

Grazyna Piesiewicz-Stepniewska
Directorate-General for Communications Networks, Content and Technology
European Commission
1049 Bruxelles/Brussel
Belgium

14 April 2021

Dear Ms Piesiewicz-Stepniewska,

In 2019, 84% of all European individuals between the ages of 16 to 74 regularly used the internet.¹ For any of those individuals to be able to visit a webpage, an internet certificate or ‘badge of validity’ is required for the site to be accessible and secure for the general public. Internet certificates are also needed for mail servers, database connections and much more. The rules and policies needed to issue and assess internet certificates are regulated by the CA/B forum, a governance body made up of the most active certification authorities and vendors of Internet browser software. The forum is based in the United States.

The forum has two categories of members: Certificate Authorities (the certificate suppliers) and Certificate Consumer Members (the browser vendors). Within the certificate supplier’s category of the forum, there are eighteen European organisations out of the total forty-eight members. The majority of the certificate market is controlled by three suppliers within the forum, of which none are based in the European Union. Within the browser vendor category, there are 8 members and no European representation. For the CA/B Forum to pass regulations, both categories separately vote and both categories require a positive result in order for these rules to come into force.

It is worth highlighting these formalities in order to demonstrate that the governance surrounding the issuing and validity of internet certificates is largely **out of European hands**. This has several negative consequences, with the most notable being the increasingly impromptu decision making of a unified body of American browser software vendors. Stringent rulings, such as lowering the duration of all certificate’s validity to a period of one year or increasing the level of auditing required to issue a credible certificate, have direct consequences for European internet usage.

The procurement and technical capacity needed to attain certificates is **time-consuming and costly**, especially for organisations requiring even a medium-sized online presence. This is not restricted to companies and business, but also the public sector, schools and Universities. When certificates are deemed ineligible or unfit for use, they are now revoked within five days. This puts organisations under **tremendous strain** to replace unfit certificates in a short time period. Whilst this short period is justified for a serious error that directly impacts security, the same short period is also applied for minor errors that do not immediately impact security. On top of this, there is a security risk also if certificates are revoked too fast, without a valid security-related reason, as this may leave sites unreachable or unsecured. The smallest of details can now constitute a mistake in issuing a certificate; for example, a misplaced hyphen in the address to where the certificate is issued could be deemed a transgression (e.g., Noord Holland instead of Noord-Holland). **These factors have created a punitive environment where end-users such as companies and institutions need to replace all of their certificates within 5 days and therefore are often the recipients of the costs for these changes in certificate regulation, to which they have no influence.**

¹ <https://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&language=en&pcode=tin00091&plugin=1>

This does not mean that the European Union is unaware of the need to ensure internet certificates in Europe. The eIDAS regulation has created the basis of rules for electronic identification and trust services for electronic transactions within the internal market, which has resulted in increased technical standards for the public and private sector. However, the unique global quality of this governance dynamic lies out of its scope.

The European Union has traditionally been committed to multilateral systems and institutions, however in a scenario where a block of actors can form rules which affect users globally, then a change in position should take place. The spontaneous re-writing of certificate regulation according to the preferences of CA/B browser vendors is largely out of European control. As a result, in this aspect of the Internet, European digital sovereignty is under threat. GÉANT therefore asks for the European Commission to begin investigating how to best rectify this balance **through constructive and transparent dialogue** with other global institutions, as it is within the interest of all regions. We see this as most of all an **opportunity** to assure that Europe takes a global lead in this sector whilst guarding its digital sovereignty. GÉANT and its NREN Membership have considerable expertise in this field and are open to contributing further to this discussion where possible.

Yours Sincerely,



Erik Huizer,
GÉANT Association CEO



Andreas Dudler,
Chairman of the GÉANT Association