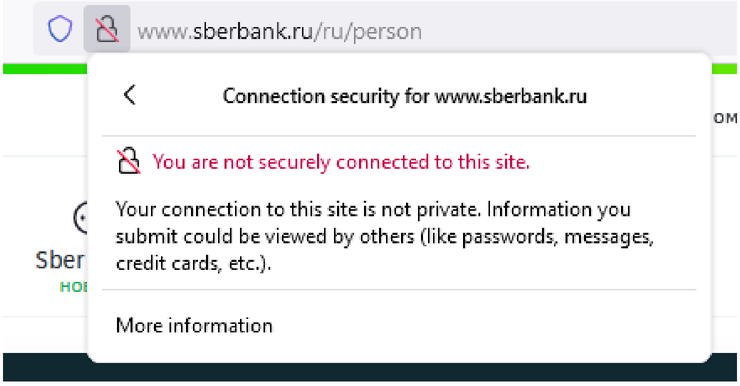
Parallels between eIDAS and actions from the Russian government?

The Digital Identity Regulation (eIDAS) is currently being negotiated in trilogues. **Unfortunately, Article 45(2)** in the original Commission wording would make it much easier for governments to spy on their citizens and intercept web traffic unless policymakers fix a critical article (45.2) in the text during the trilogues. **And to see what kind of cybersecurity risk the law would create, you need to look at what's happening in Russia right now.** A recent move by the digital ministry in response to international sanctions could make the Russian people more vulnerable to cyberattacks and snooping from their government.

If you open the website of Russia's biggest bank Sberbank on your laptop, two things are worth paying attention to.

On the left of the URL bar, for some users (likely because of a gradual rollout strategy on the part of Russia), the browser might warn you that the connection is not secure. If you click the warning sign, you're advised not to enter sensitive information on the website because attackers could steal it.

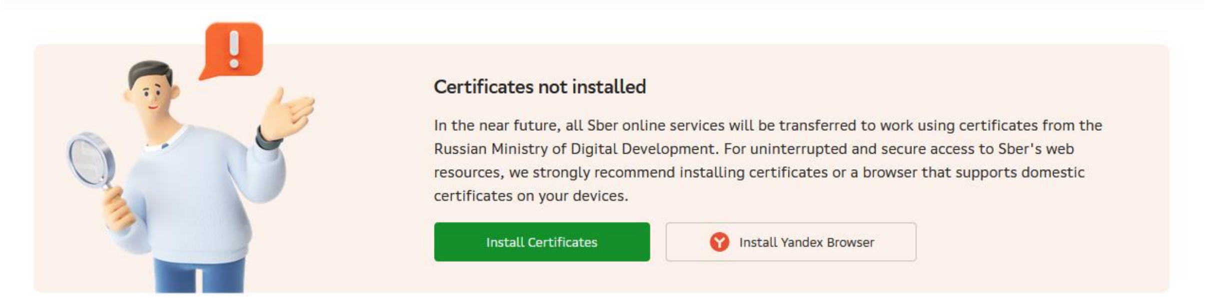


Connection security for www.sberbank.ru

You are not securely connected to this site.

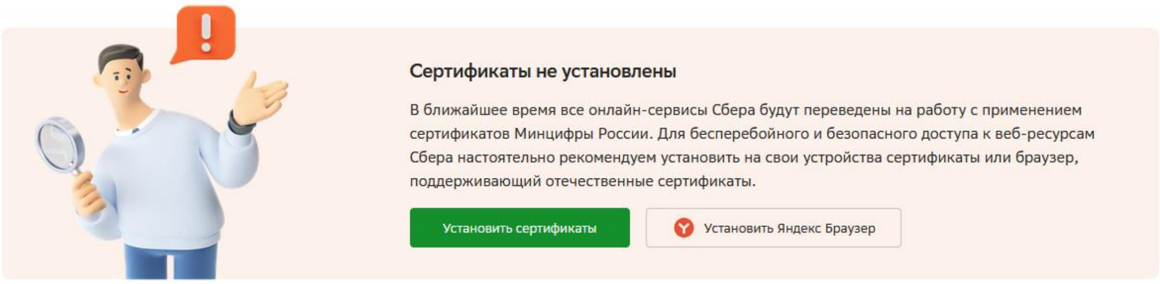
Your connection to this site is not private. Information you submit could be viewed by others (like passwords, messages, credit cards, etc.).

There is also a message from Sberbank in the middle of the web page, asking you to "install a certificate" from the Russian Ministry of Digital Development (screenshot below, original and translated) if you wish to keep accessing Sberbank in the future.



Certificates not installed

In the near future, all Sber online services will be transferred to work using certificates from the Russian Ministry of Digital Development. For uninterrupted and secure access to Sber's web resources, we strongly recommend installing certificates or a browser that supports domestic certificates on your devices.



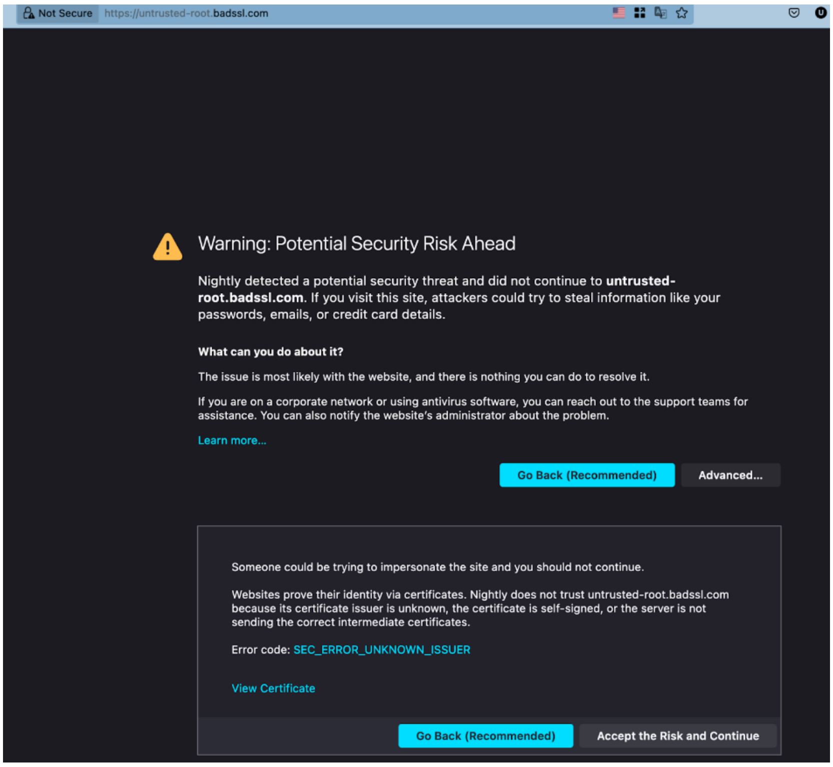
Сертификаты не установлены

В ближайшее время все онлайн-сервисы Сбера будут переведены на работу с применением сертификатов Минцифры России. Для бесперебойного и безопасного доступа к веб-ресурсам Сбера настоятельно рекомендуем установить на свои устройства сертификаты или браузер, поддерживающий отечественные сертификаты.

This is not how web security usually works.

Normally, a virtual handshake occurs between the website and your browser when you go to a website. The website presents a certificate to the browser to prove it controls the domain name. If the browser trusts the certificate, the connection is secured.

These certificates are issued by third parties called certificate authorities. Browser makers diligently vet these certificate authorities (CAs) before including them on a list of trusted organisations called a Root Store. Once these CAs are included, it means that as long as they continue to conform to the rules of the root store programs and their certificates pass due diligence security checks, browser makers consider the websites for which these certificates are issued validly protected. If one tries to access a website with a certificate from a CA not in the root store, users receive a strong warning of the risks of accessing such a website.



Warning: Potential Security Risk Ahead

Nightly detected a potential security threat and did not continue to **untrusted-root.badssl.com**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

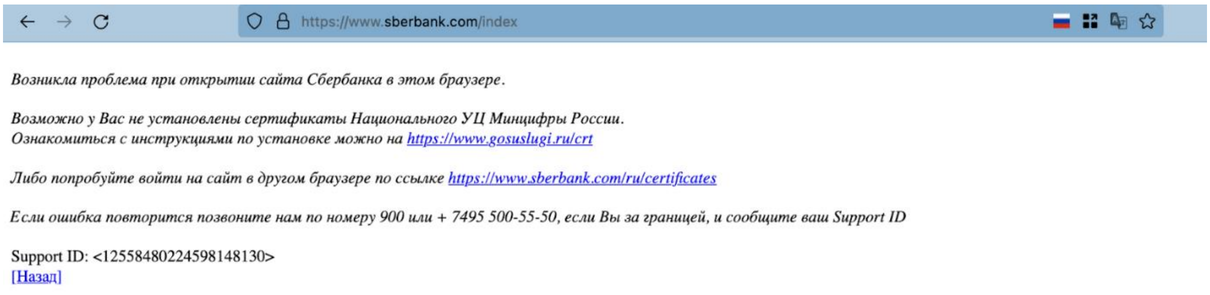
If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Nightly does not trust untrusted-root.badssl.com because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: SEC_ERROR_UNKNOWN_ISSUER

In response to international sanctions because of the war, the Russian government has created a new, state-controlled certificate authority to protect critical infrastructure. This CA's certificates are issued to Russian websites to "replace the foreign security certificate if it is revoked or expires." While Sberbank still has access to the valid certificates from a CA accepted in root store programs (GlobalSign), they seem to be testing and gradually pushing users to install the Russian government root certificate so they can start using the certificates issued by Russian government CA instead. This is leading to the error message below appearing for some users.



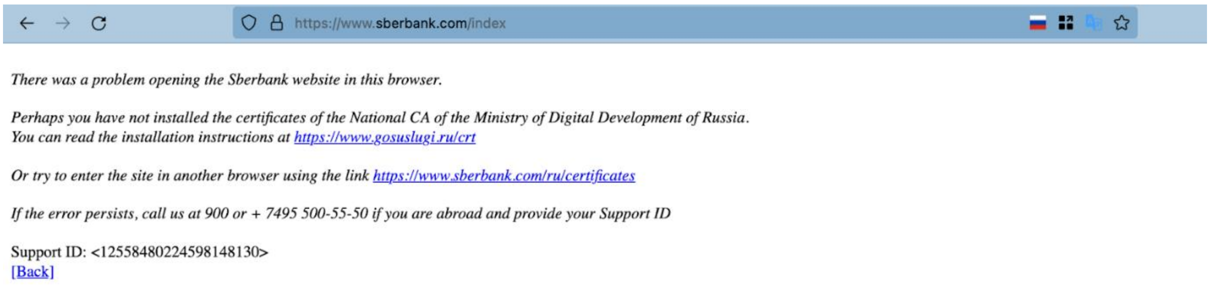
Возникла проблема при открытии сайта Сбербанка в этом браузере.

Возможно у Вас не установлены сертификаты Национального УЦ Минцифры России.
Ознакомиться с инструкциями по установке можно на https://www.gosuslugi.ru/crt

Либо попробуйте войти на сайт в другом браузере по ссылке https://www.sberbank.com/ru/certificates

Если ошибка повторится позвоните нам по номеру 900 или + 7495 500-55-50, если Вы за границей, и сообщите ваш Support ID

Support ID: <12558480224598148130>
[Назад]



There was a problem opening the Sberbank website in this browser.

Perhaps you have not installed the certificates of the National CA of the Ministry of Digital Development of Russia.
You can read the installation instructions at https://www.gosuslugi.ru/crt

Or try to enter the site in another browser using the link https://www.sberbank.com/ru/certificates

If the error persists, call us at 900 or + 7495 500-55-50 if you are abroad and provide your Support ID

Support ID: <12558480224598148130>
[Back]

None of the major browsers (apart from Yandex and Atom in Russia) trust this new government certificate authority and by extension the certificates issued by it. Therefore, the Russian government asks users to bypass the usual system and download the certificate directly onto their devices to avoid triggering a security error.

Downloading this certificate means the government could intercept and modify information, eavesdrop on online activity, and generally monitor activity on the website. So far, there is no evidence that the Russian government CA has used the certificates for this purpose. Still, the government could decide to use them for repressive surveillance in the future, especially once they are widely installed.

As crazy as it may sound, the EU is currently finalising a new law that could make this type of government surveillance a lot easier in the EU. In the new eIDAS Regulation, the European Commission has proposed that some certificate authorities (in the TSP List) should automatically be trusted by browsers, bypassing all the due diligence browser makers conduct to vet them for security practices.

Not fixing Article 45.2 would mean that if an EU government wants to leverage a state-owned certificate authority to spy on citizens, it would not even need to bypass the system by asking users to install the certificate, like the Russian government is trying. It would already have a 'free pass' into our online activity because the browsers are forced to trust their certificate authority by default.

The Digital Identity Regulation is now being discussed in trilogue negotiations. The Parliament has suggested amending the text to mitigate the cybersecurity risk, while the Council left the Commission text unchanged.

The example of Sberbank clarifies what the cybersecurity risks of this legislation could entail if the EU institutions don't get it right, and we believe it is something that the wider public should be wary of. Moreover, given that EU tech legislation is often a source of inspiration for other governments worldwide, the impact could be much more significant than expected.