National Cyber Security Centre
Ministry of Justice and Security

PKIoverheid is changing

Coordinate the necessary changes in your ICT processes

Factsheet FS-2020-05 | version 1.0 | 4 September 2020

In the coming months, changes will take place in the PKIoverheid system, in order to resolve an issue that was discovered in July. In the meantime, the certificate issuers have started replacing PKIoverheid leaf certificates. If your process depends on PKIoverheid leaf certificates that are replaced, your process could come to a standstill or be disrupted. NCSC-NL recommends that you investigate whether changes in your ICT process are necessary, and that you centrally coordinate these changes. The necessary changes will concern the way in which software in your ICT process checks leaf certificates.

Background

Digital certificates are used in many applications as a basis for gaining trust. Examples of such applications are secure connections, digital signatures and encrypted messaging. The authenticity of the certificate that is used is crucial to the security of the application in which it is used.

In practice, digital certificates are usually organised in a Public Key Infrastructure (PKI). Using a PKI, a party can check the authenticity of a leaf certificate that it is offered. A PKI consists of a number of root certificates and agreements on the way in which trust in issued leaf certificates is assigned. PKIs form the basis of applications such as HTTPS, S/MIME and authentication of people.

Every application of leaf certificates based on a PKI uses the same general approach. The holders of root certificates in the PKI appoint authorised certificate issuers[1], and provide them with an intermediate certificate. The certificate issuers issue leaf certificates to certificate holders. They create these leaf certificates using their intermediate certificate. A certificate holder can prove their identity by showing their leaf certificate to a verifying party. The verifying party checks whether the leaf certificate of the certificate holder can be traced back to a root certificate of the PKI. If so, they accept the certificate.

PKIoverheid is a Dutch governmental PKI that is managed by Logius. PKIoverheid contains three root certificates:[2]

- Staat der Nederlanden EV Root CA ('EV root')
- Staat der Nederlanden Root CA G3 ('public root')
- Staat der Nederlanden Private Root CA G1 ('private root')

Target audience

ICT policy advisors who are responsible for processes that use PKIoverheid leaf certificates

The following parties have contributed to this factsheet:

- Information Security Service of Dutch Municipalities
- Logius
- Ministry of the Interior and Kingdom Relations

[1] Another name for these parties is trust service providers (TSPs).

[2] For more information on the root certificates of PKIoverheid, see https://www.logius.nl/english/pkioverheid.

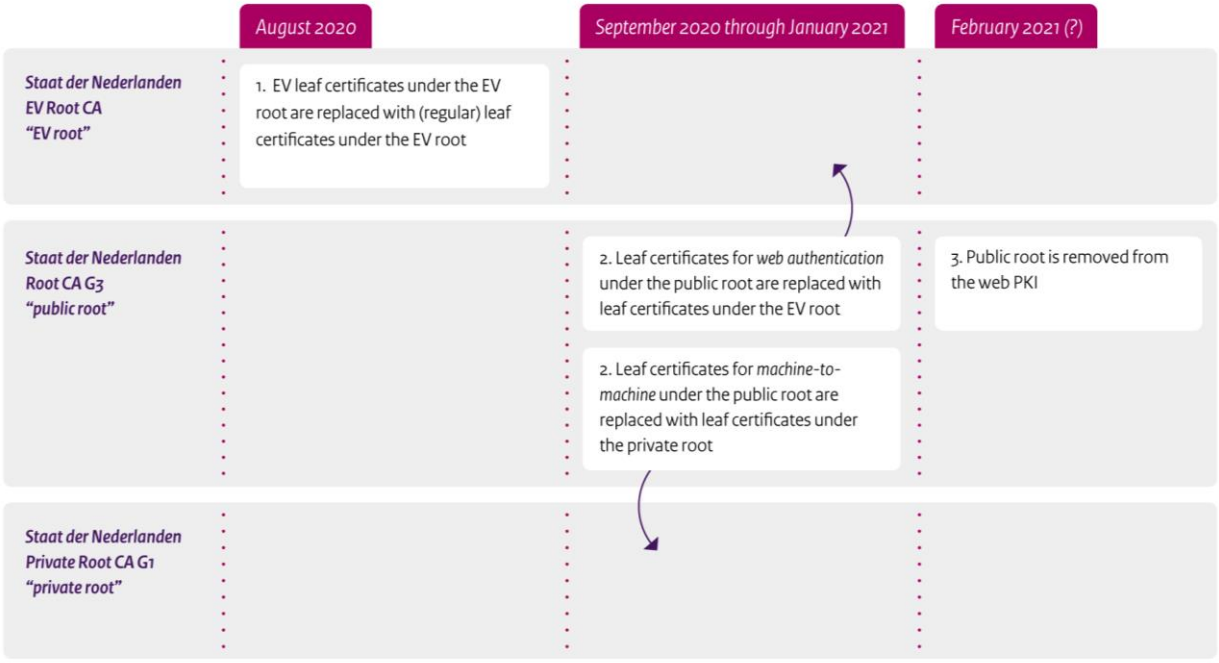

Figure 1: The action plan of Logius

Logius has appointed several certificate issuers for PKIoverheid, both government organisations and commercial certificate providers. Depending on the application, certificate holders can go to one of these issuers to acquire a PKIoverheid leaf certificate.

Every application of leaf certificates has its own rules about which PKI should be used. For example, an application might directly use PKIoverheid. Then, every leaf certificate that is used within this application needs to be traceable to a PKIoverheid root certificate. In other cases, the PKIoverheid root certificates are used together with other root certificates in a larger PKI. Certificate holders then have more options for acquiring a leaf certificate.

Web browsers use a special PKI, the web PKI. This PKI consists of over one hundred root certificates that are trusted by web browsers. Each of the holders of such a root certificate is able to issue leaf certificates that are trusted in every browser for establishing an HTTPS connection. Two of the PKIoverheid root certificates, the public root and the EV root, are part of the web PKI. Leaf certificates that are issued under these root certificates are therefore trusted in all web browsers.

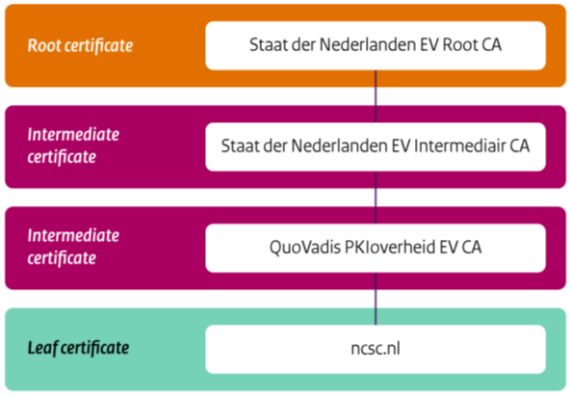

Figure 2: An example of the relation between root, intermediate and leaf certificates

The web PKI is also regularly used in other applications. For example, bookkeeping software might secure the connection to a government service by checking a leaf certificate, which it is able to trace back to a root certificate in the web PKI. This actually constitutes improper use of the web PKI. Browser vendors, the parties that decide who is part of the web PKI, do not take into

account the interests of such alternative use cases in their decisions on the rules and the composition of the web PKI. If the composition of the web PKI suddenly changes, that could lead to disruptions in such applications.

The action plan of Logius in a nutshell[3]

1. Logius and the certificate issuers replace all extended validation (EV) leaf certificates under the EV root by regular (OV) leaf certificates under the same root. This takes place before 4 September 2020.
2. Logius and the certificate issuers replace all leaf certificates under the public root that are suitable for TLS traffic, by leaf certificates under the EV root or the private root. This applies both to leaf certificates that are used for securing web traffic (HTTPS) and machine-to-machine traffic. Leaf certificates that are used for securing web traffic are moved to the EV root, leaf certificates that are only used for machine-to-machine traffic are moved to the private root. Logius has set a timeline up to and including January 2021, where shorter deadlines apply for leaf certificates for securing web traffic.
3. Logius asks the browser vendors to remove the public root from the web PKI. All remaining leaf certificates under the public root are from that point on no longer trusted in web browsers and other applications that use the web PKI. This step is planned for February 2021.

What is the matter?

At the start of July, a problem was discovered in 29 intermediate certificates of PKIoverheid.[4] This worldwide problem was present in almost three hundred intermediate certificates of the web PKI. The mistake allowed holders of PKIoverheid intermediate certificates to issue statements about the validity of each other's intermediate certificates. In the PKIoverheid system, this leads to a limited risk.[5] This mistake did, however, constitute a violation of the baseline requirements. The baseline requirements are the requirements that browser vendors impose upon holders of root certificates of the web PKI. The ultimate sanction when a holder of a root certificate does not remedy a violation of the baseline requirements, is that browser vendors remove the root certificate from the web PKI. If that were to happen with PKIoverheid, visitors of websites that use PKIoverheid leaf certificates would encounter an error message. In other applications that use the web PKI, checking PKIoverheid leaf certificates would also lead to disruptions.

Logius has decided to restructure the PKIoverheid system, in order to resolve the issue with PKIoverheid intermediate certificates. With these changes, Logius ensures that web browsers will continue to trust PKIoverheid leaf certificates. With these changes, Logius also structures the PKIoverheid system in a more future-proof way, to prevent future mistakes from having such a large impact on the system.

In the coming months, Logius and the underlying certificate issuers will issue new intermediate certificates, revoke old

[3] See also (in Dutch) https://logius.nl/actueel/logius-onderzoekt-certificaten-die-niet-voldoen-aan-de-afgesproken-richtlijnen.

[4] See also (in Dutch) https://logius.nl/actueel/logius-onderzoekt-certificaten-die-niet-voldoen-aan-de-afgesproken-richtlijnen.

[5] See also (in Dutch) https://www.ncsc.nl/actueel/nieuws/2020/juli/8/aantal-certificaten-voldoen-niet-aan-de-afgesproken-richtlijnen.

intermediate certificates and replace leaf certificates. In the replacement process, Logius prioritises certificates that are used for websites. The certificate issuers contact their customers, the certificate holders, whenever it is necessary to replace their leaf certificates.

What could happen?

If Logius and the certificate issuers revoke or replace leaf certificates upon which your process depends, your process could come to a standstill or be disrupted. This depends on the way in which verifying parties in your process check leaf certificates. If the way in which parties check leaf certificates cannot handle the changes, verifying parties will conclude that all leaf certificates that they check after the changes are invalid. This could lead to parties being unable to establish secure connections, use digital signatures, or authenticate people. Depending on the nature of your process, such a disruption could lead to major organisational or societal consequences.

Such a disruption can occur in two ways.

If parties in your process check leaf certificates using the web PKI, a disruption might occur when leaf certificates are replaced by leaf certificates outside the web PKI, or when the issuing root certificate is no longer in the web PKI. In the action plan of Logius, this applies to two types of certificates. First, leaf certificates for machine-to-machine traffic under the public root are moved to the private root (step 2). Second, leaf certificates that are not suitable for TLS traffic remain under the public root, while the public root itself is removed from the web PKI (step 3).

If parties in your process check leaf certificates using the issuing root certificate, a disruption might occur when leaf certificates are replaced by leaf certificates under another root certificate. In the action plan of Logius, this applies to two types of certificates. First, leaf certificates for securing web traffic under the public root are moved to the EV root (step 2). Second, leaf certificates for machine-to-machine traffic under the public root are moved to the private root (step 2).

The action plan of Logius contains safeguards to inform certificate holders about the upcoming changes through their certificate issuer. In consultation with the certificate holder, the certificate issuers ensure that their leaf certificates are replaced in time. Depending on the nature of your process, certificate holders might inform verifying parties or the government organisation that is responsible for the ICT process, about the upcoming changes.

Logius does not independently inform verifying parties or the government organisations that are responsible for these ICT processes, neither directly nor through the certificate issuers. They are unable to do so, because no complete list of all these parties exists. It is also impossible to draft such a list based on technical criteria.

What does NCSC-NL recommend?

NCSC-NL recommends that you investigate whether the changes in the PKIoverheid system necessitate changes in your ICT process, and that you centrally coordinate these changes. The necessary changes will concern the way in which software in your ICT process checks leaf certificates.

Make a list of your ICT processes that depend on PKIoverheid leaf certificates. For example, ask the architects of your ICT processes about it. Prioritise processes that use software other than a web browser to check leaf certificates. Securing web traffic is probably the best-known application of PKIoverheid, but only a small part of all PKIoverheid leaf certificates are used for this purpose. When securing web traffic, the required changes are relatively small, and Logius and the certificate issuers direct these changes.

For each of these ICT processes, determine who are the certificate holders, and who are the parties that check leaf certificates. Involve them in performing the necessary

investigations and changes, for example by pointing them to the perspective for action at the end of this factsheet.

Make a list of the software that verifying parties use to check leaf certificates. In some processes, all verifying parties use the same software, in others there are many different options. Take note of different versions of the software that might be in use.

Determine whether changes are to be expected in the nature of the leaf certificates that certificate holders in your process use. There are four possible cases:

- Your process uses EV leaf certificates. These are reissued as regular leaf certificates. This is step 1 of the action plan of Logius.
- Your process uses leaf certificates under the public root that are reissued under a different root certificate, either the EV root or the private root. This is step 2 of the action plan of Logius.
- Your process uses leaf certificates under the public root that are *not* reissued under a different root certificate. Eventually, the public root will be removed from the web PKI. This is step 3 of the action plan of Logius.
- Your process uses leaf certificates under the private root. For these leaf certificates, nothing changes.

Investigate in which way the software of verifying parties checks leaf certificates. Consider whether this check would still succeed after the changes of Logius. For example, if the software checks the root certificate to which the leaf certificate can be traced, then the check will no longer succeed if the leaf certificates are issued under a different root certificate.

Do you expect any consequences from the action plan of Logius for your ICT process, because you need to have the software updated to change the way it checks leaf certificates? Draft an action plan to perform these modifications and inform Logius and NCSC-NL about the expected consequences for your ICT process. This enables these parties to maintain an overview of the expected consequences. They can then also intervene in a timely manner if any disruptions are likely.

Further advice on the use and management of digital certificates is available in the NCSC-NL factsheet 'Secure management of digital certificates'.[6]

[6] See https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-veilig-beheer-van-digitale-certificaten (only in Dutch).

Perspective for action for certificate holders

1. Wait for your certificate issuer to contact you. If your leaf certificates require changes, your certificate issuer will notify you.
2. Do you want to determine whether changes are to be expected? Determine which case applies to you.

- Do you use leaf certificates under the private root? These do not change due to the action plan of Logius.
- Do you use EV leaf certificates? These are replaced by regular leaf certificates under the same root certificate, the EV root.
- Do you use leaf certificates under the public root, and do you buy these from a commercial certificate issuer? Your certificate issuer will contact you to discuss replacement. Leaf certificates that you use for securing web traffic are replaced by leaf certificates under the EV root. Leaf certificates that you use for machine to machine traffic are replaced by leaf certificates under the private root.
- Do you use leaf certificates under the public root, and do you acquire these from a government organisation?[7] Your leaf certificates will not be replaced. Eventually, the corresponding root certificate will be removed from the web PKI.

Perspective for action for parties that check leaf certificates

Determine in which way your software and systems check PKIoverheid leaf certificates, and ensure that this way can handle the changes from the action plan of Logius.

Your software depends on the web PKI. You let external parties decide for you which leaf certificates are trustworthy. This is acceptable in some cases, such as web browsers. The action plan removes one of the PKIoverheid root certificates, the public root, from the web PKI. If certificate holders that you verify keep using leaf certificates under this root certificate, your checks will fail from that moment onward.

Your software contains a configurable list of trusted root certificates. This is a flexible way to arrange leaf certificate checking. Check whether you have configured the right root certificates to handle the changes from the action plan of Logius. In the future, some leaf certificates will be issued under a different root certificate.

Your software contains hard-coded certificate information. This way of checking leaf certificates is not future-proof.[8] Every digital certificate has a lifespan, even root and intermediate certificates. Arrange your system in such a way that the administrator can configure trusted root certificates.

[7] The government organisations that issue PKIoverheid leaf certificates are the Ministry of Defense, the Ministry of Infrastructure and Water Management and the CIBG.

[8] In specific cases, such as mobile apps, this approach is acceptable. The risk of failure or disruption is then managed by installing new software versions very quickly on the devices of all users.

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 2020