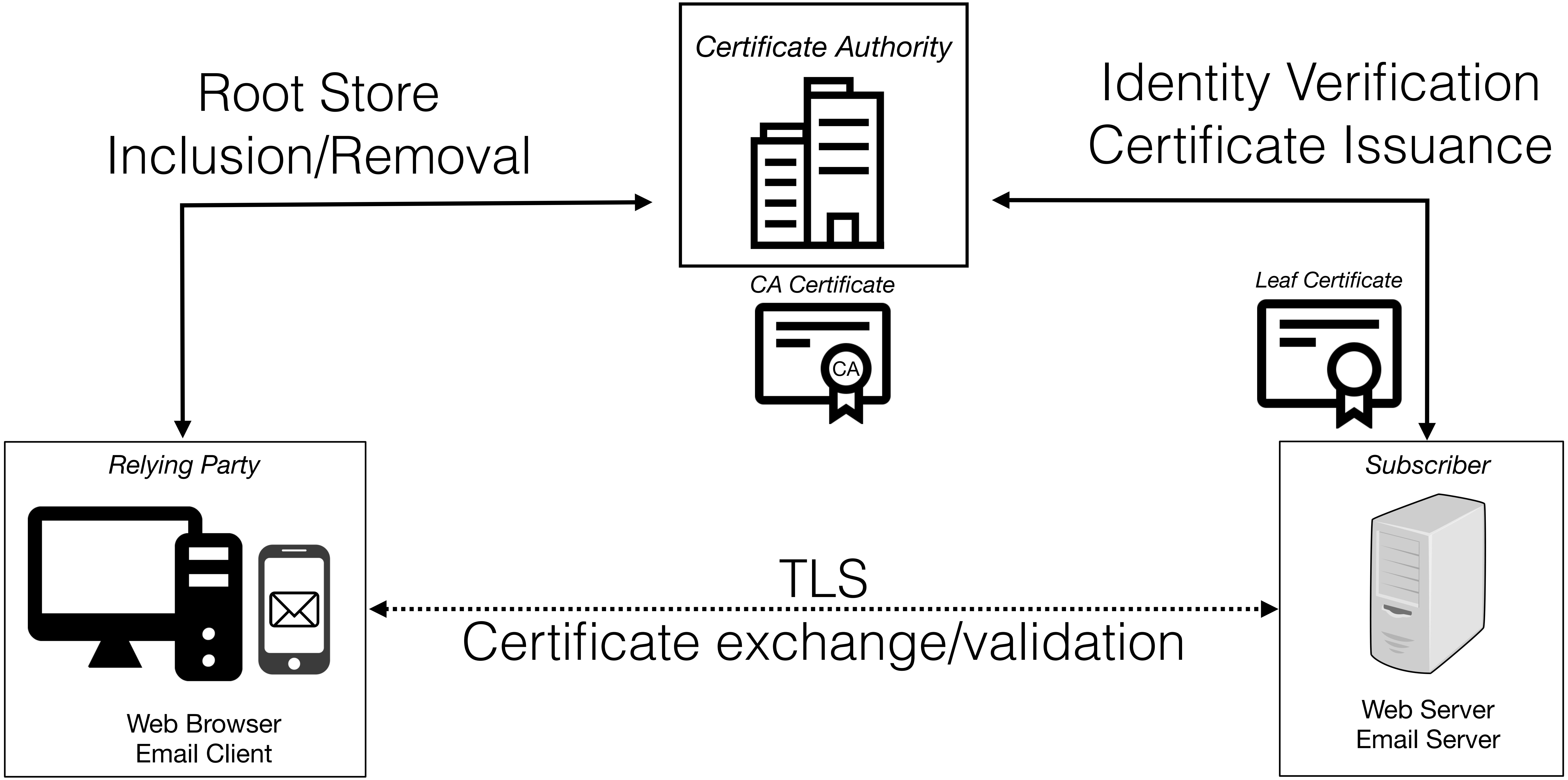
What's in a Name?
Exploring CA Certificate Control

Zane Ma[1], Joshua Mason[1]
Manos Antonakakis[2], Zakir Durumeric[3], Michael Bailey[1]

[1]University of Illinois at Urbana-Champaign
[2]Georgia Institute of Technology
[3]Stanford University

Delegated Authentication



Certificate Authority

Root Store
Inclusion/Removal

Identity Verification
Certificate Issuance

CA Certificate

Leaf Certificate

Relying Party

Web Browser
Email Client

TLS
Certificate exchange/validation

Subscriber

Web Server
Email Server

Symantec Distrust

- From 2009-2017 Symantec was responsible for over a dozen issues[1] that prompted removal from browser root stores
- Difficult to determine which root CA certificates Symantec operated!

```
commonName          = UTN-USERFirst-Client Authentication and Email
orgUnitName         = http://www.usertrust.com
orgName             = The USERTRUST Network
localityName        = Salt Lake City
stateOrProvinceName = UT
countryName         = US
```

Comodo Root #1

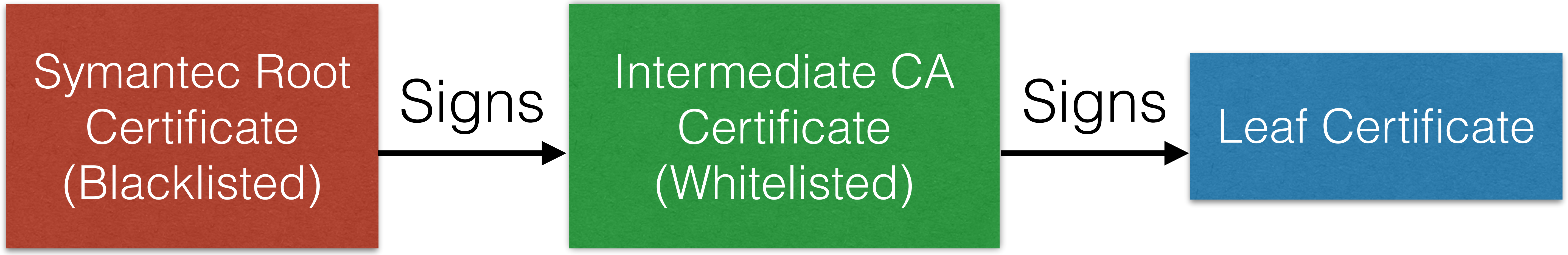
```
commonName          = UTN-USERFirst-NetworkApplications
orgUnitName         = http://www.usertrust.com
orgName             = The USERTRUST Network
localityName        = Salt Lake City
stateOrProvinceName = UT
countryName         = US
```

Symantec Root #2

[1] https://wiki.mozilla.org/CA:Symantec_Issues

Symantec Distrust

- From 2009-2017 Symantec was responsible for over a dozen issues[1] that prompted removal from browser root stores
- Difficult to determine which root CA certificates Symantec operated!
- Needed to whitelist independently-operated intermediate CAs
  - 6 Apple Intermediates
  - 1 Google Intermediate



Symantec Root Certificate (Blacklisted)
Signs
Intermediate CA Certificate (Whitelisted)
Signs
Leaf Certificate

[1] https://wiki.mozilla.org/CA:Symantec_Issues

Takeaways

1. TLS authentication trust occurs at the level of CAs (a.k.a. CA certificate operators), not CA certificates.

2. There are no guarantees that the identity in a CA certificate reflects the operator of the CA certificate.

3. Intermediate CA certificates may have separate operators that are independent of their root CA operator.

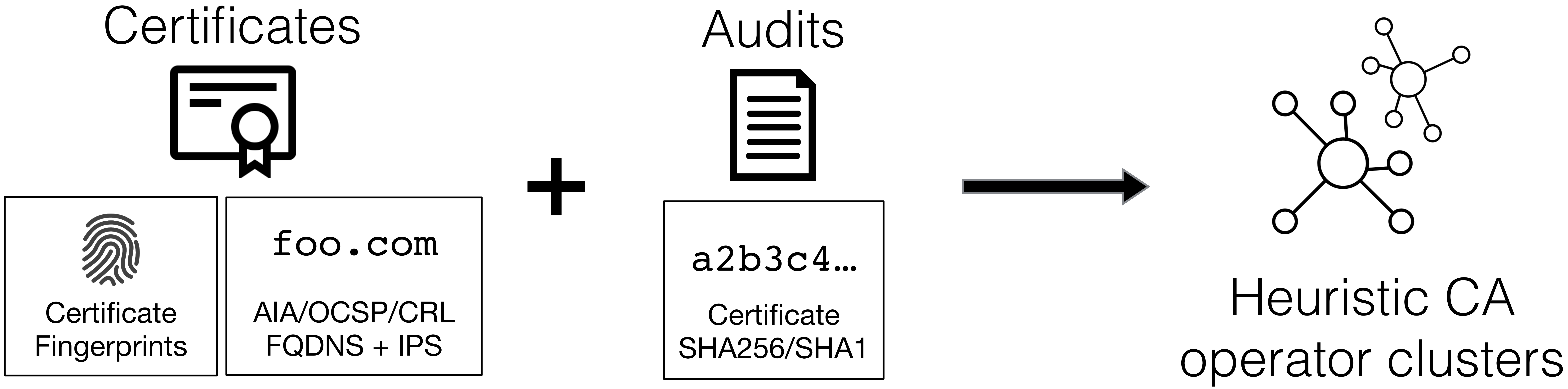
Previous Work

- No prior academic work on this problem
- Mozilla-organized Common CA Database (CCADB)
    - CCADB "owner" has intentional administrative focus - for CAs to upload policies and audits
    - E.g. Several Let's Encrypt certificates (cross-signs) are "owned" by IdenTrust, despite being operated by Let's Encrypt
    - Incomplete coverage: 20% of CA issuers trusted by Microsoft/Apple/Mozilla are not in CCADB

Approach

How can we determine the *operator* of a CA certificate / issuer?

1. Measure CA operational features to detect CA certificates with shared CA operators



Certificates

Certificate Fingerprints

foo.com

AIA/OCSP/CRL FQDNS + IPS

+

Audits

a2b3c4…

Certificate SHA256/SHA1

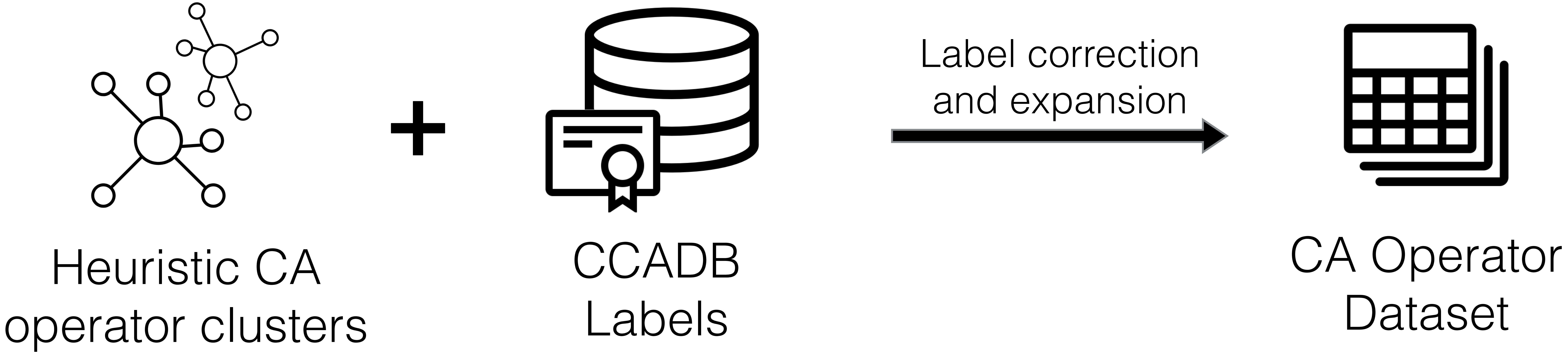
Heuristic CA operator clusters

Approach

How can we determine the *operator* of a CA certificate / issuer?

1. Measure CA operational features to detect CA certificates with shared CA operators

2. Carefully apply CCADB to label CA operator clusters



Heuristic CA operator clusters

+

CCADB Labels

Label correction and expansion

CA Operator Dataset

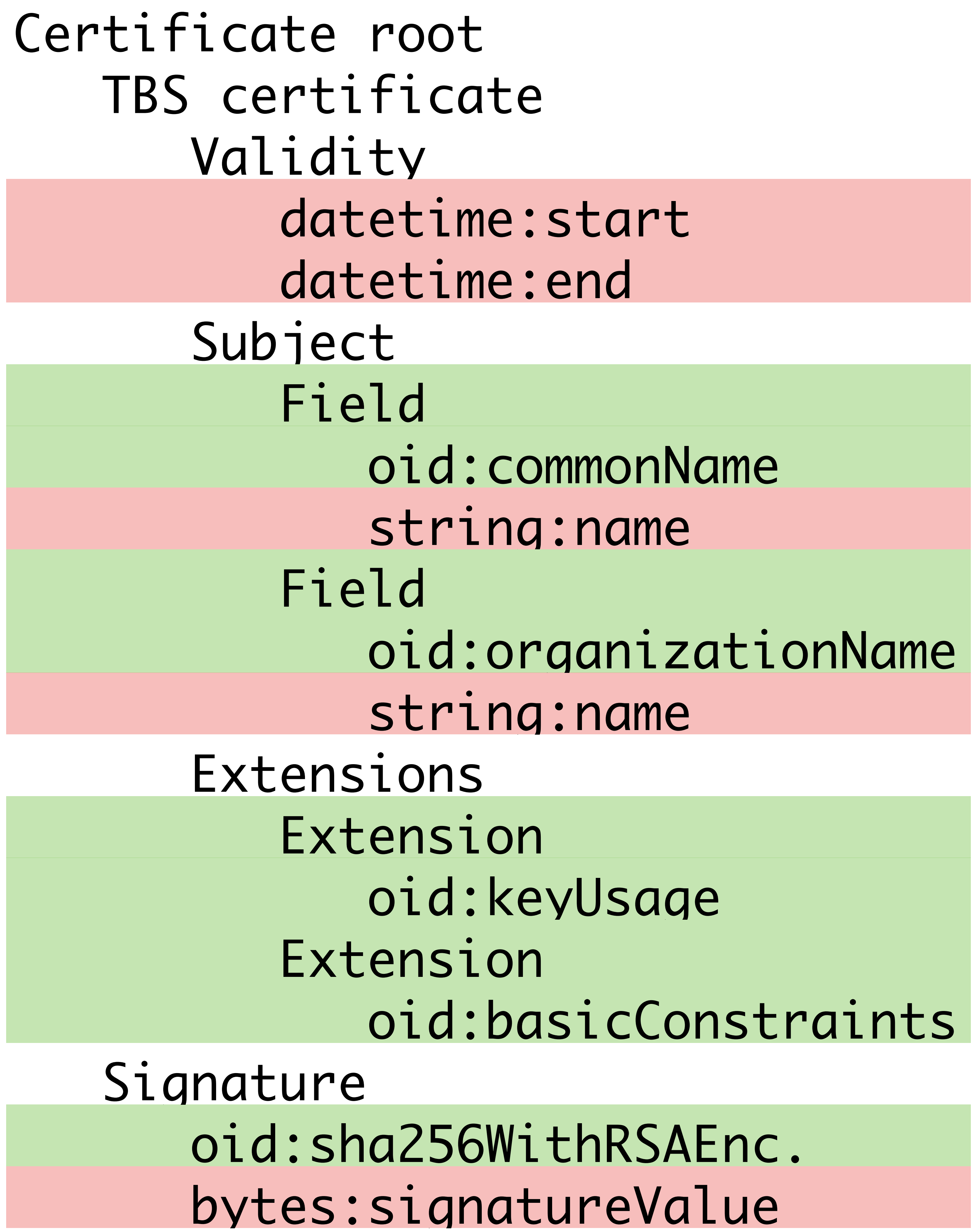
Certificate Fingerprints

Novel method to detect artifacts of issuance software/configuration

Goal: distinguish certificate entropy caused by issuance software from all other certificate entropy (e.g. serial number, public key value, subject name)

Insight: certificates are structured as an ordered tree (ASN.1 format), and issuance infrastructure controls the structure/order of tree

Certificate Fingerprints



```
Certificate root
   TBS certificate
      Validity
         datetime:start
         datetime:end
      Subject
         Field
            oid:commonName
            string:name
         Field
            oid:organizationName
            string:name
      Extensions
         Extension
            oid:keyUsage
         Extension
            oid:basicConstraints
   Signature
      oid:sha256WithRSAEnc.
      bytes:signatureValue
```

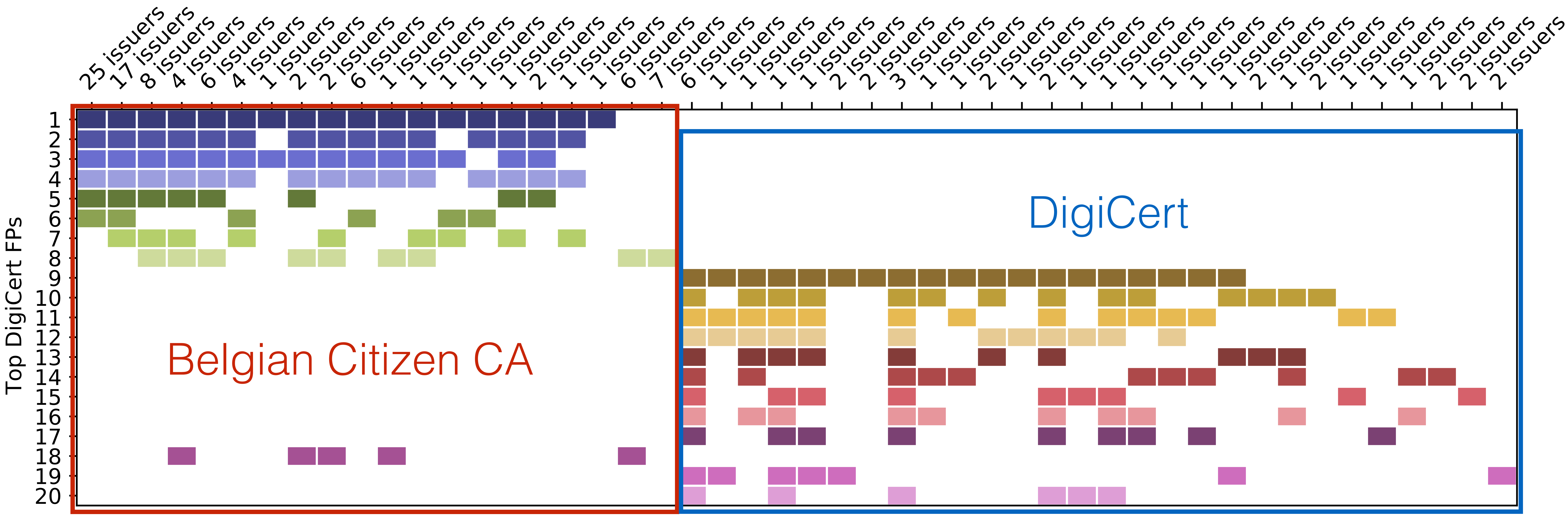
Issuance software-independent entropy:
validity, subject names, signature

Issuance software-dependent entropy:
type and order of subject fields / extensions

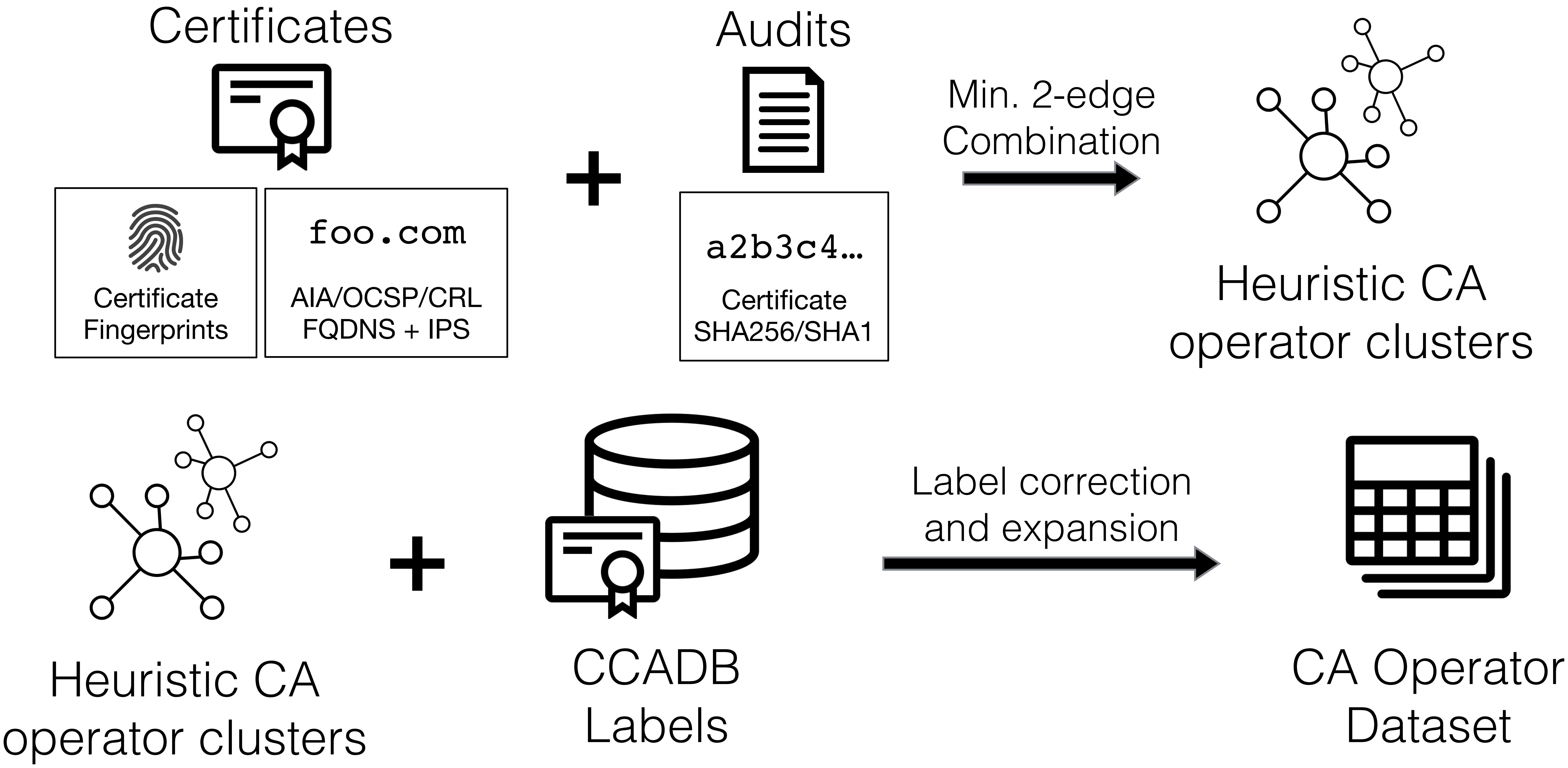
Fingerprint = structure of certificate, ignoring all leaf node values beside enumerable OID

Certificate Fingerprints

CA issuers grouped by *issuance profile,* which is the set of issued FPs



Pipeline



Certificates

Certificate Fingerprints

`foo.com`

AIA/OCSP/CRL FQDNS + IPS

+

Audits

`a2b3c4…`

Certificate SHA256/SHA1

Min. 2-edge Combination

Heuristic CA operator clusters

Heuristic CA operator clusters

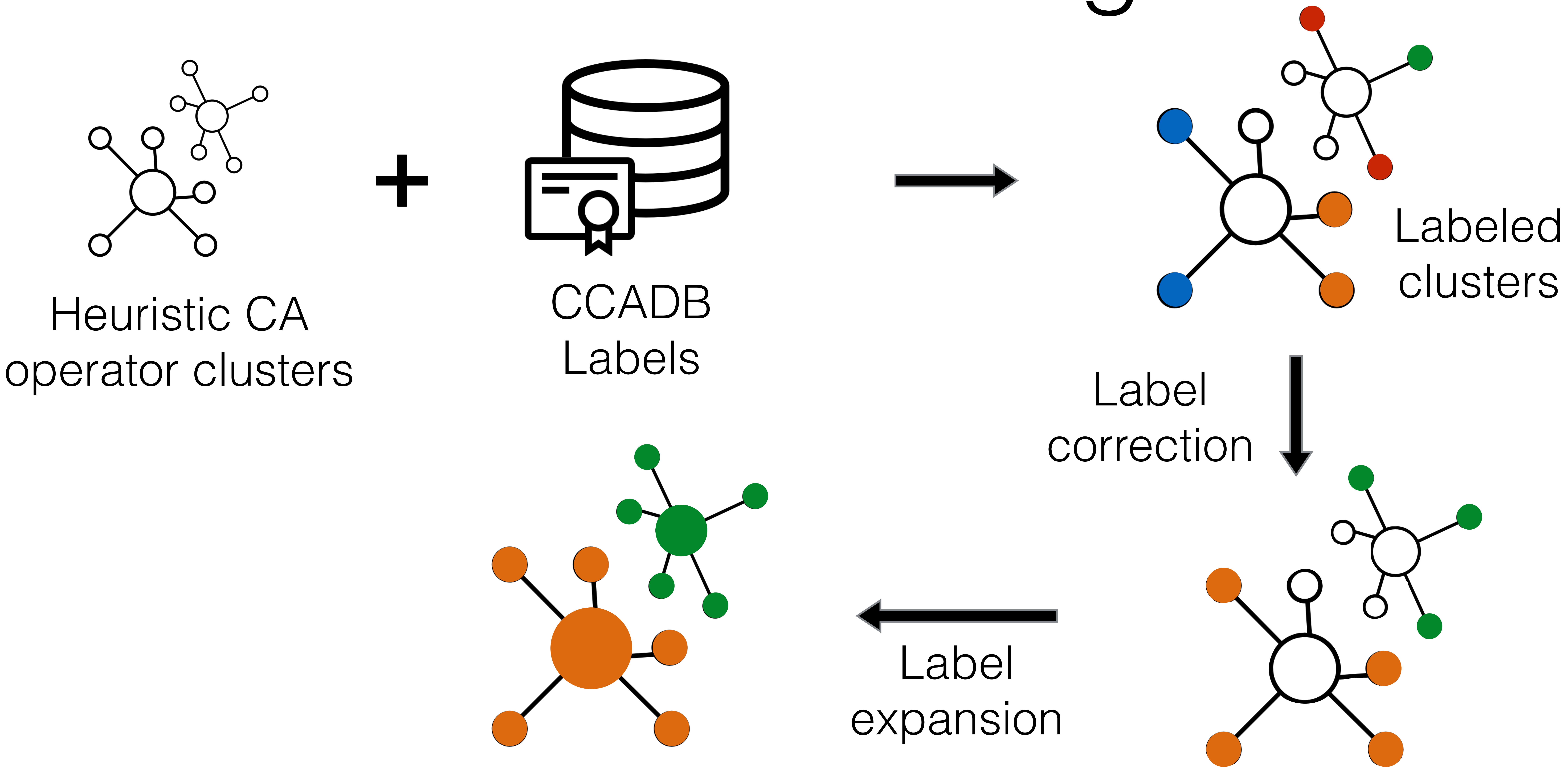
+

CCADB Labels

Label correction and expansion

CA Operator Dataset

Cluster labeling



Heuristic CA operator clusters

+

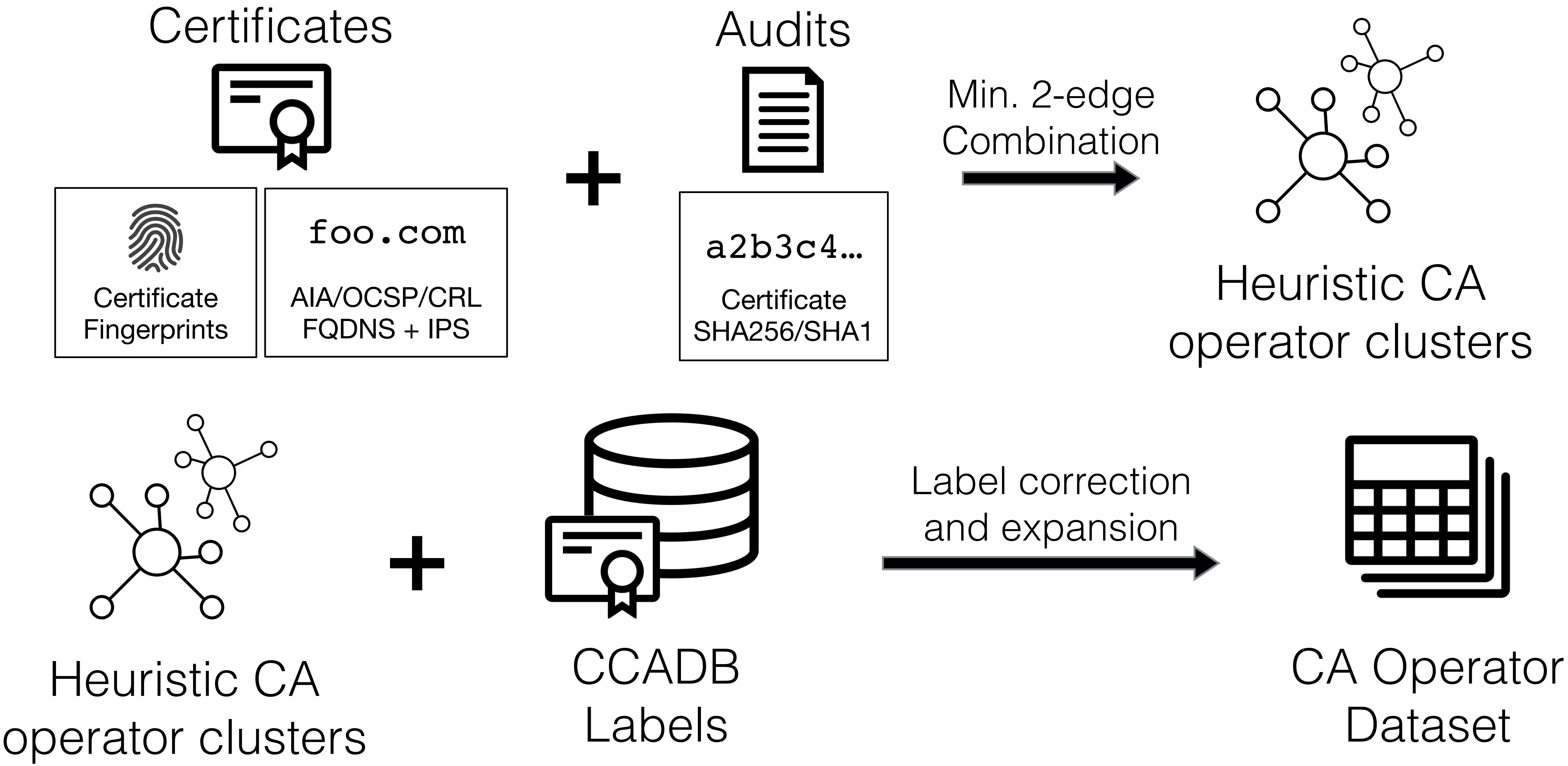
CCADB Labels

Labeled clusters

Label correction

Label expansion

Pipeline



Certificates

Certificate Fingerprints

foo.com

AIA/OCSP/CRL FQDNS + IPS

+

Audits

a2b3c4…

Certificate SHA256/SHA1

Min. 2-edge Combination

Heuristic CA operator clusters

Heuristic CA operator clusters

+

CCADB Labels

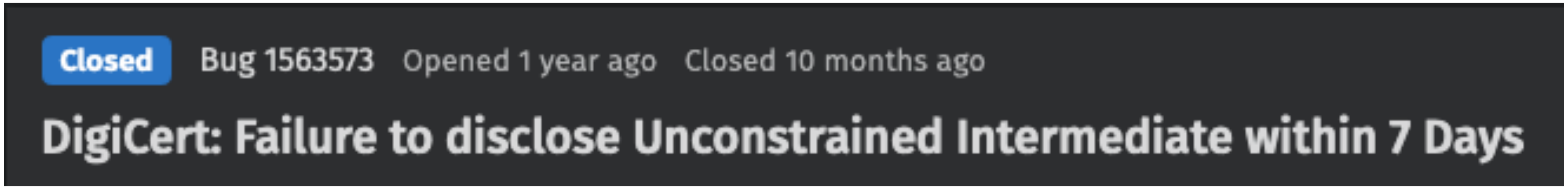
Label correction and expansion

CA Operator Dataset

Evaluation

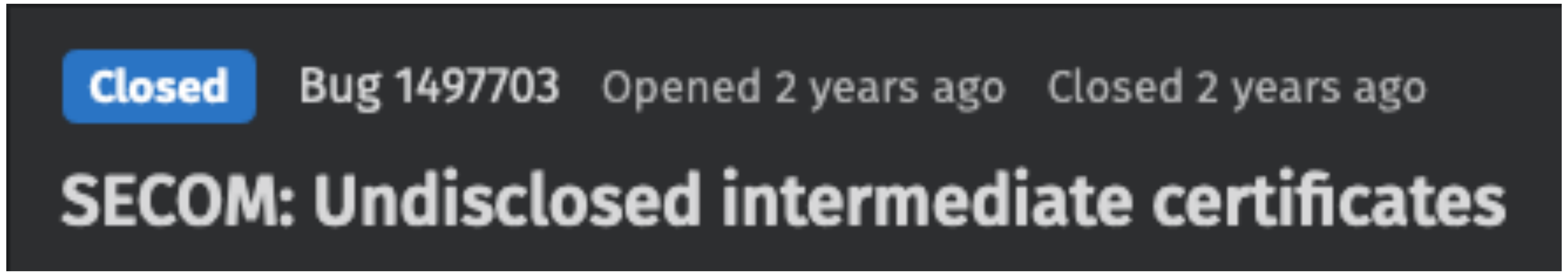
No ground truth data!

Best approximation: manually resolved disclosure issues



Closed Bug 1563573 Opened 1 year ago Closed 10 months ago

DigiCert: Failure to disclose Unconstrained Intermediate within 7 Days



Closed Bug 1497703 Opened 2 years ago Closed 2 years ago

SECOM: Undisclosed intermediate certificates

Evaluation

Found all issues from May 2014 - July 2019

	Issuers	Issuers Resolved By Dataset	Issues	Issues Resolved By Dataset
Operational Issuers	103	48 (46.6%)	22	7 (31.8%)

100% specificity

46.6% recall

Discoveries

Improperly disclosed Camerfirma subordinate CA (MULTICERT)[1], yet another issue leading to Camerfirma removal from Mozilla

Refined CA operator label for 189 issuers (241 CA certificates)

Added new labels for 404 unlabeled issuers (651 CA certificates)

[1] https://bugzilla.mozilla.org/show_bug.cgi?id=1672029

Summary

CA certificate name != CA that operates the certificate key

Measurements of CA operations —> new CA operator dataset

CA operational transparency means:

1. More informed root store decision making
2. More accurate research / issue attribution

What’s in a Name?
Exploring CA Certificate Control

Zane Ma

University of Illinois Urbana-Champaign

zanema2@illinois.edu
https://zanema.com