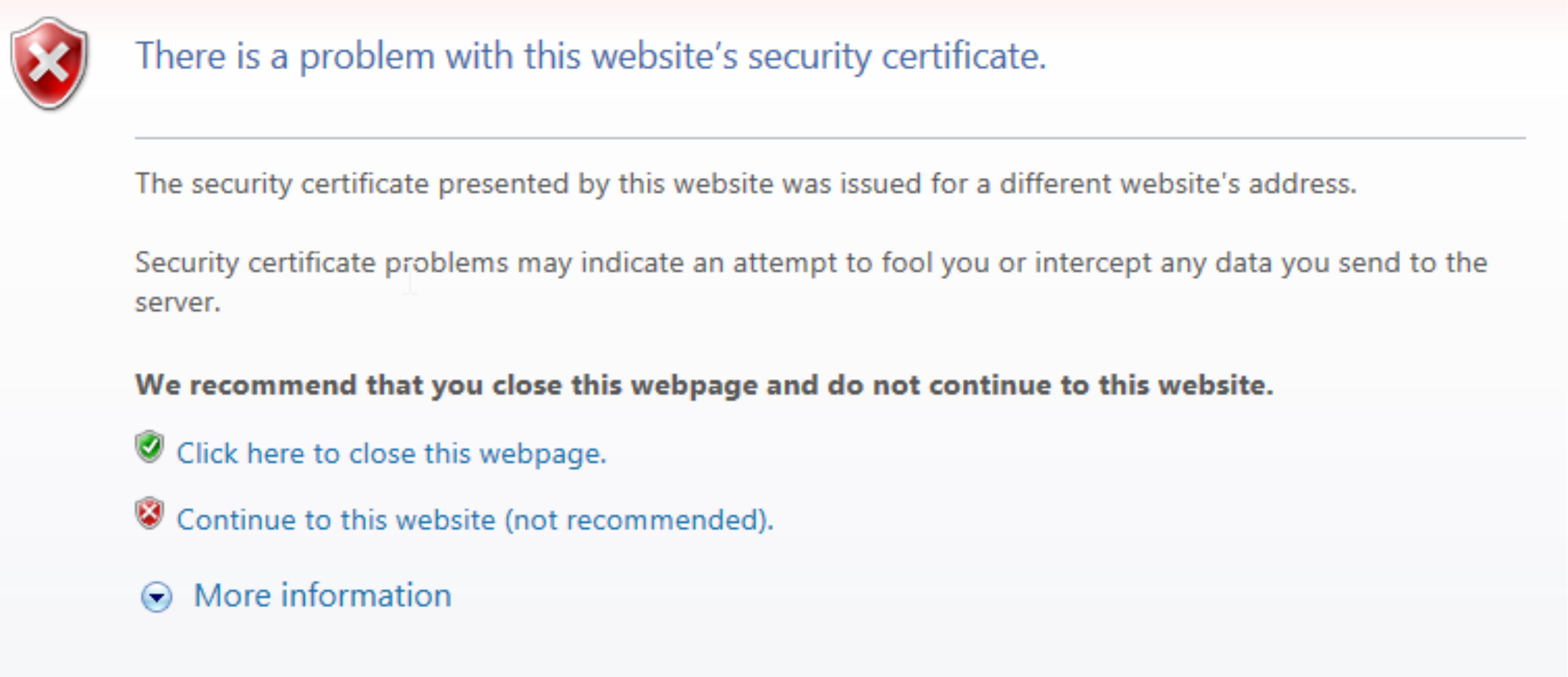
WebPKI and Non-Governmental Governance of Trust on the Internet

Karl Grindal, Vagisha Srivastava, Milton Mueller

How has trust been built into the Internet?



There is a problem with this website's security certificate.

The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

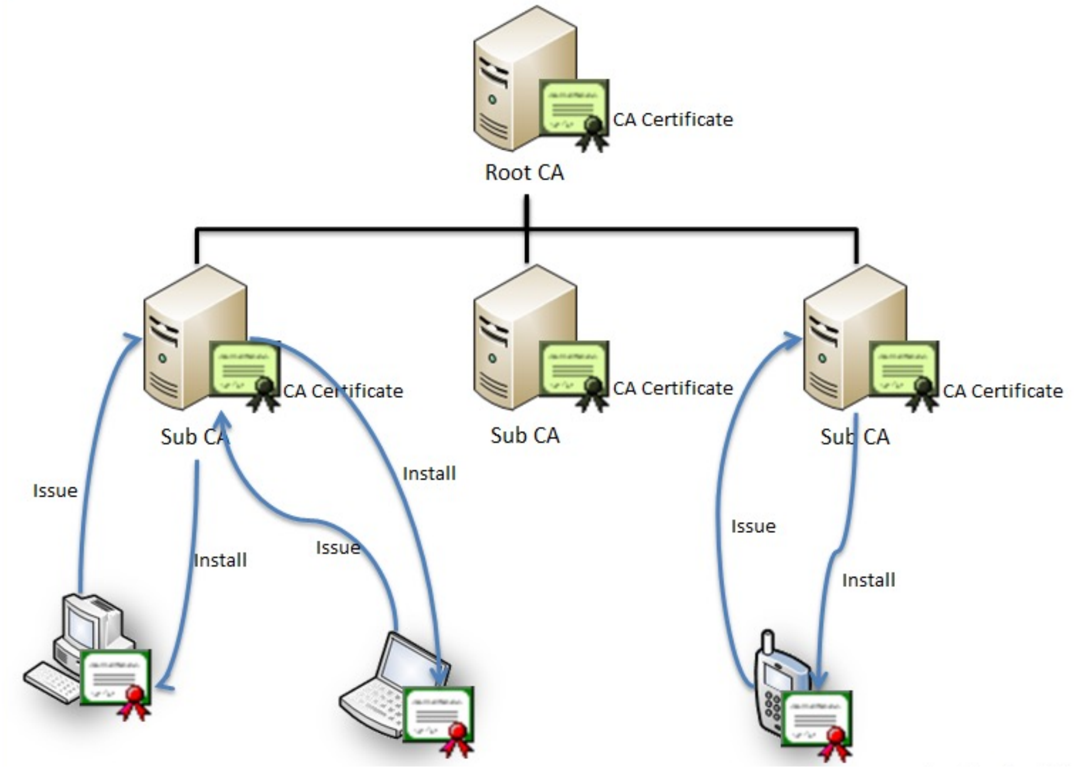
We recommend that you close this webpage and do not continue to this website.

✓ Click here to close this webpage.
✗ Continue to this website (not recommended).
More information

Public Key Infrastructure (PKI)

Trust Model

Hierarchical Trust: Certificate Authorities (CAs) manage a hierarchical tree of trust



Root Stores: A list of trusted Certificate Authorities. Most often managed by browsers and operating systems

WebPKI as Wild West:

Pre-2012 Certificates Set Their Own Standards

digicert®

Symantec

Trustwave®

GlobalSign

Go Daddy.COM

COMODO
Certification Authority

Industry Reform Instigated by Breach

A September 2011 security breach led the Dutch company DigiNotar to issue over 500 fraudulent certificates.

Investigation sponsored by the Dutch Government revealed primary aim of the breach was to man-in-the-middle Iranian Gmail users.

Industry Reform Instigated by Browsers

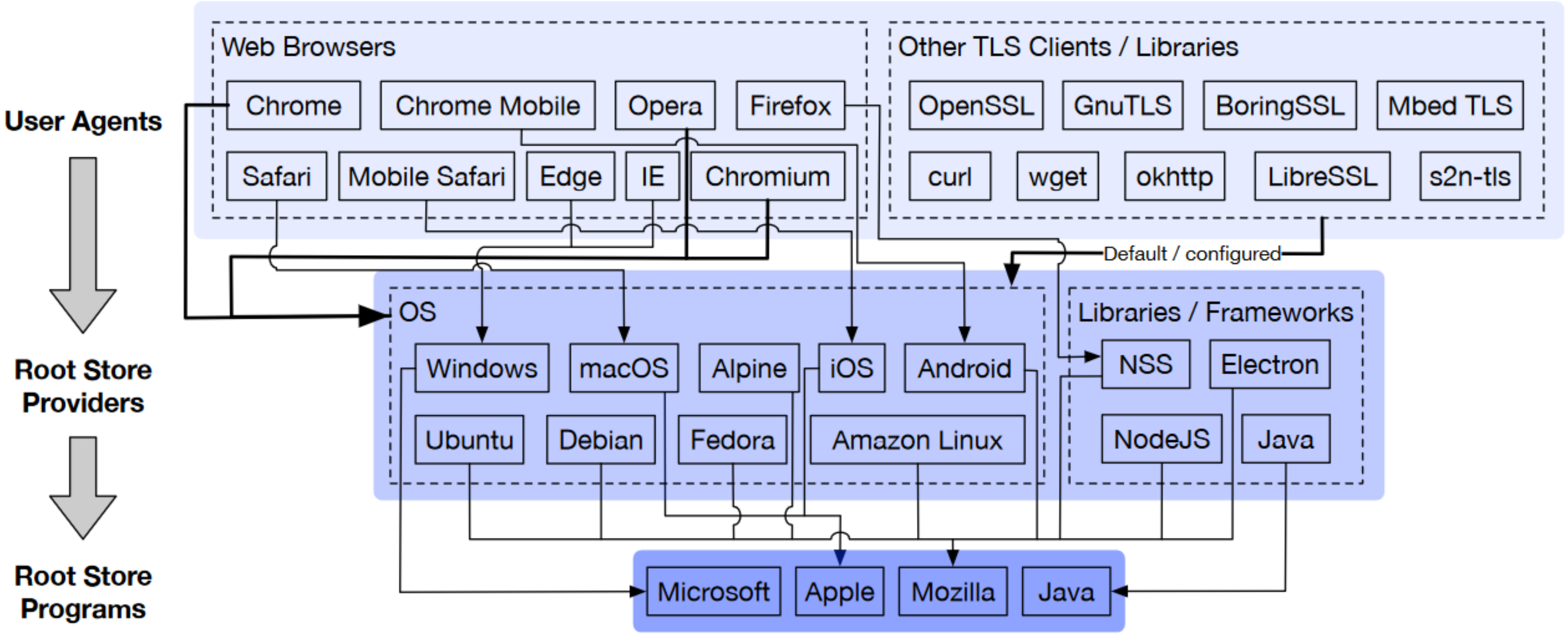


Figure 2: Root Store Ecosystem—The TLS root store ecosystem is an inverted pyramid, with a majority of clients trusting one of four root families.

Zane Ma et al. “Tracing Your Roots” (2021)

CA/Browser Forum

“Organized in 2005, we are a voluntary group of certification authorities (CAs), vendors of Internet browser software, and suppliers of other applications that use X.509 v.3 digital certificates for SSL/TLS, code signing, and S/MIME.”

Characteristics:

- An unincorporated association
- Brings together two unique constituencies
- Standards based organizations
- No enforcement powers

CAB CA/BROWSER FORUM

CA/Browser Forum Led Reforms

2012

- Organizational Reform: CA/Browser Forum Bylaws v. 1.0
- Standards for issuing SSL/TLS certs: 1.0 Baseline Requirements

2013

- Cybersecurity requirements: Network and Certificate System Security Requirements
- Standards for transparency: Certificate Transparency Initiative

2014

- Standards for auditing: WebTrust Program for Certification Authorities

2019

- Code signing standards - Baseline Requirements v1.2

The Forum’s Internal Structure

- Managed by the Forum Infrastructure Working Group (FIWG)

- CA Browser Constituencies
    - Certificate Authorities (55 voting organizations)
    - Browser Software Vendors (11 voting organizations)
    - Associate Members (7 non-voting organizations)

- Subject Area Working Groups (WGs)
    - S/MIME Certificate WG (2014)
    - Code Signing Certificate WG (2015)
    - Network Security WG (2017)
    - Server Certificate WG (2018)

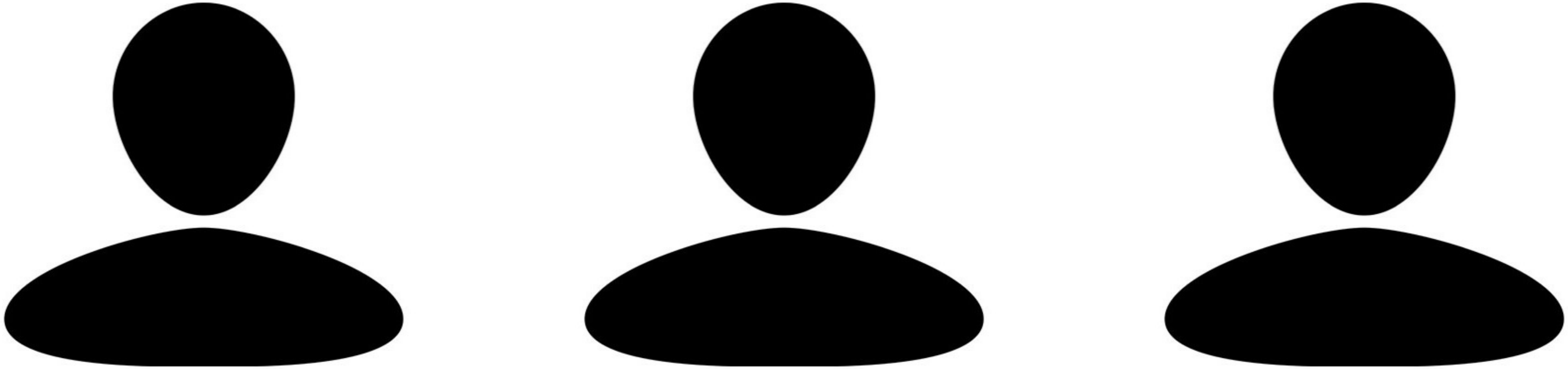
CAB CA/BROWSER FORUM

Associate Memberships

Participation of Associate Members is by invitation only.

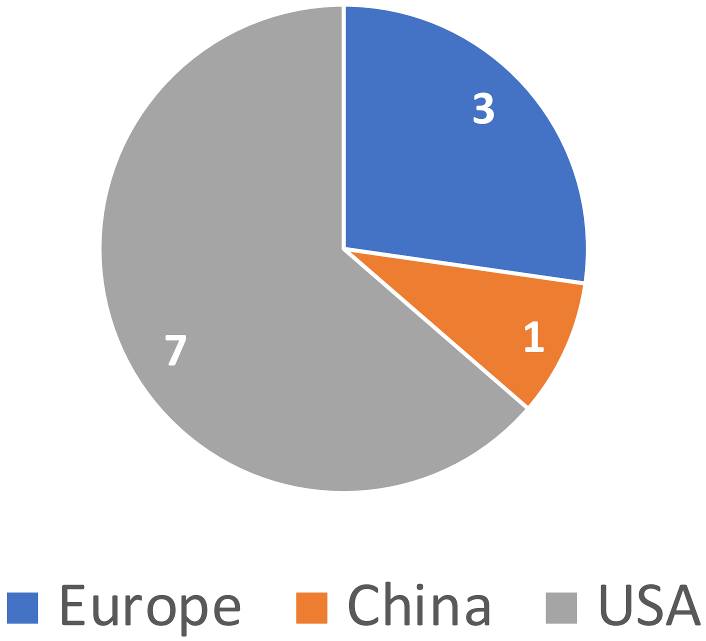
- International Organizations
  - ETSI (Europe)
  - ICANN (International)
- National Associations and Government CAs
  - ACAB’C (US)
  - tScheme (UK)
  - US Federal PKI Policy Management Authority (US)
  - WebTrust (Canada)
- Applicant Certificate Authorities
  - TrustAsia Technologies, Inc. (Chinese)
  - Zone Media OÜ (Estonia)

Membership: Who participates?

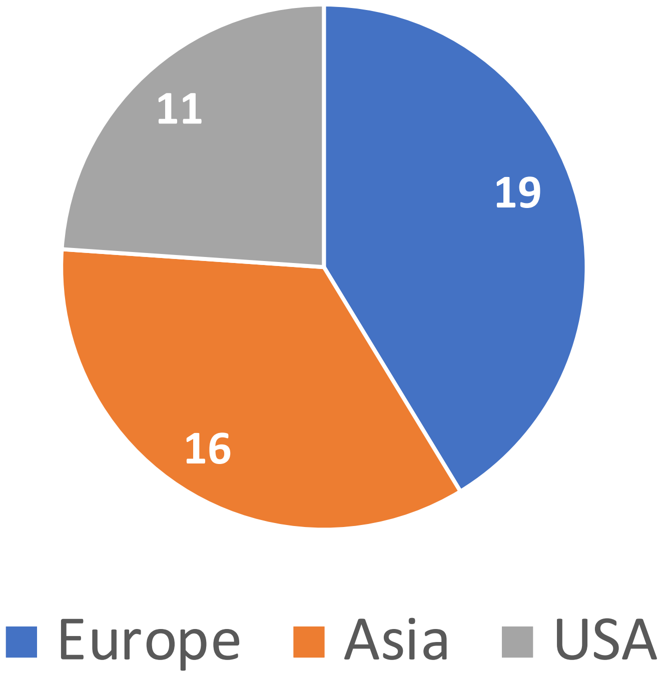


Geographical Range of CA/B Forum Members

Browser Members



CA Members



Data Methodology

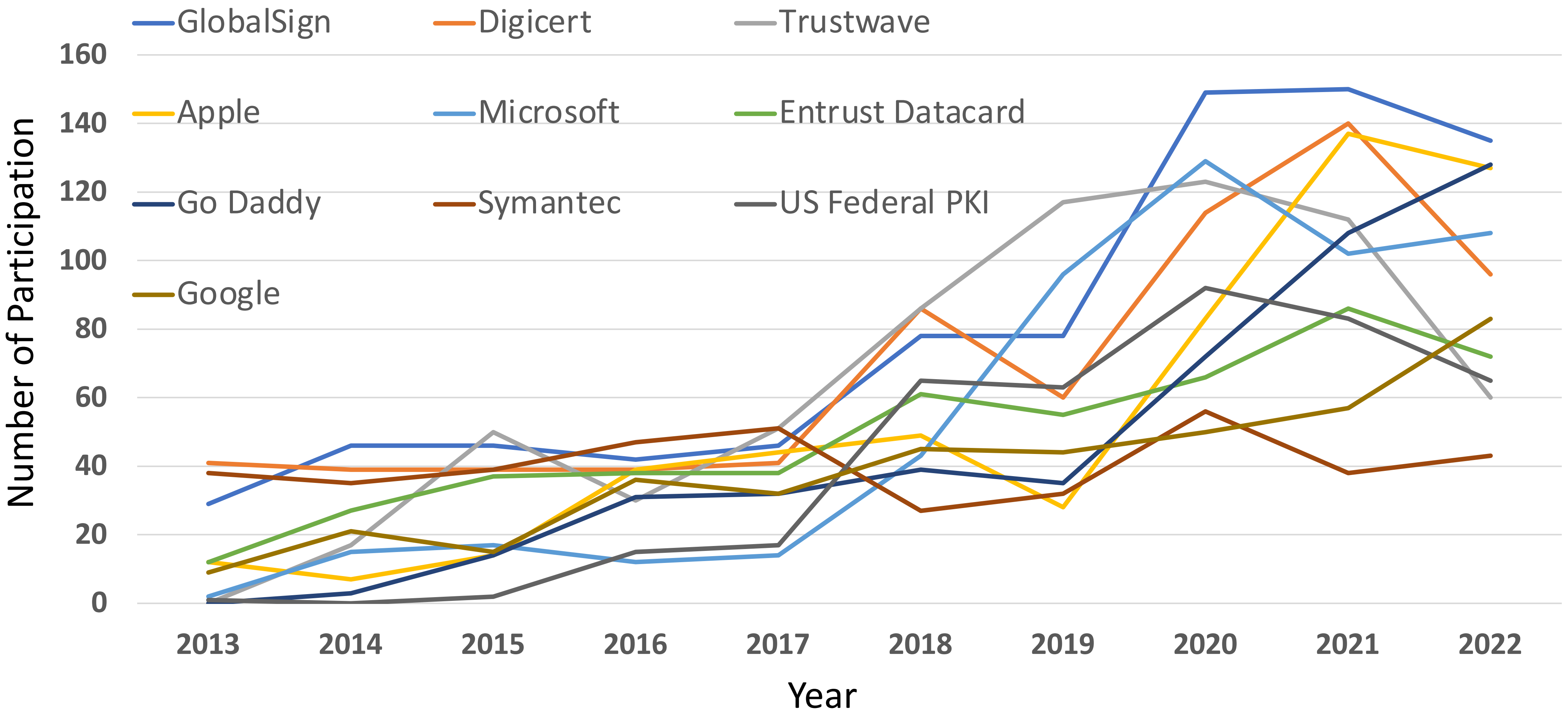
- Web-scraped 373 minutes from the CA/Browser Forum
- Cleaned 618 unique attendee records to identify 553 attendees from 123 organizations
- Coded meetings for working groups
- Coded companies for country of headquarters

Preliminary Data

Exploring the Minutes and Ballots of the CA/B Forum available online from 2013 to present

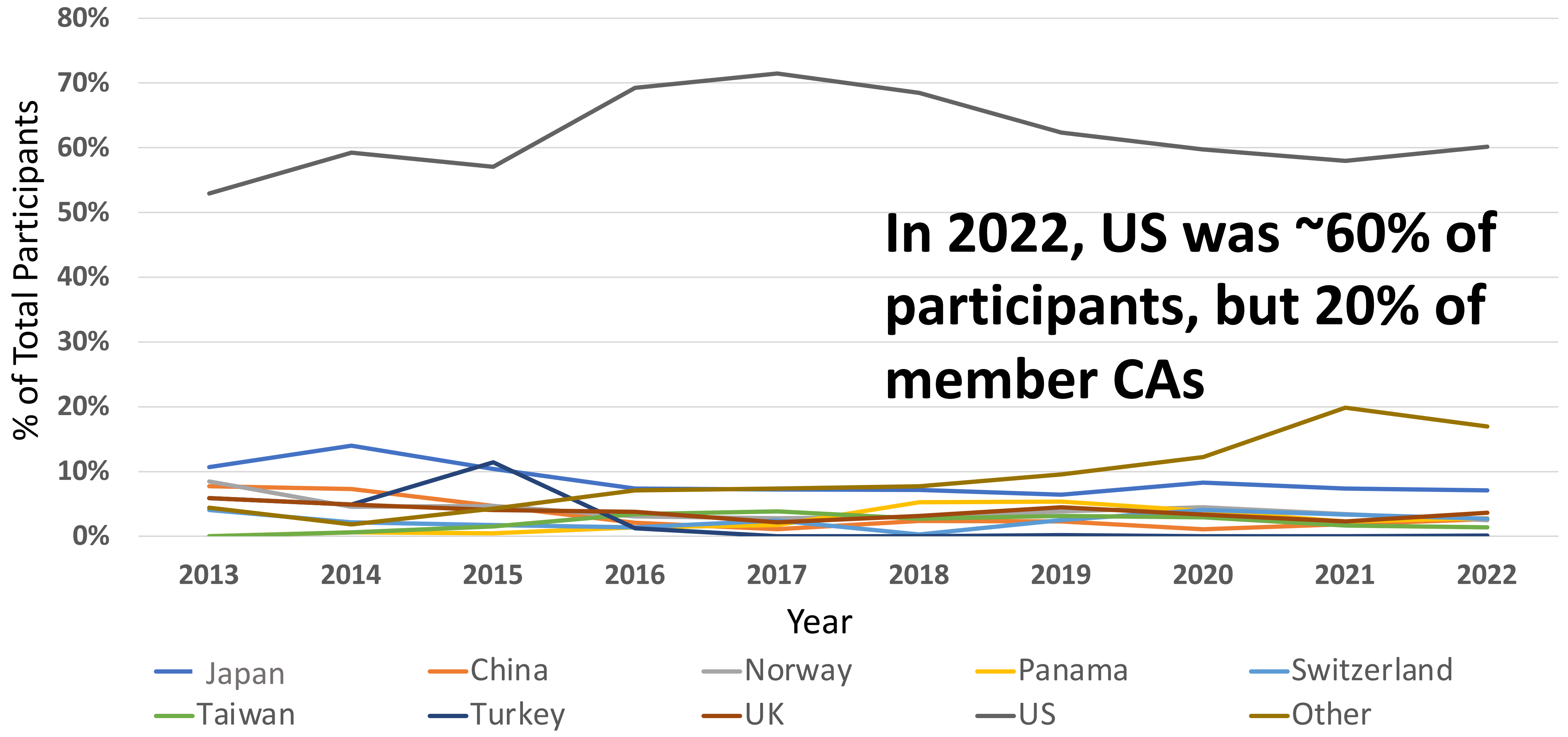
Row Labels	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	Grand Total
CA/Browser Forum	23	23	24	24	23	24	23	24	14	15	217
Code Signing Certificate WG									9	14	23
Network Security WG										1	1
Server Certificate WG						11	19	21	17	16	84
S/MIME Certificate WG								11	23	14	48
Grand Total	23	23	24	24	23	35	42	56	63	60	373

Major Organization Participation over Time



Headquarter Location of Meeting Participants

From attendees with listed organizations the percentage of yearly attendance by associated nationalities



In 2022, US was ~60% of participants, but 20% of member CAs

Concentration in the Certificate Market

Method:

- Data: CommonCrawl, non-profit Foundation crawler for whole of Internet corpus of web data.
- Random Sampling of 1 million URLs
- Python script used to extract Certificate Organizations
  - Excludes websites without Certs
  - Excludes websites with excessively long load times (10+ seconds)

Findings:

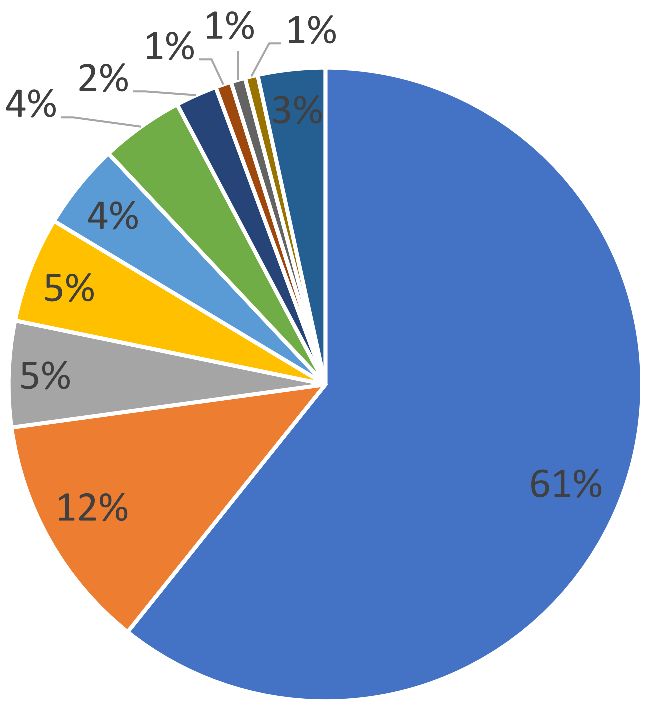
- Identified 2,366 unique Cert Orgs for 487,476 websites or 48.7% of sample.

Herfindahl Hirschman Index (HHI)

measures market concentration.

$$HHI = \sum_{i=1}^{N} (MS_i * 100)^2$$

Concentration in the Certificate Market

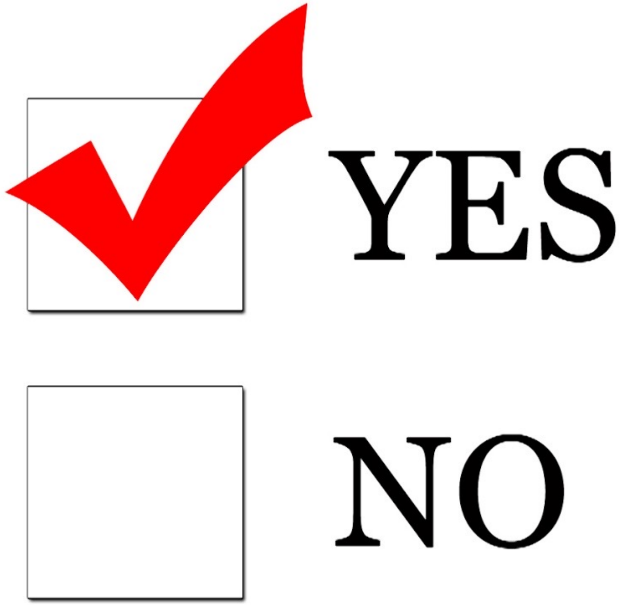


HHI: 3,942.8

High Concentration (>2,500)

80% of Sample were CA/B Forum Members

Voting: How do participants vote?



Ballots and Voting

I. Of 192 Ballots since February 2013

- 174 received quorum (Half of current active members present)
- 156 ballots were passed

  Requires support of at least 2/3rds of CAs and a majority of browsers

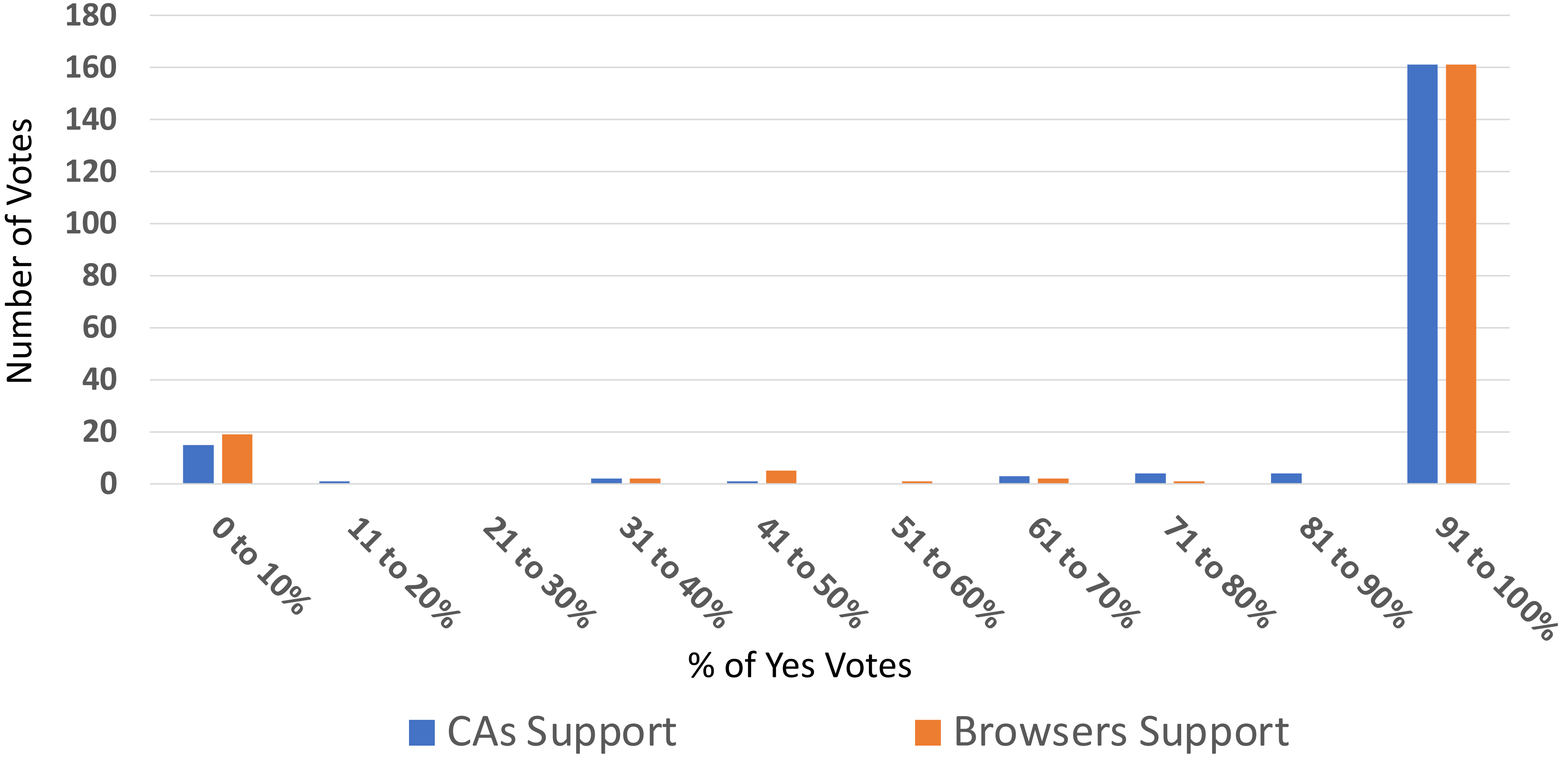
II. Voting Behavior

- Certificate Authorities average 16.6 participating members per vote
- Browsers average 3.3 participating members per vote

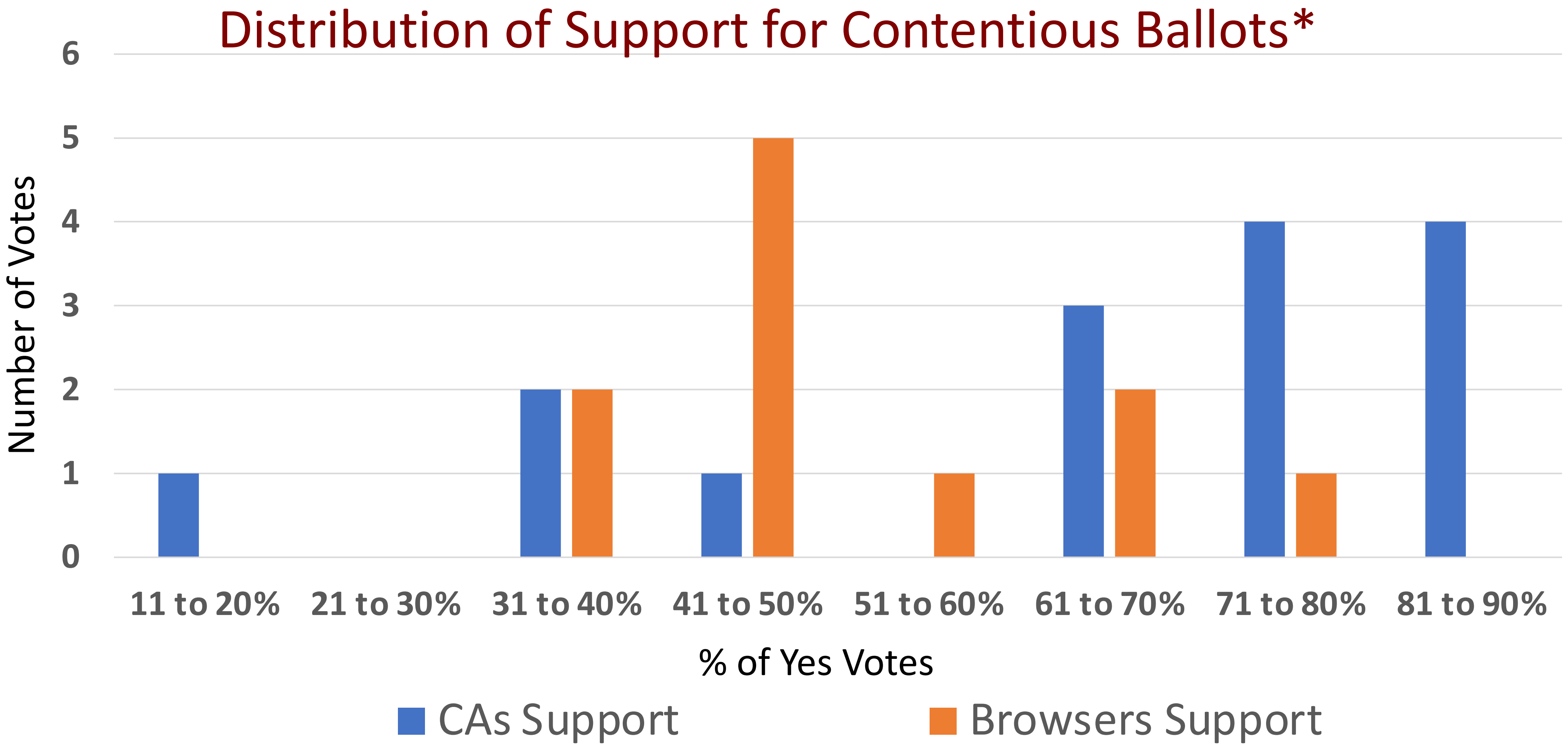
III. Contention Between Member Types

	CAs in Favor	CAs Opposed
Browsers in Favor	156	4
Browsers Opposed	11	15

Distribution of Ballot Support



Contention within Member Types



*Defined here as those ballots where between 10% and 90% of constituency supports the ballot.

Findings

- An unincorporated industry-based standards setting organization with two primary stakeholders, certificate producers and consumers.
- Pareto principle: Few members are highly active
- Active participants represent leading Certificate Authorities and Browsers
- While there are more European member organizations than US member organizations, US Participants are more active in their participation.
- If the market is not segmented, the growth of non-profit Let’s Encrypt has created high market concentration.
- Voting is consensus based with few ballots demonstrating conflict.

Questions

?