National Cyber Security Centre
Ministry of Justice and Security

PKIoverheid will stop issuing web certificates

Choose another issuer

Factsheet 2021-03 | version 1.0 | 30 September 2021

Logius has announced that it will stop issuing publicly trusted web server certificates in the PKIoverheid system. If your organisation is currently using such certificates, you will need to find an alternative. Determine which of your certificates are publicly trusted PKIoverheid web server certificates. For each of these certificates, establish the type of certificate with which you wish to replace it. Then select one or more certificate issuers who are able to issue the required certificates. The criteria in this factsheet are a tool to assist you in this process.

Background

The PKIoverheid system is managed by Logius. Various types of digital certificates are issued within this system that are used within as well as to communicate with the Dutch government. Leaf certificates that are issued within this system are also known as PKIoverheid certificates. Logius has outsourced the actual issuance of PKIoverheid certificates, among others to private parties such as Digidentity, KPN and QuoVadis.

On 2 August, Logius announced that it would stop issuing publicly trusted web server certificates in the PKIoverheid system.[1] These certificates will no longer be valid after 4 December 2022. In addition, issuers will stop issuing new certificates of this type several months prior to that date.

Web server certificates are also known as TLS certificates. They are used for various purposes, including to establish secure connections for visitors to public websites (https). Publicly trusted web server certificates may also be used on intranet sites and for so-called machine-to-machine communication. In addition to publicly trusted web server certificates, PKIoverheid also issues various other types of certificates.[2]

What is the matter?

If your organisation currently uses publicly trusted web server certificates issued by PKIoverheid, you will need to find an alternative. The fixed deadline for the expiry of these certificates is 4 December 2022. For a few months after 4 December 2021 – one year prior to the deadline – publicly trusted web server certificates from PKIoverheid will be issued with a shortened lifespan, ensuring that they too expire on the fixed deadline.

Target audience

Holders of publicly trusted web server certificates from PKIoverheid

The following parties have contributed to this factsheet:

- General Intelligence and Security Service (AIVD)/National Communications Security Agency (NBV)
- Public Information and Communications Service
- Logius
- Ministry of the Interior and Kingdom Relations

[1] See https://logius.nl/actueel/pkioverheid-stopt-met-uitgeven-publiek-vertrouwde-webserver-ssltls-certificaten (only in Dutch).

[2] Also see https://logius.nl/diensten/pkioverheid (only in Dutch).

What does NCSC-NL recommend?

NCSC-NL recommends that you determine which of your certificates are publicly trusted web server certificates issued by PKIoverheid, and that you prepare for their replacement.

Looking up certificates in CT logs

So-called Certificate Transparency logs allow you to request an overview of the publicly trusted web server certificates that have been issued for a domain name. In this example, we use 'example.nl' instead of your domain name.

1. Go to https://crt.sh and click on 'Advanced...'.
2. Enter '%.example.nl' as a search term and enable 'Exclude expired certificates'. Click 'Search'.
3. You will be shown an overview of all publicly trusted web server certificates that are currently valid for your domain name and subdomains.
4. If a certificate displays one of these values in the Issuer Name field, it is a PKIoverheid certificate:

- C=NL, O=Digidentity B.V., CN=Digidentity PKIoverheid Server CA 2020
- C=NL, O=KPN B.V., CN=KPN PKIoverheid Server CA 2020
- C=NL, O=QuoVadis Trustlink B.V., CN=QuoVadis PKIoverheid Server CA 2020

Publicly trusted web server certificates issued by PKIoverheid can be identified by verifying whether they can be traced back to the root certificate "Staat der Nederlanden Domein Server CA 2020". NCSC-NL recommends keeping records of your certificates and where you use them. You should be able to retrieve the required information from these records.[3] For a full overview, you can also consult the Certificate Transparency logs (see the section "Looking up certificates in CT logs").

For each of these certificates, establish the type of certificate with which you wish to replace it. The section "What type of certificate do I need?" will assist you in this process.

Next, select one or more certificate issuers who are able to issue the required certificates. Consult the section "Key elements to keep in mind when selecting a certificate issuer" for more information on this subject.

In general, it is recommended that you conduct a risk analysis for the selection of security products and providers. When purchasing a certificate, certain aspects will already be set in stone or will follow from requirements established on the client side of the connection. Occasionally, you may need to conduct a risk analysis yourself when selecting a type of certificate or issuer – this will be outlined in the text.

What type of certificate do I need?

In functional terms, web server certificates differ from one another in three ways: the degree of verification upon issuance, the way in which the domain name is listed, and the root certificate under which it was issued. For each of these aspects, determine which requirements your future certificates should meet.

[3] Consult the NCSC-NL factsheet 'Secure management of digital certificates' for more recommendations on certificate management: https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-veilig-beheer-van-digitale-certificaten (only in Dutch).

Please note that these recommendations only apply to purchasing web server certificates. PKIoverheid will only stop issuing publicly trusted web server certificates. If you have also purchased other types of certificates from PKIoverheid, you will be able to continue to do so. You do not need to find a new issuer for these other certificates.

Verification: DV, OV, EV, QWAC

A DV (Domain Validation) certificate is sufficient for public websites and for most other web server certificate applications. In the case of DV certificates, the issuer will verify the listed domain name but not the applicant's identity. For example, if you are requesting a DV certificate for ncsc.nl, then the issuer will verify that you are the holder of the domain name ncsc.nl, but will not request the name of your organisation or any further proof that you are acting on behalf of this organisation.

Certificates of the Organisation Validation (OV), Extended Validation (EV) and Qualified Website Authentication Certificate (QWAC) type have an increasing level of verification of the applicant's identity. These certificates will likewise list that identity, allowing visitors of a website to request the identity of the owner of the website. In the past, the use of an EV certificate would also result in a so-called 'green bar' in visitors' browsers, but none of the popular browsers still do this. The added value of an OV, EV or QWAC certificate is therefore limited for applications where lower levels, such as DV, are also accepted.

In certain sectors, the use of a certificate with a specific level of verification is mandatory for certain applications. This requirement is a result of sector-specific laws and regulations. NCSC-NL is aware of one instance in which this is the case. Under PSD2 legislation, companies in the financial sector are required to use a QWAC certificate for certain types of machine-to-machine communication.

Certain applications require a certificate to contain an Organisation Identification Number (OIN), which plays a role in automated communication with the government. Digikoppeling is the principal example of this.[4] The OIN is listed on PKIoverheid OV certificates. You will still be able to obtain these types of OV certificates from PKIoverheid after the deadline, under the root certificate 'Staat der Nederlanden Private Root CA - G1'. Go to the Logius website for more information.[5] Given that certificates under this root certificate are not publicly trusted, they cannot be used for public websites.

Domain name listing

Many certificates only list one or two domain names, but it is possible to create a certificate that applies to many more domain names simultaneously. The domain names to which a certificate applies are listed in the Subject Alternative Name field.

It is best to use different certificates for different applications. That way, if something were to go wrong with a given certificate, you would not need to replace it in several other instances as well. However, if a single application involves multiple domain names, these can be covered by the same certificate. Websites are an example of this. If one website can be reached under multiple domain names, then it makes sense to request a certificate for all those domain names at the same time. In the case of several individual

[4] See https://www.logius.nl/diensten/digikoppeling (only in Dutch).

[5] See https://www.logius.nl/diensten/oin (only in Dutch).

websites, use individual certificates – even if these websites all run on the same web server.

In certain applications, it is not known in advance which subdomains will be called up – or you may not want these subdomains to become public.[6] In such cases, you can use a *wildcard certificate*, which is a certificate that applies to all subdomains of a domain simultaneously. The listing will then be '*.example.nl'. Using a wildcard certificate does put you at a slightly higher risk than if you are using a certificate listing all domain names separately. After all, an attacker who has the private key will also be able to use that key to attack other applications with a subdomain of that domain name. Certain certificate issuers do not support wildcard certificates. If you are considering using a wildcard certificate, conduct a risk analysis first.

The root certificate

The root certificate under which a web server certificate was issued determines the trust others will place in the certificate. Whenever client software establishes a connection, it will only accept the server's certificate if it is issued under a root certificate that it trusts.

When we refer to *publicly trusted* web server certificates, we mean certificates issued under a root certificate from the web PKI. The web PKI is a collection of over a hundred root certificates that are trusted by modern browsers and many other types of TLS client software. If your application uses a certificate issued under one of these root certificates, then you can safely assume that modern TLS client software will be able to connect to your server.

The composition of the web PKI may vary slightly between browsers and other TLS client software. As such, it may be the case that a particular browser or type of TLS client software will accept a certificate while another will not. The list of root certificates that a browser or TLS client software accepts is called the _trust store_. If it is critical to you that a broad range of client software types are able to connect to your server without any difficulties, then ask your certificate issuer in which trust stores the relevant certificate is included. An overview of the key trust stores is available on the Logius website.[7]

For internal applications, there is no need to purchase a certificate that was issued within the web PKI. After all, client software can be configured to also accept an internal root certificate. For these types of applications, for example, you will be able to use PKIoverheid web server certificates under the root certificate 'Staat der Nederlanden Private Root CA - G1'. This has a number of advantages, such as a longer validity period for the certificates issued. These types of certificates can be purchased from the PKIoverheid TSPs:[8] Digidentity, KPN and QuoVadis.

Key elements to keep in mind when selecting a certificate issuer

Select a certificate issuer that is able to issue the certificates you need, based on your assessment of the criteria outlined in the previous section. This will most likely still yield hundreds of eligible parties. When conducting a further selection, you should therefore consider which issuer fits with the way your

[6] Publicly trusted web server certificates are included in public Certificate Transparency logs. All domain names for which you have purchased a certificate can therefore also be viewed by third parties.

[7] See https://www.logius.nl/diensten/pkioverheid/hoe-werkt-het/browserondersteuning (only in Dutch).

[8] TSP stands for Trust Service Provider, a party authorised by the holder of a root certificate to issue underlying certificates.

organisation uses certificates. If necessary, carry out a risk analysis to prioritise the various criteria.

Price

Certificates can vary significantly in terms of purchase price – certain issuers may issue a DV certificate for free, whereas a single QWAC certificate may cost hundreds of euros. You should therefore examine what type of certificate matches your application and refrain from purchasing certificates with more stringent verification than is necessary for your application. In addition, you can compare the rates of the various issuers.

Image

A trusted name can contribute to the image of your organisation. This applies to your certificate issuer as well. Although most of your visitors will not check to see who issued your web server certificate, it may nevertheless be important to your organisation not to engage with just any party.

You should similarly consider the country in which the certificate issuer is based. Although it has little impact on the actual level of security in place, it may be reassuring to your visitors that you use a certificate that was issued by a Dutch or European party, for example.

Past experiences

If you have had good experiences with the PKIoverheid TSP (Digidentity, KPN, QuoVadis) that previously issued your publicly trusted web server certificates, contact them. They will most likely be able to provide you with a publicly trusted web server certificate under another root certificate – even after PKIoverheid stops issuing such certificates.

Lead times for certificates

Many certificate issuers conduct the verification for new certificate manually in part. This applies in particular to the more stringent types of verification upon issue, such as for EV and QWAC certificates. This may become an obstacle if you wish to have new certificates issued on very short notice or at unusual times. Ensure that you select an issuer that is able to deliver certificates at the pace and times that fit the requirements of your organisation.

Domain validation procedure

Different certificate issuers will verify the ownership of domains in different ways. This may become a time-consuming job if you purchase many certificates. For that reason, you should pick an issuer that validates domain names in a way that does not burden your administrators to an additional degree, for example, because they previously used this method.

Automation: ACME

More and more certificate issuers are automating the process of domain validation and certificate issuance, particularly when issuing DV certificates. The best-known automation standard is ACME, which was developed and popularised by the certificate issuer Let’s Encrypt. The number of issuers that support ACME is currently still limited, but this number is expected to grow in the years to come. If you purchase a large number of certificates or are interested in automating this process, then you should choose an issuer that already supports automation or at least has plans to do so.

Incident support

Certificates play a key role in generating trust in your ICT. For incidents within your own organisation or at your certificate issuer, it may therefore become necessary to work very closely with your issuer to respond effectively. Ensure that you engage an issuer that is at least as accessible and professional as your own organisation in the event of any security incidents.

A second issuer?

NCSC-NL recommends purchasing a second certificate from another issuer for any critical applications. In the event that one issuer should experience severe security issues, administrators of trust stores may decide to revoke their trust in that issuer. If your primary issuer should unexpectedly be removed from a key trust store, then your critical application can remain available by way of a second certificate. Select an issuer for this second certificate that uses a different root certificate to your primary issuer. A risk analysis will help you determine whether purchasing a second certificate would be of value to your application.

In conclusion

In principle, which certificate issuer you purchase your publicly trusted web server certificates from makes no difference to the security of your connections. The web PKI comprises hundreds of certificate issuers. Each of these issuers has the technical capability to issue publicly trusted web server certificates for your domain name.

If there are weaknesses in the security measures of one of these issuers, an attacker will be able to hack the systems of that issuer to request a certificate for your domain names – for example, this is what happened during the Diginotar crisis in 2011. Whether you are a customer of the attacked issuer is irrelevant with regard to this type of risk.

Publication
National Cyber Security Centre (NCSC)
Postbox 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

September 2021