Russia creates its own TLS certificate authority to bypass sanctions

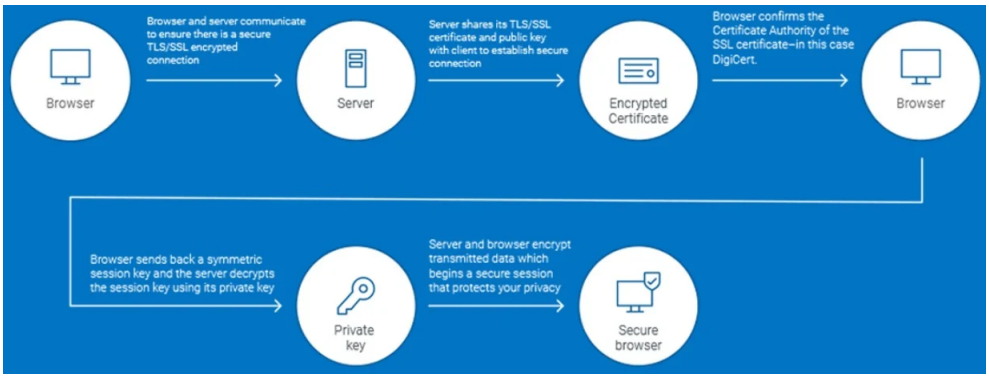
By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)**

March 10, 2022 11:06 AM 3

Russia has created its own trusted TLS certificate authority (CA) to solve website access problems that have been piling up after sanctions prevent certificate renewals.

The sanctions imposed by western companies and governments are preventing Russian sites from renewing existing TLS certificates, causing browsers to block access to sites with expired certificates.

TLS certificates help the web browser confirm that a domain belongs to a verified entity and that the exchange of information between the user and the server is encrypted.



How TLS certificates work *(Digicert)*

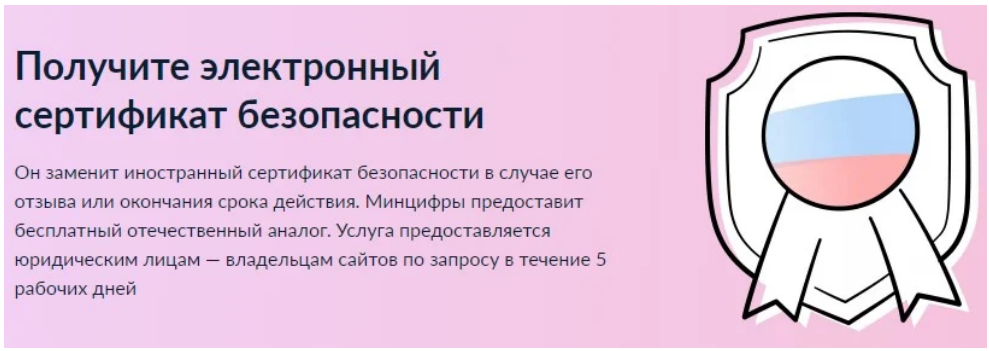
Signing authorities based on countries that have imposed sanctions on Russia can no longer accept payments for their services, leaving many sites with no practical means to renew expiring certificates.

After a certificate expires, web browsers such as Google Chrome, Safari, Microsoft Edge, and Mozilla Firefox will display full-page warnings that the pages are insecure, which can drive many users away from the site.

A domestic authority

The Russian state has envisioned a solution (https://www.gosuslugi.ru/tls) in a domestic certificate authority for the independent issuing and renewal of TLS certificates.

"It will replace the foreign security certificate if it is revoked or expires. The Ministry of Digital Development will provide a free domestic analogue. The service is provided to legal entities – site owners upon request within 5 working days," explains the Russian public services portal, Gosuslugi (translated).

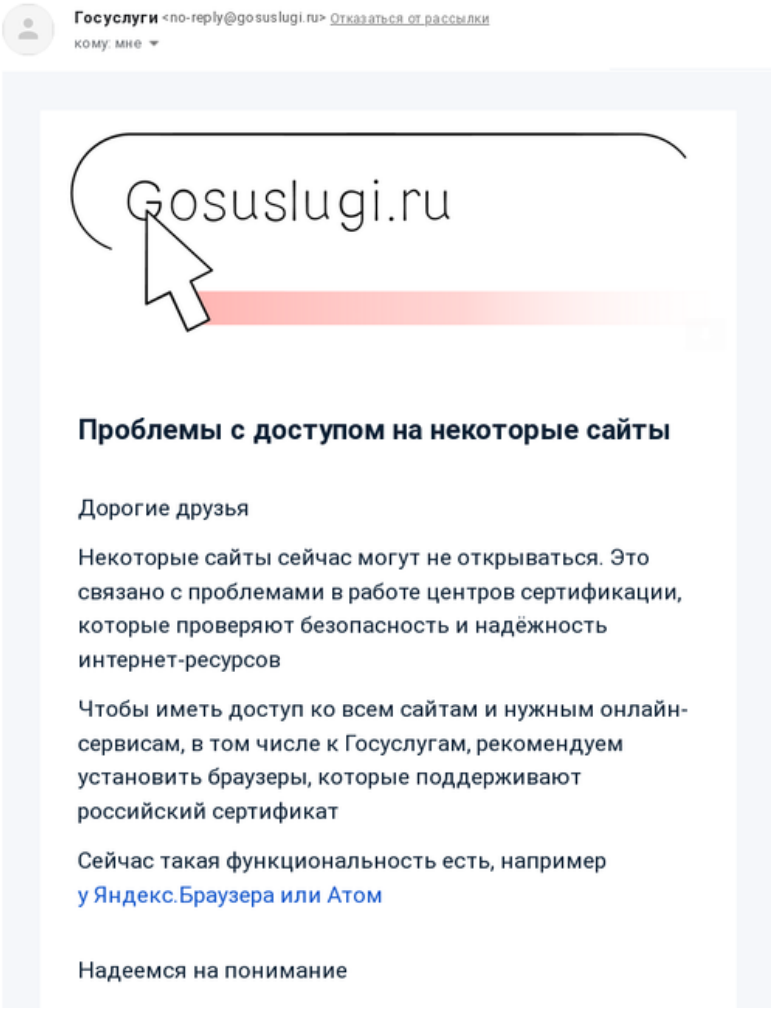


Announcing the availability of domestic certificates *(Gosuslugi)*

However, for new Certificate Authorities (CA) to be trusted by web browsers, they first needed to be vetted by various companies, which can take a long time.

Currently, the only web browsers that recognize Russia's new CA as trustworthy are the Russia-based Yandex browser and Atom products, so Russian users are told to use these instead of Chrome, Firefox, Edge, etc.

Sites that have already received and are currently using these state-supplied certificates include Sberbank, VTB, and the Russian Central Bank.



Notice sent to owners of eligible websites

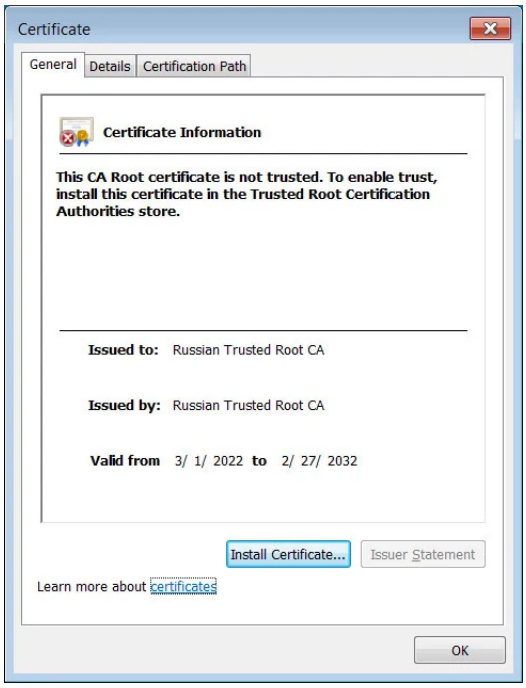
Russian media has also been circulating a list with 198 domains (https://www.documentcloud.org/documents/21408455-tls_list2?responsive=1&title=1) that reportedly received a notice to use the domestic TLS certificate, but for now, its use hasn't been made mandatory (https://www.interfax.ru/russia/827230).

A problematic proposal

Users of other browsers like Chrome or Firefox can manually add the new Russian root certificate to continue using Russian sites that feature the state-issued certificate.

However, this raises the concerns that Russia could abuse their CA root certificate (http://bugzilla.mozilla.org/show_bug.cgi?id=1758773) to perform HTTPS traffic interception and man-in-the-middle attacks.

This abuse would ultimately lead leading to the new root certificate being added to the certificate revocation list (CRL).



Russian Trusted Root CA certificate

Source: BleepingComputer

This would render these domestic certificates invalid, and Chrome, Edge, and Firefox would block access to any websites using them.

Certificate authorities are supposed to be universally trusted. However, as Russia is not currently enjoying any level of trust, it is unlikely for the major browser vendors to add them to their root certificate stores.

Russia has taken some drastic measures (https://www.bleepingcomputer.com/news/government/piracy-ok-russia-to-ease-software-licensing-rules-after-sanctions/) to lessen the impact of western sanctions on its economy. Many have presumed that the time to cut ties with the global internet and push its netizens to the "Runet" has come.

In response to these rumors, the Russian Ministry for Digital Technologies flatly denied (https://interfax.com/newsroom/top-stories/75916/) that there's a plan to switch off the internet from inside in a statement shared with local news outlets.