FAQ wijziging PKIoverheid en BCT

Deze notitie geeft een toelichting op een belangrijke voorgenomen wijziging van PKIoverheid en de impact daarvan op het BCT stelsel. De doelgroep zijn fabrikanten van BCT's en ontwikkelaars van software die bestanden uit BCT's verwerken.

Achtergrond en afbakening

Begin juli 2020 werd gesignaleerd dat bijna 300 publiek vertrouwde CA certificaten niet voldoen aan de eisen die aan publiek vertrouwde certificaten worden gesteld door het CA/Browser Forum. Dit heeft geleid tot een ingrijpende wijziging van PKIoverheid die uitgebreid is toegelicht in de NCSC Factsheet PKIoverheid verandert. Deze verandering is hieronder samengevat en beperkt tot de zaken die voor het BCT stelsel relevant zijn.

Samenvatting wijziging

Het doel van de wijziging is om het vertrouwen in PKIoverheid te behouden en tegelijkertijd de impact voor alle uitgegeven certificaten en passen zoveel mogelijk te beperken en vroegtijdige vervanging van passen te voorkomen. In de BCT context is alleen de volgende stap relevant:

- Logius zal verzoeken om de G3 root uit de diverse trust stores van o.a. Microsoft, Apple, Google en Mozilla te verwijderen danwel de G3 root niet meer automatisch te vertrouwen voor serverauthenticatie. Dit is naar verwachting in januari of februari 2021 en het precieze moment zal afhankelijk zijn van update mechanismes van de diverse leveranciers. Op dat moment zijn er alleen nog geldige certificaten van passen aanwezig onder de G3 root.

Wat betekent dit voor u?

In de CA certificaten -waaronder het Ministerie van Infrastructuur en Waterstaat certificaten uitgeeft voor boordcomputerkaarten en systeemkaarten- verandert niets. De enige wijziging is dat het stamcertificaat (de 'Staat der Nederlanden Root CA - G3') niet meer automatische geïnstalleerd zal zijn -of vertrouwd zal zijn voor serverauthenticatie- in de gangbare operating systemen en browsers. Het stamcertificaat zelf wijzigt niet.

In de software van boordcomputers zijn alle G3 CA certificaten reeds opgenomen bij de overgang van G2 naar G3 in maart 2020. Hier is dus geen enkele aanpassing nodig.

Voor software die BCT bestanden verwerkt -voor toezicht of administratieve doeleinden- dienen de leveranciers van deze software een analyse uit te voeren of hun software bij controle van de handtekeningen onder de certificaten en bestanden gebruik maakt van de CA certificaten die standaard aanwezig zijn in de Trust Store van het gebruikte operating systeem en of daarbij het vertrouwen voor serverauthenticatie nodig is. Dat laatste zou niet het geval zou mogen zijn aangezien er geen geldige servercertificaten meer zullen zijn op het moment van de wijziging. Als dat wel het geval is, zal men de klanten instructies moeten geven om vanaf februari 2021 de benodigde CA certificaten zelf te installeren of de vertrouwenseigenschappen van de G3 Root CA aan te passen.

Wat is het effect op de bruikbaarheid van BCT-kaarten?

Er is geen enkel nadelig effect op de bruikbaarheid van BCT-kaarten binnen het BCT stelsel.

Er is geen enkele technische wijziging in de certificaten zelf, alleen in de manier waarop het stamcertificaat wordt gedistribueerd -of vertrouwd wordt- wijzigt. Waar dit momenteel automatisch aanwezig is in gangbare platforms, zal dat straks een eenmalige installatie of een aanpassing van de vertrouwenseigenschappen vereisen.

De rechtsgeldigheid van gekwalificeerde elektronische handtekeningen gezet met een Chauffeurskaart of Inspectiekaart blijft ongewijzigd. De opname van de 'Staat der Nederlanden Root CA - G3' in Trust Stores staat los van de certificering en registratie van de IenW TSP als gekwalificeerde vertrouwensdienstverlener op de EU Trusted List onder toezicht van Agentschap Telecom.

Waar kan ik de CA certificaten vinden?

Alle CA certificaten die nodig zijn voor controles van certificaten op de diverse BCT-kaarten zijn te vinden op **https://bct.tsp.minienw.nl** onder de kop 'CA Certificaten generatie G3'.

Waar kan ik actuele informatie van Logius vinden?

De actuele status van de wijziging vindt u in de blog van Logius. Logius heeft daarnaast een FAQ gemaakt. De laatste details over de wijziging per browser leverancier staan bij de rubriek Technische Vragen, bij de vraag: *Hoe ziet de terugtrekking van de G3-root uit de trust stores er uit?*

Hoe kunt u zich voorbereiden?

Als leverancier van software die bestanden uit Boordcomputers analyseert (en ook de certificaten controleert die gebruikt zijn voor ondertekening van die bestanden) kunt u zich als volgt voorbereiden op de aanstaande wijziging:

- door te **inventariseren** welke systemen/applicaties nu vertrouwen op de 'Staat der Nederlanden Root CA - G3' en dat vertrouwen baseren op het feit dat dit stamcertificaat 'publiek vertrouwd is' en daarom is opgenomen in de standaard operating systeem software. Op die systemen dient u in februari 2021 mogelijk zelf dit stamcertificaat te installeren.
- **Testen** zoals hieronder is aangegeven.
- Door -indien van toepassing- een wijziging danwel instructie voor uw klanten voor te bereiden voor installatie van de CA certificaten die nodig zijn om certificaten van BCT-kaarten te controleren.

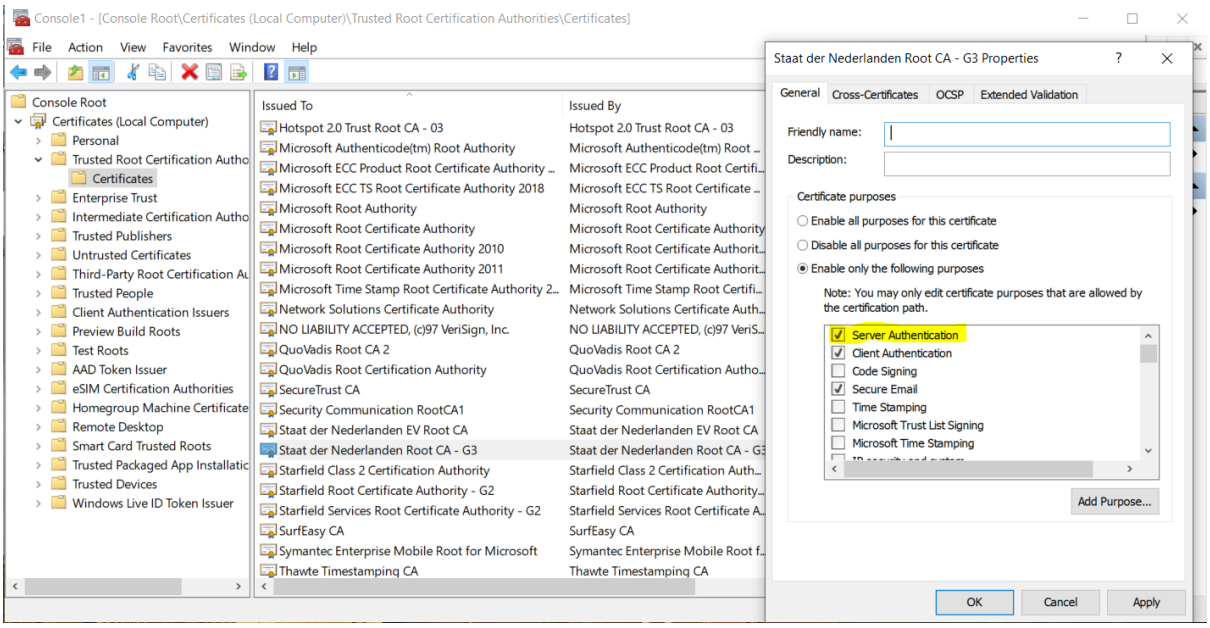
Aanpassingen per leverancier en testmogelijkheden

Microsoft en Mozilla hebben aangegeven de 'Staat der Nederlanden Root CA - G3' in hun software te behouden en alleen het vertrouwen voor serverauthenticatie verwijderen. U kunt dit als volgt simuleren en testen.

Microsoft

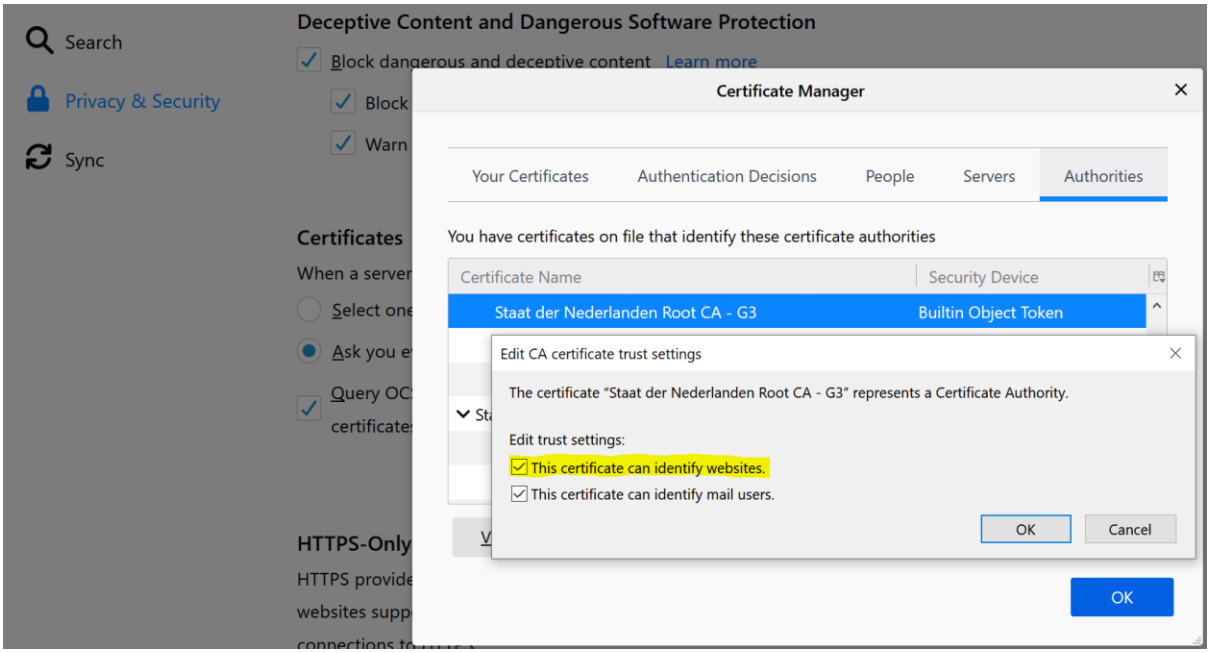
Vink in de Certificate Trust store het vertrouwen voor serverauthenticatie uit.

Hieronder is deze optie gemarkeerd weergegeven in het Management Console met de zogenaamde Certificates snap-in:



Mozilla

Vink in de Certificate Manager de hieronder gemarkeerde optie uit.



Zie voor details van overige software leveranciers de eerdergenoemde FAQ van Logius, bij de rubriek Technische Vragen de vraag *Hoe ziet de terugtrekking van de G3-root uit de trust stores er uit?*