TLP: ORANJE

# TE014

# Certificaten-wissel G4

| | | | |
|---|---|---|---|
| **Nummer:** | TE014 | **Topic sponsor:** | |
| **Datum:** | 28-10-2026 | **Topic manager:** | Bram van Straalen |
| **Versie:** | 1.0 | **Opsteller(s):** | Bram van Straalen, Joost de Graaff |
| **Status:** | Vastgesteld | | |

| Impact topic | |
|---|---|
| **Segment** | ☒Grote aansluitingen<br>☒Kleine aansluitingen |
| **Product** | ☒Elektriciteit<br>☒Gas |
| **Partijen** | ☒TSB-G<br>☒TSB-E<br>☒GSB<br>☒DSB<br>☒Leverancier (☒ reguliere leverancier / ☒ energiegemeenschap / ☒ actieve afnemer / ☒ aggregator / ☒ peer-2-peer handelaar )<br>☒BRP<br>☒BSP<br>☒CSP<br>☒MV ( / ☐ submeetverantwoordelijke)<br>☐Datagebruiker<br>☒Gegevensuitwisselingsentiteit (GUE)<br>☐Andere: Aangeslotene / datarechthebbende, toezichthouder |
| **Wet- en Regelgeving** | ☐Energiewet<br>☐Energiebesluit en MR-en (ministeriële regelingen)<br>☐Methoden en voorwaarden<br>☐Markt en sub-processen (MSP) (Afsprakenstelsel) |
| **Centrale Impact** | ☒Berichten<br>☐Ketenprocessen |
| **Privacy** | ☐Privacy |
| **Release** | ☒Release afhankelijk<br>☐Release onafhankelijk |

Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

TLP: ORANJE

# Colofon

## Versiebeheer

| Versie | Status | Wijziging | Auteurs | Datum |
|---|---|---|---|---|
| 0.1 | Concept | Initiële versie voor review door werkgroep | Bram van Straalen | 23-03-2026 |
| 0.2 | Concept | Versie ter review door de werkgroep | Bram van Straalen, Joost de Graaff | 11-05-2026 |
| 0.3 | Concept | Versie ter review door de werkgroep | Bram van Straalen, Joost de Graaff | 16-06-2026 |
| 0.6 | Peer Review | Versie ter peer review | Bram van Straalen, Joost de Graaff | 06-07-2026 |
| 0.7 | Peer review | Versie ter controle verwerking peer review | Bram van Straalen, Joost de Graaff | 14-09-2026 |
| 0.9 | Ter vaststelling | Versie ter vaststelling | Bram van Straalen, Joost de Graaff | 05-10-2026 |
| 1.0 | Vastgesteld | Vastgesteld in ALV MFF 28-10-2026 | Bram van Straalen, Joost de Graaff | 28-10-2026 |

## Distributie

| Gremium | Verstuurd (versie/datum) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 0.1 | 0.2 | 0.3 | 0.6 | 0.7 | 0.9 | 1.0 | | | |
| Werkgroep | 23-03-2026 | 11-05-2026 | 16-06-2026 | | | | | | | |
| Markt (peer review) | | | | 07-07-2026 | 14-09-2026 | | | | | |
| BOSO | | | | | | 15-10-2026 | | | | |
| ALV | | | | | | 28-10-2026 | | | | |
| Markt | | | | | | | 29-10-2026 | | | |

Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

# Begrippenlijst

| Begrip | Uitleg |
|---|---|
| BGS | Beheerder Gesloten Systeem |
| BRP | Balanceringsverantwoordelijke (balance responsible party). |
| CA | Certificate Authority.<br>Een certificaatinstantie, zoals DigiCert en KPN, die certificaten uitgeeft. |
| DSB | Distributiesysteembeheerder |
| EAN-13 | Unieke EAN-code van 13 cijfers, behorende bij een marktpartij in een bepaalde marktrol. |
| EDSN | Beheerder van centrale systemen voor de distributiesysteembeheerders en de transmissiesysteembeheerders. |
| COR | Centrale OIN Raadpleegvoorziening. |
| G1 PKIoverheidcertificaat | Een privaat vertrouwd digitaal beveiligingscertificaat (een "digitaal paspoort") dat de identiteit van personen, organisaties of clients / servers garandeert in elektronisch verkeer. Het gebruik hiervan eindigt op 12 november 2028. |
| G4 PKIoverheidcertificaat | Een nieuwe generatie digitale beveiligingscertificaten (een "digitaal paspoort") dat de identiteit van personen, organisaties of clients / servers garandeert in elektronisch verkeer. |
| GUE | Gegevensuitwisselingsentiteit - de rechtspersoon als bedoeld in artikel 4.15, eerste lid van de Energiewet. Het Normo is vanaf 1 januari 2026 de aangewezen gegevensuitwisselingsentiteit binnen de Energiewet. Het Normo zorgt als onafhankelijke autoriteit voor betrouwbare en transparante afspraken in de energiesector, zodat energiedata veilig en efficiënt kan worden ontsloten en uitgewisseld. |
| IISO | Integraal implementatie sturingsoverleg - verantwoordelijk voor het bewaken van de voortgang van de realisatie, uitvoeren van sectortesten, faciliteren van de transitie en communicatie omtrent de marktreleases met alle marktpartijen en de realisatie van sectorbrede IT ontwikkelingen. |
| LV | Leverancier. |
| MFF | Marktfaciliteringsforum - een vereniging waar iedere partij uit de energiebranche lid van kan worden, met als doel mee |



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

| Begrip | Uitleg |
|---|---|
| | te praten en mee te beslissen over afspraken. |
| mTLS | Mutual Transport Layer Security<br>Dit is een cryptografisch protocol om beide partijen (server en client) in een netwerkverbinding te verifiëren met behulp van certificaten. Bij reguliere TLS bewijst alleen de server zijn identiteit aan de client, bij mTLS bewijzen zowel server als client hun identiteit aan elkaar. |
| MV | Meetverantwoordelijke partij. |
| ODA | Overige dienstenaanbieder. |
| OIN | Organisatie Identificatie Nummer.<br>*Bron: Logius (https://oinregister.logius.nl/)* |
| PKI | Public Key Infrastructure.<br>Het is een beveiligingssysteem dat digitale certificaten gebruikt, vaak als "digitaal paspoort", om de identiteit van gebruikers, apparaten en websites te waarborgen via publieke en private sleutels. In Nederland worden specifieke certificaten voor overheidscommunicatie vaak PKIoverheidcertificaten genoemd. |
| PKIoverheid servercertificaat | Daar waar in dit topicdocument gesproken wordt over certificaten, worden zogenaamde servercertificaten bedoeld ten behoeve van een veilige verbinding tussen servers binnen de Nederlandse energiemarkt. |
| Server-tot-serververkeer (S2S) | Server-tot-server (S2S) verkeer betreft directe communicatie tussen twee of meer servers, zonder tussenkomst van een eindgebruiker, client-apparaat of webbrowser. |
| S/MIME | Secure/Multipurpose Internet Mail Extensions<br>Dit is een cryptografische standaard voor het digitaal ondertekenen en versleutelen van e-mailberichten met behulp van certificaten. |
| subOIN | Sub Organisatie Identificatie Nummer.<br>*Bron: Logius (https://oinregister.logius.nl/)* |
| TLS | Transport layer security. Dit is het belangrijkste cryptografische protocol voor het beveiligen van gegevensuitwisseling |



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

| Begrip | Uitleg |
|---|---|
| | via computernetwerken. Hiervoor wordt in de meeste gevallen een digitaal certificaat gebruikt. |
| TSB | Transmissiesysteembeheerder |
| TSP | Trust Service Provider voor de uitgifte van PKIoverheidcertificaten. |



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

# Inhoudsopgave


**1 PROBLEEMDEFINITIE ..... 8**

**2 OVERWEGINGEN ..... 9**

2.1 HUIDIG GEBRUIK G1 PKIOVERHEIDCERTIFICATEN ..... 9
*2.1.1 Wat zijn PKIoverheidcertificaten ..... 9*
*2.1.2 Gebruik EAN-13 in G1 PKIoverheidcertificaten ..... 11*
*2.1.3 Voor welke systemen worden PKIoverheidcertificaten gebruikt ..... 14*
*2.1.4 Aanvraagproces G1 PKIoverheidcertificaten ..... 15*
*2.1.5 Einde gebruik G1 PKIoverheidcertificaten ..... 16*
2.2 G4 PKIOVERHEIDCERTIFICATEN ..... 17
2.3 ORGANISATIE IDENTIFICATIE NUMMER (OIN) ..... 20
2.4 ALTERNATIEVEN VOOR PKIOVERHEIDCERTIFICATEN ..... 22
2.5 IMPLEMENTATIE ..... 24
*2.5.1 Duale periode G1 en G4 ..... 24*
*2.5.2 Testen en testfaciliteiten ..... 25*

**3 GEKOZEN OPLOSSING ..... 26**

3.1 GEBRUIK VAN G4-CERTIFICATEN VOOR CENTRALE SYSTEMEN BEHEERD DOOR EDSN ..... 26
3.2 SCOPE EN TOEPASSING VAN G4-CERTIFICATEN ..... 26
*3.2.1 In scope ..... 26*
*3.2.2 Niet in scope ..... 26*
3.3 AANSCHAF / AANVRAAG VAN G4-CERTIFICATEN ..... 27
*3.3.1 TSP-keuze en bestelproces voor gegevensuitwisseling via EDSN ..... 27*
*3.3.2 Te bestellen certificaten ..... 27*
3.4 INSTALLEREN EN TESTEN VAN DE G4-CERTIFICATEN ..... 28
*3.4.1 Installeren ..... 28*
*3.4.2 Testen ..... 28*
3.5 IDENTIFICEREN VAN MARKTPARTIJEN OP BASIS VAN EAN-13 ..... 28




Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

3.6 PERIODIEK VERNIEUWEN VAN CERTIFICATEN ..... 29

**4 IMPACT OP WET- EN REGELGEVING, AFSPRAKENSTELSEL INCL. MSP ..... 30**

4.1 IMPACT OP LAGERE REGELGEVING ..... 30

*4.1.1 Mogelijke impact op Ministeriële Regelingen (MR) en Algemene Maatregel van Bestuur (AMvB) ..... 30*

*4.1.2 Mogelijke impact op Methoden en voorwaarden ..... 30*

4.2 IMPACT OP SECTORDOCUMENTATIE ..... 30

*4.2.1 MSP Retailprocessen ..... 30*

**5 INVOERINGSSTRATEGIE ..... 31**

5.1 RELEASE-AFHANKELIJK MET DUALE PERIODE ..... 31

*5.1.1 Release-afhankelijk ..... 31*

*5.1.2 Duale periode ..... 31*

5.2 VERANTWOORDELIJKHEDEN ..... 32

*5.2.1 Verantwoordelijkheden systeembeheerders ..... 32*

*5.2.2 Verantwoordelijkheden Het Normo ..... 32*

*5.2.3 Bewaken van de voortgang van de implementatie en transitie, rapporteren aan het IISO daarover en het faciliteren van besluitvorming die nodig is voor implementatie. In geval van knelpunten kunnen in overleg met het IISO aanvullende maatregelen worden vastgesteld. Verantwoordelijkheden marktpartijen ..... 33*

5.3 TRANSITIEMAATREGELEN ..... 33

5.4 VERANTWOORDING ..... 37

**6 TE VERVALLEN TOPICS (/ NEDU-ISSUES) ..... 38**

**7 AANVULLENDE INFORMATIE TEN BEHOEVE VAN LAGERE REGELGEVING ..... 39**

**8 PRIVACY IMPACT & TOETS ..... 40**

**9 SECURITY IMPACT & TOETS ..... 42**



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

# 1 Probleemdefinitie

| Onderdeel | Omschrijving |
|---|---|
| Het probleem / de ontwikkeling / de wet- of regelgeving betreft: | Bij server-tot-serververkeer (S2S) tussen marktpartijen en de centrale systemen wordt gebruik gemaakt van G1 PKIoverheidcertificaten. De geldigheid daarvan eindigt op 12 november 2028 |
| En raakt: | Alle marktpartijen met server-tot-serververkeer (S2S) met de centrale systemen (systeembeheerders en marktdeelnemers (zoals leveranciers, balanceringsverantwoordelijken en meetverantwoordelijken). |
| Als gevolg waarvan: | Er na 12 november 2028 geen geldige certificaten zijn voor het server-tot-serververkeer (S2S) tussen marktpartijen en de centrale systemen. |
| Een goede oplossing moet: | Zorgen voor een tijdige, adequate, veilige en toekomstbestendige vervanging van de bestaande G1 PKIoverheidcertificaten, zodat het server-tot-serververkeer (S2S) tijdens de overgang en daarna ondersteund kunnen blijven worden met veilige certificaten. |
| Of deze doelen worden behaald, kan worden gevalideerd door: | De nieuwe certificaten ondersteunen het server-tot-serververkeer (S2S) en zijn tijdig beschikbaar voor alle betrokken marktpartijen. |
| Opdrachtgever te realiseren oplossing | MFF en Het Normo |
| Probleemeigenaar | De CoP Secure Architecture en Het Normo. |



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

# 2 Overwegingen

## 2.1 Huidig gebruik G1 PKIoverheidcertificaten

### 2.1.1 Wat zijn PKIoverheidcertificaten

In deze paragraaf zijn enkele overwegingen opgenomen die ingaan op de definitie wat PKIoverheidcertificaten zijn en waarvoor ze gebruikt worden binnen de scope van de MFF-processen en de toegang tot de centrale systemen.

1. **Wat zijn digitale certificaten? -** Een digitaal certificaat authentiseert de online identiteit van een persoon of organisatie. Het is daarmee een soort digitaal paspoort van een persoon of organisatie. Digitale certificaten worden uitgegeven door certificeringsinstanties en worden ook gebruikt om gegevens online te versleutelen. Digitale certificaten worden soms ook 'openbare-sleutelcertificaten' of 'identiteitscertificaten' genoemd.

   **Conclusie:** Een digitaal certificaat authentiseert de online identiteit van een persoon of organisatie. Het is daarmee een soort digitaal paspoort van een persoon of organisatie.

2. **Voordelen certificaten -** Het gebruik van certificaten zorgt ervoor dat niemand anders dan de beoogde ontvanger de inhoud kan lezen (vertrouwelijkheid), gecontroleerd wordt dat de inhoud van het bericht na verzending niet is gewijzigd (integriteit/onweerlegbaarheid) en gecontroleerd wordt dat de inhoud van een bepaalde verzender afkomstig is (authenticiteit).

   **Conclusie:** Certificaten zorgen voor vertrouwelijkheid, integriteit en authenticiteit bij de gegevensuitwisseling.

3. **Wat zijn PKIoverheidcertificaten?** - Een PKIoverheidcertificaat is een digitaal certificaat dat wordt gebruikt als ‘digitaal paspoort’ om digitale communicatie met en binnen de Nederlandse overheid veilig en betrouwbaar te maken. Met dit certificaat kan worden vastgesteld welke organisatie of welk systeem communiceert, of de gegevens onderweg niet zijn gewijzigd en of de communicatie is versleuteld. PKIoverheidcertificaten maken onderdeel uit van het landelijke PKIoverheidstelsel en worden gebruikt voor onder andere beveiligde systeem-tot-systeemcommunicatie en het digitaal ondertekenen van gegevens. Het PKIoverheidstelsel wordt beheerd door Logius.



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

**Conclusie:** PKIoverheidcertificaten maken onderdeel uit van het landelijke PKIoverheidstelsel en worden gebruikt voor onder andere beveiligde systeem-tot-systeemcommunicatie en het digitaal ondertekenen van gegevens.

4. **Root certificaat** - De echtheid van een digitaal certificaat wordt afgeleid van het certificaat van de instantie die het certificaat heeft uitgegeven. Dat certificaat wordt een stamcertificaat of 'root certificate' genoemd. Bij een PKIoverheidcertificaat is het stamcertificaat 'Staat der Nederlanden Root CA'. Voor dit certificaat is de Nederlandse overheid verantwoordelijk. Logius is betrokken bij het beheer.

   **Conclusie:** Bij een PKIoverheidcertificaat is het stamcertificaat 'Staat der Nederlanden Root CA'.

5. **Waarvoor worden certificaten gebruikt in de energiesector? -** Binnen de energiesector worden diverse soorten certificaten gebruikt voor de beveiliging van het S2S-verkeer met servers van de centrale systemen (beheerd door de systeembeheerders) om betrouwbare gegevensuitwisseling tussen marktpartijen en de centrale systemen mogelijk te maken.

6. **Certificaten bij door EDSN beheerde systemen -** Bij EDSN worden PKIoverheidcertificaten gebruikt om veilig te communiceren tussen systemen (servers) van marktpartijen en servers (systemen) beheerd door EDSN.

7. **Certificaten bij door TenneT beheerde systemen –** Bij TenneT worden geen PKIoverheidcertificaten gebruikt, maar publiek vertrouwde PKI-certificaten (die niet onder het PKIoverheidstelsel vallen). Vanwege ontwikkelingen in de wereldwijde certificaatketens van deze publiek vertrouwde certificaten, schrijft TenneT vanaf Q2-2026 het gebruik van DigiCert X9-certificaten voor. Deze vallen niet onder het PKIoverheidstelsel en worden dus niet geraakt door de certificatenwissel van G1 naar G4. .

   **Conclusie:** Bij S2S verkeer tussen servers van marktpartijen en servers van de centrale systemen beheerd door EDSN wordt gebruik gemaakt van PKIoverheidcertificaten. TenneT gebruikt andere certificaten (die niet worden geraakt door de G4-migratie)

8. **Welk root certificaat wordt gebruikt voor PKIoverheid in de centrale systemen?-** Binnen de centrale systemen beheerd door de systeembeheerders) wordt gebruikgemaakt van de Staat der Nederlanden Private Root CA – G1. Dit rootcertificaat verloopt per 13-11-2028 en is het hoogste certificaat binnen de private PKIoverheid-structuur. Onder deze root valt de Staat der Nederlanden Private Services CA – G1. Daaronder hebben Trust Service Providers (TSP's), zoals KPN, hun eigen uitgevende certificaatautoriteiten. Deze TSP-CA's geven vervolgens eindcertificaten uit, zoals PKIoverheid PRIVATE SSL servercertificaten, die worden gebruikt voor beveiligde communicatie met centrale systemen,



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

waaronder EDSN. Voor de centrale systemen die worden beheerd door EDSN, wordt momenteel voor veilige gegevensuitwisseling uitsluitend gebruikgemaakt van door TSP KPN uitgegeven certificaten, voor authenticatie bij mTLS-beveiligde SOAP- en API-services.

Voor het G1-certificaat (waarin de EAN-13 is opgenomen) ziet de huidige root chain zoals gebruikt bij EDSN er als volgt uit:

- Staat der Nederlanden Private Root CA - G1
  - Staat der Nederlanden Private Services CA - G1
    - KPN PKIoverheid Private Services CA - G1

### 2.1.2 Gebruik EAN-13 in G1 PKIoverheidcertificaten

In deze paragraaf zijn enkele overwegingen opgenomen die ingaan op het gebruik van de zogenaamde EAN-13 in de G1 PKIoverheidcertificaten.

9. **EAN-13 in serienummer -** KPN biedt op dit moment als enige partij de mogelijkheid om een EAN-13 op te nemen in het zogenaamde serienummer van het certificaat (in het veld 'Subject Serienummer'). De EAN-13 wordt gebruikt om het certificaat te koppelen aan de betreffende organisatie in een specifieke marktrol.
   Bij het S2S verkeer met de servers van de centrale systemen beheerd door EDSN, kan alleen gebruik gemaakt worden van dit type PKIoverheidcertificaten. Daarbij zijn specifieke afspraken gemaakt tussen KPN en EDSN over het valideren van de EAN-13 tijdens het aanvraagproces voor nieuwe / vernieuwde certificaten bij KPN.
   Het PKIoverheidstelsel van Logius staat andere TSP's wel toe om een EAN13-code (of een ander gevalideerd kenmerk) op te nemen in het veld 'Subject Serienummer', echter hiervoor bestaan op dit moment geen afspraken zoals die met KPN zijn gemaakt.

   **Conclusie:** In de PKIoverheidcertificaten die gebruikt worden in het S2S verkeer met de servers van de centrale systemen beheerd door EDSN is het verplicht om de EAN-13 van de organisatie in een specifieke marktrol op te nemen.

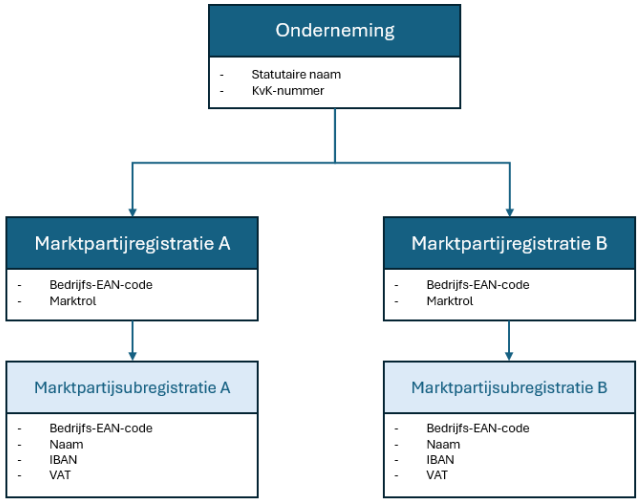
   **Conclusie:** KPN is momenteel de enige organisatie waarmee afspraken bestaan over het uitgeven van certificaten met een EAN-13 in het veld 'subject serienummer'. De EAN-13 wordt gevalideerd door EDSN als onderdeel van het aanvraagproces bij KPN.

10. **Koppeling EAN-13 met Marktpartijenregister –** In de bestaande marktpartijenregistratie (MPR, beheerd door EDSN) wordt een onderneming op het hoogste niveau geïdentificeerd op basis van het KvK-nummer. Onder een onderneming kunnen één of meerdere marktpartijregistraties bestaan, elk behorend bij een specifieke marktrol. Per marktpartij wordt een afzonderlijke EAN-13 vastgelegd. Hierdoor kunnen binnen één onderneming



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

meerdere marktpartijregistraties met verschillende marktrollen en bijbehorende EAN-13 bestaan. Het PKIoverheidcertificaat wordt gevalideerd op onderneming en de EAN-13 van de marktpartijregistratie. Deze EAN-13 van de marktpartijregistratie komt bij de marktrol leverancier overeen met de term “EAN-code leverancier” in het leveranciersregister (zie *MSP Retailprocessen SP0037 Beheer leveranciers- en netbeheerdersregister*).




11. **Marktpartijsubregistratie (administratieve marktpartij) –** Op het onderliggende niveau wordt de marktpartijsubregistratie vastgelegd. De eerste marktpartijsubregistratie heeft dezelfde EAN-13 als de marktpartijregistratie. Voor de marktrollen Systeembeheerder, Leverancier en BRP (gas) is het mogelijk om meerdere marktpartijsubregistraties te registreren met ieder een uniek EAN-13. Deze EAN-13 van de marktpartijsubregistratie komt bij de marktrol leverancier overeen met de term “EAN-code administratieve marktpartij” in het leveranciersregister (zie MSP Retailprocessen SP0037 Beheer leveranciers- en netbeheerdersregister).

    De marktpartijsubregistraties worden niet gebruikt bij de validatie van het certificaat. Daarbij wordt uitsluitend gekeken naar de EAN-13 op het niveau van de marktpartijregistratie.



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

**Conclusie:** in de centrale systemen beheerd door EDSN wordt de EAN-13 code uit het certificaat gebruikt om de marktpartij en de bovenliggende onderneming te identificeren.

12. **Gebruik EAN-13 bij verdere autorisatie in door EDSN beheerde systemen –** De EAN-13 speelt na het identificeren van de marktpartij ook een rol in het verdere autorisatieproces:
    - De EAN-13 van de marktpartij (zoals opgenomen in het certificaat) is gekoppeld aan één specifieke marktrol (bijvoorbeeld BRP, LV en MV) en is bepalend voor de autorisatie van type berichten en verzoeken die nodig zijn voor die marktrol;
    - De onderliggende EAN-13 codes in het MPR (submarktpartijregistraties met dezelfde marktrol) hebben dezelfde autorisatie als de bovenliggende marktpartij;
    - Vervolgens wordt informatie uit de berichten zelf gebruikt om meer gedetailleerde autorisatie- en validatieregels toe te passen. Bijvoorbeeld of de EAN-13 van de (sub)marktpartij in het C-AR de juiste relatie heeft met de aansluiting / het allocatiepunt waarvoor de gegevensuitwisseling is geïnitieerd. Deze gedetailleerde autorisatieregels verschillen per situatie en maken gebruik van verschillende systemen. De uitgevoerde validaties zijn vastgelegd in de Business services voor alle berichten.

**Conclusie:** In de centrale systemen beheerd door EDSN wordt de EAN-13 op basis van de identificatie ook gebruikt voor verdere autorisatie.

13. **Gebruik EAN-13 in door TenneT beheerde systemen –** in de certificaten voor gegevensuitwisseling met TenneT, zijn geen EAN-13 codes opgenomen. Als gevolg daarvan verschilt de wijze van identificatie en autorisatie:
    - Certificaten worden specifiek op EAN geconfigureerd en de koppeling van organisatie/certificaat is administratief ingeregeld in de systemen van TenneT, zonder de aanwezigheid van de EAN-13 in het certificaat;
    - In de berichtuitwisseling met de MMC-Hub wordt verder op basis van de header informatie in het bericht autorisaties uitgevoerd (vergelijkbaar als bij door EDSN beheerde systemen) op basis van de gegevens in de berichten zelf;
    - Een belangrijk verschil met door EDSN beheerde systemen is dat het bij TenneT voorkomt dat ondernemingen met meerdere marktrollen dezelfde EAN-13 gebruiken in het berichtenverkeer. Een voorbeeld hiervan is een onderneming met zowel en BRP als BSP-rol, die in het berichtenverkeer dezelfde EAN-13 gebruiken.

**Conclusie:** In de centrale systemen beheerd door TenneT wordt geen gebruik gemaakt van certificaten met een EAN-13 en is er geen controle op de aanwezigheid van de juiste EAN-13 in de certificaten.



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

**14. Gebruik EAN-13 door marktpartijen –** Het gebruik door marktpartijen van de EAN-13 in relatie tot de PKIoverheidcertificaten is verschillend en afhankelijk van het aantal EAN-13s van de marktpartij. De impact op individuele marktpartijen is niet generiek te bepalen en zal door de marktpartijen zelf in kaart gebracht moeten worden.

**Conclusie:** Het gebruik van de EAN-13 binnen de marktpartijen is afhankelijk van de marktpartij. Dit zal een markpartij zelf moeten analyseren.

### 2.1.3 Voor welke systemen worden PKIoverheidcertificaten gebruikt

In deze paragraaf zijn enkele overwegingen opgenomen die ingaan op de centrale systemen die gebruik maken van PKIoverheidcertificaten.

**15. Centrale systemen beheerd door EDSN –** Onderstaande tabel bevat een overzicht van de door EDSN beheerde centrale systemen waarvoor PKIoverheidcertificaten nodig zijn. Noot: PKIoverheidcertificaten worden gebruikt voor connecties met deze systemen via het S2S-verkeer. Toegang via de webGUI loopt via Dienst Veilige Toegang (DVT), daarvoor zijn geen PKIoverheidcertificaten nodig.

| Systeem[1] | Toelichting op het systeem | Geraakte marktrollen |
|---|---|---|
| C-AR | Centraal aansluitingenregister | LV, BRP, MV, DSB, TSB, BGS |
| TMR | Toegankelijk meetdata Register | LV |
| Portaal CTS (P4) | Centrale Toegang Service (voor P4) | LV, ODA |
| GDX / Nexus hub (ARM) | Allocatie & Reconcilliatie (GDX vervangt Nexus hub) | LV, BRP, DSB, TSB-G |
| ProFra | Profielfracties | LV, BRP, SB |
| CERES | Productie installatie management | DSB, TSB-E |
| CSS (ARM) | Centraal Stuursignaal gas | MV, DSB, TSB-G, BGS, BRP |
| Calgosboek | Calorische waarden gas | MV, DSB, LV, BRP, TSB-G |

[1] Alleen systemen zijn opgenomen waarmee marktpartijen verbindingen kunnen hebben via marktprocessen. Er zijn meer centrale systemen (zoals C-ARM), maar die geen verbindingen met marktpartijen hebben. Mogelijk hebben ze wel verbindingen met de systeembeheerders en worden daarmee wel geraakt door de certificatenwissel.



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

| Systeem[1] | Toelichting op het systeem | Geraakte marktrollen |
|---|---|---|
| PiE | Non-conformiteiten API | MV |
| AMST | ODA mandaten, storingsgegevens op afstand uitleesbare meetinrichtingen KA, meetrinrichtinggegevens KA | ODA, LV |

16. **Centrale systemen beheerd door TenneT –** TenneT gebruikt géén PKIoverheidcertificaten meer voor connecties met centrale systemen. Voor het Centraal postbus systeem (CPS) en de MMC-hub (inclusief de Activation interface en de Noodvermogen webservices) schrijft TenneT een ander type certificaat voor. Dit betreft géén PKIoverheidcertificaat.

### 2.1.4 Aanvraagproces G1 PKIoverheidcertificaten

In deze paragraaf zijn enkele overwegingen opgenomen die ingaan op het aanvraagproces van G1 PKIoverheidcertificaten.

17. **Aanvraag PKIoverheidcertificaten bij een TSP –** PKIoverheidcertificaten kunnen alleen bij een TSP (Trust Service Provider) aangevraagd worden. KPN is momenteel de enige TSP die ten behoeve van het S2S verkeer met servers van door EDSN beheerde systemen PKIoverheidcertificaten met een EAN-13 uitgeeft. Alleen de bevoegd vertegenwoordiger, of één van de gevolmachtigde contactpersonen die bij KPN zijn geregistreerd als onderdeel van de KPN Abonneeregistratie, kunnen een certificaat aanvragen.

**Conclusie:** PKIoverheidcertificaten t.b.v. S2S verkeer met door EDSN beheerde systemen kunnen momenteel alleen bij de TSP KPN aangevraagd worden.

18. **Controle EAN-13 tijdens aanvraag PKIoverheidcertificaten bij KPN -** Bij een aanvraag voor een PKIoverheidcertificaat controleert KPN, via de servicedesk van EDSN, of de aanvragende partij gemachtigd is om een certificaat voor EDSN aan te vragen. Daarbij wordt gecontroleerd door EDSN of de opgegeven EAN-13 overeenkomt met de EAN-13 en de statutaire naam die bij EDSN zijn geregistreerd.

**Conclusie:** Bij de afhandeling van een aanvraag van een PKIoverheidcertificaat via KPN vindt ook een controle door EDSN plaats.



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

### 2.1.5 Einde gebruik G1 PKIoverheidcertificaten

In deze paragraaf zijn enkele overwegingen opgenomen die ingaan op de einddatum van de G1 PKIoverheidcertificaten en de mogelijkheden tot verlenging hiervan tot die einddatum.

19. **Geldigheid G1 PKIoverheidcertificaten –** Net als met een fysiek ID-bewijs/rijbewijs heeft ook elk digitaal ID bewijs een begrensde geldigheid met een 'geldig van-' en een 'geldig tot-' datum. In het geval van PKIoverheidcertificaten kunnen deze certificaten een geldigheid hebben van 1, 2 of 3 jaar. De geldigheid is van toepassing op de zogenaamde eindgebruikerscertificaten waarmee daadwerkelijk het S2S verkeer plaatsvindt.

    **Conclusie:** Eindgebruikers-certificaten kennen een geldigheid van 1, 2 of 3 jaar.

20. **Einddatum G1 PKIoverheidcertificaten –** 'Boven' het eindgebruikerscertificaat zijn de zogenaamde bovenliggende-/uitgevende certificaten en die zijn langer geldig. In het geval van de huidige PKIoverheid G1 certificaten is dit 15 jaar met als harde einddatum 12 november 2028.

    **Conclusie:** PKIoverheid G1 certificaten kennen een uiterlijke geldigheidsdatum 12 november 2028.

21. **Uitgifte G1 PKIoverheidcertificaten tot 12-11-2028 –** KPN heeft de volgende einddatums genoemd voor de aanvraag van eindgebruikerscertificaten in de aanloop naar 12-11-2028.

| Datum | Laatste mogelijkheid uitgifte certificaten |
|---|---|
| 12 november 2025 | Laatste mogelijkheid uitgifte G1 PKIoverheidcertificaten met een geldigheid van **3 jaar** |
| 12 november 2026 | Laatste mogelijkheid uitgifte G1 PKIoverheidcertificaten met een geldigheid van 2 jaar |
| 12 november 2027 | Laatste mogelijkheid uitgifte G1 PKIoverheidcertificaten met een geldigheid van 1 jaar |
| Na 12 november 2027 | Geen zekerheid over verstrekking van G1 PKIoverheidcertificaten. Logius staat certificaten met een kortere looptijd wel toe (met uiterste einddatum 12 november 2028), maar TSP's bepalen zelf of zij dit daadwerkelijk aanbieden.<br>KPN heeft aangegeven dit 'onder voorwaarden' te kunnen aanbieden. Over de voorwaarden dient nog verder te worden afgestemd. |



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

**Conclusie:** PKIoverheid G1 certificaten worden tot zeker nog tot 12 november 2027 uitgegeven. Er is nog geen zekerheid onder welke voorwaarden TSP's na deze datum nog certificaten met een kortere looptijd aanbieden.

## 2.2 G4 PKIoverheidcertificaten

In deze paragraaf zijn enkele overwegingen opgenomen die ingaan op de nieuwe generatie G4 PKIoverheidcertificaten.

22. **G4 PKIoverheidcertificaten–** G4-certificaten zijn de nieuwe generatie PKIoverheidcertificaten die de huidige G1 en G3 PKIoverheidcertificaten vervangen.

    **Conclusie:** G4 PKIoverheidcertificaten zijn de vervanging voor de G1 en G3 PKIoverheidcertificaten.

23. **Vier rootcertificaten–** G4 introduceert een vernieuwde root-hiërarchie, een overzicht hiervan staat op de volgende website: Overview of PKIoverheid certificates. G4 beschikt over 4 rootcertificaten die ieder voor verschillend gebruik bedoeld zijn:
    - S/MIME (publiek vertrouwd);
    - EU-gekwalificeerde digitale handtekeningen;
    - Server authenticatie (privaat vertrouwd);
    - Overig (privaat vertrouwd; vooral bedoeld voor authenticatiedoeleinden**).**

    Het rootcertificaat voor server-authenticatie is relevant voor dit topicdocument. Het betreft het volgende root- en intermediate-certificaat:
    - **Root certificate:** "Staat der Nederlanden - G4 Root Priv G-TLS – 2024";
    - **Domain / intermediate certificate:** "Staat der Nederlanden - G4 Intm Priv G-TLS SYS – 2024"

    Binnen deze root is voor iedere TSP een TSP-certificaat aangemaakt, bijvoorbeeld "KPN - G4 PKIo Priv G-TLS SYS – 2025" voor KPN.

    **Conclusie:** G4 PKIoverheidcertificaten introduceert vier verschillende rootcertificaten, waarbij de "server-authenticatie (privaat vertrouwd)" relevant is. Dit betreft de volgende root: "Staat der Nederlanden - G4 Root Priv G-TLS – 2024" (Bron: Logius).

24. **Eindgebruikerscertificaten** - Een G4-eindgebruikerscertificaat kan nog maar voor één hoofddoel worden gebruikt (identificatie/authenticatie óf



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

ondertekening), wat betekent dat partijen vaker meerdere eindgebruikerscertificaten nodig zullen hebben. De G4 private TLS-certificaten blijven wel geschikt voor zowel server authenticatie als client authenticatie.

**Conclusie:** Elk type eindgebruikerscertificaat is nog maar voor één doeleinde te gebruiken (dus bijvoorbeeld niet langer zowel voor authenticatie als voor een digitale handtekening).

25. **Trust service providers –** G4-certificaten worden aangeboden door erkende Trust service providers (TSP's). Ten tijde van het opstellen van dit topic zijn er drie commerciële TSP's erkend die PKIoverheid certificaten voor rechtspersonen aanbieden: KPN, DigiCert en Digidentity (noot: Cleverbase ID is ook TSP maar biedt uitsluitend certificaten voor natuurlijke personen aan).

26. **Mogelijkheid EAN-13 in G4 PKIoverheidcertificaten–** Uit navraag bij Logius blijkt dat de EAN-13 ook in G4-certificaten kan worden opgenomen in het veld 'subject serialnumber'. De regels over de inhoud van dit veld wijzigen niet als gevolg van de overgang naar G4. Opnemen van de EAN-13 blijft wel afhankelijk van de bereidheid van TSP om dit aan te bieden - op dit moment zijn daar alleen met KPN afspraken over gemaakt. KPN heeft inmiddels bevestigd dat dit ook in G4-certificaten mogelijk blijft.

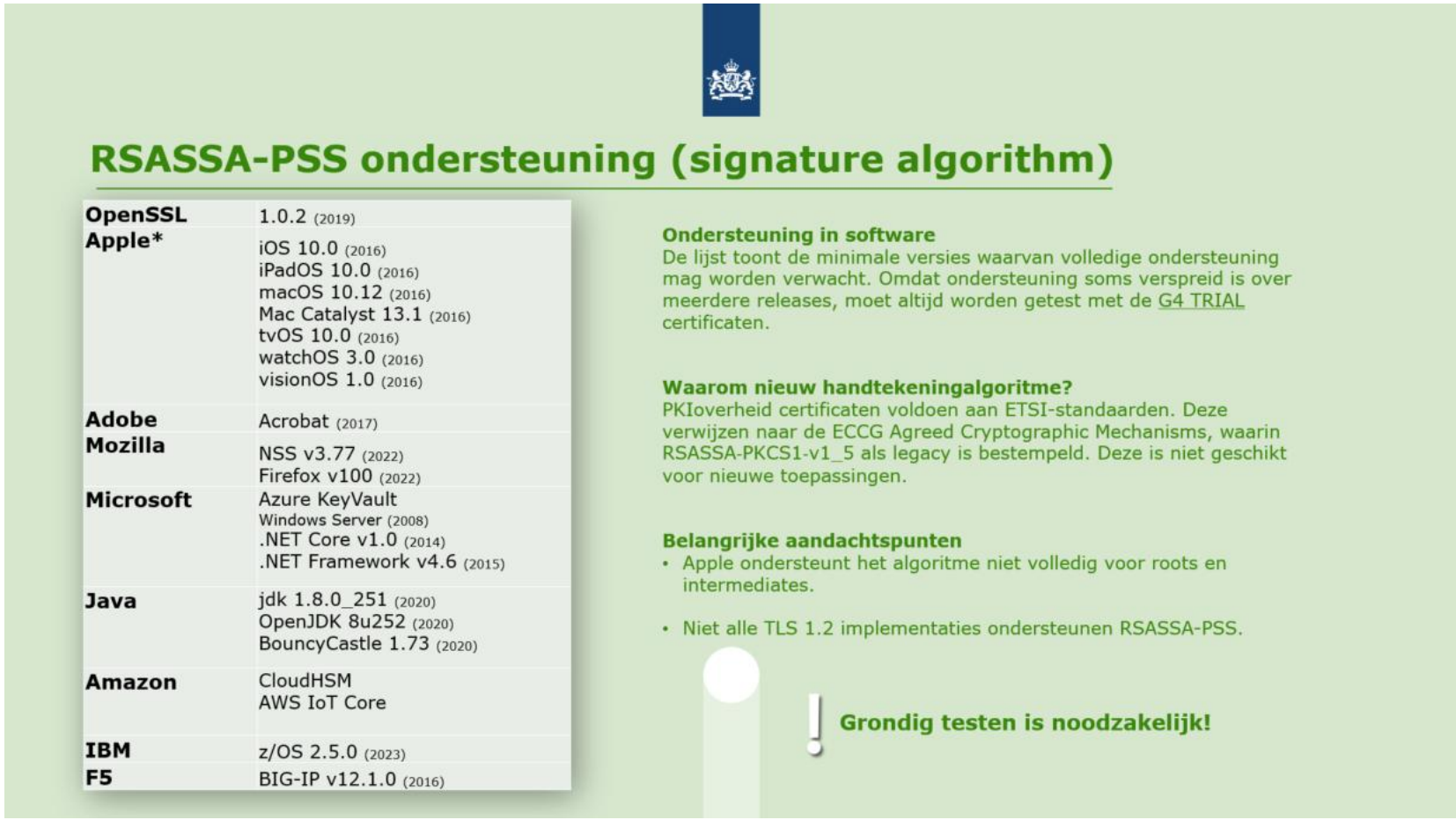
**Conclusie:** Binnen de G4 PKIoverheidcertificaten blijft het gebruik van de EAN-13 toegestaan. KPN blijft deze optie aanbieden, met andere TSP's zijn hier geen afspraken over gemaakt.

27. **Zwaardere beveiliging -** G4 bevat een moderner en strenger algoritme voor het ondertekenen van alle certificaten:
Het signature algoritme RSASSA-PKCS1-v1_5 is vervangen door RSASSA-PSS.
Het key algoritme is ongewijzigd: RSA 4096 bits voor CAs en ten minste 3000 bits voor end entity certificaten

Logius verwacht dat het RSASSA-PSS algoritme wordt ondersteund door de meeste systemen die met TLS 1.3 werken (zoals reeds wordt gebruikt voor de gegevensuitwisseling met de centrale systemen beheerd door TenneT en EDSN). Onderstaand overzicht van Logius toont de minimaal benodigde versies waarvan ondersteuning mag worden verwacht. Logius benadrukt wel dat grondig testen in alle gevallen nodig blijft om de ondersteuning door systemen en eventuele performance-impact vast te stellen.



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl




**Conclusie:** G4-certificaten gebruikt het RSASSA-PSS algoritme voor digitale ondertekening. Alle systemen die PKIoverheidcertificaten gebruiken, dienen dit algoritme te ondersteunen.



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

## 2.3 Organisatie Identificatie Nummer (OIN)

In deze paragraaf zijn enkele overwegingen opgenomen die ingaan op het gebruik van het Organisatie Identificatie Nummer (OIN).

**28.** **Wat is een OIN? –** Een OIN-nummer (Organisatie-Identificatienummer) is een uniek identificerend nummer dat door Logius wordt uitgegeven aan organisaties. Het wordt gebruikt om organisaties betrouwbaar te identificeren, authentiseren en autoriseren in digitaal berichtenverkeer. Het OIN wordt afgeleid van het KvK-nummer uit het Handelsregister. Het OIN maakt het mogelijk om in digitale koppelingen te bepalen welke organisatie communiceert en of deze geautoriseerd is om toegang te krijgen tot systemen of gegevens.

Voor verdere verfijning kunnen OIN-houders daarnaast één of meer **subOIN's** aanvragen bij Logius. Een subOIN wordt gebruikt voor een organisatieonderdeel, samenwerkingsverband of voorziening/applicatie welke niet zélf in het Handelsregister voorkomt en als zodanig géén rechtspersoonlijkheid heeft. Een subOIN valt altijd onder de verantwoordelijkheid van een OIN-houder.

**Conclusie:** Een OIN (Organisatie-Identificatienummer) is een uniek identificerend nummer dat door Logius wordt uitgegeven aan organisaties

**Conclusie:** onder een OIN kunnen één of meer subOIN's worden aangemaakt ter identificatie van een organisatieonderdeel, samenwerkingsverband of voorziening/applicatie.

**29.** **Het OIN-register. -**De Centrale OIN Raadpleegvoorziening (COR) is een webinterface om het OIN-register te raadplegen. In het OIN-register staan alle uitgegeven openbare Organisatie-identificatienummers (OIN).

**Conclusie:** Het register met alle openbare OINs is te raadplegen via de Centrale OIN Raadpleegvoorziening (COR).

**30.** **Mogelijkheden voor het gebruik van OIN / subOIN in G4-certificaten –** Er is onderzocht of OIN / subOIN het gebruik van de EAN-13 code in PKIoverheidcertificaten kan vervangen. Hierbij zijn de volgende overwegingen relevant:

- Logius en KPN hebben inmiddels bevestigd dat het gebruik van EAN-13 in de G4-certificaten mogelijk blijft. Hiermee is de introductie van een alternatief kenmerk (zoals OIN/subOIN) om de marktpartij te identificeren niet noodzakelijk voor het overstappen naar G4-certificaten.
- Het gebruik van EAN-13 in het certificaat vereist maatwerk van de TSP en een extra validatiestap in het aanvraagproces. Momenteel zijn er alleen met KPN afspraken over het aanbieden hiervan, waardoor er voor gegevensuitwisseling met EDSN in praktijk geen vrije TSP-keuze



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

mogelijk is. TSP's kunnen standaard wel een OIN genereren en opnemen in het certificaat, het vervangen van EAN-13 door OIN in het certificaat zou daarom een vrije TSP-keuze mogelijk maken.

- Het OIN is gebaseerd op het KVK-nummer en identificeert dus primair de *onderneming* die het certificaat heeft aangevraagd. Hiermee wordt niet automatisch de *marktpartij* met een specifieke *marktrol* geïdentificeerd. Het gebruik van alleen het OIN biedt dus geen volledige vervanging voor de EAN-13 (met name voor ondernemingen die meerdere marktrollen hebben).
- Het bepalen van de marktrol en het toepassen van de autorisatieregels voor die marktrol kunnen op basis van het OIN wel worden herleid op basis van de geregistreerde gegevens in het marktpartijenregister. Dit vereist echter aanpassingen in meerdere applicaties en zou daarmee de technische impact op de door EDSN beheerde centrale systemen significant vergroten. Dit heeft daarnaast impact op de configuratie van certificaten bij marktpartijen, en is er sprake van extra (keten)testimpact voor zowel beheerders van centrale systemen als marktpartijen. Het is niet wenselijk om dit als onderdeel van de overgang naar G4 uit te voeren.
- *SubOIN's* kunnen in theorie wel worden gebruikt in de G4-certificaten om marktpartijen met een specifieke marktrol te identificeren. Deze subOIN's kunnen niet door TSP's zelf worden gegenereerd, maar moeten worden aangevraagd bij Logius, waarna de OIN en subOIN's van een onderneming worden opgenomen in het OIN-register. Logius geeft aan dat subOIN's bedoeld zijn voor organisaties die voor het uitvoeren van een publieke taak behoefte hebben aan een identificerend nummer voor een samenwerking (waar het zelf deel van uit maakt), organisatieonderdeel of voorziening. Het gebruik van subOIN's is niet bedoeld voor het registreren en autoriseren van marktrollen. Bovendien kunnen buitenlandse ondernemingen in praktijk nog niet goed worden opgenomen in het OIN-register, en leidt het gebruik hiervan tot extra administratieve processen en validaties in het aanvraagproces van certificaten. Het gebruik van subOIN's heeft daarom niet de voorkeur.

Op basis van bovenstaande overwegingen is het advies om bij de overstap van G1- naar G4-certificaten gebruik te blijven maken van de EAN-13 code in het certificaat.

**Conclusie:** Het gebruik van subOIN voor het autoriseren van marktpartijen met een specifieke marktrol is onwenselijk en onnodig.

**Conclusie**: Het gebruik van OIN is mogelijk, maar is niet noodzakelijk voor de overgang naar G4 en vergroot de impact en complexiteit.

**Conclusie**: Het advies is daarom gebruik te blijven maken van EAN-13 codes in het veld 'subject serial number' in de G4-certificaten om de marktpartij te identificeren en de marktrol te herleiden.



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

## 2.4 Alternatieven voor PKIoverheidcertificaten

PKIoverheidcertificaten zijn niet de enige oplossing voor identificatie- en authenticatieprocessen binnen het S2S-verkeer. In deze paragraaf zijn enkele overwegingen opgenomen over alternatieve oplossingsrichtingen.

31. **Publiek vertrouwde TLS-certificaten –** deze certificaten worden veel gebruikt voor internetverkeer via browsers. De certificaatautoriteiten (CA's) die deze certificaten uitgeven worden automatisch vertrouwd door alle grote besturingssystemen en webbrowsers (waarvan vertegenwoordigers afspraken maken in het CA/Browser Forum). Dit soort certificaten worden veel gebruikt om internetverkeer te beveiligen, maar er vindt geen validatie plaats van de identiteit van de certificaathouder.

    Belangrijke ontwikkelingen zijn daarnaast dat deze certificaten binnenkort niet meer geschikt zijn voor client authenticatie (voor gebruikers of apparaten) en dat de maximale looptijd van deze certificaten stapsgewijs wordt verkort. Vanaf maart 2026 is de maximale levensduur 200 dagen, in 2029 zal dit nog maar 47 dagen zijn. Als gevolg hiervan is het bij dit type certificaat steeds belangrijker om het beheer van certificaten volledig te automatiseren. Deze ontwikkelingen zijn niet van toepassing op PKIoverheidcertificaten.

    Overstappen naar publiek vertrouwde TLS-certificaten zou het aanschafproces vereenvoudigen, maar vergt alternatieve oplossingen voor client authenticatie en het betrouwbaar identificeren van marktpartijen. En vergt daarnaast implementatie van geautomatiseerde certificaatbeheerprocessen door alle gebruikers. Deze optie wordt daarom niet overwogen als oplossing in dit topicdocument.

32. **Alternatieve PKI-certificaten**: naast PKIoverheid zijn er andere PKI-stelsels, met diverse aanbieders. De door TenneT gebruikte DigiCert X9 PKI-certificaten zijn hier een voorbeeld van. Vanuit technisch oogpunt bieden deze vergelijkbare functionaliteit en de looptijd van deze certificaten wordt niet ingekort zoals bij publieke TLS-certificaten (deze certificaten blijven 1 jaar geldig, dit is wel korter dan PKIoverheidcertificaten waarbij ook kan worden gekozen voor een looptijd van 2 of 3 jaar). Er gelden ook identificatie-eisen, hoewel deze minder strikt zijn dan bij PKIoverheid. Het opnemen van een eigen kenmerk zoals de EAN-13 code is niet standaard mogelijk en vergt aanvullende afspraken met de aanbieders van deze certificaten. Voor gegevensuitwisseling via EDSN biedt invoering hiervan geen grote voordelen ten opzichte van het PKIoverheidstelsel, deze optie wordt daarom niet overwogen.

33. **Privaat PKI-stelsel –** Het is ook mogelijk om privaat vertrouwde PKI-structuren op te zetten, waarbij een beherende organisatie zelf eindgebruikerscertificaten kan uitgeven binnen een besloten groep gebruikers. Zo'n stelsel is daarmee onafhankelijk van externe TSP's, en het aanvraagproces en de configuratie van de certificaten kunnen worden toegespitst op de wensen en eisen van de gebruikersgroep. Dit vereist wel



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

het opzetten van een eigen certificaatautoriteit (CA), met organisatorische, technische en operationele impact. Dit is geen passende oplossing binnen het tijdbestek van de certificatenwissel van G1 naar G4.

34. **Andere oplossingen voor identificatie en authenticatie** – er zijn ook oplossingen denkbaar waarbij gebruikers een account aanmaken en zich daarbij eenmalig identificeren (bijvoorbeeld via eHerkenning). Authenticatie vindt vervolgens niet plaats via een certificaat, maar door het gebruik van 'tokens' (bijvoorbeeld via de OAUTH-standaard) waarmee toegang wordt gegeven tot de gevraagde gegevensuitwisseling. Deze techniek wordt reeds gebruikt door Het Normo (voor Dataproducten) en EDSN (via Dienst veilige toegang) voor een aantal gegevensuitwisselingen. Het aansluiten van alle berichtstromen op deze oplossing vereist wijzigingen in al deze berichtstromen en is daarom geen passende oplossing binnen het tijdbestek van de certificatenwissel van G1 naar G4. Daarnaast is het voor het uitwisselen van gevoelige gegevens mogelijk nog steeds nodig om certificaten in te zetten voor aanvullende beveiliging van de verbinding (via mTLS).

**Conclusie:** Gezien de grotere complexiteit en verwachte impact op zowel beheerders als marktpartijen, worden alternatieven voor PKIoverheidcertificaten niet overwogen in dit topic.

35. **Toekomstige ontwikkelingen –** Er vinden continu ontwikkelingen plaats op het gebied van digitale gegevensuitwisseling en -beveiliging, die van invloed kunnen zijn op het gebruik van certificaten en andere oplossingen. Een voorbeeld hiervan is de ontwikkeling van quantumcomputers, die in de toekomst nieuwe beveiligingsalgoritmes noodzakelijk maken (post quantum cryptografie). Deze en andere ontwikkelingen kunnen leiden tot nieuwe wijzigingen in het PKIoverheidstelsel of het implementeren van andere oplossingen nodig maken.

36. **Rol van de gegevensuitwisselingsentiteit** - Sinds 1 januari 2026 heeft Het Normo als gegevensuitwisselingsentiteit (GUE) een aantal wettelijke taken, waaronder het faciliteren van de toegang tot en de uitwisseling van gegevens tussen partijen in het energiesysteem. Daarbij is zij ook verantwoordelijk voor identificatie, authenticatie en autorisatie, en een goede beveiliging van de gegevensuitwisseling. Als gevolg hiervan zal de GUE meer kaders gaan stellen aan de gegevensuitwisseling en de bijbehorende (IT-)faciliteiten – inclusief het toekomstige gebruik van certificaten of alternatieve middelen. De GUE zal hiervoor een afzonderlijk initiatief opstarten en hierover in overleg treden met marktpartijen en belanghebbenden (naar verwachting in Q4 2026). Gezien de lange doorlooptijd van de certificatenwissel, kan niet worden uitgesloten dat dit voor november 2028 tot impact leidt op een of meerdere berichtstromen die gebruik maken van PKIoverheidcertificaten.

37. **Alternatieve certificaatkeuze voor TenneT -** voor gegevensuitwisseling met TenneT via CPS wordt op dit moment geen gebruik gemaakt van PKIoverheidscertificaten. Omdat CPS steeds minder wordt gebruikt en uiteindelijk zal worden uitgefaseerd, is het niet wenselijk om te investeren in alternatieve oplossingen. Daarmee is CPS niet in scope van de certificatenwissel van G1 naar G4.



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

Voor gegevensuitwisseling via de MMC-hubworden geen PKIoverheidcertificaten gebruikt, maar schrijft TenneT vanaf Q2-2026 DigiCert X9 certificaten voor (de certificatenwissel van G1 naar G4 is hierop niet van toepassing). Het implementeren van PKIoverheidcertificaten voor deze systemen is op dit moment niet wenselijk, omdat dit extra technische impact heeft en mogelijk tot meerdere certificatenwissels achter elkaar leidt. De wens bestaat wel om een marktbrede en uniforme oplossing te verkennen, die bij voorkeur ook de beheer- en vernieuwingsprocessen vereenvoudigt. Dit is niet in scope van TE014, maar wordt meegewogen in de hierboven genoemde GUE-verkenning.

**Conclusie:** Gegevensuitwisselingen met TenneT via CPS en MMC-hub (inclusief Noodvermogen webservices en Activation interface) worden niet geraakt door de certificatenwissel van G1 naar G4 en zijn daarom niet in scope van TE014.

## 2.5 Implementatie

In deze paragraaf zijn enkele subparagrafen met overwegingen opgenomen die ingaan op de overgang van G1 naar G4 certificaten. Verdere uitgangspunten staan in het hoofdstuk ‘invoeringsstrategie’ en worden verder gedetailleerd in op te stellen implementatiedocumenten, waaronder het Implementatieplan, testplannen en het transitieplan.

### 2.5.1 Duale periode G1 en G4

38. **Waarom een duale periode?** – goed werkende certificaten zijn een randvoorwaarde voor het uitvoeren van de gegevensuitwisseling tussen marktpartijen en centrale systemen. Partijen zijn zelf verantwoordelijk voor het aanschaffen en installeren van certificaten, de impact hiervan kan per partij verschillen. Ervaringen met soortgelijke initiatieven (bijv. certificatenwissel 2016 en overgang naar TLS 1.3) leert ons dat het wisselen van certificaten een groot en intensief traject is. Ook Logius (de beheerder van het afsprakenstelsel rond PKIoverheidcertificaten) adviseert partijen om op tijd te beginnen met het organiseren van de certificatenwissel.

    Om te voorkomen dat de gegevensuitwisseling wordt verstoord als gevolg van het ongeldig worden van PKIoverheidcertificaten, is het dus wenselijk om partijen ruime gelegenheid te bieden om de certificaatwissel voor te bereiden, te testen en te implementeren. Dit beoogt ook een spreiding van instapmomenten, waardoor en geen extreme pieken ontstaan in supportvragen.



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

**Conclusie:** het is wenselijk om marktpartijen ruime gelegenheid te bieden om de certificaatwissel voor te bereiden, te testen en te implementeren. Hiervoor wordt een duale periode ingepland.

### 2.5.2 Testen en testfaciliteiten

39. **Testomgevingen -** Er dient een testomgeving (of indien nodig meerdere testomgevingen) beschikbaar te zijn waarop marktpartijen de gegevensuitwisseling met de centrale systemen op basis van G4-certificaten kunnen testen. Deze testomgeving dient vóór aanvang van de duale fase beschikbaar te zijn ten behoeve van een kopgroeptest, en gedurende de hele duale periode beschikbaar blijven. Daarbij moet worden geborgd dat andere releases gedurende de duale periode mogelijk blijven, en niet verstorend werken voor het testen van de certificaten.

40. **Kopgroeptest** – Na realisatie van de benodigde aanpassingen in de centrale systemen en het intern testen daarvan, dient de oplossing gevalideerd te worden tijdens een kopgroeptest met een aantal representatieve marktpartijen. Hiermee worden eventuele algemene inrichtingsproblemen en bevindingen vroegtijdig geïdentificeerd, zodat deze kunnen worden opgelost voordat de duale periode start.

41. **Kwalificatie** – aangezien de certificatenwissel geen functionele impact heeft op systeemprocessen, is een kwalificatie niet noodzakelijk. Marktpartijen kunnen de werking van de G4-certificaten zelf testen op de daarvoor beschikbare testomgevingen. Mogelijk worden wel verplichte testcases voorgeschreven, dit wordt in de implementatiefase verder uitgewerkt.

42. **Trial-certificaten** - Logius kan op verzoek een CA-ketentestomgeving opzetten, waarmee gebruikers de technische werking van de G4-certificaten kunnen testen, bijvoorbeeld compatibiliteit met de gebruikte systemen, en ondersteuning van het encryptie-algoritme en aangepaste sleutellengte. EDSN kan op basis hiervan een testtool faciliteren en trial-certificaten genereren, waarmee partijen in staat worden gesteld om de werking van G4-certicaten te testen. Het gebruik van deze testtool zal beperkt zijn tot het uitvoeren van een technische compatibiliteitscheck.

    Technische achtergrondinformatie over trial G4-certificaten is beschikbaar op de Github-omgeving van Logius:
    GitHub - pkioverheid/g4-trial: Generate TRIAL certificates for the PKIoverheid G4 hierarchies · GitHub



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

# 3 Gekozen oplossing

## 3.1 Gebruik van G4-certificaten voor centrale systemen beheerd door EDSN

De gekozen oplossing bestaat uit de volgende elementen, die in dit hoofdstuk verder worden beschreven:

- Scope en toepassing van G4-certificaten
- Aanschaf / aanvraag van G4-certificaten
- Installeren van de G4-certificaten
- Identificatie van marktpartijen bij gegevensuitwisseling
- Periodiek vernieuwen van certificaten

## 3.2 Scope en toepassing van G4-certificaten

### 3.2.1 In scope

- De oplossing die in dit hoofdstuk wordt beschreven, heeft uitsluitend betrekking op de overgang van G1- naar G4-certificaten binnen het PKIoverheidstelsel en de toepassing hiervan binnen het energiesysteem. Dit betreft in praktijk uitsluitend gegevensuitwisseling met de systemen beheerd door EDSN. De te gebruiken G4-certificaten blijven geschikt voor zowel server authenticatie als client authenticatie, en kunnen voor deze doeleinden worden ingezet.
- Voor gegevensuitwisseling met EDSN gebruiken sommige marktpartijen meerdere certificaten met dezelfde EAN-13 code, bijvoorbeeld voor communicatie vanuit verschillende systemen. Dit is afhankelijk van het systeemlandschap en de inrichtingskeuzes van de marktpartij. De overgang van G1 naar G4 heeft geen impact op deze inrichtingskeuzes, partijen dienen zorg te dragen dat alle gebruikte G1-certificaten worden overgezet naar G4.

### 3.2.2 Niet in scope

- Andere toepassingen dan S2S-communicatie, het aantal doeleinden waarvoor G4-certificaten mogen worden ingezet, is beperkt: de te gebruiken ‘Priv G-TLS SYS’ certificaten mogen niet langer voor e-mail signing of identificatie van natuurlijke personen worden gebruikt. Als marktpartijen de oude G1-certificaten ook voor deze doeleinden gebruikten, dan zijn zij zelf verantwoordelijk voor het aanschaffen en inrichten van afzonderlijke



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

certificaten voor dat doeleinde (buiten scope van TE014).

- Toepassingen van PKIoverheidcertificaten buiten het energiesysteem – PKIoverheidcertificaten kunnen ook worden gebruikt voor gegevensuitwisseling met andere partijen / instanties, buiten de centrale systemen van de energiesector. De impact van de certificatenwissel op die processen en systemen valt buiten scope van dit topic, en dienen door de geraakte partijen zelf te worden geadresseerd.
- Inzet van andere soorten certificaten dan PKIoverheid – de beschreven oplossing heeft uitsluitend betrekking op PKIoverheidcertificaten. Het gebruik van andere certificaten (inclusief DigiCert X9 certificaten voor de MMC-hub van TenneT) is niet in scope.

## 3.3 Aanschaf / aanvraag van G4-certificaten

### 3.3.1 TSP-keuze en bestelproces voor gegevensuitwisseling via EDSN

- KPN blijft vooralsnog de enige TSP voor het aanschaffen van PKIoverheidcertificaten met een EAN-13 code.
- Marktpartijen dienen hun G4-certificaten tijdig aan te schaffen, conform het bestelproces van KPN. Dit proces is ongewijzigd.
- De introductie van G4 heeft impact op een groot aantal organisaties, dit kan leiden tot pieken in het aanvraagproces van nieuwe certificaten bij KPN. Het advies is daarom om het bestelproces tijdig te starten, en voldoende tijd in te plannen voor het testen en implementeren. Let daarbij ook op de einddatum van de lopende G1-certificaten, en verleng deze nog eenmaal indien dit nodig is.

### 3.3.2 Te bestellen certificaten

Voor G4 zal gebruik worden gemaakt van de volgende certificaathiërarchie:

- Root CA: **Staat der Nederlanden - G4 Root Priv G-TLS – 2024**
- Intermediate CA: **Staat der Nederlanden - G4 Intm Priv G-TLS SYS - 2024**
- TSP-certificaat:
  - Gegevensuitwisseling via EDSN: **KPN - G4 PKIo Priv G-TLS SYS - 2025**
- Eindgebruikerscertificaat: de exacte naam van de G4-eindgebruikerscertificaten is nog niet bekend tijdens het opstellen van dit topic. Wanneer dit bekend wordt, zal deze worden opgenomen in implementatiedocumenten en voorlichtingsinformatie voor de certificatenwissel.



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

## 3.4 Installeren en testen van de G4-certificaten

### 3.4.1 Installeren

- Partijen dienen de certificaten conform de hierboven gespecificeerde hiërarchie te installeren en te vertrouwen in hun systemen.
- Partijen controleren hun eigen systemen en passen deze waar nodig aan om aan de systeemvereisten van G4-certificaten te voldoen – zie hoofdstuk 2 voor een overzicht van Logius met minimale systeemvereisten.
- Partijen configureren het benodigde algoritme voor digitale ondertekening:
    - Het nieuwe signature algoritme: **RSASSA-PSS**.
    - Het key algoritme is ongewijzigd: RSA 4096 bits voor CAs en ten minste 3000 bits voor end entity certificaten.

### 3.4.2 Testen

- Het wordt dringend aanbevolen om de technische werking van het certificaat en compatibiliteit met de gebruikte systemen te testen. EDSN biedt hiervoor een testtool aan die de partijen kunnen gebruiken om de technische werking te valideren. Het endpoint van deze tool kan aangeroepen worden in combinatie met een trial-certificaat dat wordt uitgegeven door EDSN. Noot: trial-certificaten staan los van een TSP en de testtool is uitsluitend bedoeld om de technische compatibiliteit met decentrale systemen van marktpartijen te toetsen.
- Daarnaast wordt een reguliere acceptatietestomgeving (of indien nodig meerdere testomgevingen) beschikbaar gesteld, waarop marktpartijen de gegevensuitwisseling met de centrale systemen op basis van aangeschafte G4-certificaten (niet de trial-certificaten) kunnen testen. Deze testomgeving dient vóór aanvang van de duale periode beschikbaar te zijn ten behoeve van een kopgroeptest, en daarna gedurende de hele duale periode beschikbaar blijven. Daarbij moet worden geborgd dat andere releases gedurende de duale periode mogelijk blijven, en niet verstorend werken voor het testen van de certificaten.
- In het op te stellen implementatieplan / testplan zal worden beschreven of verplichte testcases noodzakelijk zijn.

## 3.5 Identificeren van marktpartijen op basis van EAN-13

- De overgang naar G4-certificaten heeft geen impact op het gebruik van EAN-13 codes in certificaten voor gegevensuitwisseling via EDSN. EDSN zal de marktpartij en marktrol op dezelfde wijze vaststellen op basis van de EAN-13 code als bij de G1-certificaten.



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

## 3.6 Periodiek vernieuwen van certificaten

- Zowel de huidige G1/G3-certificaten als de nieuwe G4-certificaten hebben een looptijd (bijvoorbeeld 1,2 of 3 jaar) en dienen tijdig te worden vernieuwd. Marktpartijen blijven hiervoor zelf verantwoordelijk.
- Afhankelijk van de looptijd is het waarschijnlijk dat de huidige certificaten van marktpartijen al eerder dan 12 november 2028 verlopen. Marktpartijen worden geadviseerd om vroegtijdig te starten met het voorbereiden van de overstap naar G4-certificaten. Afhankelijk van de looptijd kan het raadzaam zijn om de huidige certificaten nog één keer te verlengen.



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

# 4 Impact op wet- en regelgeving, afsprakenstelsel incl. MSP

Niet van toepassing.

## 4.1 Impact op lagere regelgeving

### 4.1.1 Mogelijke impact op Ministeriële Regelingen (MR) en Algemene Maatregel van Bestuur (AMvB)

Niet van toepassing.

### 4.1.2 Mogelijke impact op Methoden en voorwaarden

Niet van toepassing.

## 4.2 Impact op Sectordocumentatie

### 4.2.1 MSP Retailprocessen

Niet van toepassing.



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

# 5 Invoeringsstrategie

| | Release onafhankelijk | Release afhankelijk |
|---|---|---|
| **Na vaststelling MFF** | | |
| **Sectorrelease** | | |
| **Specifieke datum** | | Duale periode:<br>• Start: vóór 12 november 2027<br>• Eind: 12 november 2028 |

## 5.1 Release-afhankelijk met duale periode

### 5.1.1 Release-afhankelijk

De invoering van de certificatenwissel is releaseafhankelijk, om de volgende redenen:

1. Er is impact op de systemen van alle marktrollen.
2. Het is nodig om de centrale en decentrale systemen te testen door meer dan één marktrol.
3. Gezien de vaststaande deadline op 12 november 2028 is het nodig om de voortgang van de invoering te monitoren.
4. Er is een transitieperiode noodzakelijk voor alle marktrollen.

### 5.1.2 Duale periode

Om marktpartijen in staat te stellen om de certificatenwissel voor te bereiden en uit te voeren, is gekozen voor een **duale periode**.

**Start duale periode**

- Marktpartijen dienen ruim de tijd te krijgen om de certificatenwissel voor te bereiden, te testen en uit te voeren. Daarnaast zijn de voorwaarden waaronder G1-certificaten nog kunnen worden verlengd ná 12 november 2027 onzeker.
- Het is daarom logisch de duale periode te starten vóór **12 november 2027**. De exacte datum wordt door het IISO vastgesteld. Vanaf de startdatum van de duale periode ondersteunen alle centrale systemen waarvoor PKIoverheidcertificaten worden gebruikt tevens de nieuwe G4-certificaten.



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

**Einde duale periode**

- De duale fase eindigt op **12 november 2028**. Op 12 november 2028 worden de huidige G1-/G3-certificaten definitief ongeldig, de duale periode kan dus niet worden verlengd. Het is daarom essentieel dat marktpartijen op tijd starten met het aanvragen en testen van de nieuwe G4-certificaten.

## 5.2 Verantwoordelijkheden

### 5.2.1 Verantwoordelijkheden systeembeheerders

- Gelijktijdig gebruik van oude en nieuwe certificaten: de centrale systemen dienen gedurende de duale periode zowel de oude G1- als de nieuwe G4-certificaten te ondersteunen. Daarbij dient het mogelijk te zijn dat één marktpartij tijdens het overstappen zowel oude als nieuwe certificaten gebruikt (bijvoorbeeld voor het connecteren met verschillende systemen en/of het gebruik van certificaten op verschillende servers van de marktpartij).
- Gedurende de duale periode wordt gerapporteerd over het gebruik van certificaten door marktpartijen, waaruit blijkt hoeveel marktpartijen reeds zijn overgestapt op G4-certificaten, en hoeveel marktpartijen nog gebruik maken van G1-certificaten.
- Gedurende de duale periode wordt er voldoende technische support beschikbaar gemaakt om marktpartijen te ondersteunen bij het installeren, testen en gebruiken van de nieuwe G4-certificaten.
- Er worden trial-certificaten en een testtool beschikbaar gemaakt, waarmee marktpartijen de technische werking van het G4-stelsel en compatibiliteit met hun eigen systemen kunnen valideren.
- Er dient een acceptatietestomgeving (of indien nodig meerdere testomgevingen) beschikbaar te zijn waarop marktpartijen de gegevensuitwisseling met de centrale systemen op basis van aangeschafte G4-certificaten kunnen testen. Deze testomgeving moet gedurende de hele duale periode beschikbaar zijn, waarbij moet worden geborgd dat andere releases gedurende de duale periode mogelijk blijven, en niet verstorend werken voor het testen van de certificaten. Deze testomgeving dient al vóór aanvang van de duale periode beschikbaar te zijn ten behoeve van een kopgroeptest.

### 5.2.2 Verantwoordelijkheden Het Normo

- Informatieverstrekking aan marktpartijen: marktpartijen dienen voor aanvang van de duale periode heldere instructies te ontvangen over de te volgen procedures en te nemen acties.
- Na realisatie van de benodigde aanpassingen in de centrale systemen en het intern testen daarvan, dient de oplossing gevalideerd te worden tijdens een kopgroeptest met een aantal representatieve marktpartijen. Deze kopgroeptest wordt gecoördineerd door Het Normo en dient te



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

worden voltooid voor de start van de duale fase, om algemene inrichtingsproblemen en bevindingen in de centrale systemen op te lossen voordat overige marktpartijen hun G4-certificaten gaan testen en in gebruik nemen.

### 5.2.3 Bewaken van de voortgang van de implementatie en transitie, rapporteren aan het IISO daarover en het faciliteren van besluitvorming die nodig is voor implementatie. In geval van knelpunten kunnen in overleg met het IISO aanvullende maatregelen worden vastgesteld. Verantwoordelijkheden marktpartijen

- Marktpartijen die certificaten gebruiken, zijn zelf verantwoordelijk voor het tijdige voorbereiding, aanvraag, implementatie en ingebruikname van de nieuwe certificaten. Zij kunnen hierbij gebruik maken van de informatie die wordt verstrekt door de beheerders van de centrale systemen en Het Normo, maar zullen zelf een impactanalyse moeten uitvoeren op basis van hun specifieke systeemlandschap en inrichtingskeuzes.
- Marktpartijen dienen zelf de reguliere geldigheidstermijn van de huidige G1-/G3-certificaten te monitoren en indien nodig te verlengen. Het kan noodzakelijk of wenselijk zijn om de huidige certificaten nog vóór de start van de duale fase te verlengen, om te voorkomen dat deze aflopen voordat de implementatie van de G4-certificaten is voltooid.
- Topic TE014 heeft uitsluitend betrekking op het gebruik van PKIoverheidcertificaten voor gegevensuitwisseling met de centrale systemen van de systeembeheerders. Het gebruik van andere typen certificaten en het gebruik van PKIoverheidcertificaten voor andere doeleinden (zoals signing van e-mails of contracten en gegevensuitwisseling met andere instanties) vallen buiten scope van TE014. Marktpartijen zijn zelf verantwoordelijk voor het identificeren van eventuele impact die hieruit voortvloeit en het tijdig nemen van maatregelen.

## 5.3 Transitiemaatregelen

Er is transitie-impact. Dit betekent dat er extra maatregelen genomen moeten worden zodat de overgang van de oude situatie naar de nieuwe situatie in goede banen wordt geleid. De werkgroep heeft in onderstaande tabel de transitie maatregelen toegelicht.



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

| ID# | Issue / proces | Transitie effect | Doelstelling transitiemaatregel | Transitie maatregel | Aanvullende Requirements |
|---|---|---|---|---|---|
| 1 | Vernieuwen van lopende G1-certificaten | Looptijd van G1-certificaten kan eindigen tijdens de duale fase | Borgen van continuïteit van de gegevensuitwisseling tijdens de duale fase | Partijen onderzoeken zelf of verlenging van lopende G1-certificaten nodig is, en vernieuwen tijdig indien dit het geval is. | • Partijen inventariseren de einddatum van alle gebruikte G1-certificaten.<br>• Afhankelijk van de einddatum en het door hen geplande overstapmoment naar G4, vernieuwen partijen hun G1-certificaten indien nodig.<br>• Partijen houden daarbij rekening met de vernieuwingsvoorwaarden en -processen van de TSP (KPN). |
| 2 | Migratieplanning | Risico op te late start van de voorbereidingen door marktpartijen en/of pieken in het aanvragen van certificaten. | Inzicht krijgen in de migratieplanning van marktpartijen | Het Normo vraagt de test- en migratieplanning uit bij alle geraakte partijen | • Uitvraag van planning en status van impactanalyse, aanvraag trial-certificaten, bestellen certificaten bij TSP, testen en migratiemoment.<br>• De uitvraag wordt enkele keren herhaald om de voortgang van de voorbereidingen te monitoren.<br>• Resultaten worden besproken in het IISO. In overleg met het IISO kunnen aanvullende maatregelen worden vastgesteld. |
| 3 | Testen van G4-certificaten | G4-certificaten stellen andere eisen aan de gebruikte systemen en encryptie-algoritmes | Valideren van de werking van G4-certificaten om verstoringen in de gegevensuitwisseling tijdens de overstap te voorkomen | De beheerders van de centrale systemen stellen een testtool met trial-certificaten ter beschikking, waarmee partijen de technische werking van de G4-certificaten en de compatibiliteit van hun systemen kunnen testen. | • Beheerders van de centrale systemen stellen de testtool vóór aanvang van de kopgroeptest ter beschikking.<br>• De testtool is beschikbaar gedurende de gehele duale periode, waarbij het testen en releasen van andere wijzigingen gedurende de duale periode mogelijk blijven.<br>• Er wordt voldoende support georganiseerd om partijen te faciliteren bij het testen. |



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

| ID# | Issue / proces | Transitie effect | Doelstelling transitiemaatregel | Transitie maatregel | Aanvullende Requirements |
|---|---|---|---|---|---|
| 4 | Monitoren G4-adoptie | Risico op verstoringen wanneer partijen niet tijdig overstappen op G4-certificaten | Tijdig signaleren van risico's voor de continuïteit van de gegevensuitwisseling na 12 november 2028 | De beheerders van de centrale systemen rapporteren aan het IISO over het gebruik van de testtool voor trial-certificaten | • Beheerders van de centrale systemen van EDSN registreren het gebruik van trial-certificaten in de testtool gedurende de gehele duale fase.<br>• Beheerders rapporteren eens per twee weken over het aantal marktpartijen dat gebruik maakt van de testtool, en hoeveel partijen de test succesvol hebben afgerond.<br>• Werkgroep Transitie en het IISO monitoren actief op de voortgang en nemen aanvullende maatregelen indien nodig. |
| 5 | Monitoren G4-adoptie | Risico op verstoringen wanneer partijen niet tijdig overstappen op G4-certificaten | Tijdig signaleren van risico's voor de continuïteit van de gegevensuitwisseling na 12 november 2028 | De beheerders van de centrale systemen rapporteren gedurende de duale fase aan het IISO over het gebruik van G1- en G4-certificaten. | • De beheerders van de centrale DSB-systemen registreren de aanschaf van G4-certificaten (op basis van de validatie van de EAN-13 tijdens het bestelproces)<br>• De beheerders van de centrale systemen registreren het gebruik van zowel G1- als G4-certificaten gedurende de gehele duale fase, op zowel de acceptatietestomgeving als de productieomgeving.<br>• Beheerders rapporteren eens per twee weken over het aantal bestelde G4-certificaten.<br>• Beheerders rapporteren eens per twee weken over het aantal marktpartijen dat gebruik maakt van G1- en G4-certificaten (bijv. alleen G1 / zowel G1 als G4 / volledig over op G4). |



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

| ID# | Issue / proces | Transitie effect | Doelstelling transitiemaatregel | Transitie maatregel | Aanvullende Requirements |
|---|---|---|---|---|---|
| | | | | | • Werkgroep Transitie en het IISO monitoren actief op de voortgang en nemen aanvullende maatregelen indien nodig. |
| 6 | Afhankelijkheid met TSP voor aanschaf G4-certificaten | De G4-migratie leidt tot een groot aantal aanvragen voor G4-certificaten en bijbehorende supportvragen. | Afspraken met TSP over bestel- en supportprocessen, zodat marktpartijen goed geïnformeerd kunnen worden en certificaten tijdig kunnen worden aangevraagd en geleverd. | Maken van afspraken over procedures en doorlooptijden met de TSP. | • Werkafspraken tussen de TSP (i.e. KPN) en EDSN.<br>• Afstemming over verwachte planning en eventuele piekmomenten (op basis van uitgevraagde implementatieplanning).<br>• Opstellen van een FAQ.<br>• Het Normo kan ondersteunen via Voorlichting en communicatie aan marktpartijen. |



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

## 5.4 Verantwoording

Er is impact op de systemen van meer dan 1 marktrol.

**Bij het opstellen van een topic is het belangrijk om te bepalen of het topic in een release thuishoort en wat de implementatiestrategie is.**
**Op basis van onderstaande beslisboom kan de release-afhankelijkheid worden getoetst. Nadat bepaald is of er release-afhankelijkheid is kan de implementatiestrategie worden bepaald.**

| Vragen bij inschatting van releaseafhankelijkheid van topic: | | | Wat is de implementatiestrategie? (opties) | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | a | Big Bang (op 1 datum) | b | Duale periode | c | Onder water | |
| | | | a | Datum livegang | b | Begin- en einddatum | c | Vanaf datum | |
| **Is het release-afhankelijk?** | | | | | | | | | |
| 1 | Is er impact op de systemen van meer dan 1 marktrol? | **Ja** → | | | | X | | | |
| | **Nee** ↙ (ga naar 2) | | | | | | | | |
| 2 | Wijzigt er een bestaand bericht (bv aanpassing in attributen, een nieuw veld of nieuwe domeinwaarde) of komt er een nieuw bericht? | **Ja** → | | | | | | | |
| | **Nee** ↙ (ga naar 3) | | | | | | | | |
| 3 | Moeten de wijzigingen in de centrale en/of decentrale systemen getest worden door middel van een gebruikersacceptatietest door meer dan 1 marktrol? | **Ja** → | | | | | | | |
| | **Nee** ↙ (ga naar 4) | | | | | | | | |
| 4 | Vergt het topic een Market Readiness, voor voortgangsmonitoring, voor een succesvolle, gelijktijdige en gecontroleerde invoering? (indicatie: er is een vaste invoerdatum/deadline. Er wordt aangegeven dat er bv communicatie of voortgang monitoring moet worden ingeregeld.) | **Ja** → | | | | | | | |
| | **Nee** ↙ (ga naar 5) | | | | | | | | |
| 5 | Is er een transitieperiode nodig die meer dan 1 marktrol raakt? | **Ja** → | | | | | | | |
| | **Nee** | | | | | | | | |

Release-afhankelijk

Release-onafhankelijk (wel afstemming vereist)

**Nee** ↗ ↘



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

| | | | | |
|---|---|---|---|---|
| | Release onafhankelijk (geen afstemming vereist) | X? | X? | X? |

# 6 Te vervallen Topics (/ NEDU-issues)

Niet van toepassing.



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

# 7 Aanvullende informatie ten behoeve van lagere regelgeving

| Vraag | Antwoord |
|---|---|
| 1. Wat is de aanleiding voor de indiening van het codevoorstel en/of MR/AMvB en wat zijn de redenen die het voorstel noodzakelijk maken? | Niet van toepassing. |
| 2. Wat zijn de doelstellingen die met het codevoorstel en/of MR/AMvB worden nagestreefd en op welke wijze draagt het codevoorstel bij aan het verwezenlijken van die doelstellingen? | Niet van toepassing. |
| 3. Op welke wijze houdt het codevoorstel en/of MR/AMvB rekening met het belang van: | |
| *a. het betrouwbaar, duurzaam, doelmatig en milieuhygiënisch verantwoord functioneren van de energievoorziening?* | Niet van toepassing. |
| *b. de bevordering van de ontwikkeling van het handelsverkeer op de energiemarkt?* | Niet van toepassing. |
| *c. de bevordering van het doelmatig handelen van afnemers?* | Niet van toepassing. |
| *d. een goede kwaliteit van de dienstverlening van systeembeheerders?* | Niet van toepassing. |
| *e. een objectieve, transparante en niet discriminatoire handhaving van de energiebalans op een wijze die de kosten weerspiegelt?* | Niet van toepassing. |
| 4. Welke alternatieven zijn mogelijk en welke afweging is gemaakt bij de keuze tussen de alternatieven? | Niet van toepassing. |
| 5. Welke effecten heeft het codevoorstel en/of MR/AMvB voor netgebruikers, systeembeheerders en andere belanghebbenden? | Niet van toepassing. |
| 6. Is er samenhang met andere topicbeschrijvingen, (voorstellen voor) codes en/of MR/AMvB en Europese netcodes? En zo ja, welke? | Niet van toepassing. |



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

# 8 Privacy impact & toets

| Vraag | Antwoord << extra informatie>> |
|---|---|
| **Type project** | |
| 1. Is er sprake van het verwerken van persoonsgegevens? <1.1 NOREA> | Nee, in die zin dat het topic niet leidt tot het verwerken van meer of minder persoonsgegevens. Er is namelijk geen sprake van nieuwe of gewijzigde gegevensuitwisselingen. |
| 2. Is het duidelijk wie verantwoordelijk is voor de verwerking van gegevens? <1.2 NOREA> | N.v.t. |
| 3. Is het doel van de verwerking van persoonsgegevens voldoende SMART omschreven? <1.5 NOREA> | N.v.t. |
| **De gegevens** | |
| 4. Zijn alle gegevens nodig om het doel te bereiken (worden er zo min mogelijk gegevens verzameld)? <2.1 NOREA> | N.v.t. |
| 5. Kan het doel met geanonimiseerde of gepseudonimiseerde gegevens worden bereikt (terwijl daar op dit moment geen gebruik van wordt gemaakt?) <2.2 NOREA> | N.v.t. |
| **Verzamelen van gegevens** | |
| 6. Verzamelt u de gegevens op basis van een van de wettelijke grondslagen? <4.3 NOREA> | N.v.t. |
| 7. Is duidelijk of u de gegevens verzamelt op basis van opt-in (verzameling uitsluitend als de betrokkene daarvoor toestemming heeft gegeven) of op basis van opt-out (verzameling tenzij de betrokkene daartegen bezwaar heeft gemaakt)? <4.4 NOREA> | N.v.t. |
| **Gebruik van gegevens** | |



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

| Vraag | Antwoord << extra informatie>> |
|---|---|
| 8. Is het gebruik van de gegevens verenigbaar (in lijn) met het doel van het verzamelen? <5.1 NOREA> | N.v.t. |
| **Bewaren en vernietigen** | |
| 9. Is een bewaartermijn voor de gegevens vastgesteld? <6.1 NOREA> | N.v.t. |
| 10. Kunnen de gegevens na afloop van de bewaartermijn fysiek worden verwijderd (uit een bestand) of vernietigd (papier)? <6.2 NOREA> | N.v.t. |
| 11. Zo ja, worden de gegevens na verstrijken van de bewaartermijn op zo'n manier vernietigd of verwijderd dat ze niet meer te benaderen zijn en te gebruiken zijn? <6.2.1 NOREA> | N.v.t. |



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

# 9 Security impact & toets

De volgende vragen moeten worden beantwoord om de niet-functionele requirements t.a.v. de security, technische impact en overige te verduidelijken. Dit is belangrijke input voor de Topic Architectuur.

| Vraag | | Antwoord met korte toelichting |
|---|---|---|
| 1. | **Is er sprake van een nieuw of gewijzigd marktproces en/of gegevensuitwisseling (in een marktproces) en/of bericht (in een gegevensuitwisseling)?**<br>Zo ja, beschrijf wat er functioneel/inhoudelijk nieuw of gewijzigd is op niveau van proces, gegevensuitwisseling (bijv. nieuwe berichten) en/of berichten (bijv. nieuwe entiteiten of attributen). | Nee |
| 2. | **Beschrijf de nieuwe of gewijzigde niet-functionele kenmerken van het proces, de onderliggende gegevensuitwisseling, en/of de berichten:**<br>1. de omvang van het (de) bericht(en), een indicatie van het aantal attributen per entiteit, aantal entiteiten per bericht (overigens hebben kleinere berichten de voorkeur boven grotere berichten)<br>2. de aantallen / frequentie (aantallen per tijdseenheid) van het (de) bericht(en), beschrijf ook of er verwachte pieken of periodes met verhoogde of verlaagde aantallen zijn<br>3. de tijdskritischheid van het (de) bericht(en), beschrijf ook of er bepaalde momenten zijn waarop de tijdskritischheid hoger is dan andere momenten<br>4. de systematiek van de gegevensuitwisseling: a) pull of b) push.<br>a. **pull**: de partij die het gegeven nodig heeft vraagt deze op bij de partij die dit gegeven heeft (ook wel request-reply-receive)<br>b. **push**: de partij die het gegeven maakt/wijzigt stuurt deze naar de partij(en) die dit gegeven (mogelijk) nodig heeft (ook wel message-publish-subscribe). | N.v.t. |
| 3. | **Beschrijf ook of en hoe de belangen van een (direct of indirect betrokken) stakeholder veranderen en of er een verandering optreedt in de potentiële schade die verbonden is aan mogelijke fouten aan dit proces.**<br>Geef een indicatie hoog/midden laag op basis van de TABEL 1 BIV Classificatie Kolom 2: Schade. | N.v.t. |
| 4. | **Beschrijf de eisen aan die worden gesteld aan de beschikbaarheid (of continuïteit) van het proces (en de resulterende gevolgen voor de tijdigheid), de onderliggende gegevensuitwisseling, de berichten en de gegevens.**<br>• In welke mate moet de informatie beschikbaar en toegankelijk zijn.<br>• Classificatie gaat in op de mogelijke gevolgen als informatie, of een informatie set, niet beschikbaar is. Geef een indicatie hoog/midden/laag op basis van TABEL 1 BIV Classificatie Kolom 3: Beschikbaarheid. | N.v.t. |



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl

| | | |
|---|---|---|
| 5. | **Beschrijf de eisen aan die worden gesteld aan de integriteit (of betrouwbaarheid) van het proces (en de resulterende gevolgen voor de juistheid, actualiteit en volledigheid), de onderliggende gegevensuitwisseling, de berichten en de gegevens.**<br>• In welke mate moet de informatie in overeenstemming zijn met de werkelijkheid (juist, volledig en actueel).<br>• In welke mate is beheer van bevoegdheden en mogelijkheden tot muteren, toevoegen, of vernietigen van gegevens voor een gedefinieerde groep gerechtigden vereist<br>• Classificatie gaat in op de mogelijke gevolgen wanneer informatie onjuist, onvolledig of niet actueel is. Geef een indicatie hoog/midden/laag op basis van TABEL 1 BIV Classificatie Kolom 4: Integriteit. | N.v.t. |
| 6. | **Beschrijf de eisen aan die worden gesteld aan de vertrouwelijkheid van het proces, de onderliggende gegevensuitwisseling, de berichten en de gegevens.**<br>• In welke mate is beheer van bevoegdheden en mogelijkheden om kennis te nemen van informatie voor een gedefinieerde groep gerechtigden vereist.<br>• Classificatie gaat in op de mogelijke gevolgen wanneer informatie in handen komt van derden die hiertoe niet zijn geautoriseerd. Geef een indicatie hoog/midden/laag op basis van TABEL 1 BIV Classificatie Kolom 4: Vertrouwelijkheid. | N.v.t. |
| 7. | **Beschrijf de resulterende BIV-classificatie** (bijvoorbeeld: L-M-M of M-H-H)<br>• Houdt hierbij rekening met de evt. verwerking van persoonsgegevens en de verplichtingen die daaruit volgen vanuit de AVG; deze kunnen leiden tot hogere eisen aan de bescherming van met name de vertrouwelijkheid en de integriteit. | N.v.t. |
| 8. | **Beschrijf of en welke procedurele, niet-geautomatiseerde maatregelen worden genomen in het proces** om de potentiële schade te beperken, en de beschikbaarheid (c.q. tijdigheid), integriteit (c.q. juistheid en volledigheid), vertrouwelijkheid en privacy te beschermen. | N.v.t. |
| 9. | **Beschrijf of en evt. welke additionele (IT) securitymaatregelen getroffen zouden moeten worden op dit proces/gegevensuitwisseling/berichten** om de potentiële schade te beperken, en de beschikbaarheid (c.q. tijdigheid), integriteit (c.q. juistheid en volledigheid), vertrouwelijkheid en privacy te beschermen. | N.v.t. |



Beheerder Afsprakenstelsel (BAS) B.V.
Van Asch van Wijckstraat 55
3811 LP Amersfoort
KvK: 84811439
www.mffbas.nl