(19)

DNB-INTERN

DeNederlandscheBank
EUROSYSTEEM

Toezicht beleid
Algemeen beleid en governance

Onderwerp:
Standpunt DNB m.b.t. Wetsvoorstel Generieke Digitale Infrastructuur (Wet GDI)

1. Wet GDI op hoofdlijnen

Het wetsvoorstel voorziet (op hoofdlijnen) in:

(1) een stelsel van erkenningen door de minister van BZK van onder andere *authenticatiediensten* en de door publieke en private partijen aangeboden authenticatiemiddelen;
(2) de aan erkende partijen te stellen uniforme set van eisen m.b.t. de werking, beveiliging en betrouwbaarheid van de door erkende partijen verleende diensten, inclusief een uniforme set van eisen waaraan de authenticatiediensten en authenticatiemiddelen dienen te voldoen;
(3) toezicht op de naleving van de Wet GDI door het Agentschap Telecom,

Authenticatie in het private domein (bijvoorbeeld webwinkels) valt niet binnen de werkingssfeer van de Wet GDI. De Nederlandse banken vallen dus uitsluitend binnen de werkingssfeer van de Wet GDI wanneer zij opteren voor de mogelijkheid van het aanbieden van authenticatie d.m.v. iDIN [1] in het publieke domein.

We spreken in deze nota over banken. Dat is gezien de huidige situatie terecht. Echter, het valt niet uit te sluiten dat ook andere financiële ondernemingen met een vergunning van DNB – bijvoorbeeld (zorg)verzekeraars – in de toekomst ook een authenticatiedienst gaan aanbieden, en die ook wordt aangeboden voor gebruik in het publieke domein. Voor die sectoren is alsdan de in deze nota besproken casuïstiek van overeenkomstige toepassing.

Datum
13 maart 2017

Kenmerk
2017/122081

Kopie

[1] Het authenticatiemiddel iDIN is een dienst van de Nederlandse banken, aangesloten bij de Betaalvereniging Nederland, waarmee hun klanten zich bij andere instellingen zoals verzekeraars en webwinkels en bij overheidsinstanties, zoals de belastingdienst, online kunnen *identificeren* (iemand geeft aan wie hij/zij is) en *authentiseren* (vaststellen dat hij/zij ook daadwerkelijk de persoon is zoals hij/zij zegt) door gebruik te maken van de inlogmiddelen van hun eigen bank. Een dergelijke dienst wordt in de Wet GDI als authenticatiedienst gedefinieerd.

2. Inrichting van het toezicht – sectorale overlappingen

Toezicht van de Minister van BZK en van het Agentschap Telecom op de naleving van de Wet GDI door de Nederlandse banken (authenticatiediensten) i.v.m. het door hen gezamenlijk aangeboden *authenticatiemiddel* iDIN, leidt in beginsel tot dubbel toezicht. Dit omdat ook de ECB (rechtstreeks voor de significante banken), alsmede DNB op grond van haar toezichttaak ingevolge de Wft, onderscheidenlijk haar oversight taak ingevolge de Bankwet 1998, toezicht/oversight uitoefenen op het door de Nederlandse banken aangeboden authenticatiemiddel iDIN als onderdeel van de bedrijfsuitoefening van de banken gericht op het waarborgen van de goede werking van het betalingsverkeer.

Aan dat toezicht en oversight liggen Europese regelingen ten grondslag, in casu:

- de richtlijn en verordening kapitaalvereisten, met vergaande bevoegdheden voor de ECB, de (herziene) richtlijn betaaldiensten, de (vierde) anti-witwasrichtlijn;
- de op die richtlijnen gebaseerde Europese regelgeving in de vorm van verordeningen, technische standaarden - onder andere de RTS on strong customer authentication and secure communication - en door de EBA opgestelde richtsnoeren - onder andere de Richtsnoeren van EBA met betrekking tot het beheersen van de operationele risico's en de beveiligingsrisico's onder de herziene richtlijn betaaldiensten), alsmede
- de eIDAS verordening en de daarop gebaseerde verordeningen, en de overige internationaal gangbare standaarden, daaronder de PCIDSS standaard (Payment Card Industry Data Security Standard), een internationale beveiligingsstandaard, opgesteld door de diverse betaalkaart maatschappijen, die wereldwijd wordt toegepast.

De overlap van het toezicht ziet op de erkenning en op het doorlopend toezicht:

(1) De erkenning door de Minister van BZK m.b.t. iDIN van de *authenticatiedienst(en)* - elk van de banken afzonderlijk die gezamenlijk iDIN aanbieden - en van het aangeboden *authenticatiemiddel* iDIN, die afhankelijk is van de naleving van de vereisten ingevolge de Wet GDI; en

(2) Het doorlopend toezicht op de banken in hun hoedanigheid als authenticatiedienst en het door hen aangeboden authenticatiemiddel iDIN op de naleving van de vereisten ingevolge de Wet GDI.

Erkenning van een middel of een dienst door de Minister van BZK ziet op de bij amvb ingevolge artikel 7 Wet GDI te stellen eisen m.b.t. de werking, beveiliging en betrouwbaarheid van dat middel of die dienst. Deze eisen zijn op dit moment nog niet uitgewerkt, uitgezonderd de 1.0 versie van de Uniforme set van standaarden voor authenticatiemiddelen. In de Memorie van Toelichting is benadrukt dat voorzien zal worden in gelijkluidende (uniforme) eisen waaraan authenticatiediensten en de door hen aangeboden authenticatiemiddelen moeten voldoen. De versie 1.0 van de (zogeheten) Uniforme set van standaarden voor authenticatiemiddelen is daar een eerste proeve van.

In de MvT van de Wet GDI is verwoord dat de Minister van BZK beslist over erkenningen, daarin geadviseerd door het Agentschap Telecom en dat het in de rede ligt het Agentschap telecom te belasten met het doorlopend toezicht.

Indien de Nederlandse banken willen dat iDIN ook als authenticatiemiddel voor het publieke domein mag worden gebruikt, dan zullen zij zich moeten onderwerpen aan het toezicht ingevolge de Wet GDI.

3. Standpunten DNB m.b.t. opzet en reikwijdte consultatieversie Wet GDI

3.1 **Voorkomen van dubbel toezicht** - dubbel toezicht op private authenticatiediensten en middelen (banken, iDIN), door het Agentschap Telecom ingevolge de Wet GDI enerzijds en door DNB ingevolge de Wft én de Bankwet 1998 anderzijds, kan worden voorkomen als;

- **Banken worden uitgezonderd van het ingevolge artikel 7 Wet GDI bepaalde**: bij of krachtens artikel 7 Wet GDI zou moeten worden voorzien in een uitzondering van het bij en krachtens dat artikel bepaalde voor erkende authenticatiediensten die voor de uitoefening van het bedrijf van bank een door de Europese Centrale Bank of de Nederlandsche Bank verleende vergunning hebben;

- **Niet uniforme eisen, maar equivalente eisen uitgangspunt zijn van de Wet GDI**: het uitgangspunt van de Wet GDI dat de authenticatiediensten en de door hen aangeboden authenticatiemiddelen moeten voldoen aan *gelijkluidende (uniforme) eisen,* zou moeten worden veranderd in: *equivalente (gelijkwaardige) eisen.* Voorwaarde voor erkenning als bedoeld in artikel 7 Wet GDI is dan dat de onder het eerste gedachtestreepje bedoelde banken voldoen aan de equivalente eisen ingevolge de Bankwet 1998 / Wft;

- **Wordt afgezien van een <u>exclusieve</u> toezichttaak van het Agentschap Telecom:** in de memorie van toelichting, paragraaf 4.8 (Erkenning van authenticatiemiddelen en partijen) zou ruimte moeten worden gelaten voor betrokkenheid van andere toezichthoudende instanties dan het Agentschap Telecom bij de beoordeling of de aanvrager aan de eisen ingevolge de Wet GDI voldoet. In casu kan dat DNB zijn die op verzoek van de Minister van BZK beoordeelt of een authenticatiedienst als bedoeld onder het eerste gedachtestreepje voldoet aan eisen die equivalent zijn aan de bij of krachtens artikel 7 Wet GDI gestelde eisen;

- **Wordt afgezien van doorlopend toezicht ingevolge art. 10 Wet GDI op banken:** voor erkende authenticatiediensten die voor de uitoefening van het bedrijf van bank een door de Europese Centrale Bank of DNB verleende vergunning hebben, kan voor de realisatie van de doeleinden van de Wet GDI worden volstaan met toezicht door DNB ingevolge de bestaande voor banken geldende regelgeving; en

- **Wordt voorzien in een (Wft) grondslag voor de uitwisseling van informatie:** met het oog op het verlenen van erkenningen (artikel 6 Wet GDI) en het mogelijk schorsen of intrekken van erkenningen (artikel 13), moet DNB bevoegd zijn om informatie uit te wisselen met degene die belast is met het toezicht ingevolge de Wet GDI voor zover het banken betreft. **Onderzocht moet nog wel of een dergelijke uitwisseling van informatie mogelijk is onder de huidige voor banken geldende Europese richtlijnen – de authenticatiedienst (middel + proces) treft immers een belangrijk en geïntegreerd deel van de organisatie van een bank en de inrichting van de bedrijfsprocessen.**

3.2 Vereisten voor erkenning transparant (in de wet) en gebaseerd op het equivalentieprincipe:

In het eerste lid van artikel 7 is bepaald dat een erkenning wordt verleend als de authenticatiedienst en het middel voldoen aan de voor die dienst en dat middel bij of krachtens het eerste en tweede lid van dat artikel gestelde eisen. Niet gespecificeerd wordt in het wetsvoorstel zelf wat de aard is van die eisen. Het ware te overwegen om in artikel 7 de vereisten voor erkenning principle based uit te werken, zodat de begrenzing van het toezichtraamwerk in de wet zelf wordt bepaald en niet in lagere regelgeving.

3.3 Geen uniforme set van eisen, maar een equivalente set van eisen:

Het ware te overwegen om voor het publieke domein niet te streven naar een uniforme set van eisen. De versie 1.0 van de Uniforme Set van Eisen (versie 15-12-2016) is een rule based uitwerking van de regels en standaarden, genoemd in paragraaf 2, waaraan ook de banken in het publieke domein zullen moeten voldoen. Met betrekking tot banken (iDIN) worden de Europese vereisten (eIDAS) die aan de Uniforme Set van Eisen ten grondslag ligt, binnen het domein van DNB (de Wft en de Bankwet 1998) echter principle based toegepast, en dat is ook in andere Europese landen het geval, waaronder sommigen - Italië, Slovenië en Finland – niet verder gaan dan de regelgeving ingevolge eIDAS. En mogelijk worden er nog toezichtkaders ontwikkelt door de ECB in dezen.

Een rule based benadering draagt daarom het risico in zich niet technologie- neutraal te zijn en op gespannen voet te staan met een benadering gericht op het realiseren van een gelijk speelveld in Nederland, maar ook in Europa. Het ware daarom te overwegen authenticatiediensten niet te confronteren met een rule based uniforme set van eisen, maar de eisen principle based te baseren op meergenoemde Europese en internationaal gangbare vereisten.