Non-governmental Governance of Trust on the Internet: WebPKI as Public Good

Karl Grindal, Milton Mueller, Vagisha Srivastava[1]

Dr. Karl Grindal
Department of Security Studies
University of New Hampshire
Manchester, NH 03101
USA

(603) 641-4102
karl.grindal@unh.edu

Dr. Milton Mueller
School of Public Policy
Georgia Institute of Technology
Atlanta, GA 30332
USA

Ms. Vagisha Srivastava
School of Public Policy
Georgia Institute of Technology
Atlanta, GA 30332
USA

[1] Alphabetical ordering of co-authors.

Abstract (350 words)

This paper provides a detailed analysis of how private actors cooperate to facilitate authentication and provide trust and security to the Web. The World Wide Web's Public Key Infrastructure (WebPKI) is a global governance structure forged through collective action among industry actors. Drawing on collective action theory and institutional analysis, we show how this regime of non-state actors produces a public good: global authentication of website identities in a way that enhances security, privacy, and trust for websites and their users.

Stakeholder analysis demonstrates how the production of digital certificates and the utilization of certificates for authentication and encryption necessitate interdependencies among Certificate Authorities (CAs) and Browsers/Operating Systems. These relationships are institutionalized by the Certificate Authority/Browser Forum and other voluntary industry organizations. Since their founding, these institutions have developed through stages of formalization, specialization, and the expansion of their scope, and sought to address various security and efficiency challenges through new standards. We conclude by exploring some measures for evaluating the efficacy of this governance regime. Quantitative findings include assessments of CA market concentration, institutional membership and participation trends, stakeholder voting behavior, and the composition of Browser root stores.

Introduction

Security has been characterized by some as a public good, by others as a private good. In real-world, empirical settings, it obviously can be either one. Police and governmental military forces - non-market organizations supported by taxes - provide collective security at the local and national level. Nevertheless, individuals still subscribe to home security services by buying locks, surveillance cameras and guns in the market for private goods.

The same combination of private and public security production characterizes cybersecurity. Information security issues arise at different levels of social organization: the individual user, the organization, an industry sector, individual countries, and globally available online services. There is a large and growing market for cybersecurity tools, devices and services, and commercial online service providers often internalize the costs of protecting the security and privacy of their users to make their products more appealing in the market.

Increasingly, however, governments are asserting a bigger role for themselves in cybersecurity and privacy. These initiatives are based on claims that there is a market failure and/or that cybersecurity is a national-level, collective good. By the same token, nation-state rivalries make governments one of the chief threat actors in cyberspace. Underlying claims that governments protect public security at the national level is the fact that other governments are the primary adversaries. This challenge makes it difficult, if not impossible, for governments to produce collective cybersecurity *globally*. Even when nation-states are not hostile to each other, they are usually unwilling to trust other states with the sensitive information about their citizens and critical infrastructure that would be needed to produce cybersecurity collectively. Cooperative collective action among nation-states to secure cyberspace, therefore, can suffer from a political failure as severe as any market failure.

What gets provided by the state and what gets supplied privately is a question of great significance in policy debates. This is especially true of cybersecurity, because it is a new, rapidly evolving field where state-market and state-state relationships have not been fully institutionalized. In these debates, public policy makers or advocacy groups calling for "regulation" often overlook the capability of private actors to produce the desired public goods on their own.

This paper provides a detailed analysis of how private actors are cooperating to provide trust and security governance on the Web. It is a case study of the private provision of a global collective good. Since about 1996, the Web ecosystem has applied public-key cryptographic technology to the problem of enabling secure communications at scale. This system is commonly known as a Public Key Infrastructure for the Web, or WebPKI.

Although there are still many flaws in it, WebPKI has evolved over the past 20-odd years into a more widespread, institutionalized and technically efficient system. The infrastructure is global and affects billions of internet users and hundreds of millions of websites, domain names, and digital objects. It is responsible for enabling the encryption of an ever-larger portion of internet traffic. While individual end users collectively benefit, a small minority pay for this service; the costs are borne by organizations.

There is a great deal of computer science literature about the technical workings of WebPKI, [1-7] but there are far fewer analyses of its economics, and almost nothing recognizing its status as a globalized governance institution. This paper aims to fill that gap. We explain how the underlying crypto technologies require a set of institutionalized trust and authority relationships to perform their functions securely. While some of these functionalities can be automated via code, they ultimately must be grounded in agreements about standards and procedures among humans and organizations, and subject to negotiations over acceptable cost/risk tradeoffs. Collective action is an essential component of the system.

This paper describes and analyzes the private sector-led governance arrangements formed around the Web PKI. The Certificate Authority/Browser Forum (CA/B Forum) serves as the nexus for much of the cooperative regulation of the WebPKI. We analyze additional forms of collective action, such as the Certificate Transparency logging infrastructure and the emergence of a "free" certificate authority (Let's Encrypt) that now issues the majority of domain-validated certificates. We analyze the stakeholders in the WebPKI, their relative market power and their incentive structures, and show how collective governance arrangements among the private actors responded to serious security incidents such as the Diginotar breach in 2011.

The analysis is founded upon theories of collective action and public/private goods. It explores why and how a governance structure has emerged and why it is private sector-based rather than governmental. Drawing upon institutional theory, we also examine the way the WebPKI governance institutions structure the relationship between divergent business interests.

Theories of Collective Action and Public Goods

Public goods are defined in economic theory as goods that are non-rival in consumption and non-excludable [8]. Originally, the theory of public goods was an attempt to theorize the boundary between the public and private sectors [9-10]. Resources or products with the special economic characteristics of public goods 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 the ability of private businesses to recoup their costs) [11]. The literature implied that the market would always underproduce public goods, and that only state action, which could draw upon the state's power to coerce, could produce the proper amount.

The equation of public goods with state action, however, fell apart on both theoretical and empirical grounds [12]. Many services the state provides do not meet the defined criteria of a public good.[2] On the other hand, many instances of collective action are executed by non-state actors. The extensive literature on political economy and governance that has developed since the 1960s has reframed the problem in this way: the production of public goods (and some non-public goods such as common pool resources) requires *collective* action, but not necessarily *state* action. Governments are one vehicle for collective action, but not the only one, and not

[2] 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. See [56] for a useful literature review.

necessarily the best one in all circumstances. Non-state actors routinely overcome coordination costs and exclusion problems to engage in effective collective action [13].[3] Non-proprietary technical standards, which play an essential role in Internet and Web governance, are obvious examples of privately-produced collective goods [14-15]. Another important insight is that collective action can be used to govern common pool resources (CPRs), which are not non-rival in consumption and hence not public goods. The work of Elinor and Vincent Ostrom has emphasized the ability of communities to engage in self-governance of common pool resources [16-19]. Efficient management of CPRs poses exclusion and coordination problems, necessitating collective action, but CPRs, by definition, are rival in consumption and thus do not qualify as public goods.

This paper draws upon this richer and more complex approach to public goods to identify the collective action problems WebPKI attempts to solve. We also try to explain why it has evolved within the industry with little involvement by states so far.

Method

Our research method approaches the WebPKI as a governance institution, not simply as a technical system. Our method is based on institutional analysis. As we pursue it in this paper, institutional analysis consists of three steps.

1. Identify the benefit that is sought by the actors and explain why it is a public good that requires collective action. In the next section, we indicate that the public good being sought is a ubiquitous and reliable system of *authenticating the identity of holders of public keys*.

2. Identify the stakeholders that cooperate to achieve the public good. This step also involves identifying the distinct political-economic interests of each stakeholder group and how they conflict and/or converge with the other stakeholders' interests.

3. Identify the institutionalized equilibrium among these stakeholder groups. Political economy theory characterizes institutions as an equilibrium around commonly known and accepted rules [20-22]. Although some institutional economists use formal game-theoretic models to define relevant equilibria, this paper does not. A mathematical model of equilibrium would require a level of abstraction and artificiality that would make it of no scientific value in the analysis of the real-world system. Instead, we identify the common rules and procedures that have been explicitly ratified and commonly implemented by the stakeholders, and consider it to be a de facto equilibrium. We analyze their substance to detect which requirements were included, which actions were

[3] Olson's [13] 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.

left unregulated or discretionary, and what were the distributional effects of the equilibrium.[4]

To carry out this mode of analysis we employed various 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 24 January 2013 and ended on 28 July 2022 and yielded 564 names of individuals, their organizational affiliation, and a measure of how many meetings they attended over time.

- We conducted 10 semi-structured interviews with practitioners who had high participation rates in the CA/B meetings. Our choice of interview subjects was not random but favored some of the most active participants, sought to balance representatives of browsers and CAs, and to find some diversity of world regions. A pre-defined interview guideline ensured consistency while allowing for in-depth exploration. The guideline covered individual experiences within the CA/Browser Forum, organizational histories of engagement and policy adoption, observations on competition and contentious issues within the forum, and participant perspectives on the forum's consensus-building process, pace of change, and future challenges.

- 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 significant decisions.

- We counted and reviewed the ballots of the CA/B Forum from 2012 to 2022, which are available online.

- We developed measures and drew upon third-party sources to estimate the market share of Certificate Authorities, the market share of different browsers, and levels of adoption of encryption and certificate transparency.

- We collected and compared records of the certificates listed in browser root stores.

Our empirical findings are targeted to support the institutional analysis; this differs from the more measurement-focused work of Stark et al. [7] which investigated Certificate Transparency adoption, Jo's [62] study on the economics of browser software vulnerabilities, and Dong, et al's [63] study of vulnerable certificates issued by trusted CAs,. While we developed our own market share measurements, we did not collect the pricing data seen in Arnbak [37].

[4] For an excellent description of an analysis of institutionalization that combines political analysis, property rights analysis and legal/legislative analysis, see Thomas Hazlett's analysis of the nationalization of the broadcast spectrum and the formation of the Federal Radio Commission in 1927. [23]

Step 1: Authentication as a public good

Understanding the role of and need for collective action in WebPKI requires a description of the technical system. The following paragraph and Figure 1 provide an abbreviated overview sufficient to highlight the governance issues.

Public key cryptography provides a method for secure communication and data exchange over the Internet. It does so by breaking the key used to encode data, known as the cryptographic key, into two parts: a public key and a private key. The two keys are mathematically related, but it is not computationally feasible to derive the private key if one knows only the public key. The recipient of the key pair keeps the private key secret and distributes the public key to anyone who wants to send them a message. A sender encrypts their message with the recipient's public key, while the recipient of the message decrypts the message with their private key.

Split key cryptography was a powerful enabler of online security at scale because it eliminated the need to transmit cryptographic keys over insecure networks. However, it also created an impersonation problem. A public key, being public, can be copied and announced by anyone who wants to present themselves as the holder of the private key. If bad actors manage to steal or discover another party's private key, they can present that person's public key to anyone, and impersonate them in a session. A bad actor can thus gain access to traffic that is supposed to be confidential. Without some form of authentication of identity, the parties communicating cannot be sure that the person announcing a public key is who they say they are.

WebPKI and the Problem of Authentication

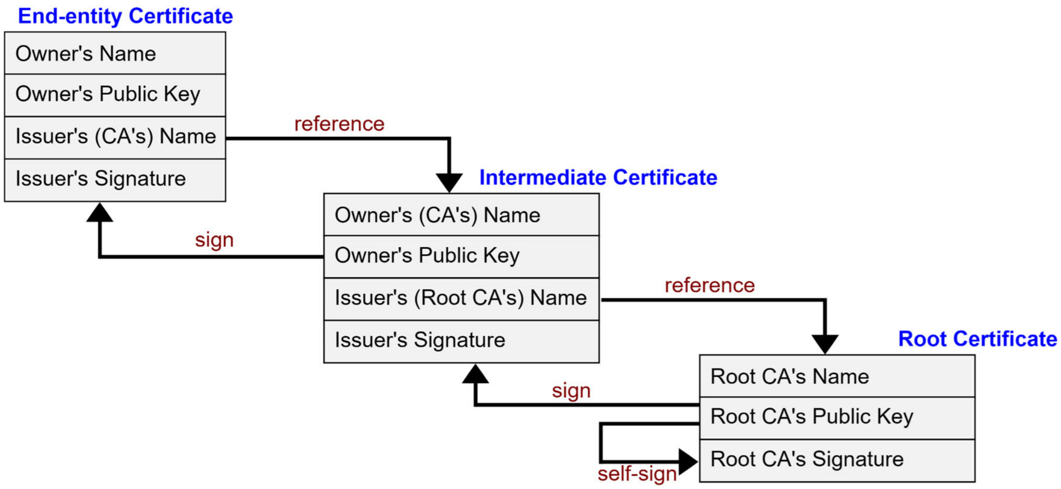
Digital certificates are intended to be a solution to the authentication problem. A digital certificate binds a public key to an identifier such as a domain name and/or organization name[3] Certification Authorities (CAs) issue digital certificates to website operators (or other entities needing authentication) upon request. Before issuing certificates they are supposed 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. When a browser connects to a website using HTTPS, it requests the website's certificate and checks if it is valid, up-to-date, and issued by a trusted CA. If the certificate passes these tests, the browser establishes a secure connection with the website and displays a signal indicating a secure connection in the address bar.

Relying on a trusted third party to authenticate, however, is recursive. A CA can issue certificates that lie or impersonate just as easily as a bad actor impersonating the rightful owner of a public key. How do you know you can trust the CA?

The Chain of Trust

The answer is not *prima facie* a very satisfying one. A CA tells us it can be trusted by referring to another third party - which is just another CA that is supposed to have validated it. If recursion is not to go on indefinitely (turtles all the way up?) the buck must stop somewhere. In WebPKI it ends in a smaller number of "root" CAs. A root CA is signed only by itself, but goes through a special, much more rigorous vetting process. Among other things, its signing key is kept in a physically secure location not connected to the Internet, and its technological and business practices are audited and subject to specific standards and requirements. These vetting processes are known as *root store* programs. Who runs these root store programs?

Figure 1: Process Diagram



Source: AboutSSL.org[5]

WebPKI does not have a single, centralized root like the domain name system (DNS).[6] Instead, the chain of authentication terminates in multiple root stores. They are administered by producers of browser softwares and operating systems, which embed lists of trusted CAs in their software. Currently there are six primary WebPKI trust hierarchy termination points [3]:

- Apple
- Microsoft
- Mozilla
- Google
- Oracle
- Java

In effect, root store programs are producing knowledge about which CAs (and which certificates) are valid and trusted. It is a semi-centralized certification regime. The CAs deemed "trusted" are automatically disseminated to users via the browser software. 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 rigorous root store programs of a small number of software vendors. Certifications of trustworthiness derived from those programs are distributed in a branching hierarchy to millions of other certificates. Root CAs sign for multiple intermediate CAs, the intermediate CAs issue

[5] https://aboutssl.org/root-certificates-vs-intermediate-certificates/

[6] The DNS name space operates as a strict hierarchy with a uniform list of top level domains in a single, global root zone maintained by PTI, which is currently a subsidiary of ICANN.

certificates to other CAs or to websites or other objects in cyberspace. Users (clients) receive information about the trustworthiness of websites as their browser attempts to track the hierarchy of CAs up to its root. Users receive warning alerts on their browsers if these authentication attempts fail.[7]

The authentication process creates strong technical interdependencies between browser software (clients), the CA services, and the websites (servers) acquiring certificates for HTTPS. The user's browser software must read the website's digital certificate and check its trust chain to see if it can be authenticated. It notifies the user of danger if the certificate is invalid or the CA cannot be trusted. It displays a green lock icon or some other signal if it has been properly authenticated. The system is supposed to prevent users from relying on certificates of untrustworthy CAs, or on expired or invalid certificates. Its reliance on functional interdependencies across many autonomous actors is one of the reasons why private sector cooperation has taken the lead in establishing governance arrangements.

Why is Authentication a Public Good?

We still have not fully explained why the WebPKI necessitates *collective action* to produce a *public good*. Public goods, to recall, are non-rival and non-exclusive. Like all information, knowledge about the trustworthiness of CAs is non-rival in consumption, but it is possible for someone possessing this knowledge to exclude others from it. The root stores are maintained by software vendors, which are competing private firms, and information about trustworthiness is embedded in their commercial software products. The vendors could keep this information private if they thought it would give their products a competitive advantage. But in fact, they do not exclude others. They all openly share the contents of their root stores, and cooperate in maintaining a common institutional rule set - the CA/B Forum Baseline Requirements. They also maintain a shared infrastructure for certificate transparency. Why do these firms engage in collective action and treat the data needed for accurate authentication as a public good?

There are two answers. One is that the software vendors - especially the web browsers - have a huge vested interest in maintaining general public confidence in the security of the Web. By supporting confidential, secure communications for everyone, encryption and authentication encourage more users to participate in online commerce and culture. Effective authentication makes everyone on the Web - consumers, suppliers, operators - better off; there are no benefits to exclusion. The other, closely related reason is that untrustworthy CAs or mis-issued certificates create externalities across all websites and all browsers. Specter [24, p. 56] 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, … but intermediates and the number of leaves each intermediate owns are often not known. The result is that the CA system has

[7] Notably, the reliability of this hierarchical dissemination of knowledge of trustworthiness is predicated on the transitivity of trust. This transitivity is one of its weaknesses, as knowledge of trustworthiness degrades, and opportunities for impersonation increase the further it gets from the source.

> become so interdependent that it is functionally impossible for a user, however knowledgeable, to distrust a specific certificate authority." [24]

Arnbak, Asghari et al [37, p. 52] make a similar point. p. 52 "The failure of a single CA impacts the whole ecosystem, not just that CA's customers." Even if the software vendors' narrow self-interest led them to not be fully committed to the public good of security, the externalities would come back to bite them.

Trustworthiness, however, is still a *private* good for CAs. CAs reap exclusive benefits from achieving certain levels of integrity and trust, and can suffer targeted penalties if they do not. CAs must be accepted by root stores (either directly or indirectly) or else no one will buy their certificate services. As a clear indication of the private good nature of trust for CAs, CAs with root status can monetize their status if they are part of an acquisition; the sale price will be directly affected by whether they are in the browser root store.[8]

The techno-economic ecosystem, however, also imposes clear limits upon the scope of collective action. If software vendors need to cooperate to maximize the trustworthiness of CAs, why do they not come together to maintain a common, jointly administered root store? The answer seems to be that each vendor wants to maintain private control of the security tradeoffs and risks related to their own software products. These risks and tradeoffs may vary with the characteristics of the software. We note below that each root store maintains slightly different lists of root certificates. Instead of a common, collectively produced root store, we get transparency and coordinated standards and policies regarding certificate issuance. However, each Browser vendor can still make independent decisions about which CAs they will trust. Because of the small number of browser producers, it is relatively easy for them to coordinate major actions when necessary. For example, each major browser decided to withdraw trust from DigiNotar, a compromised CA, within days of each other. The WebPKI governance regime has arrived at a mix of autonomy and coordination in the maintenance of root stores. But the important point is that the burden of supporting a general *public* good (authentication of public keys) has been assumed by leading *private* actors in the industry, not by governments, regulatory agencies, or public law.

Step 2: Stakeholders

We identify four categories of stakeholders in the WebPKI institution: Certificate Authorities (issuers of certificates), Browser/OS vendors, Subscribers (certificate consumers), and Web End Users (relying parties on certificates). As we shall see, due to transaction costs, only the first two are direct participants in collective action around authentication.

Certificate Authorities (CAs)

As noted before, CAs issue digital certificates that bind a public key to an identifier. The commercial CA market is surprisingly small. The company Mordor Intelligence estimates a

[8] There is a secondary market for CA root status, as a CA's acquisition price will reflect its root status. Although the root programs are costly, the browser vendors do not appear to be auctioning off access.

market size of 160 million USD in 2023 [25]. Another market intelligence firm estimated market value at 127 million USD in 2021 [26]. The CA/B Forum had 55 members in the CA category as of July 2023 [27].

CAs are a registration service business similar to domain name registrars (some DNS registrars, such as GoDaddy, span both business lines). CAs maintain records of which public keys are associated with which identifiers, and publish cryptographically signed certificates attesting to that linkage. Each certificate is assigned a unique identifier (a serial number).

There are two basic types of CA: a) providers offering service to the public; and b) internal CAs run by private organizational networks. The second category applies to larger companies and some governments that maintain an internal Certificate Authority to provide certificates for organizational domains. This research is focused only on the public CAs. Public providers can be commercial, for-profit businesses, such as Sectigo, or non-profit organizations, such as Let's Encrypt.

CAs use various methods to verify the identity of the organizations or entities to which they issue certificates. The three certificate types correspond to different verification methods: Domain Validated (DV) certificates are the most basic; they only verify the ownership of a domain name by sending verification messages to it.[9] Organization Validated (OV) certificates require the CAs to verify the identity of the organization operating the website. Extended Validation (EV) certificates entail further verification of additional business-related attributes.

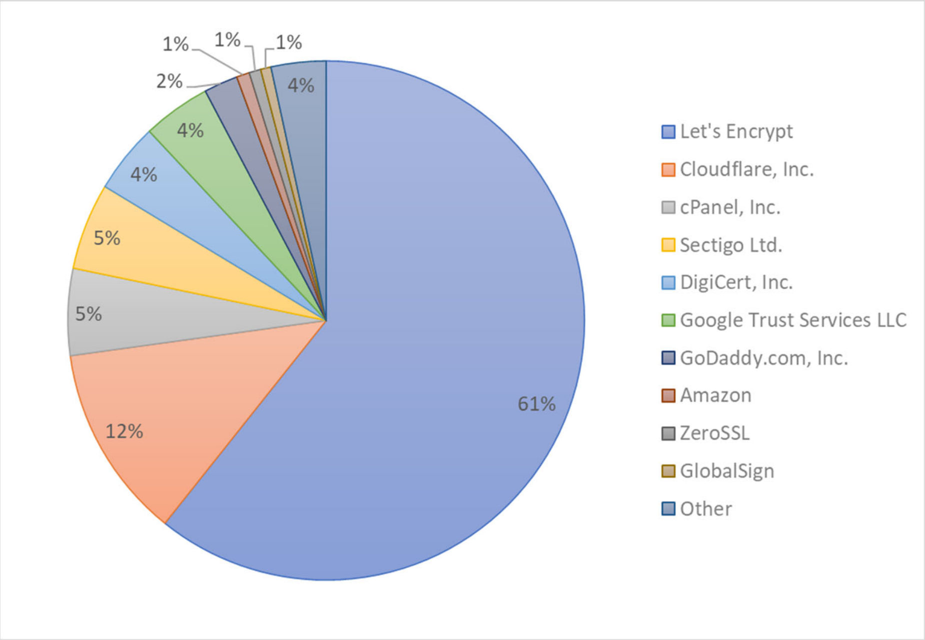
CAs can create security vulnerabilities that can be exploited. Sometimes, these problems are the result of bad implementations.[4] At other times, they can be deliberate acts of rogue CAs [28]. A well-known example of the latter is when the government of Kazakhstan used its control of the national telecommunications company to force Web users in its jurisdiction to install a root CA that it could exploit to spy on the private communications of users [29].

To measure the distribution of certificates over CA issuers, we took a random sample of 1 million URLs from the approximately 3 billion unique URLs in January 2023. The population of sites we sampled from 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 was not 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 identified 2,366 unique names of organizations issuing certificates.[10] A small proportion of the sample consists of organizations which use their own certificates internally but do not provide this service to third parties, such as universities or large corporations.

[9] Having control of a domain is not the same as being the proper owner. If an attacker succeeded in gaining control of a domain through fraud or phishing, the Web PKI regime would still validate the domain.

[10] Some bias in this sample might be induced by assigning a time limit of 10 seconds for the page to load when requesting certificate data.

Figure 2: CAs Share of Website Certificates



The sample shows that 61% of the digital certificates can be traced to Let's Encrypt. We discuss Let's Encrypt in more detail in the section on Institutional equilibrium below. Of the identified firms, 80% were members of the CA/B Forum, but this is likely an undercount. Both Cloudflare and cPanel rely on CAs like Let's Encrypt, Google Trust Service, and Sectigo for their certificates.

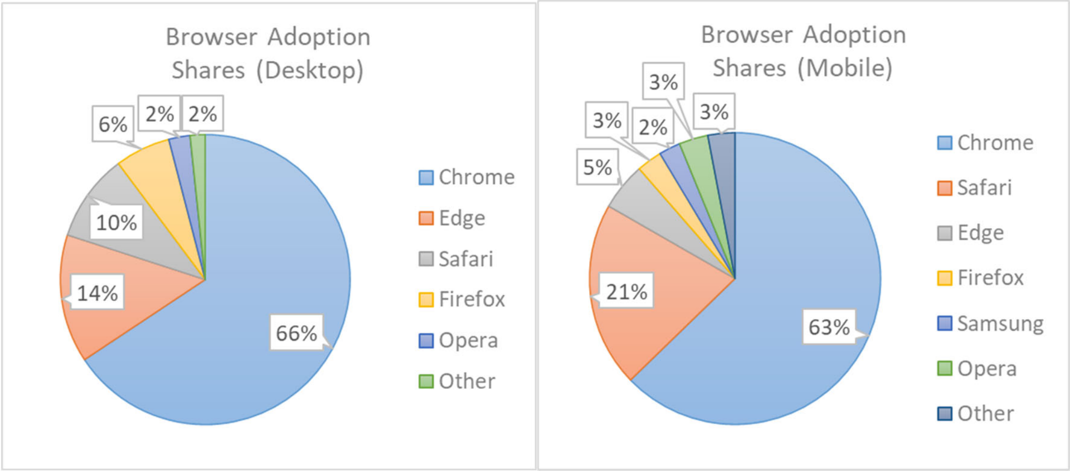
Browser/OS vendors

Browsers act as gateways into the Web ecosystem. Through advertising revenue and data collection, the browsers profit indirectly from attracting more users and more traffic. Browsers' interest in authentication is closely aligned with that of the end users. End users (clients) can be considered "relying parties" in the certificates. Users adopt browser software to navigate the Web and want their communications and identity safe from external attack. The software vendors' position in the ecosystem often puts them at odds with the interests of CAs. From the Browsers' point of view, CAs should do as much work as possible to verify certificate holders, and the certificates should be updated as often as possible to protect against compromise or obsolescence.

While browsers/software vendors are generally good proxies for end user security, their interactions with CAs are constrained by user demand for compatibility and access. Overly aggressive enforcement of what they consider to be secure certificate policies might prevent users from accessing many websites. Constant warnings to click away from a site might prompt users to replace browsers that block connections or issue warnings with less secure products that do not erect barriers to access. Access barriers also undermine user confidence and suppress usage, just as security vulnerabilities do. Hence, while browsers' control of the root stores gives them a powerful position, they cannot unilaterally dictate the practices of CAs but must negotiate standards with them, nor can they unilaterally impose security standards on end users as their actions are constrained by user choices. By the same token, the prospect of user defection due to high security standards strengthens the incentives of browsers to engage in collective action with other browsers - if they all adopt the same standards the impact of user defection will be minimized.

The browser market is concentrated. Over the past decade, the producers of browser software have become increasingly aligned with the dominant operating system (OS) vendors: Apple (iOS), Microsoft (Windows), and Google (Android). These three platforms account for 89% of mobile browser use and 90% of desktop browser use.

Figure 3: Browser Adoption Shares (a: Desktop; b: Mobile)



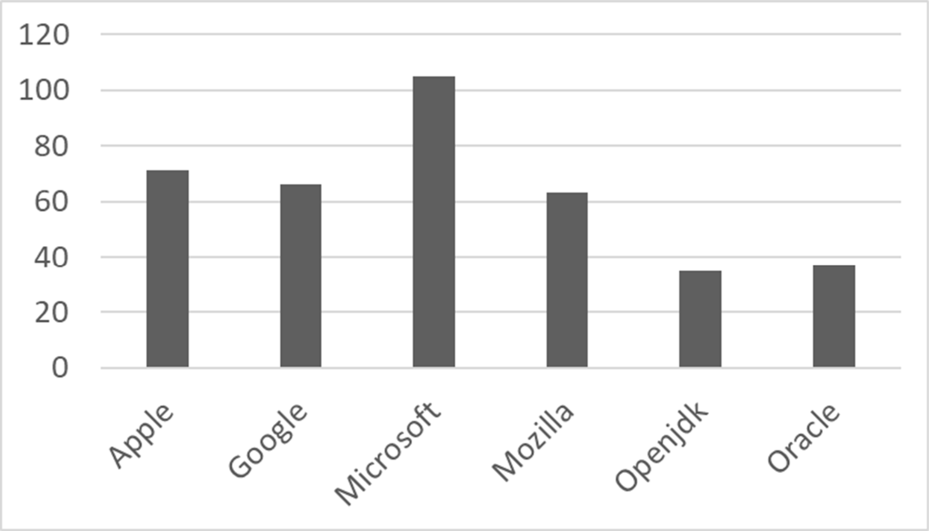
Source: gs-statcounter.com[11]

Different browsers will choose to admit different Certificate Authorities into their Root Stores. While they recognize the need for collective action to impose standards on CAs, as noted before, they want to maintain firm-level control of their own root programs. Using records pulled on July 30, 2023 from Alban Diquet's Trust Stores Observatory, we can identify the number of CA Roots listed by Browser Trust Stores [30].[12]

[11] gs-statcounter.com 'Desktop Browser Market Share Worldwide' (August 2023) https://gs.statcounter.com/

[12] Root certificates should be distinguished from Certificate Authorities; a single CA can operate multiple root certificates. While an imperfect proxy for corporations with 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.

Figure 4: Count of CAs in Browser Root Stores



Certificate Subscribers

This stakeholder group includes Web server operators, website owners, corporate network managers, and other organizations who buy or install digital certificates. Certificate subscribers, who number in the millions, are not directly represented in the membership structure of the CA/B Forum; the CA stakeholders are *de facto* proxies for their interests. Subscribers' 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. Some of the actors in this class are experienced ICT managers with knowledge of WebPKI operations and the reliability of CAs, but they still need to outsource this function to CA services.

This stakeholder group's capability for organized collective action is undermined by its size and diversity. Because of these obstacles, they are not directly represented in Web PKI institutions; their preferences are proxied by the CAs.

End users

Like Subscribers, end users (the individuals who download browser clients and use them to navigate the Web) are not formally represented in the CA/Browser Forum's membership structure. Their capability for collective action is even more limited than subscribers because they are even more diverse and numerous. Their interests are proxied by the Browser vendors. The purchase, installation, revocation and management of digital certificates is largely invisible to them.

End users choose one of three major software ecosystems (Android, iOS, Windows), the use of which is sticky over the long term due to high switching costs. Regardless of OS choice, they can use almost any browser, any app, and access any website. They have the choice to ignore or override browser warnings, but they rely heavily on the Browsers for warnings/advice and usually follow it. Their security incentives are similar to the Browsers in that they want generalized safety and security in their Web interactions, they want their login information and other sensitive data to be confidential in transport, they want their interactions with e-commerce transactions to be secure and confidential, and they want to avoid data breaches, cybercrime, phishing scams and the like.

Some of the existing literature on the security economics of Web PKI refers to the concentration of market power in the hands of the browsers and/or the information asymmetries between users and CAs. As we will show below, these analyses tend to misunderstand the public good nature of Web PKI authentication. While the browsers do have discretionary power over which CAs they include in their root stores, they do not participate in the CA market and do not gain economically from arbitrary or discriminatory exclusions. Their primary interest is in the security of Web traffic. Likewise, while users are not in a position to know very much about which CAs are trustworthy, the browsers *are* in such a position, and can use their power over root stores to implement that knowledge in a way that supplies that knowledge to end users.

Step 3: Institutional Formation

Because institutionalization is path-dependent, understanding the institutional equilibrium requires looking at its history. The process of institutionalization in this case was driven by critical events that disrupted established patterns or provoked new initiatives to solve problems.

The early CA industry was experimental and not well organized. For the first ten years (1995-2005), certificates were issued with no rules at all, according to one of our interviews. 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. According to one of the participants in that meeting, its ostensible purpose was to “come up with a plan to kill DV Certs.” The emergence of low-cost DV (domain-verified) certificates from CAs like Geotrust and GoDaddy at that time was perceived as a threat by incumbent CAs because it was turning the certificate business into a low-margin, high-volume industry. The impetus for browser-CA collective action, in other words, came from a perception that competition from DV certificate-issuers was contributing to a “race to the bottom” in which CAs were prioritizing volume over security and issuing certificates to anyone. A common “baseline” set of requirements enforced by the browser software was seen as the answer to that problem. The original proposal was to use the leverage of browsers to mandate an OV profile for all publicly-trusted certificates. Instead, 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.

These early efforts did not succeed in regulating 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 [31-32]. The Electronic Frontiers Foundation started an SSL Observatory that released a critical report about WebPKI in 2010 [33], to which the CA/B Forum found it necessary to publicly reply [34]. In April 2011, the CA/B Forum released a request for public comment on a new set of "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [35]."

Problems kept proliferating. Managers at Comodo, one of the top three CAs at the time, revealed that it had been compromised in a March 15th, 2011 attack that yielded the username and password of a Comodo Trusted Partner in Southern Europe. That entity then suffered an attack that resulted in a compromised account being used to issue nine digital certificates across seven different domains controlled by Yahoo, Google, Skype and Mozilla. All of these certificates were revoked immediately upon discovery.

The strongest incentive to clean up WebPKI was the massive disruption created by the July 2011 breach of Diginotar, a major Dutch CA, by an Iranian hacker [36]. The compromise of this CA allowed the attacker to forge certificates for many major websites, compromising the websites and email services of the major browser firms. Google certificates were compromised and Google, Microsoft and Apple were forced to revoke trust of Diginotar.

An analysis of the "security collapse in the HTTPS market" in 2011 [37] applied concepts from the economics of information security to an analysis of the Web PKI ecosystem at that time. They asserted that the HTTPS authentication model allowed "any CA to sign certificates for any domain name," leading to a "weakest link problem" and a "race to the bottom." They argued that information asymmetries existed, making it very difficult for other stakeholders to know about the security of CAs. They spoke of "liability dumping" in which websites, browsers, and CAs push responsibility for the damage from security breaches on to end users or subscribers. They claimed that the CAs of authoritarian states "can issue a certificate for any website in the world, which will be accepted as trustworthy by browsers of all Internet users." They also criticized concentration in the market, noting that "around 75% of SSL certificates in use on the public Web have been issued by just three companies: Symantec, GoDaddy, and Comodo."

Below, we show how each of the problems analyzed in [37] were addressed and significantly mitigated if not eliminated by the collective governance arrangements that developed after 2011. The paper presented these as "market failures," yet ultimately they were remediated not by government intervention but by industry-led collective action involving the CA/B Forum, nonprofit advocacy groups, and pressure from the browser vendors.

The CA/Browser Forum version 2.0

The CA/Browser Forum as we know it today was forged in response to the Diginotar Incident. It remains an unincorporated industry association, but in 2011-12 it became a more active and formalized vehicle 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 for its members.

Critically, in the year following the Diginotar incident, the CA/B Forum became more formalized, adopting written bylaws on 23 November 2012 drafted by Kirk Hall, then of AffirmTrust, who had a legal background. The Bylaws established officer titles, qualifications for membership, voting rules, and developed a process for creating working groups. Despite this formalism, the first version of the bylaws emphasizes 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 [38]." The 2012 bylaws established a voluntary Forum Infrastructure Working Group to maintain the infrastructure that hosts its dialogue.

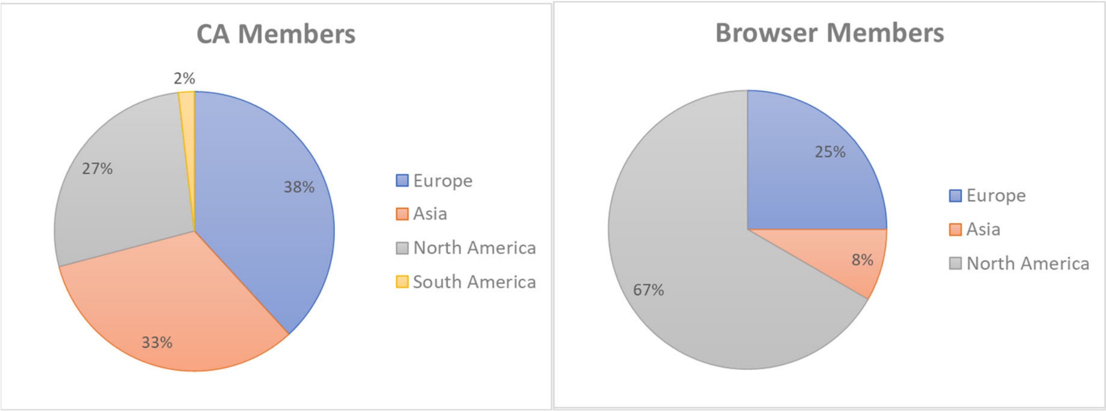
Table 1: CA/B Forum Constituency (2023)

Certificate Authorities	55 voting organizations
Browser Software Vendors	11 voting organizations
Associate Members	7 non-voting organizations

The bylaws identify two voting constituencies, Certificate Authorities and Browsers, and a third non-voting group of Associate Members. Increasingly, Forum work takes place at the working group level.

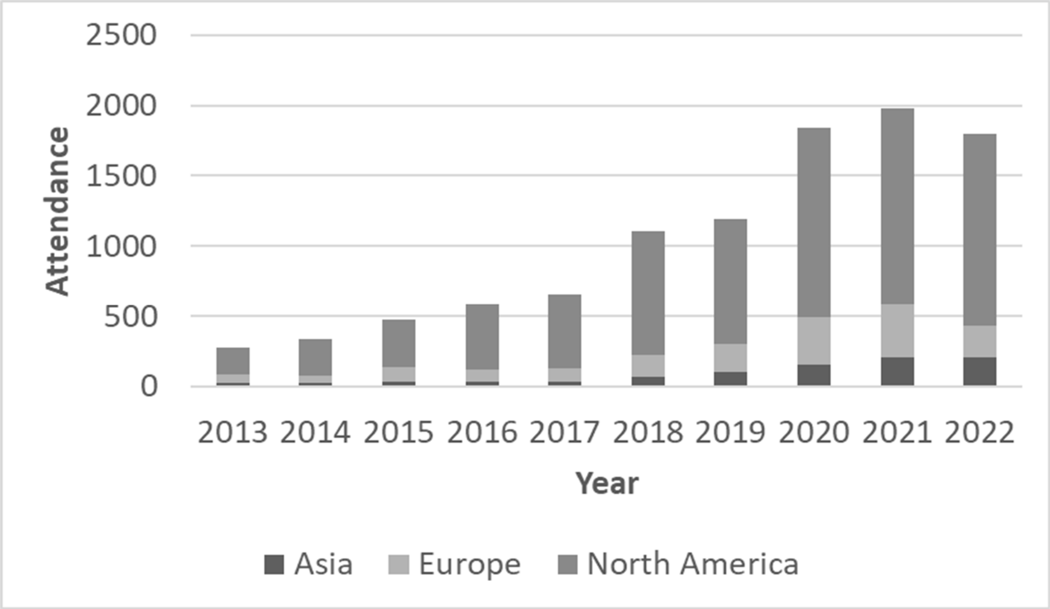
While membership ensures an equal vote, it does not imply an equal level of participation in ideation and discussion. To get at engagement, we reviewed the publicly reported meeting minutes of the CA/B Forum which are archived through 2013 and include 369 posted meeting minutes including those from various working groups. As working groups are added the number of yearly meeting minutes grows. We were able to scrape these meeting minutes, extract, and then clean attendee records. Ultimately, this data provided attendance records for 553 participants from 123 organizations.

Figure 5: Membership in CA/B Forum



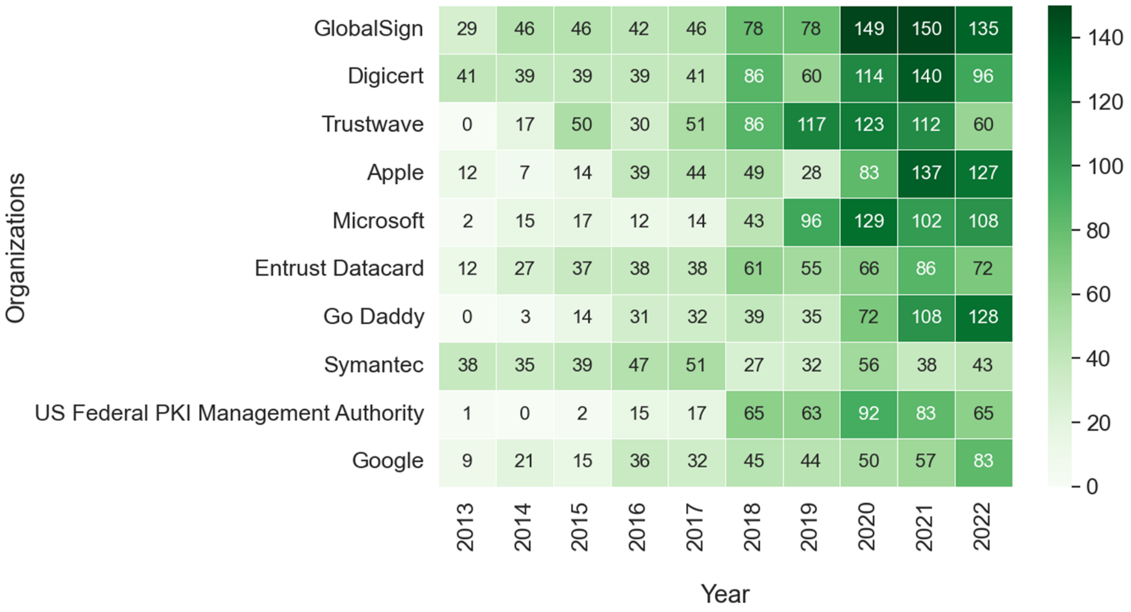
If we look at the national headquarters of participating firms, the CA/Browser Forum is very clearly dominated by US firms, though this chart does identify a recent increase in the diversity of participants from other countries. These US-headquartered firms represented, on average, about sixty percent of participants. Other prominent countries represented are concentrated in either Europe or East Asia.

Figure 6: CA/B Forum Participation by Organizational HQ Region



The vast majority of participants attend fewer than 20 meetings. However, a few highly active participants have attended more than two thirds 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 7: CA/B Forum Top Organizational Participation Over Time[13]



Organizations	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
GlobalSign	29	46	46	42	46	78	78	149	150	135
Digicert	41	39	39	39	41	86	60	114	140	96
Trustwave	0	17	50	30	51	86	117	123	112	60
Apple	12	7	14	39	44	49	28	83	137	127
Microsoft	2	15	17	12	14	43	96	129	102	108
Entrust Datacard	12	27	37	38	38	61	55	66	86	72
Go Daddy	0	3	14	31	32	39	35	72	108	128
Symantec	38	35	39	47	51	27	32	56	38	43
US Federal PKI Management Authority	1	0	2	15	17	65	63	92	83	65
Google	9	21	15	36	32	45	44	50	57	83

[13] In Figure 7, the participation for each organization is calculated through the cumulative addition of the total number of participants attending all meetings throughout the year. This

After 2017, the Forum proliferated working groups to expand certificate standards to areas beyond the web, such as code signing and server certificates. The Subject Area Working Groups (WGs) include - S/MIME Certificate WG (2014), Code Signing Certificate WG (2015), Network Security WG (2017), Server Certificate WG (2018).

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. 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, they said "We have raised the bar significantly over the past 15 years."

Equilibrium: The New Rules

In this section we study various policies and governance mechanisms that have come out of the CAB Forum for WebPKI. 1) The Baseline Requirements (BRs), 2) Certificate Transparency, 3) shorter certificate durations, and 4) Automation are the primary outcomes of institutional change and collective action to clean up authentication functions in WebPKI. There was also 5) a major action to remove trust from a CA perceived as not following the rules. Together, they constitute a rule-based equilibrium that coordinates the behavior and converges the expectations of stakeholders to achieve the public good of authentication of public keys. The convergence of stakeholder interests is revealed in subsection 6), an analysis of CA/B Forum voting distribution below.

1. The 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 1 July 2012. It 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 [38]." The Baseline Requirements were revised about once every 6 months, utilizing 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 [40].

captures meeting frequency, the number of attendees from each organization, and the expanded scope of additional working groups.

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 (CA) operations [41]." In 2021 the CASC was restructured and renamed the "Public Key Infrastructure Consortium."

2. Certificate Transparency

Certificate Transparency (CT) is a new tool supporting the self-regulation of authentication. It developed around leading CA/B Forum members and was actively discussed in the Forum, but is enforced by browser root store policies rather than CA/B Forum Baseline Requirements. CT was very much a response to the Diginotar incident.[14] That incident revealed that the controller of a compromised CA can issue certificates that were not requested by and not known to the legitimate owner of a domain. CT combats such certificate mis-issuance by creating a public, shared log of certificate registrations so that anyone can check for illegitimate certificates issued for their domain.

Implementing CT requires the construction of an extensive, complex infrastructure, and the specification of standards governing the communications among its component parts. The initial proposal was published in June 2013 as IETF RFC 6962 by several Google employees [42]. The standard promotes the publication of append-only certificate logs that would be publicly auditable and improve assurances that certificates are linked to the appropriate entity. CT logs allow an organization to search newly published certificates to see if anyone is improperly using their organizational name.

As of August 2023, both Google and Apple require CT logs to be published by any CA accepted in their root stores. The CT infrastructure involves an open and growing set of voluntarily-run logging servers, a set of monitors that check the logs for suspicious activity, and modifications to the browsers (or user agents) that enable them to convey warnings or trust to end users regarding certificates that have not been properly logged. The infrastructure reflects collective action among diverse firms with an interest in Web security: Apple, Google, Cloudflare, Sectigo, DigiCert, Censys, Facebook, Let's Encrypt, and sslmate [43].

Like certificate duration (see #3 below), CT initially sparked tension between CA and Browser stakeholders in the CA/B Forum. Browsers saw it as a vital check on certificate mis-issuance; many CAs saw it as added overhead that would retard their ability to issue certificates as quickly as their subscribers wanted. The 15 February 2014 CA/B Forum meeting minutes contain contentious discussions of CT. Google's Ryan Sleevi stated, "while we can certainly appreciate the multi-stakeholder nature of [the CA/B Forum], it [CT] is certainly not in the interests of some CAs —their business interests are not aligned entirely with our security goals for our users

[14] The website of the initiative states, "Certificate Transparency was a response to the 2011 attack on DigiNotar and other Certificate Authorities." https://certificate.transparency.dev/

[44].” As with certificate duration, this conflict of interest was resolved by a combination of unilateral action by browsers and gradual acceptance and cooperation by CAs. A statement from the official website of the group supporting CT provides a clear example of how smooth implementation of the new governance rules required collective agreements and negotiations:

> “...no single organization could convince the entire Internet to adopt and benefit from [CT] at once. Similarly, user agents [browsers] could not begin requiring all websites to support CT at once due to the risk of breaking large numbers of websites. So the members of the CT ecosystem worked together to define the standards and to incrementally deploy and later enforce CT [45].”

CT has rendered Certificate Revocation Lists (CRLs) and certificate pinning largely obsolete for mitigating certificate mis-issuance. They have limitations that CT helps to address. CRLs require CAs to maintain and publish frequently updated lists of revoked certificates, which can be inefficient and time-consuming. Additionally, relying solely on CRLs necessitates frequent checks by users, hindering real-time security. Certificate pinning, on the other hand, fixes a website's trust to a specific certificate or CA, but this becomes problematic if that CA becomes compromised. CT addresses these limitations by providing a public, centralized log of all issued certificates. This allows for efficient verification of a certificate's legitimacy and faster detection of revoked or suspicious certificates, offering a more dynamic solution compared to traditional methods.

However, CT deployment requires a substantial investment from browsers; implementations must minimize warnings and breakages to their users, who may switch browsers or bypass warnings. The risk of user bypass and browser switching means that to realize its full security benefits, most browsers must adopt CT.[15] CAs must also assume some of the burdens of CA implementation, but they have been incentivized to do so by browser requirements. Here again, collective action is facilitated by a small number of leading firms taking the initiative, gradually incentivizing adoption among CAs, and avoiding the need for subscribers or end users, a group too large to coordinate, to jointly take action.

3. Shorter Certificate Duration

As noted before, policy toward the expiration of certificates pits the interests of many CAs (and by proxy, their subscribers) 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 [46].” 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 advocated 13 month durations, while CAs argued for longer durations or more extended periods to phase in shorter durations. In 2017, the CA/B Forum agreed to reduce the length of TLS certificate lifetimes down to 825 days (27.5 months) with unanimous support for

[15] “Initial implementation can be a substantial engineering effort. For example, Firefox’s experimental CT implementation has been disabled by default for over a year due to unresolved regressions. Firefox developers have expressed concerns about whether the security properties of CT are valuable enough to warrant this investment.” [7]

the provision except for a few abstentions. Nevertheless, the Browser representatives insisted that a 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 requirements and root store policies. The Certificate Authorities, in contrast, argued that shorter renewals would cause business disruptions and put undue burden on their customers, the website administrators.

Google proposed a vote to reduce certificate lifespans 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 announced at the Forum that they would *unilaterally* implement the 13 month duration[47]. Mozilla followed Apple's lead and Google followed shortly after. The ability of the browsers with substantial market share to set certificate durations unilaterally demonstrates a power imbalance in standards well understood by the participants. Arguably, in this case the power imbalance allows the Browsers to be agents for a broader public good for Internet-users whereas the CAs are reflecting private interests.

4. Automation and "Free" Certificates

Let's Encrypt (LE) represents a notable civil society effort initiated in the wake of DigiNotar and the Snowden revelations. LE offers subscribers a highly automated method of getting digital certificates at no charge. The project to build Let's Encrypt was initiated in the Summer of 2012 and became operational in the second quarter of 2015. The team of two Mozilla employees together with individuals from the Electronic Frontier Foundation and the University of Michigan subsequently incorporated as Internet Security Research Group (ISRG) in May of 2013 [48]. Closely associated with the development of LE was the development of a new IETF standard, Automatic Certificate Management Environment (ACME). ACME describes "a protocol that a CA and an applicant can use to automate the process of verification and certificate issuance," as well as methods to facilitate other certificate management functions, such as certificate revocation [49].

LE has transformed DV certificates into a free public good, and captured a very large market share. As shown in Figure 3, the Let's Encrypt CA has taken over the bulk of the DV market, and accounts for 61% of the total number of certificates counted by our methodology. Cross-signing from IdenTrust, a major CA, gave LE access to the root stores, so its intermediate certificates were widely recognized and rapidly adopted.[16] Let's Encrypt's ISRG Root X1 certificate is now so widely recognized that it will allow its cross-signatures to expire in September 2024 [50].

It is already evident that LE did not drive commercial CAs out of business, as some feared. But how are traditional CAs coping? How much does the regime rely on their survival? Commercial

[16] Cross-signing provides an alternative path to a root certificate; this redundancy can provide resilience to a subordinate certificate chain of trust.

CAs have gravitated to OV and EV certificates, which are not as susceptible to automation. These services are sometimes bundled with security or website hosting.

5. Enforcing the Rules: Untrusting Symantec

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). In response, Google requested in a blog post that Symantec adopt Certificate Transparency, amend its incident report, and improve overall security [51]. Google claimed that Symantec CAs had improperly issued more than 30,000 certificates over the years, while Symantec disputed this and admitted to only 127 [52].

As the largest CA in the market, some Browser representatives perceived Symantec as "irresponsible" and thought of itself as too big to be disciplined. 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 27 July 2017 to a development listserv clarifying that they would move to distrust Symantec-issued TLS certificates [53].[17] 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 widespread outages for users 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, they 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 over 30 percent of the Internet's valid certificates by volume in 2015, Google staggered the mass nullification over time.

Efficacy Measures

Assessing the efficacy of the regime can be done across a number of metrics. This includes 1) balloting behavior; 2) the growth in the number of certificates issued and in the use of encryption on the Web; 3) convergence in the contents of the different root stores; 4) a reduction in the number of CAs in the root stores; and 5) enhanced detection and revocation of mis-issued certificates.

1. Balloting Behavior

Voting behavior reflects the ability of the Forum to coordinate the interests and resolve conflicts among the two key stakeholder groups. Under the CA/B Forum governance rules, passage of a

[17] According to [52], "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."

ballot requires the support of both a majority of browsers and 2/3rds of the voting CAs. Half of the current member organizations must be present for a quorum to be achieved. Table 2 shows that of 192 ballots since 2013, 174 received quorum and 156 were passed.

Table 2: CA/B Forum Voting Pattern

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

Figure 8 shows the level of support ballots have received since 2013. In the vast majority of cases, ballots receive either unanimous or near-unanimous consensus. This is also true when firms were determined to oppose the ballot. CA and Browser behavior are fairly similar in this respect. These figures do not account for abstentions.

Figure 8: Distribution of Ballot Support

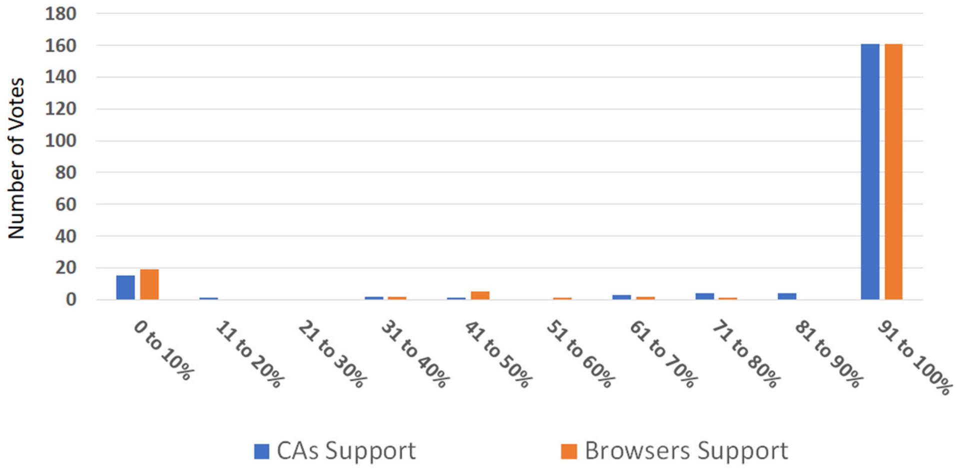
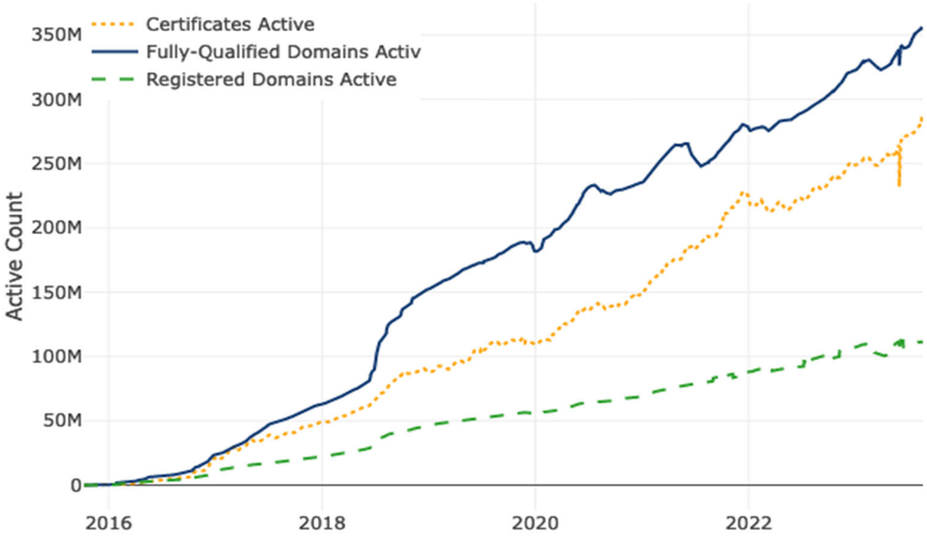


Figure 9: Growth in Let's Encrypt Certificates and Domains



2. Growing use of encryption

While the HTTPS protocol was specified by RFC 2818 in 2000, it was not until years later that encryption on the web would become the norm. A number of factors led to website adoption including the 2013 Edward Snoweden revelations, the 2015 HTTPS Now campaign by EFF and the 2016 launch of Let's Encrypt. Let's Encrypt free certificates have shown consistent growth as demonstrated by Figure 9.[18] On 28 December 2013, Google measured encrypted traffic crossing its domains at 48%. By 22 July 2023, that percentage was 95%. In October 2013, Firefox measured 27% of the web pages loaded with HTTPS, which grew to 79% by July 2023.

3. Convergence across Browsers/OS's

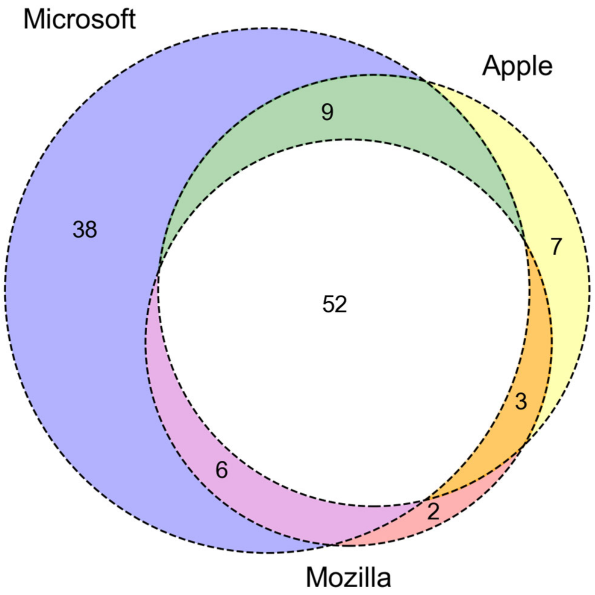
If externalities caused by poor CA security practices are the main driver of collective action, we should expect to see the gradual homogenization of the root stores across browser/OS producers over time. A common, standardized set of Baseline Requirements for CAs should reduce differences among the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

We do see 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

[18] This statistics was taken from Let's Encrypt as of 28 November 2023. https://letsencrypt.org/stats/

by Microsoft are operated by governments, including the Dutch, Saudi, Swedish, Swiss, and Thai national CAs.

Figure 10: Overlap in Browser Trust Stores[19]

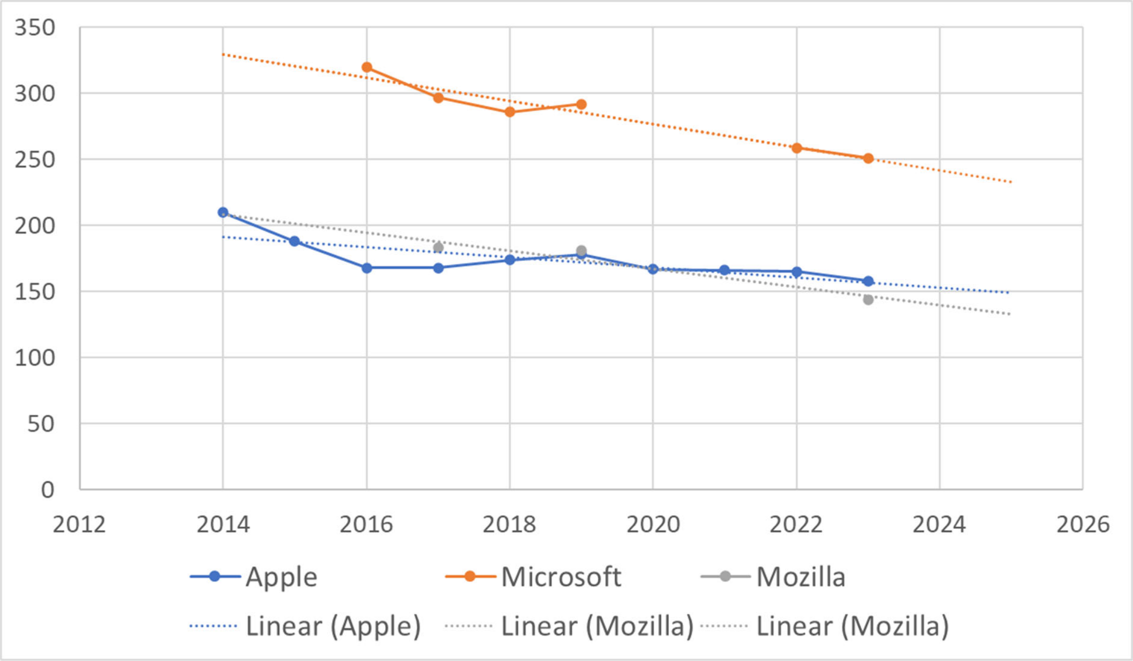


4. Reduced number of CAs in the root stores

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.

[19] We coded these entities for shared brand names. For example, 'DigiCert Assured ID Root CA' and 'DigiCert Trusted Root G4' would be coded as DigiCert.

Figure 11: Number of Root Certificates in Browser Trust Stores



5. Reduction of mis-issued certificates

A systematic study of CT efforts at Google found that implementation of CT helped prevent certificate breakage. "With over 60% of the web's HTTPS traffic now supporting CT", there is minimal breakage, even with the rollout of new CT requirements. According to the study, "even when breakage does occur, it is often due to bugs or misconfigurations in how certificate authorities (CAs) implement CT [54]."

Misissued certificates were already a declining problem according to a study conducted in 2018. More than 12% of the issued certificates in 2012 contained errors or were mis-issued. Nearly one-third of these violated community recommendations, which at that time were loosely defined. In 2017, only 0.02% of the issued certificates violated any form of standards [55]. While the global mis-issuance rate is low, this is predominantly due to a handful of large authorities that consistently issue certificates without error. The three largest CAs by the organization - Let's Encrypt, Comodo, and cPanel - signed 80% of the certificates in our dataset and have near-zero mis-issuance rates.

The Role of Governments

If trust on the Web is a public good, why haven't governments provided the vehicle for it? Collective security is generally considered one of the primary functions of states. A review of theoretical literature on public goods and collective action provides several explanations for the absence of states from this regime, as well as normative reasons for keeping them at arm's length.

One key finding of this research is that there should be a match between the scope of the externality to be dealt with through collective action, and the collective decision-making unit. As Boettke put it in [19] "Different public goods are most efficiently produced at different scales"; local governments pick up garbage, state governments administer most inter-city highways, and the national government provides protection from foreign invasion (p. 130). The required scope of governance explains why global service providers, rather than territorial governments, would be developing the institutions governing WebPKI. States have not been authoritative players in Web PKI governance because the scope of the Web is global, not territorial. The jurisdictional fragmentation of governments does not match the 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 issues of identity authentication. While international agreements are possible, achieving universal scope would take a very long time, and would be unlikely to overcome persistent political and military rivalries among certain blocs of nations. Many states will view any exposure or co-governance with certain other states as inherently insecure.

Another reason is the intricate technical interdependencies in the system. In *Governing the Commons*, [16] Ostrom identified one of the key "design principles" for self-governance as groups' autonomy to make and enforce rules for their own interactions rather than having them imposed by external agencies not directly affected by or knowledgeable about the system being governed. For effective governance, the processes of rule-making, monitoring, sanctioning and dispute resolution should be closely integrated with the people and organizations who actually use and produce the resources [19]. Web infrastructure operators have been the primary source of collective action to produce authentication and trust because they operate the various components of an integrated system and have more direct knowledge of the costs, functionalities and cost-benefit trade-offs involved. Direct intervention by states into the complex socio-technical ecosystem could easily be misguided. The absence of interference by state authorities has allowed the key actors in the space to self-organize their own governance mechanisms.

There are more fundamental problems with governmental involvement. After the Snowden revelations, and following decades of debate about state attempts to undermine encryption by private actors [59], it is evident that governments must be classified as potential security adversaries, adversaries of both users and each other. Some industry experts have asserted that the Iranians executed the Diginotar hack because they were not allowed to put their Certificate in the browser store, which would have allowed them to read the Gmail of their dissidents.[20] While many governments participate in the WebPKI as CAs for their own departments or citizens, governments can and have abused this authority to spy on Web traffic and users. [29, 57, 58]

Conclusion

This work identifies the private production of a public good in the digital certificate ecosystem. The public good is the authentication of the linkage between a public key and an identifier. Given that online threat actors seek to misappropriate others' identities, authentication is a

[20] We thank an anonymous reviewer of this paper for this observation.

necessary security function for Web users. Governments sometimes serve this authentication function in our daily lives by assigning identification records like driver's licenses for citizens and articles of incorporation for businesses. But in the global Web, that function has been assumed by private actors.

Market incentives first drove businesses to adopt certificates to establish trust in e-commerce and other online interactions. In its early days, the issuing of certificates was poorly controlled. Increased competition, information asymmetries, and externalities produced falling standards and security incidents that threatened Web industry leaders. With government intervention constrained by their territorial scope and the status of many governments as untrusted adversaries, an industry standards association, the CA/B Forum, served as the nexus for collective action to incrementally improve security and transparency. Intractable issues like a shortened Certificate length or transformative initiatives like Certificate Transparency were advanced outside of the Forum with individual corporate action.

Given the wealth of insights available to researchers exploring the contribution of multistakeholder models, these non-governmental industry-led initiatives should be understood as critical to the Internet's success and as novel governance arrangements that depart from established regimes based on state sovereignty. More narrowly, the targeted technical consensus achieved between two stakeholder groups in the CA/B Forum and the pressure valve of independent Browser action appear to be effective governance features. Our analysis was limited to WebPKI, however the CA/B Forum's working group on code signing, suggests the potential for other applications. These governance features, while seemingly novel, may be applicable to other industry-led standards initiatives.

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 issuers. Another important area of future research is the prospect of governmental interventions in the Web PKI, such as the European Commission's eIDAS rules. While there is some scholarly and policy literature on eIDAS, it is disconnected from studies of the Web PKI and shows little awareness of the potential clash between global self-governance and territorial state governance. [60, 61] The impact of OS/browser concentration on the Web, as well as the impact of Let's Encrypt's growing dominance on the overall resilience of Web PKI, needs to be investigated. 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 proxy relationship in greater depth. What information feedback loops inform this attention? What principal-agent challenges arise?

Funding

This work was supported by a 2022 Research Grant from the Internet Society Foundation (ID: G-202201-05564).

References

[1] 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.

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

[3] 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).

[4] 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 the 30th *USENIX Security Symposium (USENIX Security 21)* (pp. 4383-4400).

[5] 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.

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

[7] Stark, E., Ryan Sleevi, Rijad Muminovic, Devon O'Brien, Eran Messeri, Adrienne Porter Felt, Brendan McMillion, and Parisa Tabriz. "Does certificate transparency break the web? Measuring adoption and error rate." In *2019 IEEE Symposium on Security and Privacy (SP)*, pp. 211-226. IEEE, 2019.

[8] Samuelson, P. A. (1954) "The Pure Theory of Public Expenditure," *Review of Economics and Statistics* 36(4): 387-89.

[9] 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.

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

[11] McMillan, J. (1979). The free-rider problem: a survey. *Economic Record*, *55*(2), 95-107.

[12] Coase, R. H. (1974). The lighthouse in economics. *The Journal of Law and Economics*, *17*(2), 357-376.

[13] Olson Jr, M. (1971). The Logic of Collective Action: Public Goods and the Theory of Groups, with a new preface and appendix (Vol. 124). *Harvard University Press.*

[14] Kindleberger, C. P. (1982). *Standards as public, collective and private goods*. IIES.

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

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

[17] Ostrom, E. (2010). Beyond markets and states: polycentric governance of complex economic systems. *American Economic Review*, *100*(3), 641-672.

[18] Wagner, R. E. (2005). Self-governance, polycentrism, and federalism: recurring themes in Vincent Ostrom's scholarly oeuvre. *Journal of Economic Behavior & Organization*, *57*(2), 173-188.

[19] 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.*

[20] North, D. C. (1990). Institutions, institutional change, and economic performance.

[21] Knight, J. (1992). Institutions and social conflict. *Cambridge University Press.*

[22] Acemoglu, D., & Robinson, J. A. (2008). The persistence and change of institutions in the Americas. *Southern Economic Journal*, *75*(2), 281-299.

[23] Hazlett, T. W. (1990). The rationality of US regulation of the broadcast spectrum. *The Journal of Law and Economics*, *33*(1), 133-175.

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

[25] Mordor Intelligence Report. (2023) Certificate Authority Market - Share & Companies.

[26] Polaris Market Research. (2023). Certificate Authority Market Size Global Report, 2022 - 2030

[27] Members list at CAB Forum, Members – CAB Forum. Website accessed 16 November 2023.

[28] 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.

[29] Raman, R. S., Evdokimov, L., Wurstrow, E., Halderman, J. A., & Ensafi, R. (2020, October). Investigating large scale HTTPS interception in Kazakhstan. In *Proceedings of the ACM Internet Measurement Conference* (pp. 125-132).

[30] Github Repository, "Trust Stores Observatory," as of 29 November 2023. https://github.com/nabla-c0d3/trust_stores_observatory. GO TLS Observatory. Published: Jun 23, 2021 https://pkg.go.dev/github.com/PinkNoize/tls-observatory#section-readme

[31] 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.

[32] 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.*

[33] Eckersley, P. and Burns, J, "An observatory for the SSLivserse." Defcon 18, July 2010. https://www.eff.org/files/defconssliverse.pdf

[34] 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

[35] Public Comment Release Of "Baseline Requirements For The Issuance And Management Of Publicly-Trusted Certificates." April 11, 2011 https://cabforum.org/wp-content/uploads/Announcement-Baseline_Requirements.pdf

[36] Prins, J. R., (2011). Diginotar certificate authority breach "operation black tulip". *Cybercrime Business Unit, Fox-IT.*

[37] 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.

[38] Bylaws Of The Ca/Browser Forum, Adopted, Effective as of 23 November 2012 https://cabforum.org/wp-content/uploads/CA-Browser-Forum-Bylaws-v.-1.0.pdf

[39] Frequently Asked Questions for Baseline Requirements, CAB Forum, as of October 23, 2023 https://cabforum.org/faq-about-the-baseline-requirements/

[40] Comparison of changes documents: https://github.com/cabforum/servercert/compare/2c63814fa7f9f7c477c74a6bfbeb57e0fcc5dd5b..aa9fc5d0b2b59504a31638e880cb81c69aefa018

[41] PKI Consortium, "World's Leading Certificate Authorities Come Together to Advance Internet Security and the Trusted SSL Ecosystem," February 13, 2014. https://pkic.org/2013/02/14/worlds-leading-certificate-authorities-come-together-to-advance-internet-security-and-the-trusted-ssl-ecosystem/

[42] Internet Engineering Task Force, RFC 6962, "Certificate Transparency", June 2013.https://www.rfc-editor.org/rfc/rfc6962

[43] Certificate Transparency website (https://certificate.transparency.dev/) as of 16 November 16 2023.

[44] CAB Forum, Face to Face Meeting minutes, 31st meeting, 18-20 February, 2014. https://cabforum.org/2014/02/19/2014-02-19-minutes-of-mountain-view-f2f/

[45] Community, Certificate Transparency website, as of 16 November 2023. https://certificate.transparency.dev/community/

[46] 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

[47] Cimpanu, C. "Apple strong-arms the entire CA industry into one-year certificate lifespans," June 28, 2020. https://www.zdnet.com/article/apple-strong-arms-entire-ca-industry-into-one-year-certificate-lifespans/

[48] Aas, J., "Let's Encrypt", 16 November 2014. https://web.archive.org/web/20151208115156/https://boomswaggerboom.wordpress.com/2014/11/18/lets-encrypt/

[49] Barnes, Hoffman-Andrews et al, "Automatic Certificate Management Environment (ACME)" RFC 8555, March 2019. https://datatracker.ietf.org/doc/rfc8555/

[50] Gable, A., "Shortening the Let's Encrypt Chain of Trust," July 10, 2023. https://letsencrypt.org/2023/07/10/cross-sign-expiration.html

[51] Sleevi, R, "Sustaining Digital Certificate Security," October 15, 2015. https://security.googleblog.com/2015/10/sustaining-digital-certificate-security.html

[52] Ars Technica, Goodin, D., "Google takes Symantec to the woodshed for mis-issuing 30,000 HTTPS certs," March 24, 2017. https://arstechnica.com/information-technology/2017/03/google-takes-symantec-to-the-woodshed-for-mis-issuing-30000-https-certs/

[53] Google Group, Sleevi,R, "Intent to Deprecate and Remove: Trust in Existing Symantec-issued Certificates," March 23, 2017. https://groups.google.com/a/chromium.org/g/blink-dev/c/eUAKwjihhBs/m/El1mH8S6AwAJ

[54] 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).

[55] Kumar, Deepak, Zhengping Wang, Matthew Hyder, Joseph Dickinson, Gabrielle Beck, David Adrian, Joshua Mason, Zakir Durumeric, J. Alex Halderman, and Michael Bailey. "Tracking certificate mis-issuance in the wild." In *2018 IEEE Symposium on Security and Privacy (SP)*, pp. 785-798. IEEE, 2018.

[56] Lai, L. W., Davies, S. N., & Lome, F. T. (2008). The political economy of Coase's lighthouse in history (part I): A review of the theories and models of the provision of a public good. *The Town Planning Review*, 395-425.

[57] P. Eckersley, "A Syrian man-in-the-middle attack against Facebook," https://www.eff.org/deeplinks/2011/05/ syrian-man-middle-against-facebook, May 2011.

[58] A. Langley, "Maintaining digital certificate security," http://googleonlinesecurity.blogspot.com/2015/03/maintainingdigital-certificate-security.html, March 2015.

[59] Jarvis, C. (2020). *Crypto wars: the fight for privacy in the digital age: A political history of digital encryption*. CRC Press.

[60] Sharif, A., Ranzi, M., Carbone, R., Sciarretta, G., Marino, F. A., & Ranise, S. (2022). The eIDAS regulation: a survey of technological trends for European electronic identity schemes. *Applied Sciences*, *12*(24), 12679.

[61] Lips, S., Bharosa, N., & Draheim, D. (2020, November). eIDAS implementation challenges: the case of Estonia and the Netherlands. In *International conference on electronic governance and open society: challenges in Eurasia* (pp. 75-89). Cham: Springer International Publishing.

[62] Jo, Arrah Marie. (2017). The effect of competition intensity on software security - An empirical analysis of security patch release on the web browser market. *WEIS 2017 : 16th Annual Workshop on the Economics of Information Security.*

[63] Dong, Z.; Kane, K., Camp, L.J. (2016). Detection of Rogue Certificates from Trusted Certificate Authorities Using Deep Neural Networks, *ACM Transactions on Privacy and Security,* Volume 19 Issue 2 (p 1-31).