FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS

# Congress of the United States

## House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

June 9, 2015

Winifred Mitchell Baker
Executive Chairwoman
Mozilla Corporation
331 E Evelyn Ave.
Mountain View, CA 94041

Dear Ms. Baker:

We are writing with several questions concerning digital certificates, which are used to ensure the confidentiality and security of sensitive information transmitted through Internet transactions. The Internet has facilitated enormous economic growth around the globe; according to the Organisation for Economic Co-operation and Development (OECD), in 2010 the Internet economy accounted for 4.1 percent of overall GDP in most industrialized countries.[1] That growth is continuing; the OECD estimates that by 2016, the Internet economy will account for 5.3 percent of GDP in those countries.[2]

However, the vitality of Internet-based economic activity is dependent on an obvious and fundamental premise: for the Internet to continue to foster such economic growth, individuals must trust that when they click "buy" or "send" on a website or e-mail, the confidentiality and security of their financial and personal information will be protected.

Digital certificates are one of the cryptographic tools used by businesses and organizations to protect Internet-based transactions that involve sensitive information. For example, when a bank wants to make online banking services available to its customers, the bank will establish a website and (among other things) acquire a digital certificate for that website. These digital certificates are issued by Certificate Authorities (CAs). The CA will "sign" the certificate to authenticate that the website indeed belongs to the bank. When an Internet user logs onto the bank's website to conduct an online transaction, the user's Internet browser is programmed to recognize the authenticated certificate and allow the user's confidential personal information to be transmitted to the bank's website.

---

[1] THE INTERNET ECONOMY IN THE G-20 8 (Boston Consulting Group 2012) (March 2012).
[2] *Id* at 9.

Browsers are able to recognize authenticated certificates because they maintain lists of "approved" CA signatures and only accept a website's certificate if it contains such a signature. These lists, known as "trusted root stores," are controlled by each browser developer,[3] and CAs (with a few exceptions) must have their signatures included in each browser's trusted root store if they wish to be commercially successful. To protect the health of the digital certificate ecosystem, browsers have imposed strict security and business controls on the CAs, and only add a CA's signature to their trusted root stores after a CA has proven that they meet these controls.

Once a CA's signature is accepted by browsers, it has substantial authority and latitude in Internet commerce. In the current model, a CA with an accepted signature has the ability to issue certificates for any website, at any time. The CA is not limited by geographic region (such as a Swedish CA being limited to domains ending in .se), or by subject matter.

This unconstrained authority can be abused to issue fraudulent certificates, such as certificates for organizations that have not sought them, or for organizations that already have a valid certificate. In 2011, for example, a CA called Diginotar suffered a compromise that resulted in the issuance of over 500 fraudulent certificates for sites such as Google and Skype. At least one of these certificates was then used to impersonate Google's e-mail service Gmail, and the private communications of some Gmail users were therefore put at risk.[4] While the Diginotar compromise resulted from poor security controls and malicious intent, we are also concerned that the unconstrained ability of CAs to issue certificates may be abused intentionally.

Our concern with a CA's unfettered authority to issue certificates is heightened when the CA is owned and operated by a government.[5] Because digital certificates are used to ensure the security and confidentiality of private communications like e-mail and social media, such services can be targets for actors who wish to inhibit political freedoms such as free expression. A government-owned CA that is accepted by the browsers may issue certificates for e-mail providers or social media sites in order to seek out political dissent. Although the intent behind these certificates would be fraudulent, they would appear valid to a user's browser. Exacerbating this issue, the traditional control put in place by the browsers to discourage this kind of malfeasance – the removal of the CA's signature from the root store – would not be an effective deterrent to government CAs. Where a commercial CA would be forced out of business should their signatures be removed, a CA owned and operated by a government would likely be minimally affected.

We are writing to seek your views on the significance of this potential weakness as it relates to CAs owned by governments and whether there are changes that could be implemented to protect the integrity and trustworthiness of digital certificates. Certificate experts have proposed to address some of these concerns by restricting CAs run by governments to issuing

---

[3] The four most popular browsers worldwide are Google's Chrome, Microsoft's Internet Explorer, Mozilla Foundation's Firefox, and Apple's Safari.

[4] Kim Zetter, *Diginotar Files for Bankruptcy in Wake of Devastating Hack*, WIRED, Sept. 20, 2011, *available at* http://www.wired.com/2011/09/diginotar-bankruptcy/.

[5] The majority of CAs are private organizations (Comodo, Symantec), but a few – such as the Agence nationale de la sécurité des systems d'information (ANSSI) – are owned by governments. In other cases, CAs may result from public-private partnerships (LuxTrust), and in others it is sometimes not obvious whether a CA is government owned or not (CNNIC).

certificates for their own properties, within their own Country Code Top-Level Domains (ccTLDs). For example, a certificate authority run by the French government would only be permitted to issue certificates for websites that end in .gouv.fr. To assist the committee in its understanding of this issue, we would appreciate your responses to the following questions by no later than June 23, 2015.

1. Would restricting CAs run by governments to issuing certificates for their own properties within their ccTLDs improve the security and stability of the certificate ecosystem? If so, how? If not, why not?

2. Is it currently technically feasible to restrict government CAs to their own properties in their respective ccTLDs?

   A. If so, how would this change be implemented?
   B. If not, what technological barriers exist? Could these barriers be removed or mitigated?

3. Are there any potential negative effects to such a restriction? If so, please describe them.

4. If the restriction of government CAs to their own properties in their respective ccTLDs would not improve the security and stability of the certificate ecosystem, are there policies or technologies that would? If so, please describe them.

If you have any questions regarding this request, please contact Jessica Wilkerson of the committee staff at (202) 225-2927.

Sincerely,

Fred Upton
Chairman

Tim Murphy
Chairman
Subcommittee on Oversight
and Investigations

Greg Walden
Chairman
Subcommittee on Communications
and Technology

Michael C. Burgess, M.D.
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade

cc: The Honorable Frank Pallone, Jr., Ranking Member

The Honorable Diana DeGette, Ranking Member
Subcommittee on Oversight and Investigations

The Honorable Anna G. Eshoo, Ranking Member
Subcommittee on Communications and Technology

The Honorable Jan Schakowsky, Ranking Member
Subcommittee on Commerce, Manufacturing, and Trade