[redacted]

20

equensWorldline SE

ATOS Nederland

Loket wet GDI

[redacted]

Subject

Internetconsultatie wet GDI en toelichting set van eisen

[redacted]

[redacted]geachte leden,

Met belangstelling hebben wij kennis genomen van uw voorstellen in het kader van de voorgestelde wet GDI. Naar aanleiding van deze wetvoorstellen hebben wij in het kader van de rol van ontsluitingsdienst de volgende vragen, opmerkingen en kanttekeningen. Wij verzoeken u hier aandacht aan te schenken in de nadere uitwerking van de wet en regelgeving.

1) De uniforme set van eisen bevat de eisen voor deze publieke en private authenticatiemiddelen. Deze eisen worden gesteld aan de rollen (partijen) die worden onderscheiden in de keten. De rollen waarvoor erkenning noodzakelijk is zijn:

- Authenticatiedienst
- Middelenuitgever
- Toegangsdienst

Overige rollen zijn

- Dienstverlener
- Ondersteunende rollen, zoals BSNk .

De laatste rollen vallen niet onder de noemer van participant in het domein wet GDI waardoor onduidelijk is in welk domein deze wel behoren.

2) De wet maakt een ander onderscheid in terminologie en definitie wat de regeling en toelichting onduidelijk maakt. Volgens de definitielijst in de regels inzake de generieke digitale infrastructuur worden de volgende partijen onderscheiden:

- Attributendienst
- Authenticatiedienst
- Elektronische dienstverlener
- Machtigingen dienst
- Ontsluitingsdienst (etc)

Daarnaast is sprake van "bestuursorganen" en "aangewezen organisaties" in de rol van dienstverlener. Er is daarmee onduidelijkheid in de rolbeschrijving en de definitie van deze partijen waardoor zij te weinig weten wat van hen wordt verwacht. Het advies is om in de wet en de toelichting uniformiteit aan te brengen in rolomschrijving en wat van partijen wordt verwacht.

3) Volgens de toelichting die is opgenomen in de uniforme set van eisen, versie 1.0, zou een authenticatiemiddel meerdere statussen kunnen krijgen en zou volgens de wet, artikel 13, een dienst op enig moment kunnen worden geschorst. De mogelijke gevolgen die een schorsing van een authenticatiemiddel heeft op de al geleverde diensten door de dienstverlener met het betrokken authenticatiemiddel is niet eenduidig terug te vinden in de toelichting bij het wetsontwerp. Een nadere uitwerking is te meer van belang indien sprake is van een transactie (overeenkomst) op basis van de uitgevoerde identificatie zoals aangegeven in de toelichting. Wellicht kan hier een nadere uitwerking aan worden gegeven en de finaliteit te definiëren voor transacties die met het identificatiemiddel worden afgesloten. Dit zou duidelijkheid moeten geven wanneer transacties wel of niet geldig zijn na een schorsing.

4) In de wet wordt meerdere keren gesproken over aanvullende eisen krachtens algemene maatregelen van bestuur. Evenals in de uniforme set van eisen vinden nog aanvullingen plaats op deze set van eisen, wat een succes van een generieke digitale infrastructuur in de weg kan staan. Het is voor de deelnemers nog onvoldoende duidelijk waaraan zij nu moeten voldoen in de nabije toekomst. Bijvoorbeeld ten aanzien van:

- Verwerking van persoonsgegevens door de partijen
- Uitwerking van de overige rollen genoemd in de uniforme set van eisen
- Toezicht en handhaving en de verstrekking van informatie
- De openbaarheid van deze informatie
- Eisen op het gebied van monitoren van misbruik en fraudebestrijding.

Het is van belang dat de betrokken deelnemers ook voldoende worden gekend in de voorstellen en wijzigingen en het borgen van een "equal-level-playing field" voor de participanten in Europa. Het Artikel 22 voorziet alleen in een evaluatie binnen 5 jaar na de inwerkingtreding waarbij in het ongewisse blijft op welke wijze de participanten in het stelsel worden betrokken in de evaluatie.

5) Zoals aangegeven is het onderscheid in alle rollen binnen de voorgestelde wetgeving nog onduidelijk. Wij bevelen aan om te kijken naar een 3 -lagen model zoals binnen het betalingsverkeer gebruikelijk is, met sectoraal toezicht en een eenduidige onderverdeling tussen rollen en verantwoordelijkheden van wetgever, afsprakenstelsels en deelnemers daarbinnen. Zo kan voorkomen worden dat de minister kosten afwendt aan private partijen en tegelijkertijd een prijsstelling oplegt, wat marktverstorend werkt.

6) De wet GDI en Uniforme set van Eisen zijn gericht op het uitwerken en voorschrijven van (technische) regels (oplossingen) om het gedag te beïnvloeden. Het is aan te bevelen een meer "principle based" benadering te volgen zodat de focus op relevante principes wordt gezet waarmee bestaande en nieuwe diensten doorontwikkeld kunnen worden.

De technische eisen voor koppelvlak en toegangsdienst zijn zeer specifiek (rule-based). Hierdoor is er geen ruimte voor het innoveren en ontwikkelen van mogelijke betere technische oplossingen. Onder "principle based" wordt verstaan het opnemen van "doelstellingen" waaraan dient te worden voldaan. Als voorbeeld: polymorphe encryptietechniek is zeker niet de enige privacy oplossing en gaat niet uit van neutrale technologiestandaarden. Daarnaast is het geen proven technologie en werkt het kostenverhogend. We bevelen aan om uit te gaan van een open principle based model waarbij de technologie niet wordt opgelegd. Dit is tevens in lijn met de eIDAS regelgeving waar ook geen technologische standaard wordt opgelegd.

7) De wet GDI en Uniforme set van Eisen is nu vooral gericht op de publieke domein in Nederland met specifieke oplossingen en technische eisen voor de deelnemers. Wij bevelen aan aandacht te geven aan het "equal-level-playing field" voor de deelnemers in het voorgestelde wet en regelgeving ten opzichte van de wet en regelgeving voor de authenticatiestelsels elders in Europa. De vastgestelde specifieke en technische oplossingen blokkeren wellicht de deelnemers om eenvoudig en succesvol deel te nemen in meerder stelsel op termijn en het nieuwe stelsel.

8) In de memorie van toelichting op de wet wordt in sectie 4.6 beschreven dat:

Met behulp van zogeheten PKIoverheid-certificaten (public key infrastructure) kunnen websites worden

geïdentificeerd en kan het verkeer met deze websites worden beveiligd. Ook kan met PKIoverheid

informatie-uitwisseling van systeem naar systeem worden beveiligd en kunnen gekwalificeerde elektronische handtekeningen worden gezet. Daarnaast kunnen personen zich met een middel waarvoor het PKIoverheid-certificaat is afgegeven, authenticeren op systemen. Een dergelijke middel zou, indien wordt voldaan aan de in en krachtens dit wetsvoorstel gestelde eisen, de status van erkend middel kunnen verkrijgen."

In de WGDI noch in de eIDAS is dit verder opgenomen of uitgewerkt. Daarmee is het niet duidelijke of een provider van PKI certificaten een authenticatieprovider kan worden of als attribuut provider optreden.

9) Het is niet duidelijk hoe de overheid wil omgaan met een onbeperkt aanbod van gecertificeerde identificatie en authenticatie providers en ontsluitingsdiensten. Om de Europese integratie te bespoedigen en het aantal private diensten te beperken tot internationale leveranciers zou een keuze gemaakt kunnen worden om alleen private partijen te accepteren die én gecertificeerd zijn volgens de regels van WGDI én EiD én geaccepteerd zijn door de EU na aanmelding door Nederlandse overheid conform artikel 9 van de eIDAS verordening. Hierdoor moet dit middel dan ook geaccepteerd worden door alle andere Europese overheden.

Indien dat niet gedaan wordt is er geen limiet aan het aantal te accepteren erkende middelen. Voor kleinere overheidsorganisaties is dat een model wat dan ook ongelimiteerde kosten met zich mee kan brengen. Iedere nieuwe organisatie zou de acceptatie kunnen afdwingen bij een rechter.

10) In de wet en de toelichting is niet duidelijk gemaakt op welke wijze er voor een private partij een verdienmodel mogelijk is. De kosten worden door de overheid afgewenteld op de dienstverleners en vanuit eIDAS-wetgeving mogen aan een gebruiker van een Europees geaccepteerde dienstverlener (zoals bedoeld onder artikel 9 van de eIDAS-verordening) geen kosten worden doorberekend. Daarnaast worden door de overheid op dit moment geen kosten in rekening gebracht voor DigiD en is ook niet aangegeven dat dit voor de opvolgers het geval zal zijn. Hierdoor verstoort de overheid de private markt voor het gebruik van private middelen voor toegang tot overheidsdiensten en zal het gebruik van private middelen voor deze doeleinden niet zomaar van de grond komen door de prijsconcurrentie. Een mogelijk verdienmodel is het gebruik van reclame-inkomsten op de eID middelen en in de portaalfuncties voor het gebruik van deze middelen. Het is mogelijk onwenselijk voor de overheid om te worden geconfronteerd met marketing uitingen die tegen het overheidsbeleid voor bv de gezondheid ingaan.

11) In Nederland is er één provider die ook de controle bij de dienstverleners afdwingt door middel van DigiD-audits en de resultaten hiervan controleert. In de nieuwe situatie kunnen er in een controleperiode meerdere providers (zowel publiek als privaat) worden toegevoegd. Dient dan per

applicatie-interface een nieuw rapport te worden toegevoegd? Nu is er met de samenwerking met NOREA de eis bepaald dat er alleen RE auditors de rapportage mogen ondertekenen. Dat is een strikt Nederlandse eis die niet in lijn is met de andere landen binnen de EU waarvan Nederland de middelen wel moet accepteren indien aangemeld onder artikel 9 van de eIDAS-verordening. Wij bevelen aan dat dan ook CISA-auditors kunnen worden ingeschakeld en dat gekeken wordt dat er een onafhankelijke toezichthouder komt.

Wij verzoeken u de beschreven punten te betrekken in de uitwerking van de voorgestelde wet GDI en uniforme set van eisen voor de volgende fases van het programma eID. Indien wenselijk kunnen wij een toelichting op de punten en aanbevelingen geven.

[redacted]

equensWorldline SE en ATOS Nederland BV

[redacted]