Web PKI and the Private Governance of Trust on the Internet

Vagisha Srivastava, Karl Grindal, Milton Mueller

Keywords: Internet Governance, Certificate Authority, Cybersecurity, Public Key Infrastructure

Introduction

Security in the digital realm, both in the physical and virtual domains, is a multifaceted concept that has sparked debates about its nature as a public good or a private good. At one end of the spectrum, public security is upheld by non-market organizations such as police forces and governmental military forces, funded through taxation, to ensure collective safety at local and national levels. Yet, even in these environments, individuals opt for private security measures, including home security services, locks, surveillance cameras, and firearms. In this capacity, security features are attributes akin to a private good, wherein individuals and businesses, irrespective of their size, engage in purchasing or self-production of services geared towards augmenting their physical security. Competing demands of public and private underscores the collective and individual demand for security which is sought both at the marketplace and the ballot box.

Similarly, the realm of cybersecurity mirrors this blend of public and private goods. Information security concerns manifest at various social levels, spanning from individual users to entire nations and global online applications and services. A thriving market has evolved around cybersecurity tools, devices, and services, with numerous commercial online service providers internalizing security costs to enhance their products' appeal. However, governments have increasingly asserted themselves in the cybersecurity and privacy domains, often citing market failures or the characterization of cybersecurity as a national-level, collective goods problem. Concurrently, geopolitical tensions impede global collective action in cybersecurity, as nations are reluctant to share sensitive information or cede authority over such a crucial domain.

This paper delves into the intricacies of security, exploring its dichotomous character in real-world contexts, where it can function as either a public or private good. In essence, the provision of security involves a blend of collective and individual efforts, encompassing a wide array of actors and domains. This paper conducts an in-depth analysis of how private actors collaborate to establish trust and security within the web ecosystem. It serves as a case study of the private provisioning of a global collective good, focusing on the evolution of the Public Key Infrastructure for the Web (WebPKI). The paper brings into focus an industry-formed entity, the Certificate Authority/Browser Forum (CA/B Forum), which acts as a nexus for cooperative regulation within WebPKI.

WebPKI, while not without its flaws, has evolved into a widespread and institutionally robust system, responsible for securing a significant portion of internet traffic, impacting billions of users and millions of websites. Importantly, most individual users do not bear the direct costs of this system; instead, organizations shoulder the financial burden. Although there exists an extensive body of computer science literature elucidating the technical intricacies of WebPKI, there remains a

dearth of economic analyses and minimal exploration of its status as a globalized governance structure.

Drawing on theories of collective action and public goods, this paper seeks to explain why and how the CA/B Forum emerged as a private sector-based governance structure, distinct from governmental intervention. It delves into questions regarding the economic sustainability of this arrangement and examines how the institution shapes relationships among diverse business interests. Furthermore, the paper identifies threats to the stability and resilience of the CA/B Forum, including its interactions with conventional territorial forms of political governance.

Relevant Literature

The classification of security as either a public or private good has long been a subject of debate within economic theory and policy studies. This section provides an overview of the literature that addresses this dichotomy, emphasizing the evolution of thought on public goods and collective action.

In economic theory, public goods are defined by their nonrivalrous consumption and non-excludability. (Samuelson, 1956) Originally, the theory of public goods was an attempt to theorize the boundary between the public and private sectors. (Stum, 2010; Desmarais-Tremblay, 2017) Resources or products with those special economic characteristics were supposed to make private production both inefficient (because non-rival consumption made it inefficient to exclude anyone) and practically impossible (because the inability to exclude "free riders" would undermine any chance for private businesses to recoup their costs). The market would "underproduce" public goods. As a result, it was posited that only state intervention, with its taxing authority and coercive powers, could remedy the underproduction of public goods.

However, the alignment of public goods exclusively with state action faced theoretical and empirical challenges. Many services provided by the state do not meet the defined criteria of a public good,[1] prompting a reframing of the problem in terms of collective action. It became evident that collective action did not inherently necessitate state involvement; instead, it could be achieved through non-state actors.[2] This shift in perspective paved the way for extensive literature on political economy and governance, emphasizing that governments represented just one avenue for collective action, not necessarily the most effective one in all scenarios. Non-state actors repeatedly demonstrated their ability to overcome coordination and exclusion challenges to engage in effective collective action, underscoring that private actors could contribute to the provision of public goods.

Non-proprietary technical standards, which play an important role in Internet and Web governance, are one of the most obvious examples of privately produced collective goods. (Kindleberger, 1974; Berg, 1989) Another important insight is that collective action can be used to produce outputs that are not, strictly speaking, public goods. The work of Elinor and Vincent Ostrom (E. Ostrom 1990,

[1] K-12 education is one obvious example. Schools are neither nonrival in consumption nor impossible to exclude. Many services formerly or currently provided by the government, such as telephone and postal services also do not meet public good criteria.

[2] Mancur Olson's (1971) economic analysis of collective action showed various ways in which self-interested actors could overcome incentive barriers to joint action. The paradigmatic public good cited by Samuelson - broadcasting - was even at that time a service provided by private industry. The exclusivity problem was overcome via a two-sided market, which used advertisers rather than the state to subsidize audience access to programming.

2010; V Ostrom 1999; Lemke and Tarko, 2021) has emphasized the ability of communities to engage in self-governance of common pool resources (CPRs). Efficient management of CPRs does pose exclusion and coordination problems, necessitating collective action, but CPRs by definition are not non-rival in consumption and thus do not qualify as public goods. Thus, the production of goods necessitating coordination and cooperation, whether strictly public or not, could be facilitated through collective action by diverse entities.

This paper leverages this nuanced approach to collective governance to investigate the collective action challenges addressed by WebPKI and elucidate why it evolved predominantly within the private sector, with limited state involvement. In doing so, it offers an innovative perspective on the dynamics of public and private goods in the context of Internet security.

Methodology

Our research method approaches the WebPKI as a governance institution instead of simply as a technical system. Our method is based on institutional analysis which consists of four core steps:

1. Identification of the sought-after benefits that necessitate collective action, elucidating why these benefits require coordination and cooperation.

2. Identification of stakeholder groups and interests that have converged to negotiate coordination and cooperation modes, accompanied by an assessment of how these groups' political-economic interests align or diverge.

3. Identification of the institutionalized equilibrium among these stakeholder groups, viewed through the lens of political economy theory, with an emphasis on the explicit rules and procedures ratified by the stakeholders.

4. Evaluation of the resilience and stability of the institutional equilibrium, exploring potential destabilizing factors and elucidating why private actors have assumed a predominant role in this context.

This analytical approach combines qualitative and quantitative techniques:

- We obtained data about the identity, company affiliation, and meeting attendance of participants in the CA/B Forum from published meeting minutes. The twice-monthly meeting records we scanned began on January 24, 2013, and ended on July 28, 2022. This provided a list of 564 names of individuals, their organizational affiliation, a measure of how many meetings they attended, and how their attendance changed over time. This data also allowed us to track the participation of major organizations and to identify some of the most active players in the regime.
- We conducted 10 semi-structured interviews with practitioners with high participation rates in the CA/B meetings. Our choice of interview subjects was not random but favored some of the most active participants, and of course, was dependent upon the willingness of individuals to be interviewed. We also engaged in a purposive selection of interview subjects based on categories that we felt might have distinct perspectives, such as which company they worked for, whether they worked for a CA or a browser/OS company, their geographic region, and native language.

- We used keyword searches to retrieve meeting minutes that addressed some of the known areas of change, conflict, and negotiations. We manually read these minutes to identify issues of contention or discussions of major decisions. We also used ChatGPT to query the whole record of meeting minutes around issues of interest.
- We counted and reviewed the ballots of the CA/B Forum, which have been available online from 2012 to 2022.
- We developed measures of the market share of Certificate Authorities by randomly selecting 1 million URLs from the approximately 3 billion unique URLs indexed by the non-profit foundation Common Crawl. We then used a Python script to pull certificate organizational info from our sample websites. One limitation of this method is that we set a time limit of 10 seconds for the page to load, a necessity given we ran through a million sites but one that potentially induces bias.
- We estimated the market share of browsers and root store holders drawing upon industry statistics. Employ quantitative metrics to identify how factors like market share in browsers and certificates relate to organizational behavior in the consortium.

These methods converge to offer a comprehensive analysis of the WebPKI governance structure, shedding light on its evolution, actors, economic sustainability, and potential challenges to its stability.

Authentication as a Collective Good

Understanding the role of and need for collective action in WebPKI requires a somewhat detailed description of the technical system. WebPKI is a web-based component used for document encryption, digital signature, and signature verification. It relies on a combination of cryptographic techniques, digital certificates, and a hierarchy of trusted entities to provide a secure method of data transmission over insecure networks, notably the Internet.

A. Public Key Cryptography

WebPKI uses public-key cryptography or asymmetric cryptography to establish secure connections between web users and websites. In this cryptographic system, each participant (usually a web server or a web browser) has a pair of cryptographic keys: a public key and a private key. These keys are mathematically related, but it is computationally infeasible to derive the private key from the public key. The public key is intended to be widely shared and is used for encryption and verification. It can be freely distributed to anyone. When someone wants to send you secure data or messages, they use your public key to encrypt the information. The private key, on the other hand, is kept secret and known only to the owner. It is used for decryption and signing. When you receive encrypted data that was encrypted with your public key, you use your private key to decrypt it and retrieve the original information. Additionally, when you want to digitally sign a document or message to prove its authenticity, you use your private key to create a unique digital signature.

In addition to cryptographic techniques, secure communication requires some form of authentication - a means of binding the person holding a private key to that person's public key.

B. The problem of Authentication

Once the client and the server have authenticated each other, they can encrypt their communications by running TLS, a standardized transport protocol that allows two parties to encrypt and decrypt their messages. Running the TLS protocol is the easy part, however. Both the website operator and the party they are transacting with have an incentive to keep their traffic confidential. Their use of encryption depends only on their choice of communication partners, not on anyone else. While encryption requires industry-wide technical standards such as TLS, which are collective goods (Berg, 1989), as long as the two parties can authenticate each other, the adoption and use of encryption on the public Web does not require any special forms of institutionalized collective action.

The hard part - the public good that necessitates collective action - is the authentication process. It requires a reliable and trustworthy mapping of the private key holder to the public key. In the WebPKI ecosystem, this mapping is facilitated by public key cryptography using digital certificates. When a server presents its digital certificate (which includes its public key) during a secure connection setup, the client can verify the certificate's authenticity and trustworthiness. This helps prevent man-in-the-middle attacks and ensures that the client is communicating with the intended server. The operation of issuing and managing certificates requires a common authority structure.

Digital certificates are issued by Certificate Authorities (CA) to any entity on the web that needs authentication (web servers). Before issuing certificates, the process requires them to verify the identity of the organization or entity making the request. The certificates then act as recorded attestations that the holder is who they say they are, which can be queried over the network as needed. This verification may relate a certificate to a registered domain name or a legal person, like a corporation.

CAs are at the top of the trust hierarchy in WebPKI. They are responsible for establishing trust and vouching for the authenticity of entities and therefore act as third parties to provide a promise of security. But how do you know you can trust the CA to not be a bad actor? Who authenticates the authenticator?

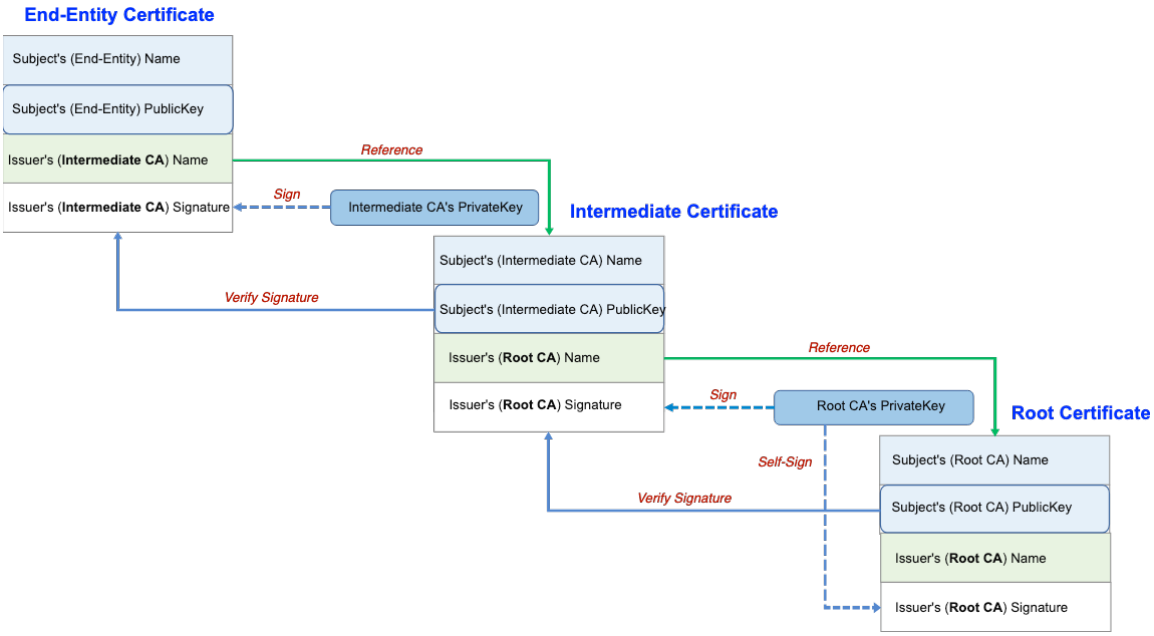
C. Trust Anchors and Chain of Trust

The answer is not prima facie, a very satisfying one. There are two types of CAs – a subordinate CA and a root CA. Subordinate CAs are validated by other CAs up until the chain reaches the root CAs which in turn uses root certificates for authentication. These are self-signed and act as trust anchors in X.509 architecture from which the chain of trust is derived.[3] Trust anchors, in cryptographic hierarchical system structure – like the CAs, are entities for which trust is not derived but assumed.[4]

[3] Reddy, Raksha, and Carl Wallace. Trust anchor management requirements. No. rfc6024. 2010. (https://www.ietf.org/rfc/rfc6024.txt)

[4] Housley, Russ, Sam Ashmore, and Carl Wallace. Trust anchor format. No. rfc5914. 2010.(https://datatracker.ietf.org/doc/html/rfc5914)

Figure 1 – Certificate Chain of Trust[5]



Root certificates are often managed by large entities – organizations, corporations, and governments, go through a special, and much more rigorous vetting process, and have a longer validity, roughly around 20 years.[6] Root CAs undergo comprehensive audits of their technological and business operations, adhering to the specific standards and criteria outlined in WebTrust.[7] These audits are conducted by entities known as root store operators, which primarily include web browsers and operating systems. When a root certificate successfully passes this rigorous vetting process and becomes part of the root store, it assumes the role of a trust anchor. As a trust anchor, it is inherently accepted, providing the foundation for trust in the entire PKI system.

Currently, there are six WebPKI trust hierarchy termination points, or root stores (Ma, Austgen et al, 2021), though two of them are relatively minor: Apple, Microsoft, Mozilla, Google, Oracle, and Java. The authentication process creates strong technical interdependencies between browser software, the CA services, and the websites using HTTPS. The WebPKI system leverages these interdependencies to align the incentives of CAs, website operators, and the OS/tech platforms to enhance security for end users. The system is supposed to prevent certificates of untrustworthy CAs, or expired or invalid certificates, from working their way up the chain of trust. Websites with fake or untrusted certificates will receive warning messages from their browser software that the website is dangerous. The websites so deemed will still work, but users are more likely to turn away from them. This is WebPKI's only real method of penalizing/excluding bad actors.

---

[5] Source: https://support.mozilla.org/en-US/kb/secure-website-certificate

[6] This varies depending on the root store policy – See Microsoft's Root Store Policy requirement - https://learn.microsoft.com/en-us/previous-versions//cc751157(v=technet.10)?redirectedfrom=MSDN
Any entity is free to create longer-duration root certificates, but it will not be adopted and accepted by the root operators owing to their internal policy. So, it can be interpreted that they act as gatekeepers to this system, discussed in detail later in the paper.

[7] Housley, Russ, and Karen O'Donoghue. "Problems with the public key infrastructure (PKI) for the world wide web." IETF Draft (2017). (https://datatracker.ietf.org/doc/html/draft-iab-web-pki-problems-01)

The authentication of digital identities thus requires a collective governance structure. The CA/B Forum is analyzed as an instance of industry collective action; it brings together the small number of root store operators with dozens of CA providers to work out common standards and practices. The paper attempts to explain why collective action is needed to perform the authentication function. We want to see how well collective action/public goods theory can explain why the CAB Forum exists. Can they predict which problems are addressed by collective action in the browser forum and which problems are not? Can it explain why the production of collective security was conducted by private actors and not by governments? Can we say anything about the effectiveness of this mode of governance?

Stakeholders in the WebPKI ecosystem

There are two primary categories of stakeholders in the WebPKI ecosystem: Certificate Authorities (issuers of certificates) and Browsers and operating systems (OSs) vendors (consumers of certificates). Each group in turn claims to be sensitive to the needs of a larger consistency. CAs that issue certificates are attentive to their buyers. Browsers/OS vendors want to provide security to their end users. Only the first two are direct participants in the CA/B Forum.

A. Certificate Authority

Certificate Authorities are trusted entities or organizations that issue and manage SSL/TLS certificates. Digital certificates are used to establish the authenticity and identity of individuals, devices, or entities in online communications and transactions by linking the entity with its public key. There are three basic types of certificates: Domain Validated (DV), Organization Validated (OV), and Extended Validation (EV) certificates. DV certs are the most basic as they only verify the ownership of a domain name by sending verification messages to it. However, having ownership and being the proper owner is different. OV certs require the CAs to verify the identity of the organization operating the website. EVs entail further verification of additional business-related attributes.

In some cases, CA delegates the process of request collection, validation of users' information, and physical credential distribution to Registration Authorities (RAs). RAs are option systems in the WebPKI ecosystem. To create an efficient chain of trust, CAs and RAs should be separate entities.[8] But it is not uncommon to have CAs perform both tasks, as in the case of Godaddy and Comodo which offer EV SSL.

B. Browser/OS Vendor

Browsers and OSs play a crucial role in establishing trust in the web Public Key Infrastructure (PKI) system by acting as intermediaries between users and CAs. They are the root store operators, responsible for managing the trust anchors. Browsers and OS come pre-installed with a list of trusted root certificates, known as the root store. These root certificates belong to well-known CAs that have undergone rigorous validation processes. When users visit a secure website (using HTTPS), the web server presents its digital certificate, issued by a CA. Browsers and OS verify the

[8] Section [3.1.1.3.], Adams, Carlisle, Stephen Farrell, Tomi Kause, and Tero Mononen. Internet X. 509 public key infrastructure certificate management protocol (CMP). No. rfc4210. 2005. (https://www.ietf.org/rfc/rfc4210.txt)

authenticity of this certificate by checking if it has been signed by a trusted root certificate. If the certificate chain is trusted, the browser displays a padlock icon or a similar visual indicator to assure the user that the website is secure. They also maintain and regularly update a list of trusted root certificates referred to as a trust store.

C. Certificate Subscribers

This category is comprised of the entities to whom the certificate is issued. It includes Web server operators, website owners, corporate network managers, and other organizations. Certificate subscribers are not directly represented in the membership structure of the CA/B Forum. The CA stakeholders are proxies for the interests of this stakeholder group. Their interest in lowering the cost and maximizing the efficiency of the authentication process is balanced by their interest in the reliability of the authentication services.

The CA/B Forum: An Overview

A. Formation and Purpose

The early CA industry operated without a structured framework, characterized by experimentation rather than formal organization. From 1995 to 2005, certificates were issued with virtually no standardized governing rules in place. The CA/Browser Forum was founded in 2005 by a meeting in New York City initiated by Comodo, one of the larger CAs at the time. Interestingly, the initial objective of this meeting was to strategize the phasing out of Domain-Validated (DV) Certificates or in the words of one of our interview participants "come up with a plan to kill DV Certs." The emergence of affordable DV certificates, offered by CAs like Geotrust and GoDaddy, threatened the incumbent CA landscape by transforming the certificate industry into a high-volume, low-margin sector. The original proposal was to use the leverage of browsers to mandate an OV profile for all publicly-trusted certificates. This collective action between browsers and CAs was driven by concerns that DV certificate issuers were fueling a detrimental "race to the bottom," where CAs prioritized quantity over security. The solution was seen in establishing a shared set of fundamental requirements enforced by browser software.

The 2005 New York meeting morphed into the CA/B Forum, an unincorporated, informal meeting ground for CAs and Browsers. Its main accomplishment was to develop baseline requirements for EV certificates in 2007.

B. Governance Structure

These early efforts did not succeed in controlling the issuance of certificates. As the Internet grew, criticism of the inadequacies of the digital certificate system mounted. Academic literature called attention to the structural flaws in CA practices. (Roosa & Schultz, 2010; Vratonjic et al, 2011) The EFF started an SSL Observatory that released a critical report about WebPKI in 2010,[9] which the CA/B Forum found it necessary to publicly reply to.[10] In April 2011, the CA/B Forum released a

[9] Peter Eckersley, Jesse Burns, "An observatory for the SSLivserse." Defcon 18, July 2010. https://www.eff.org/files/defconssliverse.pdf

[10] Statement of the CA/Browser Forum Concerning the EFF's SSL Observatory (undated but some time in 2010). https://cabforum.org/wp-content/uploads/EFF_SSL_Observatory.pdf

request for public comment on a new set of "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates."[11]

The CA/Browser Forum as we know it today was transformed in the wake of the Diginotar Incident, described later in the paper. It is still an unincorporated industry association, but in 2011-12 it became a more vigorous and formalized vehicle for collective action to regulate certificate issuance and to coordinate trust. In November 2011, the Forum strengthened and finalized version 1.0 of its "Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates." Within a few years, the Forum oversaw the introduction of transparency, cybersecurity, and auditing standards.

Critically, in the year following the incident, the CA/B Forum became more formalized, adopting written bylaws on November 23, 2012, drafted by Kirk Hall, a lawyer at GeoTrust. The Bylaws established officer titles, qualifications for membership, and voting rules, and developed a process for creating working groups. Despite this formalism, the first version of the bylaws clarifies the loose formation of the Forum, stating "The Forum has no corporation or association, but is simply a group of CAs and browsers which communicates or meets from time to time."[12]

C. Balancing Cooperation and Competition

Within the CA/Browser Forum, the 2012 bylaws established a voluntary Forum Infrastructure Working Group to maintain the infrastructure that hosts this dialogue. The bylaws identify three distinct stakeholders: Certificate Authorities and Browsers which constitute the voting group, and a third non-voting group of Associate Members. The total voting and non-voting members are listed in Table 1. Increasingly, forum work takes place at the working group level. After 2017, the Forum created new working groups to expand certificate standards to areas beyond the web, such as code signing and server certificates. Some of these Subject Area Working Groups (WGs) include - S/MIME Certificate WG (2014), Code Signing Certificate WG (2015), Network Security WG (2017), Server Certificate WG (2018).

Table 1: CA/B Forum Constituency (2023)	
Certificate Authorities	55 voting organizations
Browser Software Vendors	11 voting organizations
Associate Members	7 non-voting organizations

While membership ensures an equal vote, it does not imply an equal level of participation in ideation and discussion. To get at engagement, we reviewed the publicly reported meeting minutes of the CA/B Forum which are archived through 2013 and include 369 posted meeting minutes including those from various working groups. As working groups are added the number of yearly meeting minutes grows. We were able to scrape, extract, and then clean attendee records from these meeting

[11] https://cabforum.org/wp-content/uploads/Announcement-Baseline_Requirements.pdf
[12] https://cabforum.org/wp-content/uploads/CA-Browser-Forum-Bylaws-v.-1.0.pdf

minutes. Ultimately, this data provided attendance records for 553 participants from 123 organizations. The CA/B Forum was described by one of our interviewees as "a place for the root stores to coordinate their policy, so that they don't create conflicting policies, and to get feedback from the CAs on those policies." With respect to compliance, he said "We have raised the bar significantly over the past 15 years."

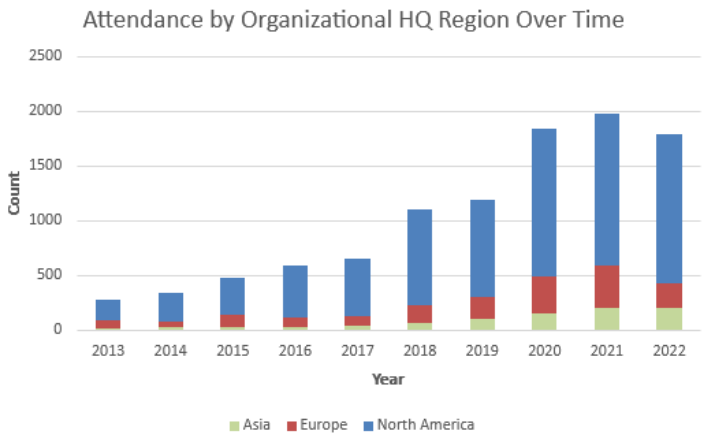
Findings and Discussion

A. CA/B Forum Participation

If we look at the national headquarters of participating firms, the CA/Browser is very clearly dominated by US firms, though this chart does identify a recent increase in the diversity of participants from other countries. These US-headquartered firms represented, on average, about sixty percent of participants. Other prominent countries represented are concentrated in either Europe or East Asia. CA participation by region is represented in Table 2. Out of the 11 Browser Software members, 7 are based in the US. The remaining 4 are based in China, Norway, Austria, and Germany.

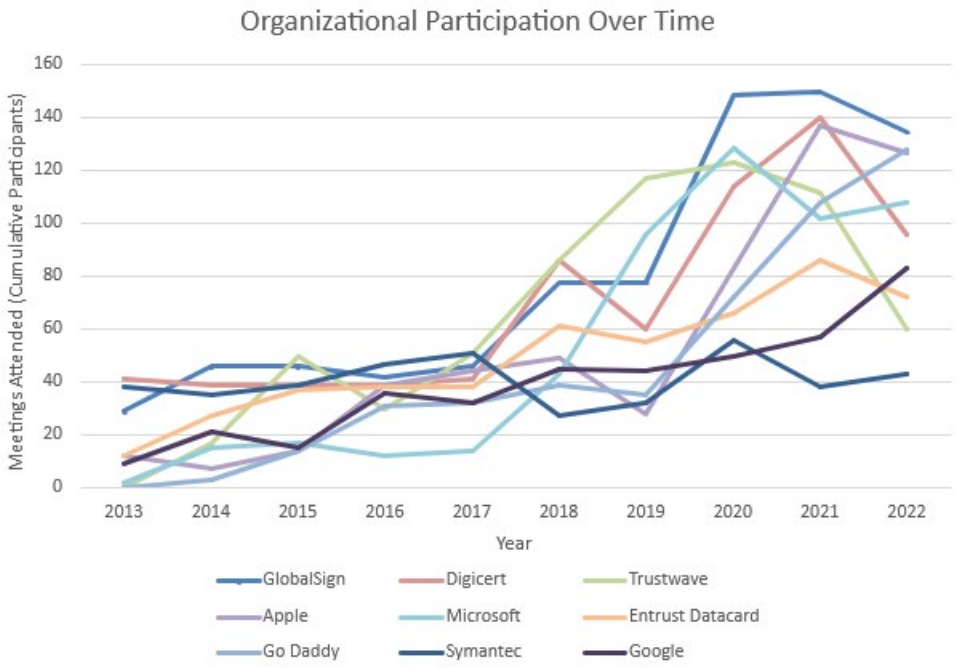
Table 2: Voting CAs at CA/B Forum by Region	
Europe	21
Asia	13
North America	15
South America	1
Middle East	5

Figure 2 - CA/B Forum Attendance Records by Organizational HQ Region over time



The vast majority of participants attend fewer than 20 meetings. However, a few highly active participants have attended more than 2/3rds of all recorded meetings. These highly active volunteers are leaders within the organization, show many years of active participation, and often represent major Certificate Authorities or Mozilla.

Figure 3 – CA/B Forum Top Organizational Participation Over Time



Of the highly participating entities displayed above, we see an increase in participation following 2017 in conjunction with the addition of the new working groups, which increased the venues for engagement. It is also notable that since 2013 it appears like the browsers have become more active participants. In 2022, Apple and Microsoft were the third and fourth most active participants in the forum.

B. Market share of CAs

The commercial CA market is surprisingly small. The company Mordor Intelligence estimates a market size of 160 million USD in 2023.[13] Another market intelligence firm estimated market value at 127 million USD in 2021.[14] The CA/B Forum had 55 members in the CA category as of July, 2023.[15] Apple lists 172 Root Certificates from 166 different Issuers.[16] In contrast, Microsoft's Root Store in July 2023 includes 251 Root Certificates from 246 unique Issuers.[17] However, corporations can operate multiple CA roots and Issuer names. While an imperfect proxy for corporations with

[13] https://www.mordorintelligence.com/industry-reports/certificate-authority-market
[14] https://www.polarismarketresearch.com/industry-analysis/certificate-authority-market
[15] https://cabforum.org/members/
[16] https://support.apple.com/en-us/HT213080)
[17] https://learn.microsoft.com/en-us/security/trusted-root/participants-list#current-list

complex ownership structures, if coded for brand names, the number of actors admitted into the trust stores is less than half that of total root certificates.

There are three different classes of CA: a) public, commercial service providers; b) public, non-profit CAs, the primary exemplar of which is Let's Encrypt; c) internal CAs run by private organizational networks. Many larger companies, including the Browsers, maintain an internal Certificate Authority to provide certs for corporate domains.

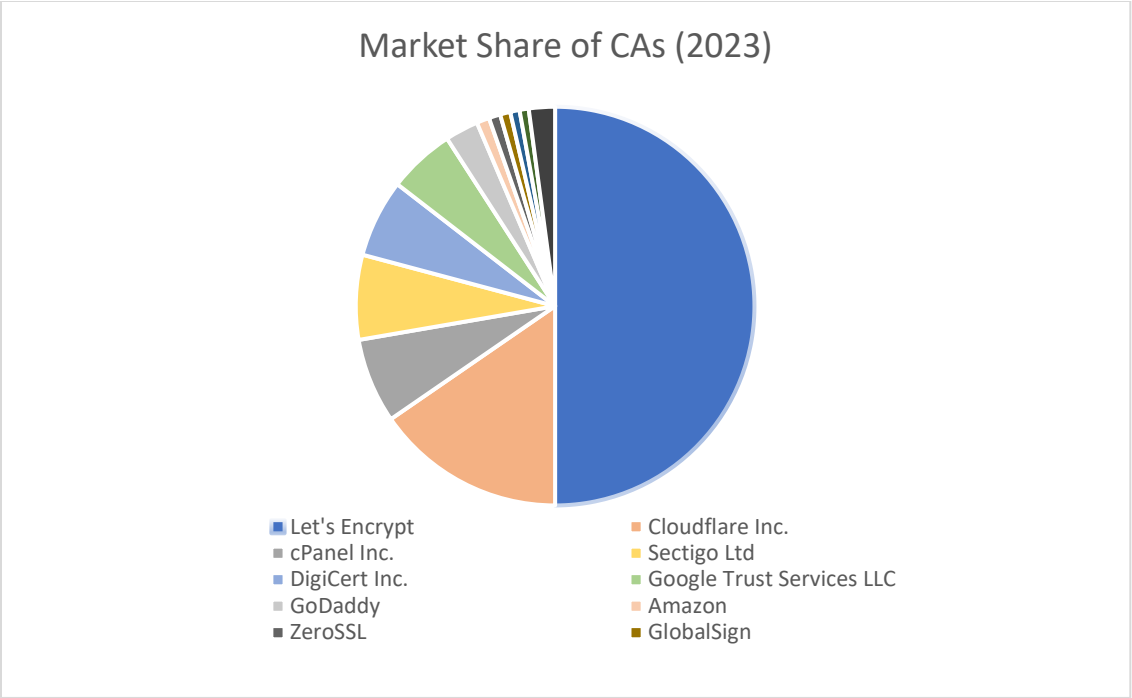
Commercial certificate authorities strive to maximize their certificate sales by offering certificates at competitive prices while keeping their operational costs low. However, market dynamics have started to introduce more diversity into the certificate authority landscape. The issuance of Domain Validated (DV) certificates has become highly standardized and automated, leading to a situation where new entrants like Let's Encrypt emerged in 2013. Let's Encrypt, a project of the non-profit Internet Security Research Group (ISRG), disrupted the market by offering DV certificates at no cost. This innovative approach gained significant traction. Let's Encrypt's intermediate certificates, with cross-signing support from a major CA, IdenTrust, gained access to root stores and were widely accepted and adopted.

Cross-signing creates an alternative route to a root certificate, enhancing the resilience of the certificate chain of trust. Remarkably, Let's Encrypt's ISRG Root X1 certificate achieved such widespread recognition that it can now allow its cross-signatures to expire in September 2024.[18] Let's Encrypt's zero-cost business model has proven to be exceptionally effective. In response to this evolving landscape, many commercial CAs have shifted their focus toward offering Organization Validated (OV) and Extended Validation (EV) certificates. These types of certificates are less susceptible to automation and are often bundled with additional security services or website hosting packages.

To measure the distribution of certificate uses over CA issuers we took a random sample of 1 million URLs from the approximately 3 billion unique URLs in January 2023. The sample population was indexed by the non-profit Foundation Common Crawl. We then employed a script to pull certificate information from our list of URLs. Slightly more than half the sample did not return certificate information either because it wasn't present or the page did not load in the 10-second timespan we allocated before pulling data from the next URL. Of our sample of 487,476 URLs (48.7%) we then identified 2,366 unique organization names issuing certificates. While a small proportion of the sample, this list of organizations included entities like universities or large corporations which may use their own certificates, but do not provide this service to third parties.

[18] https://letsencrypt.org/2023/07/10/cross-sign-expiration.html

Figure 4 - Market Share of CAs in 2023 (*from sample)



The sample shows that 62% of the certificates can be traced to Let's Encrypt. We discuss Let's Encrypt and its dominance of DV certificates as a potentially destabilizing factor in the institutional equilibrium below. Of the identified firms, 80% were members of the CA/B Forum, however, this is likely an undercount. Both Cloudflare and cPanel rely on CAs like Let's Encrypt, Google Trust Service, and Sectigo for their certificates.

C. Baseline Requirements

The BRs are an equilibrium in which tighter and more costly requirements were imposed on the CA stakeholders. The process was driven by the Browser stakeholder group and larger, more technically advanced CAs. As a small group with large stakes, the Browsers were in the strongest position to initiate collective action and (using the leverage of inclusion in their root stores) induce compliance with the new standards. The 1.0 version of the CA/B Forum Baseline Requirements first went into effect on July 1st, 2012. The first standard tackled a range of issues including, "identity vetting, certificate content and profiles, CA security, certificate revocation mechanisms, use of algorithms and key sizes, audit requirements, liability, privacy and confidentiality, and delegation of authority."[19] The Baseline Requirements were regularly revised, about once every 6 months, by means of formal ballots approving amended text. In April 2023, the CA/B Forum published version 2.0, consolidating edits from the Server Certificate Working Group Validation Subcommittee which substantially revised the language around certificate profiles and the application of RFC 5280.[20]

[19] https://cabforum.org/faq-about-the-baseline-requirements/
[20] Comparison of changes documents: https://github.com/cabforum/servercert/compare/2c63814fa7f9f7c477c74a6bfbeb57e0fcc5dd5b..aa9fc5d0b2b59504a31638e880cb81c69aefa018

Other forms of industry collective action piggybacked on the CA/B Forum. The Certificate Authority Security Council (CASC) was formed in February 2013 as an advocacy body formed by Comodo, DigiCert, Entrust, GlobalSign, Go Daddy, Symantec, and Trend Micro. These major commercial CAs explicitly endorsed improving security through standards bodies, saying "CASC supports the efforts of the CA/Browser Forum and other standards-setting bodies in their important work, and will continue to help develop reasonable and practical enhancements that improve trusted Secure Sockets Layer (SSL) and certificate authority operations." Certificate Transparency, another tool supporting the self-regulation of authentication, was also developed around leading CA/B Forum members but was not directly administered by it (see below).

The Baseline Requirements (BRs) are the primary product of collective action to clean up authentication functions in WebPKI - though they are not the only product. Other forms of collective and unilateral action emerged in the wake of the crisis of late 2011, such as Certificate Transparency and Let's Encrypt, a subsidized CA intended to promote widespread encryption by issuing largely automated, "free" certificates. It is explored in more detail in the last finding.

D. Need for Collective Action

Why is collective action necessary in the first place? A Web client's confidence in the identity of the object they are interacting with on the Web depends on CAs doing their job properly. While end users want seamless access to anything on the Web, they are in no position to assess the trustworthiness of individual CAs or specific websites. The process of authentication is invisible to them. It is often difficult to even know which organization has issued a certificate.[21] Assessments of the trustworthiness of CAs is a task performed for end users by their browser. The browser developers operationalize trust by embedding a reference to a list of trusted CAs in their root stores. One interviewee described the requirements of the vetting process required here as "onerous" and said that they may consume up to $150,000/yr on audits, with additional infrastructure requirements and evidence collection costs.

In effect, root stores are producing knowledge about which CAs (and which certificates) are valid and trusted. It is a semi-centralized certification regime. The CAs certified as "trusted" are automatically disseminated to users via the browser software. Information is also conveyed indirectly to customers of CAs (websites, organizations), as their users receive warning alerts (on their browsers!) if authentication attempts fail. A (partially) centralized root store thus economizes on assessments of the trustworthiness of CAs and on the monitoring of individual certificate validity. A relatively small number of CAs go through the root programs of a relatively small number of software vendors; certifications of trustworthiness derived from those programs are distributed in a branching hierarchy to millions of other certificates, as root CAs sign for multiple intermediate CAs, the intermediate CAs issue certificates to other CAs or to websites or other objects in cyberspace. Importantly, the reliability of the dissemination hierarchy is predicated on the transitivity of trust.

[21] Ma, Mason et al, (2021, p. 4384) describe some of the difficulties in identifying CAs: "CA certificates often live longer than CAs themselves, and a certificate's subject can be misleading in the case of a merger or acquisition, or if a CA decides to sell a root to another company. For example, … Symantec/ DigiCert and Comodo/Sectigo control two certificates that both appear to belong to UserTrust. UserTrust was an independent CA that transferred several of its root certificates to GeoTrust, which was acquired by VeriSign, then Symantec, and ultimately DigiCert. UserTrust and its remaining root certificates were acquired by Comodo, which eventually rebranded as Sectigo. While in some cases, it is possible to reassemble a CA certificate's history, many business transactions occur in private and there is often no paper trail that explicitly lays out the transfer of ownership/control of a CA certificate."

This is one of its weaknesses, as knowledge of trustworthiness degrades the further it gets from the source.

An analysis of the presence or absence of collective action raises many interesting questions about industrial organization. Knowledge about the trustworthiness of CAs is non-rival in consumption. But because the information is developed by competing private firms and encapsulated in their commercial software products, the root stores could exclude others from that knowledge. This means that knowledge of CA trustworthiness is not a pure public good. Browser vendors could enclose it if they thought it would give their browsers or operating systems a competitive advantage. But in fact, they do not enclose. They all cooperate in the maintenance of a common institutional rule set (CA/B Forum BRs) and various shared infrastructures (Certificate Transparency logging), and openly share the contents of their root stores. Why do Google, Microsoft, Mozilla, Apple, Oracle and Java feel the need for collective action in these areas?

The answer appears to be that untrustworthy CAs create externalities across all websites and all browsers. Specter (2016, p. 57) argues that the sharing of public keys and cross-signing by intermediary CAs means that trust cannot be produced and consumed as a private good by website operators or individual browser users. "[A] user can explicitly distrust a root, should that root's CA prove to be untrustworthy, but intermediates and the number of leaves each intermediate owns is often not known. The result is that the CA system has become so interdependent that it is functionally impossible for a user, however knowledgeable, to distrust a specific certificate authority." This indicates that the trustworthiness of CAs and certificates is a collective good across the entire Web ecosystem. There is also a "softer" public good involved, which is a generalized promotion of safety and security on the Web. Encryption and effective authentication are building blocks of a Web environment that discourages criminal activity and makes users (feel, and sometimes be) more secure and thus more likely to participate in online commerce and culture. Everyone is better off, none need be excluded.

Trustworthiness, however, is still a private good for CAs. They still reap exclusive benefits from achieving certain levels of integrity and trust. CAs must have access to root stores to sell certificate services, for example. Their pathway into the browser software will be easier if they can demonstrate reliability. CAs with root status can monetize their access if they are part of an acquisition. The incentive structure of the CA industry is heavily influenced by the demand for access to the root stores.

This raises another interesting question about the scope of collective action. If software vendors need to cooperate to maximize the trustworthiness of CAs, why don't they come together to maintain a common, jointly administered root store? The answer seems to be that each vendor wants to maintain control of the security tradeoffs and risks in certificates related to their own software products. These risks and tradeoffs may vary with the characteristics of the software, too.

We note that each root store does maintain slightly different lists of root certificates (see convergence across Browsers/OS). They do not jointly execute a shared root program. So, the scope of collective action is limited. Instead of a purely collective root store, we get coordinated standards and policies regarding CAs, but each Browser vendor can still make independent decisions about who or what they will trust. Because of the small number of browser producers, it is relatively easy for them to coordinate major actions when necessary; each major browser made the decision to

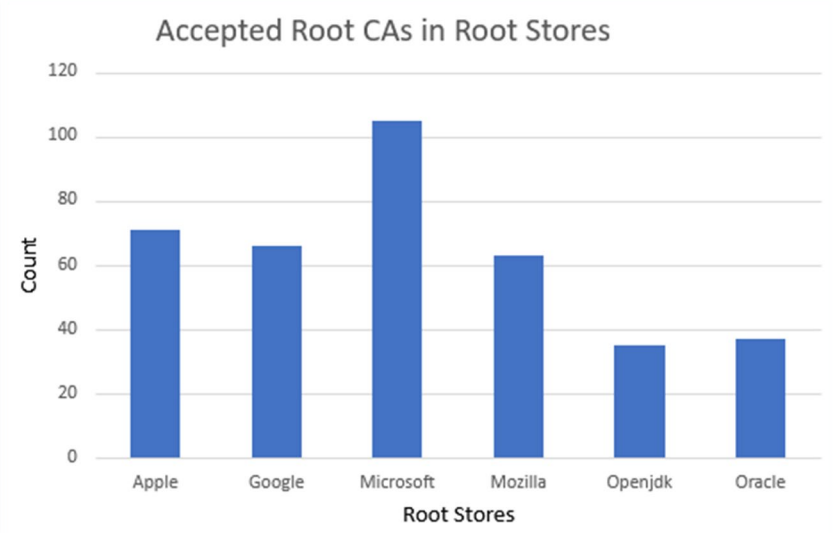
withdraw trust from DigiNotar, for example, within days of each other. The WebPKI governance regime has arrived at a mix of autonomy and coordination in the maintenance of root stores.

E. Power Dynamics between CAs and Browsers

Browsers and OS act as the root store operators responsible for maintaining and updating the list of trusted root certificates. They periodically assess the trustworthiness of CAs and their compliance with industry standards. If a CA's practices are found to be subpar or compromised, the root store operator may revoke trust in that CA's certificate. Conversely, they can include new, trusted CAs in the root store.

Browsers also perform periodic checks to ensure that the presented certificate has not been revoked. They consult Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP) servers to verify a certificate's status. A CRL is a list of certificates revoked by the CA before the expiration date. This is crucial in maintaining the security of the PKI system, as revoked certificates should not be trusted. The shorter the list, the better it is for security and to avoid latency from the browser's end. The latency occurs because of periodic checks to cache and download CRLs at browser endpoints. However, this is a necessary step executed through proprietary revocation checks, which is currently not adequate (Liu et al. 2015). Embedded in this structure is the authority of browsers (root stores) to decide which CAs' root certificates are included in their trust store.

Figure 5 – Count of CAs in Browser root stores



As such, it wouldn't be unrealistic to assume some power imbalance in the CA/B Forum between the Browsers and the CAs. However, our interviewees did not converge neatly in one direction. Three out of the eleven interviewees suggested that the CAs and Browsers hold an equal interest in the security of the web and therefore, have an equal say in the forum. There is "good cooperation" with "little tension at times" but "sufficient discussions happen before a ballot." Moreover, CAs and Browsers can discuss the issue outside of the forum to reach a consensus before a vote. It is important to note that two out of three interviewees represented Browsers at the Forum. However, four other interviewees suggested that Browsers are more powerful since they have the power to

"kick out CAs from root stores" given the baseline requirements of the Forum and specific browser policies were not met.

Untrusted CAs

This dependence means that CAs must adhere to the policies and requirements set by root store operators, often through a consultative process at the Forum. If a CA's practices or certificates fall out of compliance with these requirements, root store operators can take actions such as revoking trust or removing the CA's root certificate from their store. We see collective action at play here. For instance, when Mozilla decided to distrust WoSign and Startcom roots following an investigation on backdating SHA-1 certificates,[22] Apple and Google immediately followed suit.[23] In a similar vein, in September 2015, Google discovered that Symantec's Thawte CA had issued an EV certificate for google.com as part of a testing process. Symantec had acquired two CAs in 2010 which had improperly issued certificates (Thawte and Geotrust).[24] In response, Google requested in a blog post that Symantec adopt Certificate Transparency,[25] amend its incident report and improve overall security.[26] Google claimed that Symantec CAs had improperly issued more than 30,000 certificates over the years not complying with BRs while Symantec disputed this and admitted to only 127.[27]

As the largest CA in the market, some Browser representatives labeled Symantec as viewing itself to be too big to fail (Hadan et al. 2021). There was also a perception that it was not following consistent policies across the many CA brands it had acquired over the years. Unsatisfied with Symantec's efforts to improve security over the subsequent 18 months, Google published a plan on July 27, 2017, to a development listserv clarifying that they would move to distrust Symantec-issued TLS certificates.[28] This announcement was shared with the CAs at an in-person annual CA/B Forum meeting. Over time, the move significantly reduced Symantec's market share of certificate adoption.

Browser action against root CAs is not unconstrained. Immediate and complete removal of a CA from the root store might cause the browser's users to experience outages when encountering websites using that CA's certificates. Google updated Chrome to nullify all currently valid certificates issued by Symantec-owned CAs, but to minimize user disruption staggered the nullification over time by decreasing the "maximum age" of Symantec-issued certificates over a series of browser software releases. With Symantec certificates representing more than 30 percent of the Internet's

[22] Ma, Mason et al, 2021, p. 4383 provide a case of a bug in the Chinese CA WoSign that allowed owners of a subdomain (e.g., evil.github.com) to receive certificates for the base domain (i.e., github.com).
[23] https://pkic.org/2016/11/11/trust-on-the-public-web-the-consequences-of-covert-action/
[24] This is not an uncommon practice. Housley and O'Donoghue call it Surprising Certificates here in https://datatracker.ietf.org/doc/html/draft-iab-web-pki-problems-01#section-3.3
[25] Certificate Transparency is an Internet security standard for monitoring and auditing the issuance of digital certificates to avoid occurrences of "surprising certificates".
[26] https://security.googleblog.com/2015/10/sustaining-digital-certificate-security.html
[27] Dan Goodin, Google takes Symantec to the woodshed for mis-issuing 30,000 HTTPS certs. Ars Technica, March 24, 2017.
[28] Ryan Sleevi, "Intent to Deprecate and Remove: Trust in existing Symantec-issued Certificates." https://groups.google.com/a/chromium.org/g/blink-dev/c/eUAKwjihhBs/m/El1mH8S6AwAJ According to Sleevi, "Symantec allowed at least four parties access to their infrastructure in a way to cause certificate issuance, did not sufficiently oversee these capabilities as required and expected, and when presented with evidence of these organizations' failure to abide to the appropriate standard of care, failed to disclose such information in a timely manner or to identify the significance of the issues reported to them."

valid certificates by volume in 2015, stagger the mass nullification in a way that requires they be replaced over time.

Shorter Certificate Duration

We also see an alignment on shorter certificates. Policy toward the expiration of certificates pits the interests of many CAs (and by proxy, their customers) against the interests of the Browsers (and by proxy, their users). As one IETF draft noted, "The shorter the life of the certificate, the less time there is for anything to go wrong. If the lifetime is short enough, policy might allow certificate status checking to be skipped altogether." (Housley and O'Donoghue, 2016) However, shorter durations increase the complexity of certificate management for subscribers.

Predictably, the issue of certificate duration was contentious within the CA/B Forum. The Browsers were advocating 1-year durations, while CAs were arguing for longer durations or extended phase-in periods. In 2017, the CA/B Forum reduced the length of TLS certificate lifetimes down to 825 days (27.5 months) with unanimous support for the provision except for a few abstentions. However, when discussing certificate length, the Browser representatives insisted that a shorter certificate lifetime of 13-months would make validation information more accurate, create better security habits for subscribers, and reduce the time to bring issued certificates into alignment with evolving baseline and root store policy. Ultimately, Google proposed a vote to reduce this certificate lifespan before the CA/B Forum in September of 2019. While the proposal (SC22) received the support of all 7 participating Browsers it only received 35% support from participating CAs and thus failed. This represents one of the most contentious votes before the Forum.

Despite the failed vote, Apple's Trust Store decided to unilaterally announce at the Forum that they would implement the 13-month duration. Mozilla followed Apple's lead and Google followed shortly after.[29] The ability of the browsers with substantial market share to set trust recognition unilaterally demonstrates a power imbalance in standards developed well understood by the participants. Arguably, in this case the power imbalance allows the Browsers to be agents for a broader public good whereas the CAs are reflecting private interests.

Convergence across Browsers/OSs

If externalities caused by poor CA security practices are the main driver of collective action, we should expect to see the gradual homogenization of the root stores across browser/OS producers over time. A common, standardized set of Baseline Requirements for CAs should reduce differences among the different software vendors' lists of root-trusted CAs.

We do see a substantial overlap in which Root Certificates the Browsers admit into their Trust Stores. Using the data above we can identify the overlap of the three traditionally largest root stores (Google's Chrome Root Program was officially established in 2022). While Microsoft has become more in line with the other browsers, its Trust Store includes substantially more CAs that are not supported by the other browsers. Notably, some of the CAs exclusively supported by Microsoft's Trust Stores are those operated by governments including the Dutch, Saudi, Swedish, Swiss, and Thai national CAs.

[29] https://www.zdnet.com/article/apple-strong-arms-entire-ca-industry-into-one-year-certificate-lifespans/

Figure 6 – Root Certificates recognized exclusively by Microsoft

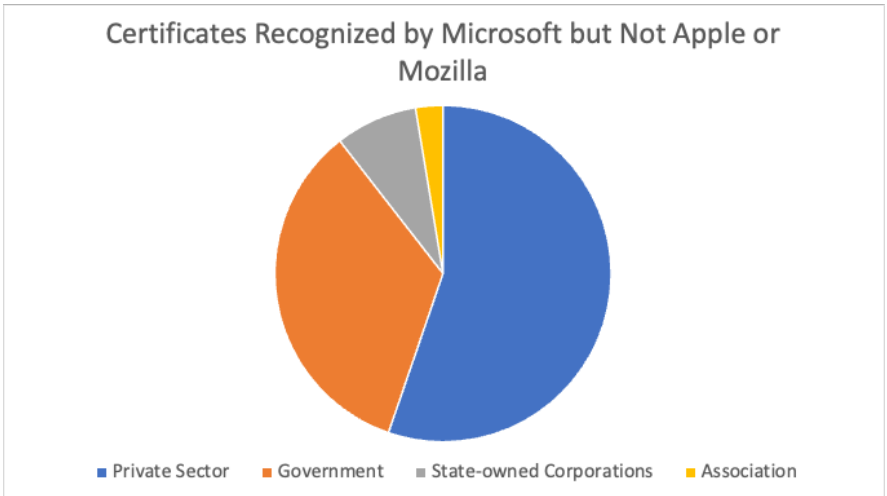
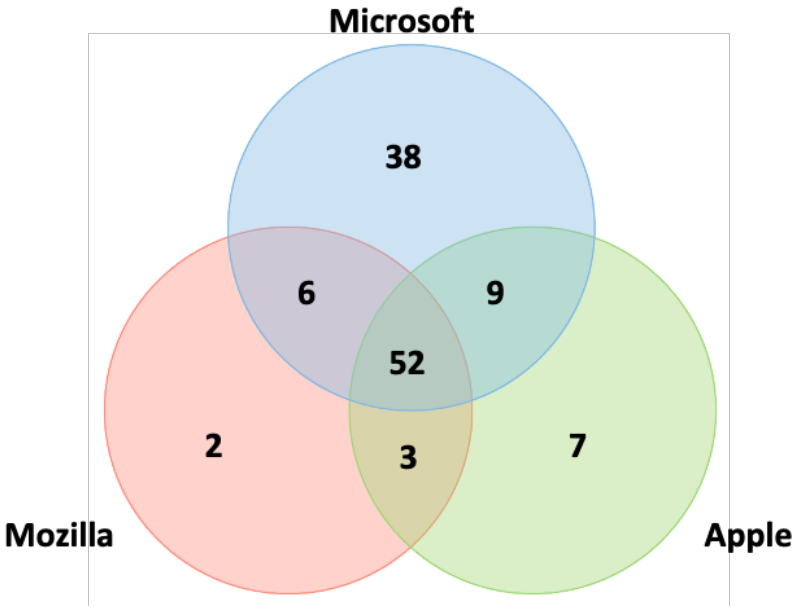
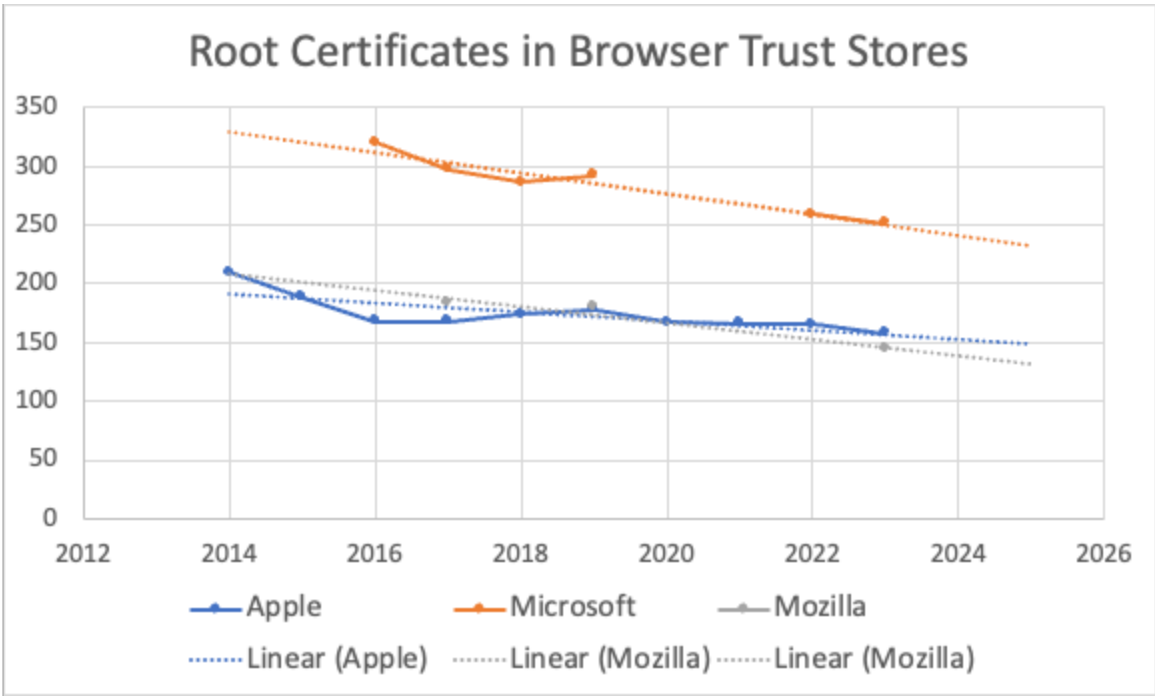


Figure 7 – Overlap count of Root CAs in the dominant Root Stores



We should also expect equilibrium around the common governance structure to reduce the number of CAs in the root stores. Examining archived root stores from these three browsers shows modest reductions in the number of root certificates listed in the Trust Stores over time. Microsoft declined from over 300 in 2016 to below 250 in 2023; Apple went from slightly over 200 in 2014 to nearly 150 in 2023. Mozilla followed the trajectory of Apple (or vice-versa) closely.

Figure 8 – Decline in # of Root Certificates in Root Stores over time



F. Is the State Entirely Absent from the discussion?

We noted earlier that the governance model in the security landscape of WebPKI is privately led. Though it's not completely devoid of government participation. Governments have a substantial stake in ensuring secure online communications. We observed a few examples of direct involvement by the government in PKI space. Although these involvements are typically more indirect compared to private sector-led entities, government agencies or representatives may participate indirectly through organizations or industry bodies that are members of the CA/B Forum. Their participation involves contributing to discussions, sharing insights, or advocating for specific security practices.

It can be bucketed into three categories 1) Regulatory Oversight, 2) Compliance, and 3) National Interests. Governments wield the power to enact regulations and policies that indirectly influence the operation of CAs and webPKI. These regulations can include requirements for CAs to adhere to specific security standards, conduct audits, or follow certain practices. Some governments establish compliance frameworks for CAs operating within their jurisdiction. CAs may need to obtain certificates or certifications from government-recognized bodies to demonstrate their adherence to specific security and operational standards. These certifications can be seen as a form of government involvement in ensuring trustworthiness within the WebPKI.

The DigiNotar incident in September 2011 brought to light vulnerabilities within WebPKI where multiple false certificates were created in a breach attempt. The company had known of the breach for almost two months before it was brought to public notice. Arnbak and Eijk explain that DigiNotar held root status with major browser vendors, leading to automatic trust in all these fraudulent SSL certificates. In response, the Dutch government took control of DigiNotar's operations, emphasizing the paramount importance of trust in online services. Surprisingly, the CA

had managed to pass multiple periodic audits, as per ETSI standards, for EV certificates and Qualified signatures issuance. Subsequently, EU involvement in the CA/B Forum increased significantly, driven by EU regulations on digital signatures and trust services, which mandate stringent compliance with security standards.

Analysis of the meeting minutes indicates active participation of the European Telecommunications Standards Institute (ETSI) in the discussion process at the CA/B Forum from early on.[30] ETSI is a key player in the development of global standards for information and communication technologies. Their focus of discussion can be taken as an indication of EU's interest in regulating the SSL/TLS to include identity proofing and extended signature validation. These discussions are in line with the Electronic Identification, Authentication, and Trust Services (eIDAS) regulation, a significant topic debated extensively at the forum. Especially around the requirement of Personal Identity Validation seal (ETSI TS 119 461). There were also mentions of the use of Legal Entity Identifiers (LEIs) to verify EV requests for organizations where registration number is not available. LEIs in the ETSI framework are identification codes defined by government standards or regulatory bodies. The eIDAS is expected to have a significant impact on electronic signatures with new rules being mandatory for CAs and Trust Services to provide a predictable regulatory environment.

The current audit process requires the audit to be conducted in line with WebTrust for CAs, or ETSI EN 319 411-1 by a qualified auditor.[31] ETSI also provides detailed audit checklists for auditors who audit CAs. These checklists include 395 specific controls and provide precise audit criteria for OV/DV/EV. However, there have been discussions about potential issues and conflicts between ETSI's standards and those of other bodies. For example, there have been debates about the acceptance of ETSI audits and the need for better responses from ETSI on feedback from other bodies. There have also been discussions about the potential for incompatibilities between ETSI's standards and those of the CA/B Forum, particularly in relation to certificate issuance and signing services.

While the EU is prominently engaged in the CA/B Forum, other nations, even those without national champions, actively participate. Their involvement is often consultative, focusing on enhancing security and ensuring compliance with global standards. For example, discussions of government entities (US Federal PKI, Government of Japan, Government of Spain, Government of Taiwan) and their relation to the baseline requirement.[32] Section 9.16.3 of the Baseline Requirements (BR) deals with the disparities that may arise between the governance stipulations outlined in the BR and those specified by a country or jurisdiction's regulations. This has proven to be useful in multiple instances. For example, there was an issue raised about the government database in Taiwan. The current Baseline Requirements state that for OV certificates, one of the fields has to be either localityName or stateOrProvinceName. Owing to the nature of geopolitical tensions, there was a proposal to provide a carve-out for Taiwan provided that the entity that is the subject of the certificate is registered in the government database.

There was a mention of India's adherence to national legal requirements regarding root auditing procedures, which included a government equivalency audit. Furthermore, governments engage in

[30] Concerns around eIDAS and its effect on CA operation are discussed in at least 37 meetings out of 369 meeting minutes.
[31] https://cabforum.org/2009/06/08/ballot-28-membership-criteria/
https://cabforum.org/2018/10/01/ballot-forum-6-update-etsi-requirements-in-the-bylaws/
[32] https://cabforum.org/2016/10/19/2016-10-19-20-f2f-meeting-39-minutes/

collaborative efforts with Certificate Authorities (CAs), particularly in cases where prominent CAs are absent within their countries. This engagement often occurs through industry-led bodies such as e-Mudhra in the case of India which worked in close collaboration with the Controller of Certifying Authorities (India CCA) to bolster security measures. Our research, which encompassed interviews and insights from CA/B Forum meetings, substantiates the increased involvement of governments, or entities closely affiliated with governments, in nations where significant CAs are lacking. This proactive engagement serves the dual purpose of enhancing security and ensuring compliance with international standards.

Additionally, the IETF document underscores the principle that when a root CA is operated by a government department, root store providers have the option to rely on audits conducted in alignment with the government's internal audit processes.[33] This exception acknowledges the unique requirements and priorities associated with government-operated CAs. Interestingly, Microsoft seems to be an exception when it comes to hosting government-operated root stores (see Figure 6).

Analysis of the meeting minutes and insights from various interviews suggest that the CA/B forum is open to recommendations from regulators, governments, and civil societies participating as associate members in these meetings. However, the responsibility lies with the CAs operating in these regions to provide an adequate explanation of the issue put forward and present a reason for its importance to the CA/B Forum and WebPKI. They are also expected to identify the direction, describe the goals, and propose actionable steps toward the completion of those goals.

There are also deeper problems with governmental involvement. The coercive power of the state can be abused. Governments can deliberately undermine user confidentiality in order to spy on their citizens. They can also relieve themselves of the need to earn trust by legally requiring trust. For instance, in 2019 citizens in Kazakhstan were forced to import government-built root CAs on their devices. (Thayer interview; Zhang, Liu. et al., 2021). Additionally, the jurisdictional fragmentation of governments does not match the global or transnational interoperability requirements of the Web. There is likely to be substantial variability in any laws or new institutions formed by national or lower-level governments to address these complex issues. While international agreements are possible, to achieve universal scope they would take a very long time and would be unlikely to overcome persistent political and military rivalries among certain blocs. Many states will view any exposure or co-governance with certain other states as inherently insecure. We intend to follow up with additional analysis and research on this topic.

Conclusion

This work identifies the private product of public trust within the certificate ecosystem. Given that online threat actors seek to misappropriate others' identities, authentication is a necessary security function for Internet users to navigate the web with a modicum of trust. In our daily lives, governments sometimes serve this authentication function assigning identification records like driver licenses for citizens and articles of incorporation for businesses.

[33] I. Barreira, B. Morton, April 29, 2015 "Trust models of the Web PKI". (https://www.ietf.org/proceedings/92/id/draft-ietf-wpkops-trustmodel-04.txt)
Note that this document was set to expire on October 31, 2015. However, we haven't encountered any discrepancy with this provision in any of the future versions of the trust model.

Market incentives first drove businesses to adopt certificates as a means of differentiating their security and establishing trust with their users. In its early days, the issuing of certificates was a means to essentially print money as the marginal cost for issuing certificates was negligible companies could grow and prosper. However, increased competition produced falling standards and security incidents that threatened industry leaders who sought to differentiate their products. This differentiation was ultimately facilitated as leading browsers and operating systems began to acknowledge this differentiation. Absent meaningful government intervention, the industry standards association known as the CA/B forum has been able to serve as a nexus for collective action to incrementally improve security and transparency. Intractable issues like a shortened Certificate length or transformative initiatives like Certificate Transparency can still advance outside of the forum with individual corporate action.

There are a number of topics in this area worthy of future research. We would like to see future Internet Governance and security research engage with the challenges that state actors face as Certificate producers in adopting best practices and achieving global trust. Having identified a trend toward market concentration, we think future researchers should be attentive to the risks of further centralization. While we acknowledge that Certificate Authorities and Browsers/OSs are unique stakeholders that are attentive to the respective needs of website operators and internet users, we did not have the opportunity to explore this dynamic in greater depth. What information feedback loops inform this attention? What principle agent challenges arise? Given the wealth of insights available to researchers in exploring the contribution of multistakeholder models, these non-governmental industry-led initiatives should be understood as equally critical to the Internet's success and pose novel governmental questions.

References/Bibliography

Acemoglu, D., & Robinson, J. A. (2008). The persistence and change of institutions in the Americas. Southern economic journal, 75(2), 281-299.

Arnbak, A, H. Asghari, M. van Eeten, N.A.N.M. van Eijk, Security Collapse in the HTTPS Market, Communications of the ACM, 2014-10, vol. 57, p. 47-55.

Arnbak, Axel, and Nico ANM van Eijk. "Certificate Authority collapse: regulating systemic vulnerabilities in the HTTPS value chain." (2012).

Asghari, H., van Eeten, M., & Bauer, J. M. (2016). Economics of cybersecurity. Chapter 1 in, Bauer, J. M., & Latzer, M. (Eds.). Handbook on the Economics of the Internet. Edward Elgar Publishing. 262.

Barnes, R, Hoffman-Andrews, J., McCarney, D., Kasten, J. Automatic Certificate Management Environment (ACME), RFC 8555 (March 2019).

Berg, S. V. (1989). Technical Standards as Public Goods: Demand Incentives for Cooperative Behavior. Public Finance Quarterly 1989 17:1, 29-54

Berkowsky, J. A., & Hayajneh, T. (2017, October). Security issues with certificate authorities. In 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON) (pp. 449-455). IEEE.

Bodó, B. (2021). Mediated trust: A theoretical framework to address the trustworthiness of technological trust mediators. New Media & Society, 23(9), 2668–2690. https://doi.org/10.1177/1461444820939922

Desmarais-Tremblay, M. (2017). Musgrave, Samuelson, and the crystallization of the standard rationale for public goods. History of Political Economy, 49(1), 59-92.

Farhan, Syed M. (2023). Exploring the Evolution of the TLS Certificate Ecosystem. MS Dissertation submitted to the Faculty of the Virginia Institute of Technology.

Go TLS Observatory. Published: Jun 23, 2021 https://pkg.go.dev/github.com/PinkNoize/tls-observatory#section-readme

Hilda Hadan and others, A holistic analysis of web-based public key infrastructure failures: comparing experts' perceptions and real-world incidents, Journal of Cybersecurity, Volume 7, Issue 1, 2021, tyab025, https://doi.org/10.1093/cybsec/tyab025

Housely, R and O'Donoghue, K. (2016) Problems with the Public Key Infrastructure (PKI) for the World Wide Web. Internet draft. February 21. Draft-iab-web-pki-problems-01.txt

Lemke, J., & Tarko, V. (Eds.). (2021). Elinor Ostrom and the Bloomington School: building a new approach to policy and the social sciences. McGill-Queen's Press-MQUP.

Liu, Y., Tome, W., Zhang, L., Choffnes, D., Levin, D., Maggs, B., Mislove, A., Schulman, A., and C. Wilson, "An End-to-End Measurement of Certificate Revocation in the Web's PKI", October 2015, <http://conferences2.sigcomm.org/imc/2015/papers/p183.pdf>

Ma, Z., Austgen, J., Mason, J., Durumeric, Z., & Bailey, M. (2021, November). Tracing your roots: exploring the TLS trust anchor ecosystem. In Proceedings of the 21st ACM Internet Measurement Conference (pp. 179-194).

Ma, Z., Mason, J., Patel, S., Antonakakis, M., Raykova, M., Durumeric, Z., ... & Wang, T. (2021). What's in a Name? Exploring {CA} Certificate Control. In 30th USENIX Security Symposium (USENIX Security 21) (pp. 4383-4400). https://www.usenix.org/system/files/sec21-ma.pdf

Olson, M (1971). The Logic of Collective Action: Public Goods and the Theory of Groups, With a New Preface and Appendix. Cambridge: Harvard Economic Studies.

Ostrom, E. (1990). Governing the commons: The evolution of institutions for collective action. Cambridge university press.

Ostrom, E. (2010). Beyond markets and states: polycentric governance of complex economic systems. American economic review, 100(3), 641-672.

Patil, V. T., & Shyamasundar, R. K. (2022, September). Evolving Role of PKI in Facilitating Trust. In 2022 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA) (pp. 1-7). IEEE.

Prins, J. R., (2011). Diginotar certificate authority breach "operation black tulip". Cybercrime Business Unit, Fox-IT, November, 18.

Roosa, S.B., Schultze, S. The "Certificate Authority" trust model for SSL: a defective foundation for encrypted Web traffic and a legal quagmire. Intellectual Property & Technology Law Journal 22. 11 (2010), 3.

Ruggie, J. G. (1972). Collective goods and future international collaboration. American Political Science Review, 66(3), 874-893.

https://www.theregister.com/2020/02/20/apple_shorter_cert_lifetime/

Serrano, Nicolas and Hadan, Hilda and Camp, L. Jean, (2019) A Complete Study of P.K.I. (PKI's Known Incidents) (July 23, 2019). TPRC47: The 47th Research Conference on Communication, Information and Internet Policy 2019, Available at SSRN: https://ssrn.com/abstract=3425554 or http://dx.doi.org/10.2139/ssrn.3425554

Soghoian, C. and Stamm, S. Certified lies: detecting and defeating government interception attacks against SSL. In Financial Cryptography and Data Security. Springer, 2012, 250-259.

Specter, M. A. (2016). The economics of cryptographic trust: understanding certificate authorities (Masters Thesis, Massachusetts Institute of Technology).

Stark, Emily (2023) estark@chromium.org The Dirty Laundry of the Web {PKI}. Usenix Enigma, 2023. https://www.usenix.org/conference/enigma2023/presentation/stark

Steinmueller, W. E. (2003). The role of technical standards in coordinating the division of labour in complex system industries (pp. 133-151). Oxford: Oxford University Press.

Sturn, R. (2010). 'Public goods' before Samuelson: interwar Finanzwissenschaft and Musgrave's synthesis. The European Journal of the History of Economic Thought, 17(2), 279-312

Vratonjic, N., Freudiger, J., Bindschaedler, V. and Hubaux, J.-P. The inconvenient truth about Web certificates. In Proceedings of the Workshop on Economics of Information Security, 2011.

Zhang, Y., Liu, B., Lu, C., Li, Z., Duan, H., Li, J., & Zhang, Z. (2021, November). Rusted Anchors: A National Client-Side View of Hidden Root CAs in the Web PKI Ecosystem. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (pp. 1373-1387).