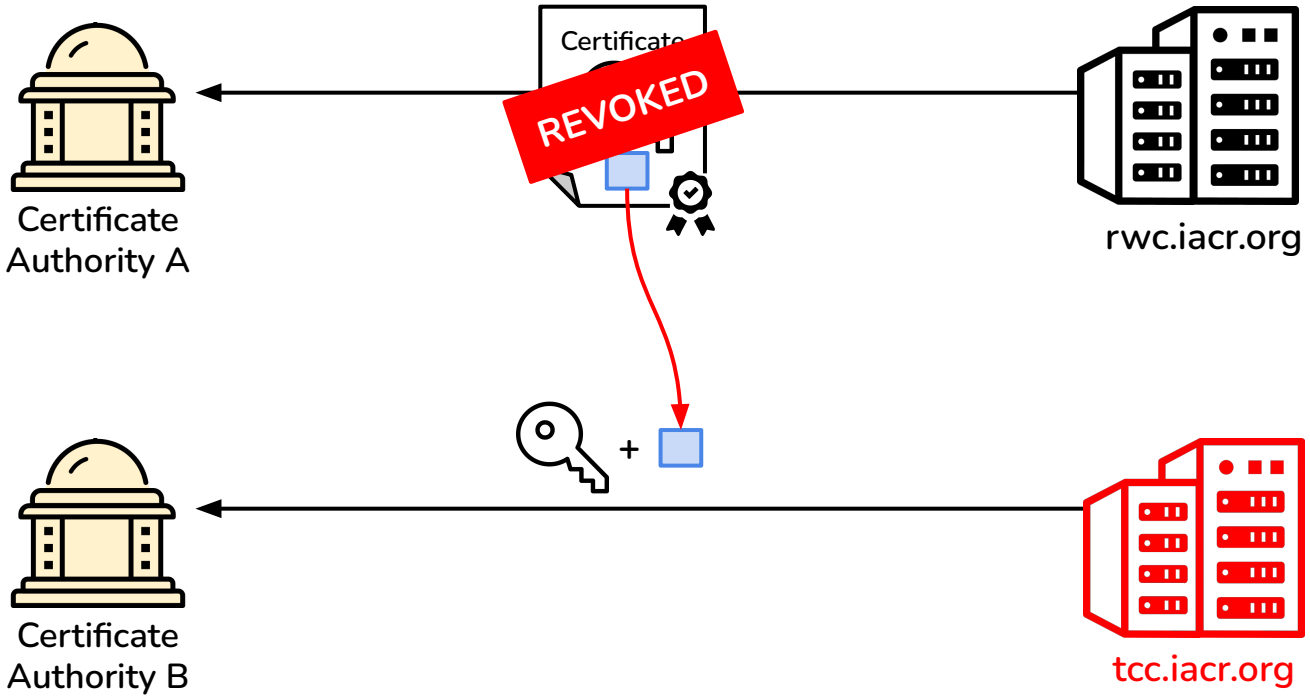


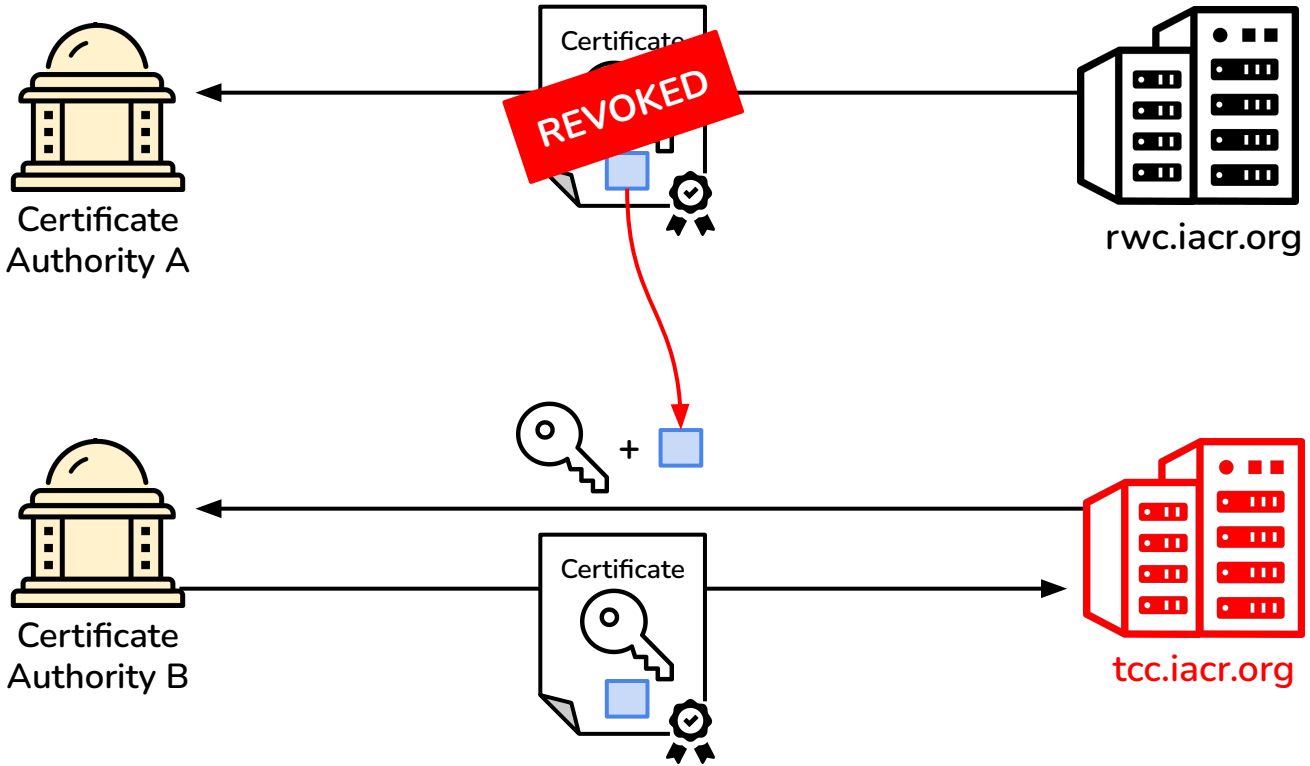
One challenge: how to revoke these proofs?

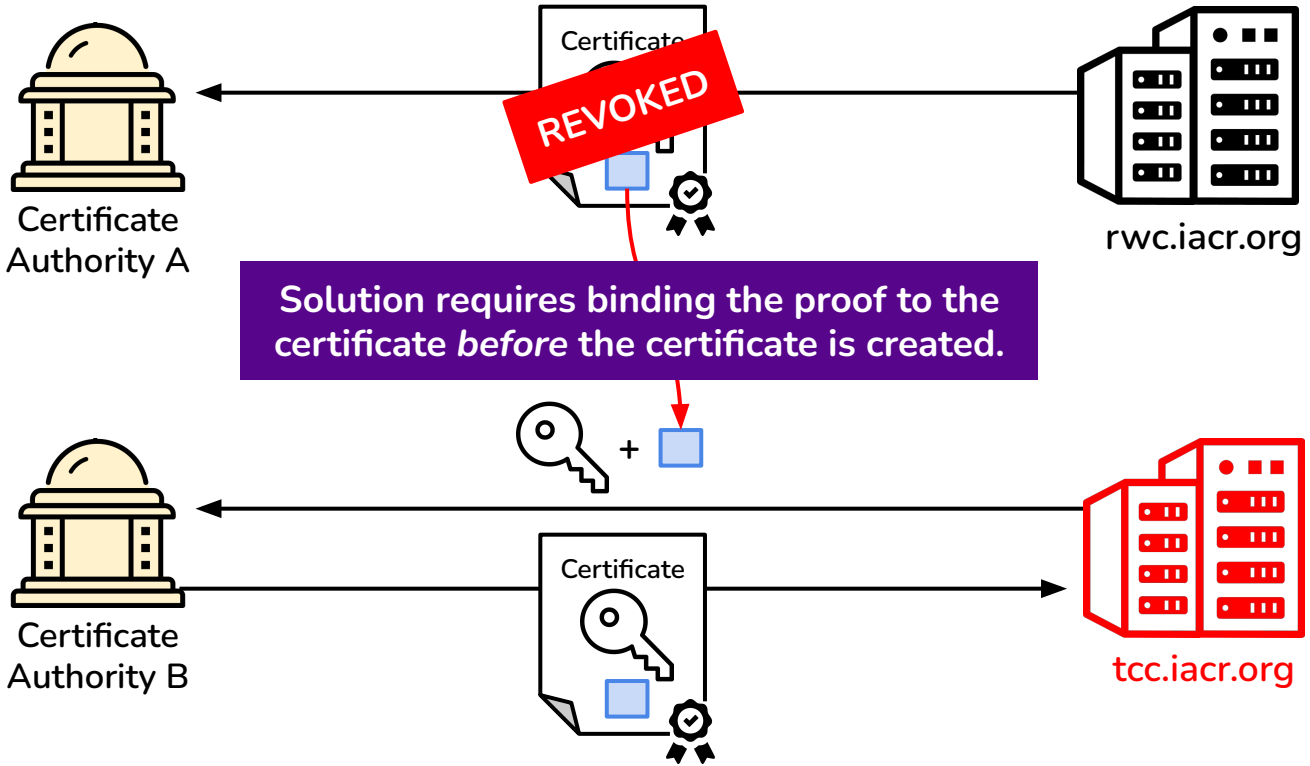

Certificate
rwc.iacr.org
I know your
secret key!
tcc.iacr.org

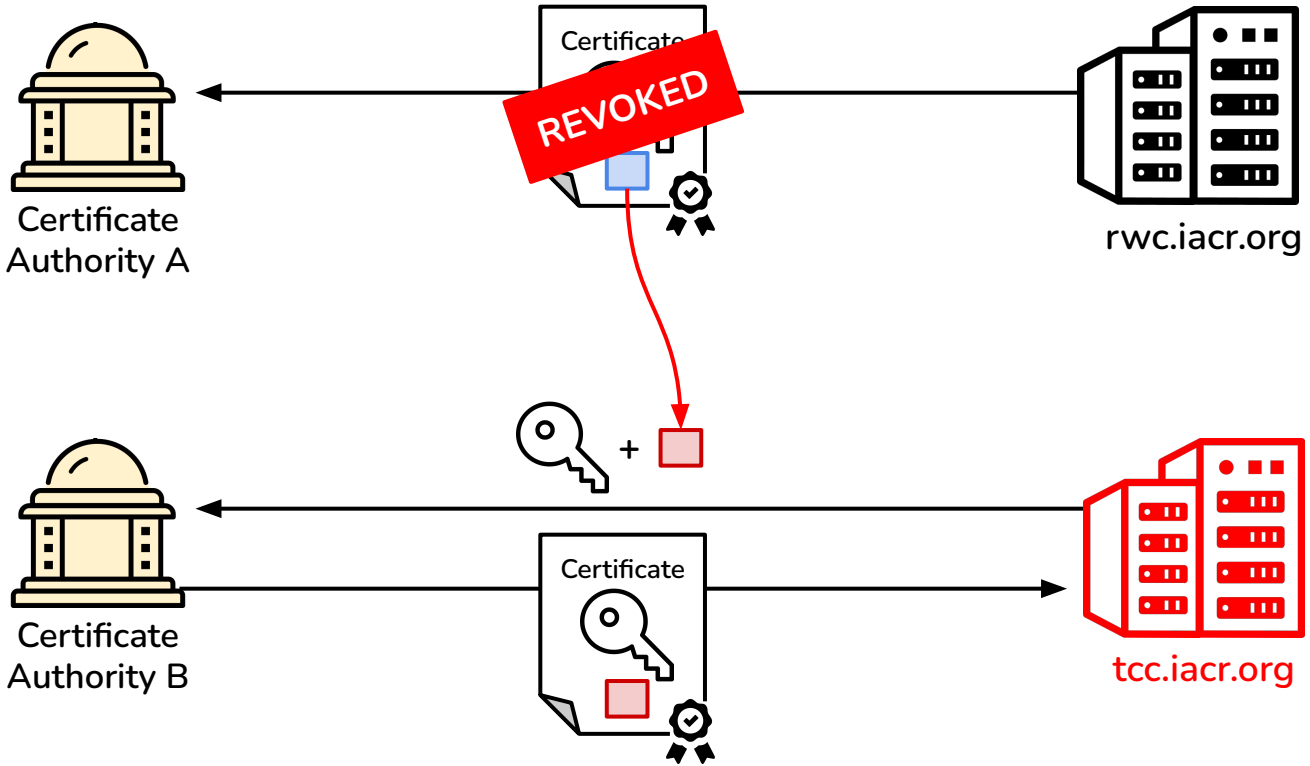

Please revoke this certificate
Certificate
Certificate Authority
rwc.iacr.org
tcc.iacr.org


Certificate
REVOKED
Certificate Authority
rwc.iacr.org
tcc.iacr.org


Certificate
REVOKED
Certificate Authority A
rwc.iacr.org
+
Certificate Authority B
tcc.iacr.org


Certificate
REVOKED
Certificate Authority A
rwc.iacr.org
+
Certificate Authority B
Certificate
tcc.iacr.org

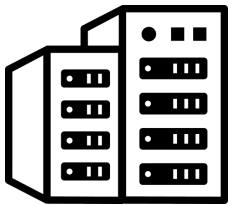

Certificate
REVOKED
Certificate Authority A
rwc.iacr.org
Solution requires binding the proof to the certificate *before* the certificate is created.
+
Certificate Authority B
Certificate
tcc.iacr.org


Certificate
REVOKED
Certificate Authority A
rwc.iacr.org
+
Certificate Authority B
Certificate
tcc.iacr.org

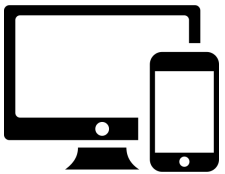
Implementation and evaluation of NOPE

(a) Can NOPE be concretely instantiated?

(b) What are the costs of NOPE?



iacr.org

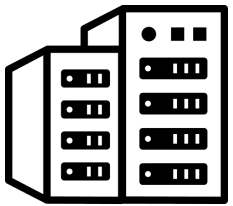


Browser

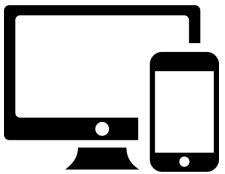
Implementation and evaluation of NOPE

➡ **(a) Can NOPE be concretely instantiated?**

(b) What are the costs of NOPE?

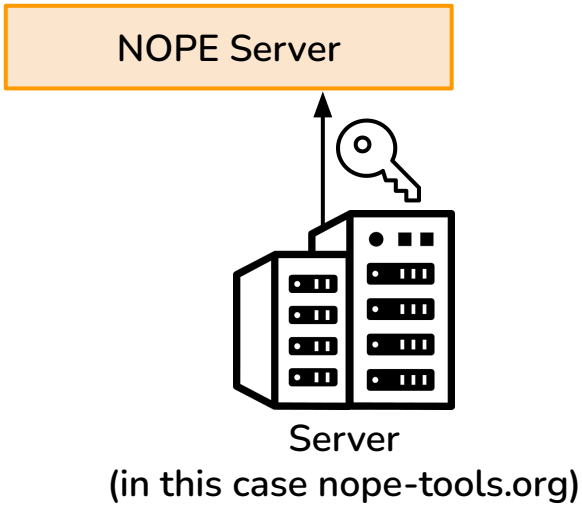


iacr.org

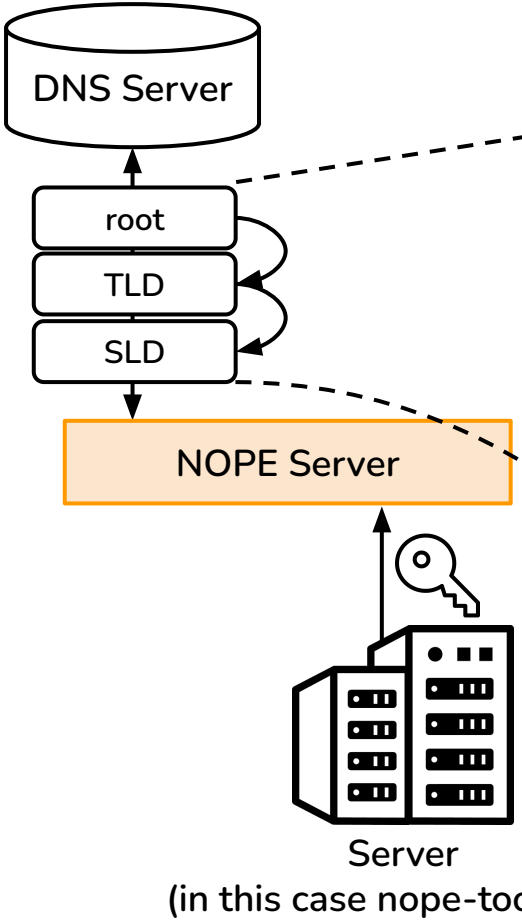


Browser

Implementation of NOPE



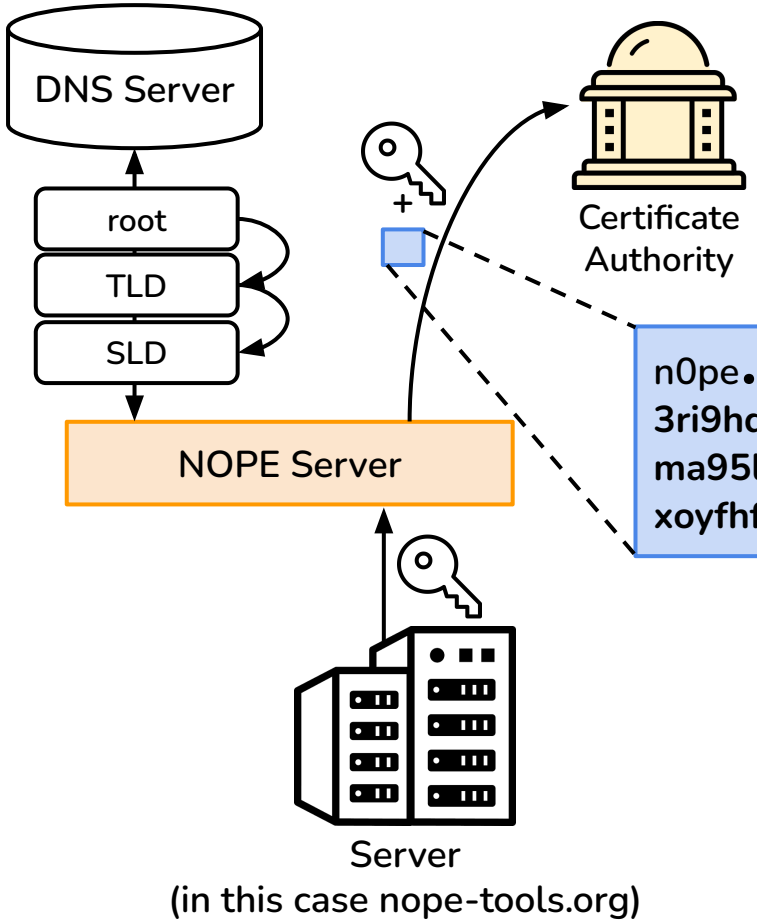
Implementation of NOPE




```
. 172800 IN DNSKEY 257 3 8 (
        AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTO
        iW1vklbzxeF3+/4RgWOq7HrxRixHlFlExOLAJr5emLvN
        7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5
        LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF0jLHwVN8
        efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7
        pr+eoZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLY
        A4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnXGXws
        9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU=
        ) ; KSK; alg = RSASHA256 ; key id = 20326
. 172800 IN DNSKEY 256 3 8 (
        AwEAAc0SunbHdS0KFEyZbYIl/+tzsrNzIwurKxmJA+0f
        hAYlTPA/5LrMGkGEqvvufzM0w/CaVtdm5eWkZYQcsoSK
        T5bycx0C4jxnLEb3ZiZUQSqu1rWcKGF1fj/GyDWLkOu7
        a5h3el+gPmglj/4l4V31ugNYfqYq84vCB+3D6Sodrd+8
        5KyonnzWJ8cS7aZ57x0d0sGqsAKA+6tRnlXjVNVe7Ro5
        xJuz8lR7rOxdzfuRLriN+Z00EL3U5E7s9SISU/hDh7Q7
        N70W1mLMc1o2+tCRGjEWrw4wmCWMzc1kegbLES/dUOWF
        vPjJz0+AEeWDhd2GqtXk02BzAhdfeIAEIv68FTs=
        ) ; ZSK; alg = RSASHA256 ; key id = 61050
. 172800 IN RRSIG DNSKEY 8 0 172800 (
        20241121000000 20241031000000 20326 .
        guknao8E8o7kxflB/XbQjNz70XbtHa4gEtCfekSXTxLJ
        unSBHPmdWrOm5AIU9c2lcZS/Q2t2O7GMns+gqxlgGr1K
        zrckLgyjgagNCl4Syn0YVP+8Knopf/0+8evDwdPqbzJL
        DE6u6cY4e35tY7lMtxK/6rNtqElOPimnLgdviDaky2zD
        GH+PeGKNK7HuE3BH/46c2IAzDntONnRqHn/Uimi/clEf
        qt725uESM7FBfUw6QWz+EMk5RpfIHXVwczM8nmrVhPzi
        moSrCT1GP3hzWUE1a/8VchnT2nHGoyHQBs1K5hipmxBx
        MMmLpz50c6P1Jh+Rd8e+aU5yAwkyvaw0zA== )
org. 86400 IN DS 26974 8 2 (
        4FEDE294C53F438A158C41D39489CD78A86BEB0D8A0A
        EAFF14745C0D16E1DE32 )
org. 86400 IN RRSIG DS 8 1 86400 (
        20241117050000 20241104040000 61050 .
        Xsu6YWdRdBan11kR7M1Uhq9vmj4UfV5E/ikwsdFiPpvY
        8yuSegDuYA94RWESWe9hrcEGYlQrWsFIUe1JWaB35Now
        PkoRCHv/iv16NmskXXxNpmCkUvfsOkiYjMl5bUsIxCU/
        AV8aynRon9x5uj3v3e+XBBE1KKVCMYfUyyeCrWhnJSQC
        5K5eZ8U3zbo+ZngTLnXcdQ0MzaNpcNBNy8cpCs2WePYh
        OqRUBZdx34XFtLZBk8v7GvcTnv3wdVYz3n+AATHwzQE9
        SL8GeyP2V1ES9KUrSTF3XrirBLRABMfMHuCyB/770j3N
        RVpj9z3hMOzVJwUjb+coAEqhMWGVdWoKIQ== )

org. 3600 IN DNSKEY 256 3 8 (
        AwEAAdim1OsPrczOdlnedsci34awEy8Y2z3wk/vBneTp
        BcMqZ/RMbIR628sT7w1DmLTqtVGxJZseiWV4ZPopdncr
        aq3psjtMZ09Aacdho5aToAlRGkemALvc41l0fxt1oORr
        4UxHjx0oYWgpVgFfn8WrolxfJs1HojL4KvHtGbOOLrod
        ) ; ZSK; alg = RSASHA256 ; key id = 42393
org. 3600 IN DNSKEY 257 3 8 (
        AwEAAexZJ/1wfyNCxNPrTZizaG7UlibGhP+AyogR6bqj
        ptKweEgE4gD8GxRQJkt+Fn5pCoNqzmm1ZnEoKqvm93uO
        YtbKkYQDGH+W69J66MSKpglyS+mT/4iaXn+Ipb5o99l/
        sf7lHMa975O/fqN6aPUll4hUbN2T1LHv6HzQuQCtNRJA
        8jHGwX5q0NMmh2Z+yaG6B9clSerje9l5L+ID2ydJ6zXq
        uYteolUvX2xzqnXCdHPSvD+oL6R/weW+tztdFS1hok/1
        z3tn5NzmcaOLll9nXniCozEpLFEGPswyvtphWgCYhI8b
        BTqhUslwfIwLSBQTEg2oCX7sS5CbXg44OqwhIW8=
        ) ; KSK; alg = RSASHA256 ; key id = 26974
org. 3600 IN RRSIG DNSKEY 8 1 3600 (
        20241122152312 20241101142312 26974 org.
        FL3LJdeBG+6xuISibgk+FN2b5JRDDY4zhEvgXXu5IWFg
        3qjYGBIW6ed6WobmVqKk4nTmlcmGOlRtdstCYF8TsY6A
        ap7QSNbBkzDQj5bG3CknMsCuwU8Nv7E58WzkzkHJyW/2
        LV70UXx6Tbtq7azqiu9bLs4sTbbo8Q5Oh++LQ6C5QNYQ
        Ok1kUzXskzrrWazgygwgmnCB/9SYCq4STG5KScnF1PJ+
        +mT50BIIwelxVrZl9HlZYJoXwBJTwd1tE4nCJc7ffqbf
        ZFOzMyltHx7L5UZAHL0WHuNxmOC0rYEeq5eOD20uXLQY
        Dq3FU3y5PKTA+4SgBaVkk4kDKk9JHqkMYA== )
nope-tools.org. 3600 IN DS 24071 13 2 (
        7FEDB3256082F9772FB264B58D04DD398A1E7211137E
        1E6234F86E1AC09BB79D )
nope-tools.org. 3600 IN RRSIG DS 8 2 3600 (
        20241122152312 20241101142312 42393 org.
        C50zMlPjLQcvlipjcDpqzLMhA8CsZisDG0miSPlfRFPm
        IChd21HdRKMxuBnmFlN2QsTYquvpvIzcHD/O2akUsAVa
        cNCN/gbYYKc/ELnLtu1n6K7Rvkm2JP9SXvMUFk+R/pFl
        PAu0El1jTZrU2jf64CJDxi+4k+BeMDj0/lAwycc= )
nope-tools.org. 600 IN DNSKEY 256 3 13 (
        Bj2WG9xitWiMHFltAn0eldZTJhem8n+6hc0DMP7N0ABE
        8uXagReAkW6DhDTECjFVZYol4LTrP4bqXUALg9zUUA==
        ) ; ZSK; alg = ECDSAP256SHA256 ; key id = 51774
nope-tools.org. 600 IN DNSKEY 257 3 13 (
        l8Y9CtL7l9OpCvKgXVIrN8YzANwPUAxuKCkrQRfhAPn4
        1EaKHKSgfRN8N0RsMaExDDc3RJQnZ+Z9NTkY4aV68A==
        ) ; KSK; alg = ECDSAP256SHA256 ; key id = 24071
nope-tools.org. 600 IN RRSIG DNSKEY 13 2 600 (
        20241117184555 20241103180010 24071 nope-tools.org.
        5QFVPtlQG4smABJT1m0BbbWSYz3yaQlHGvQVQklwj4D6
        Pia4e/+UpRbGz5uWXT7vKw8dOAhaeaG61oZaR/QjEg== )
```

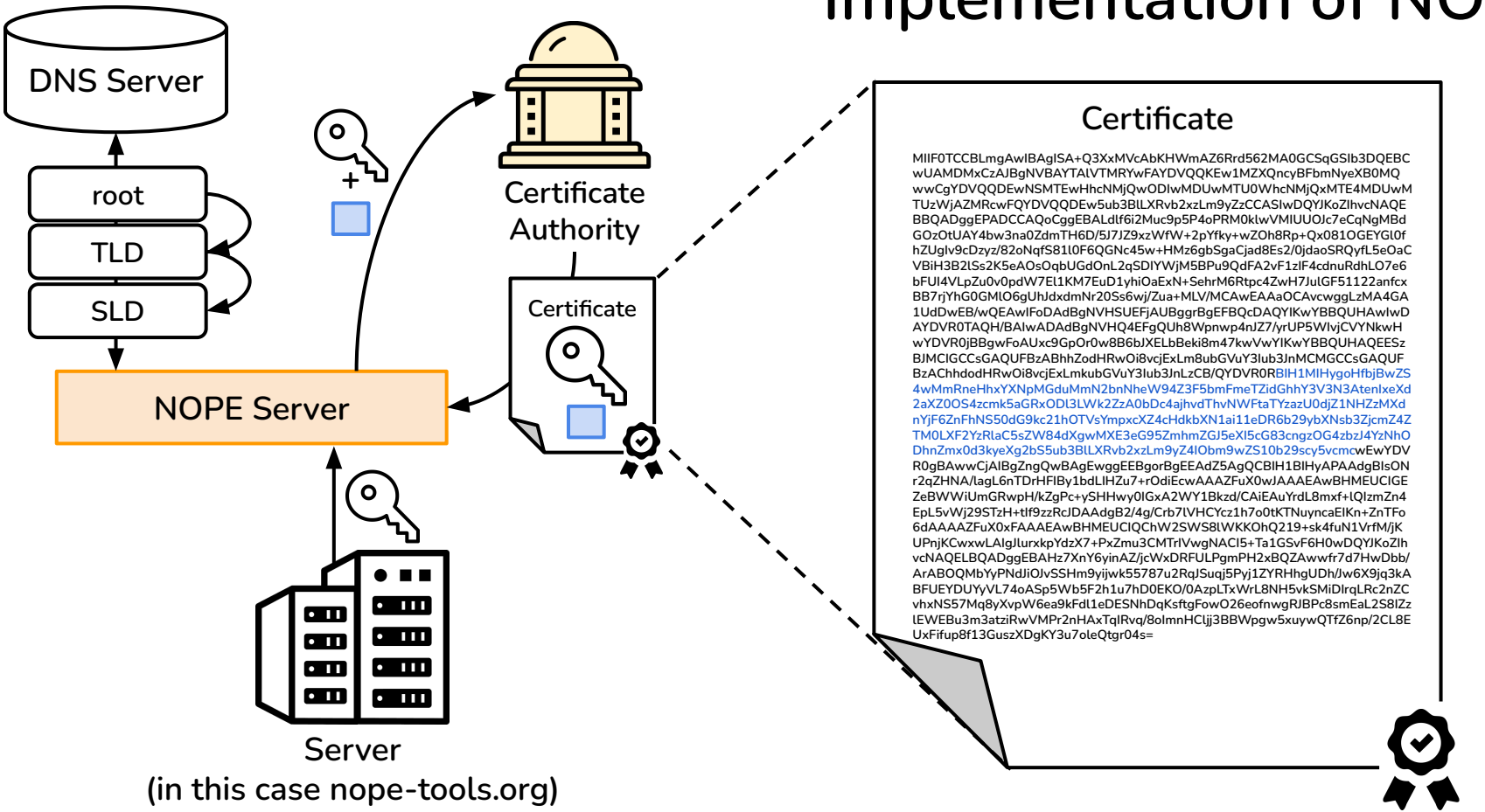
Implementation of NOPE



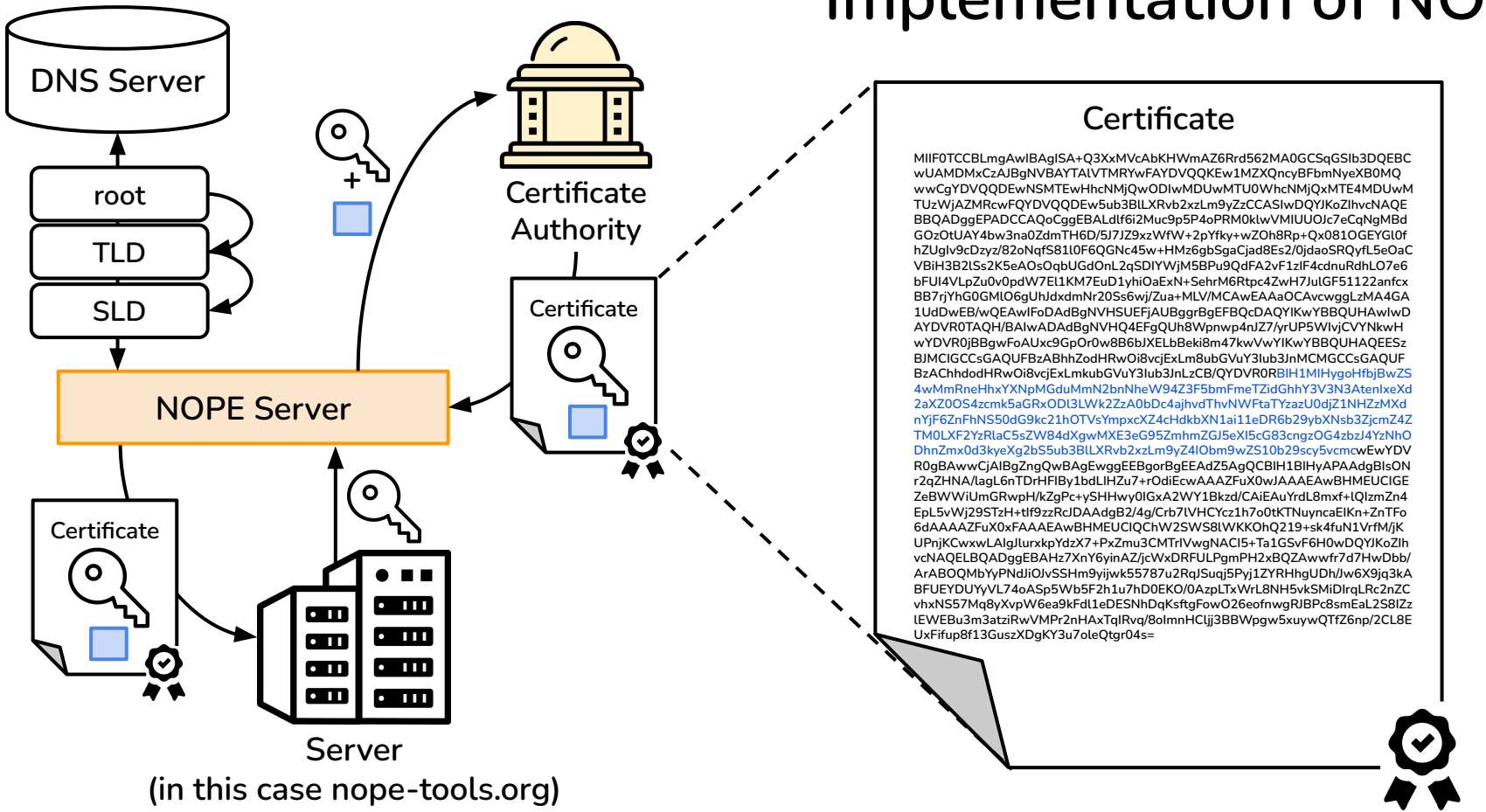
n0pe.02dgxxqasi0gn2cvnsayoxgqynafy6bthacuw7p-zr1ywvivt9.3ri9hdq89w-i6g04l78j8ou8o5ami63k54v6u4vs1wgb1zfqa5.ttodsma95lbjqqvxpwdmsuj-ux4zoormslovcrfxe34-qvc4eh.leo8ux01q7xoyfhfdbyyr9po7rx38n3o2xc3a88gfltwy2yx6m.nope-tools.org

The proof is encoded in a domain owner's **subdomain**

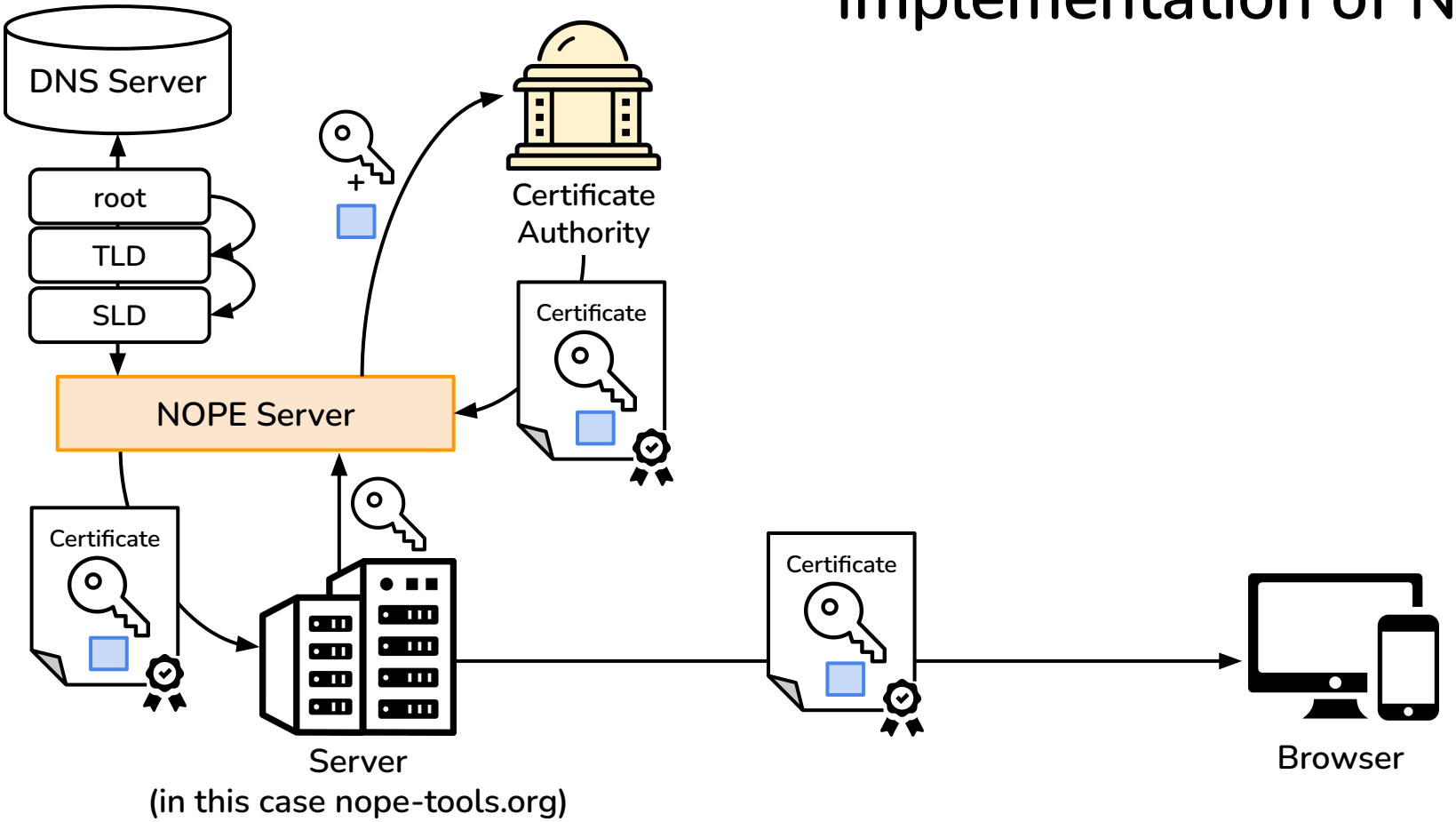
Implementation of NOPE



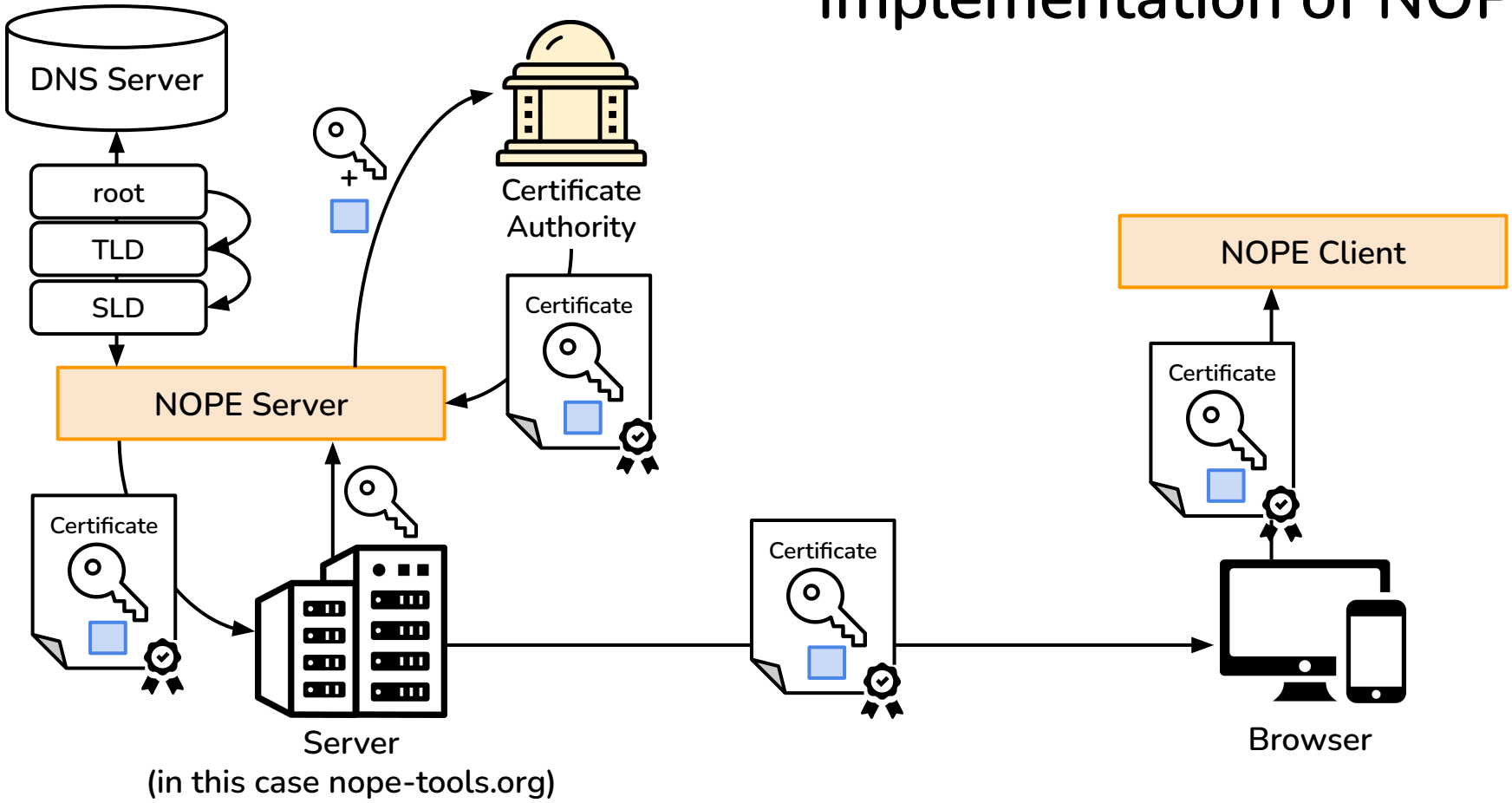
Implementation of NOPE



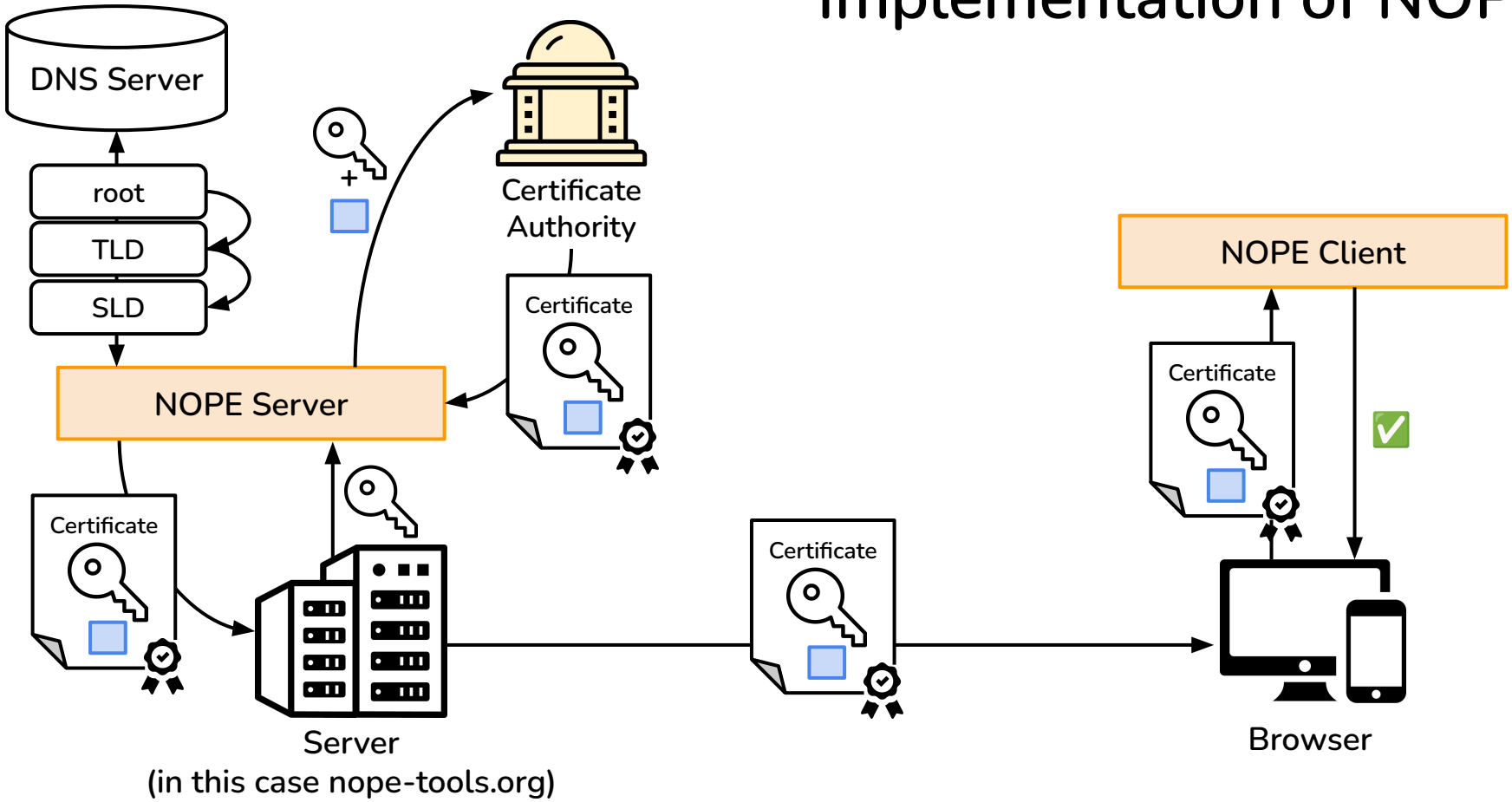
Implementation of NOPE



Implementation of NOPE



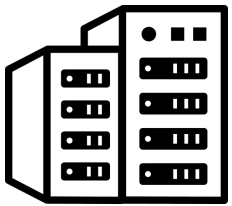
Implementation of NOPE



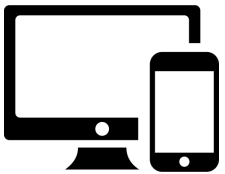
Implementation and evaluation of NOPE

(a) NOPE **can** be concretely instantiated

➡ **(b) What are the costs of NOPE?**



iacr.org



Browser

Overheads of NOPE are manageable

	Status quo	NOPE
Certificate chain size	2.5 KB	2.7 KB

All benchmarks run on a Google Cloud [59] e2-highmem-2 machine on a single thread

Overheads of NOPE are manageable

	Status quo	NOPE
Certificate chain size	2.5 KB	2.7 KB
Certificate issuance time	30 s	84 s

All benchmarks run on a Google Cloud [59] e2-highmem-2 machine on a single thread

Overheads of NOPE are manageable

	Status quo	NOPE
Certificate chain size	2.5 KB	2.7 KB
Certificate issuance time	30 s	84 s
Verification time (in browser)	0.3 ms	34.9 ms

All benchmarks run on a Google Cloud [59] e2-highmem-2 machine on a single thread

Overheads of NOPE are manageable

	Status quo	NOPE
Certificate chain size	2.5 KB	2.7 KB
Certificate issuance time	30 s	84 s
Verification time (in browser)	0.3 ms	34.9 ms
Verification time (native)	0.3 ms	1.5 ms

All benchmarks run on a Google Cloud [59] e2-highmem-2 machine on a single thread

Related Work

Domain Authentication

Efficient Constraint Representations

Succinct Proofs for Networking

Related Work

Domain Authentication

Efficient Constraint Representations

Succinct Proofs for Networking

Domain Authentication

Alternative designs: AKI, ARPKI, CertLedger, ENS, MonkeySphere, RHINE, Sovereign Keys
CA Strengthening: CAge, CAA, CertLock, Convergence, HPKP, Multi-Perspective Validation, TACK
Reactive approaches: CIRT, CRL, Forced perspectives, Gossip, Short-Lived Certificates, OCSP, YPIR

Related Work

Domain Authentication

Efficient Constraint Representations

Succinct Proofs for Networking

Efficient constraint representations

Control Flow: Buffet, Fairplay, Ginger, Libsnark, Pantry, Pinocchio, vRAM, vSQL, xJsnark, Zaatar
Cryptographic operations: circom-ecdsa, Cinderella, vSQL, WARPfold, xJsnark, Zombie
Parsing and string manipulation: Cinderella, zkLogin, ZK-JSON

Related Work

Domain Authentication

Efficient Constraint Representations

Succinct Proofs for Networking

Succinct proofs for networking

Digital Identity: Aptos Keyless, Cinderella, IDEA-DAC, zk-creds, zkPassport, ZK Email, ZK-JSON
Network protocols: DiStefano, DECO, DIDO, Janus, TLSNotary, zkTLS, ZKMB, Zombie

Takeaways of NOPE

It is practical to enhance Internet security right now, without any changes to existing Internet infrastructure.

Takeaways of NOPE

It is practical to enhance Internet security right now, without any changes to existing Internet infrastructure.

Succinct proofs provide an efficient interface between legacy protocols and systems.

Takeaways of NOPE

It is practical to enhance Internet security right now, without any changes to existing Internet infrastructure.

Succinct proofs provide an efficient interface between legacy protocols and systems.

Future work:

- Deploying NOPE natively in browsers
- Applying succinct proofs of DNSSEC, beyond server authentication