Belastingdienst

Wijziging levensduur PKIo-certificaten

DigiCom-overleg 31-08-2018

Marcel Ermers, procesarchitect

Als ik een PKIO-services servercertificaat wil kopen is deze nog maar twee jaar geldig.

Wat is het alternatief?

De formulering van deze vraag berust op een misvatting…

Agenda

- Waarvoor worden certificaten gebruikt?
- Wat is er veranderd?
- Wat is het alternatief?
- Voor- en nadelen van dat alternatief
- Wat doet de rijksoverheid?

Waarvoor worden certificaten gebruikt?

- Identificatie
- Opzetten veilige verbinding
- Versleutelen van informatie

- Toepassingsgebieden zijn vooral:
  - Software (bijvoorbeeld SBR)
  - Beveiligen websites

Beveiligen websites

- Identificatie op internet:

- Browserfabrikanten stellen steeds strengere eisen aan certificaten die gebruikt worden op internet

2 jaar geldig

Wat is er veranderd?

- Wereldwijd zijn niet alle certificaten even betrouwbaar.
  (PKIo-certificaten zijn wel betrouwbaar)
- Van browserfabrikanten mogen servercertificaten daarom nog maar twee jaar geldig zijn.
- Naar verwachting wordt de levensduur in de toekomst nog korter.
- De looptijd van reeds uitgegeven certificaten verandert NIET.

  →

  géén impact op ontvangen of versturen van berichten
  géén impact op beheren van machtigingsregistraties

Wat is het alternatief?

- Alternatief is een ander type PKIo-services servercertificaat:
  met private root

- Private-root-certificaten kennen een langere levensduur als de nu meestal gebruikte public-root-certificaten

- Private-root-certificaten zijn 3 jaar geldig

certificaat van
Hulpvaardig B.V.

certificaat van
Certificaatleverancier

public root
Staat der Nederlanden

certificaat van
Hulpvaardig B.V.

certificaat van
Certificaatleverancier

private root
Staat der Nederlanden

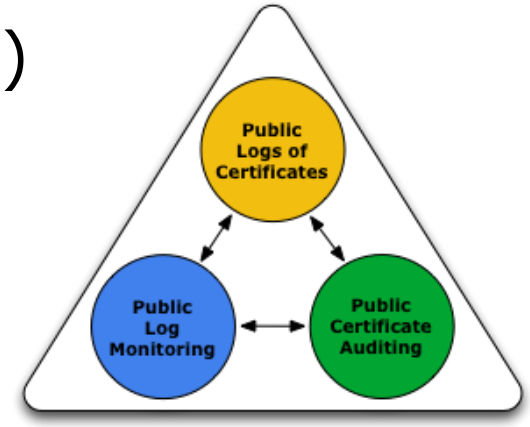
public-root certificaat

Openbare logging public-root-certificaren

- Per 1 mei 2018 is het loggen van publieke PKIoverheid-certificaten verplicht in zogenaamde Certificate Transparency logs.

  https://www.certificate-transparency.org/what-is-ct

- Betreft logging van certificaatbeheer (niet het gebruik)
- In deze openbare logging staan zaken zoals:
  - Identificerend gegevens zoals een KvK-nummer
  - Bedrijfsnaam
  - Plaatsnaam
  - Fully Qualified Domain Name (zoals www.belastingdienst.nl)



Private-root PKIo-certificaten

- Eisen van browserfabrikanten gelden alleen voor certificaten met een public root.
- Private-root PKIo-certificaten zijn verder identiek aan public-root PKIo-certificaten.

  →

  veilig en betrouwbaar
  bruikbaar voor ontvangen of versturen van SBR-berichten
  bruikbaar voor beheren van machtigingsregistraties

- De tot nu toe voor SBR gebruikte PKIo-certificaten met een public root worden in de volksmond wel SBR-certificaten genoemd.

private-root certificaat

Voor- en nadelen private-root PKIo-certificaat

VOORDELEN

- Langere looptijd
- Onafhankelijk van wensen browserfabrikanten
- Inzetbaar voor tenminste system-to-system verkeer via Digipoort, zoals SBR en DigiInkoop

NADELEN

- Minder breed inzetbaar (waar bewust geaccepteerd)
- Niet te gebruiken voor eigen websites certificaathouder (tegelijke inzet voor zowel SBR als websites komt waarschijnlijk niet vaak voor)

Wat doet de rijksoverheid?

- Duidelijk maken dat de SBR-architectuur (conform Digikoppeling) geen onderscheid maakt tussen public en private root.
- Zorgen dat Digipoort private root certificaten accepteert.
- Afstemmen met SBR Banken.
- Afstemmen met certificaatleveranciers:
  - bespreken werkwijze en beschikbaarheid rondom private-root-certificaten
  - private-root-certificaat moet ook beschouwd worden als een “SBR-certificaat”
- Communiceren naar softwareontwikkelaars en aanleveraars.

aandachtspunt:
volgend jaar moeten veel certificaten vervangen worden

Als ik een PKIO-services servercertificaat met public root wil kopen is deze nog maar twee jaar geldig.
Het alternatief is een certificaat met private root.

Vragen?