Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

# Main changes to PKIoverheid

## 1 Attention: PKIoverheid is changing

With the help of this infographic you can gain insight into the changes taking place within the PKIoverheid infrastructure. Investigate the situation yourself (with your technical colleagues or supplier). This infographic is a simplified representation, not all technical aspects and details are covered. No rights can be derived from this infographic.

## 2 Short overview of changes

A replacement plan has been drawn up to restore all certificates to international standards. We have summarised this plan in this infographic.

Date: October 5 2020
Version 1.1 - EN

**Make sure you are viewing the latest version**

https://logius.nl/diensten/pkioverheid/infographic

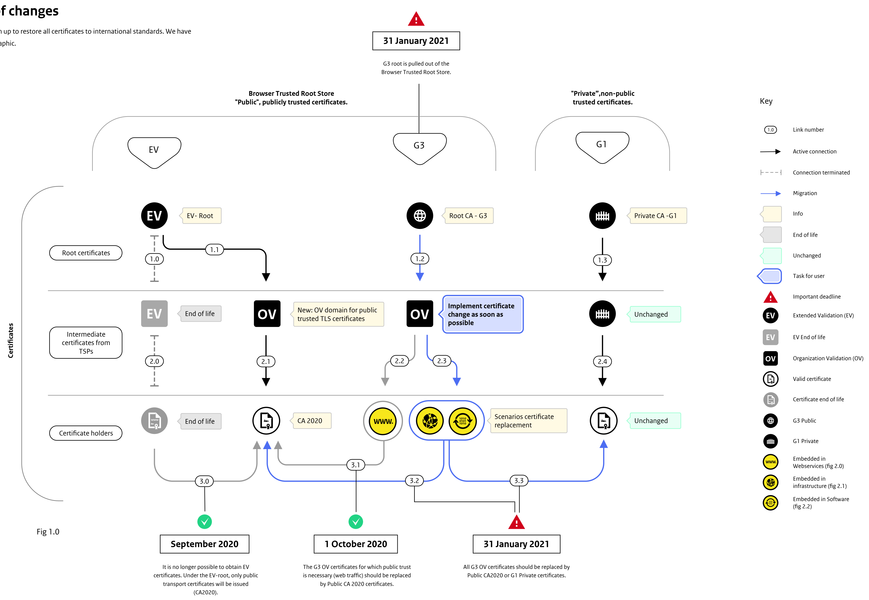


Fig 1.0

## 3 Scenarios for certificate replacement

Below are three common locations in digital services where certificates are used. Each location is circled where certificates may need to be replaced. Investigate yourself (with your technical colleagues or supplier) how the situation actually is.


Fig 2.0

### Embedded in Webservices

This is a mixed use case. Certificates used for machine-to-machine traffic (M2M) and Web services must be separated from each other. Please contact your TSP trust service provider for more information. Examples: SAML, Apps, Websites, etc.


Fig 2.1

### Embedded in infrastructure

This is mainly an infrastructure chain with many places where the certificate is used by different parties, not agile enough when it comes to replacing certificates. Examples: (reverse) proxies, load-balancers, certificate pinning, etc.


Fig 2.2

### Embedded in software

Software settings must be adjusted to make the certificate work
Examples: SBR, etc.

## 4 Frequently asked questions

On our website (logius.nl) we collect answers to frequently asked questions. That page is regularly updated. If your question is not there, in most cases it is best to contact your certificate issuer (the party from which you purchased your certificate). They will be able to help you best. Also point your technical colleagues to the fact sheet of the National Cyber Security Centre (NCSC).

### logius.nl

https://logius.nl/diensten/pkioverheid/pkioverheid-update/certificaat-vervangingsplan-veelgestelde-vragen

### ncsc.nl

https://www.ncsc.nl/documenten/factsheets/2020/september/4/factsheet-pkioverheid-verandert

## 5 Glossary

In the overview below we explain frequently used terms. The explanation can help you to have a discussion within your organisation about the necessary certificate replacement.

**Public Key Infrastructure (PKI)**
A Public Key Infrastructure (PKI) is a set of roles, policies, hardware, software and procedures required to create, manage, distribute, use, store and revoke digital certificates and to manage public key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential e-mail.

**Certificate Authority (CA)**
In cryptography, a certification authority or a certification body (CA) is an entity issuing digital certificates. A certificate provides very strong evidence that a person or organisation is who they claim to be. This is done by means of keys. This makes it possible for others (dependent parties) to rely on signatures or claims about the private key corresponding to the certified public key. A CA ensures that the owner of the certificate and, for example, an applicant for a digital service can trust each other.

**Trust Service Provider (TSP)**
A TSP is an organisation or legal entity that provides one or more trust services as a qualified or non-qualified trust service provider. They (may) act as a CA under the eIDAS Regulation as issued by the European Commission.

**Certificaathouders**
A certificate holder shall enter into an agreement with a telecommunications service provider on behalf of one or more certificate holders.

**Transport Layer Security (TLS-connections)**
Transport Layer Security (TSL) and its predecessor Secure Sockets Layer (SSL) are encryption protocols that secure communication between computers (e.g. on the Internet). TLS is mainly used in situations where it is necessary to verify that one is indeed connected to the desired server. This is particularly important in banking applications (internet banking) or communication with the government, as financial interests are often at stake, or personal or otherwise confidential information is exchanged.

**Extended Validation (EV)**
Extended validation certificates are designed to be "one step above" the public transport certificates (see below). Issuance of EV certificates must comply with strict international standards regarding identity validation (e.g. the information contained in an EV certificate). Although in theory this gives a reliable party more information about the identity of the website operator, in practice it is very difficult to do so. The special UI treatment of EV PKI certificates (the so-called "green bar") has therefore been discontinued by major browser suppliers in 2019. For the rest, with the exception of identity information, an EV certificate is identical to an OV certificate.

**Organization Validation (OV)**
Similar to EV certificates, public transport certificates are intended to provide a reliable party with more information about a website or server operator. Although there are a number of basic industry requirements, there is a much wider range of identity information in a certificate and the level of validation by a TSP/CA. For example, the level of validation required for PKI Overheid OV certificates is in some respects close to the EV standards.

**Browser Root Stores**
A rootstore shows which certificates web browsers trust in internet traffic. A visit to a website that does not have a valid certificate, for example, results in an error message on the screen. A root store can be maintained by a large software supplier (such as a browser or OS supplier such as Microsoft, Google or Apple) or defined by a server administrator. In the first case, a CA can apply to be included in a root store (which usually has admission requirements). In the context of this fact sheet, the focus is on the browser-related variant.

**G1 Private (Staat der Nederlanden Private Root CA – G1)**
A Root CA / hierarchy created by Logius in 2014 which, by design, is not included in a public root store. This is the first generation of certificates of this type (hence the G1 appendix). Although the PKI government regulations and supervision are fully in force, not all requirements of the G3 or EV certificates apply. There is therefore more room for specific cases of government use that conflict with the requirements of the browser (e.g. deadlines for the replacement of certificates or the lifetime of certificates).

**G3 (3rd generation)**
The third iteration of publicly trusted PKI government certificates. Introduced in 2014, in active use since 2018. As a public trusted hierarchy, it was the default choice of many subscribers, even though public trust was not necessarily necessary (see Private Root). The issuance of TLS (public transport) certificates is currently being phased out.