notarisid

aan Ministerie Binnenlandse Zaken en Koninkrijksrelaties
Alexandra C. van Huffelen
Staatssecretaris Digitalisering en Koninkrijksrelaties

NotarisID B.V.

Hogewilweg 6
1101 CC Amsterdam

datum 05/12/2022
onderwerp Internetconsultatie Regeling nadere eisen eID's
kenmerk Intertnetconsultatie/NID/1
bijlage(n) (geen)

kvk 76121526
btw NL860514924B01
bank NL12 INGB 0007 2870 26

Excellentie,

NotarisID B.V. (hierna te noemen "NotarisID of wij") heeft met genoegen kennis genomen van de Regeling nadere eisen identificatiemiddelen, authenticatiediensten en machtigingsdiensten Wdo (hierna te noemen "Concept-regeling of Regeling")[1]. Met deze brief vraagt NotarisID uw aandacht voor enkele knel- en zorgpunten met betrekking tot kardinale thema's zoals geregeld in de Concept-regeling, te weten: certificering, open source, verzekerbaarheid en eIDAS-notificatie. Hieronder zetten we onze zorgen en verzoeken uiteen en vragen wij u in de definitieve Regeling de knel- en zorgpunten weg te nemen.

1 Certificering

In artikel 9 lid 5 Wdo[2] wordt gesteld dat bij de aanvraag voor een erkenning een verklaring wordt gevoegd van een geaccrediteerde certificerende instelling, waaraan het vermoeden kan worden ontleend dat is voldaan aan de eisen die gelden voor de betreffende houder van de erkenning van dat middel. In de AMvB worden in artikel 9 eisen gesteld aan een verklaring van certificering, inhoudende dat de verklaring is afgegeven door een instelling die is geaccrediteerd door een nationale accreditatie-instantie als bedoeld in verordening (EG) nr. 765/2008[3] en de verklaring[4] ziet op het identificatiemiddel waarvoor

[1] Regeling van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties [PM] 2022, nr CZW/S&B/…., houdende nadere eisen en regels voor het verlenen van een toelating voor publieke en private identificatiemiddelen (Regeling nadere eisen identificatiemiddelen, authenticatiediensten en machtigingsdiensten Wdo)

[2] Algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur

[3] in artikel 2, onderdeel 11, van de verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EG) nr. 339/93 (PbEU 2008, L 218).

[4] als bedoeld in het eerste lid

de erkenning wordt aangevraagd en de conformiteit van de systemen en processen die daarvoor worden gebruikt met de eisen voor het betrouwbaarheidsniveau waarop de aanvraag ziet.[5] ***In artikel 2.2 Concept-regeling ziet NotarisID echter staan dat enkel een ISO 27001 certificaat vereist wordt. Dit is wat ons betreft te beperkt.***

Zowel door de Minister als in de toelichting bij de AMvB[6] is gezegd dat gekwalificeerde vertrouwensdienstverlener die in het bezit zijn van ETSI-certificeringen zoals ETSI 319 411-2 al de nodige waarborgen hebben voor het kunnen bieden van elektronische identificatiemiddelen waardoor zij minder voorbereidingskosten hebben. In de toelichting bij de AMvB is het als volgt geformuleerd:

> *"Het bezit van een ISO/IEC 27001-certificaat met betrekking tot informatiebeveiliging of een ETSI 319 403-certificaat met betrekking tot de uitgifte van gekwalificeerde certificaten kan de* ***additionele kosten*** *voor de erkenning van een dienst verlagen. De verlaging is mogelijk op voorwaarde dat de operationele infrastructuur waarop de te erkennen dienst draait in zijn geheel of deels in de scope van het genoemde certificaat is opgenomen.*
> *Een ISO/IEC 27001-certificaat is in beginsel passend voor alle te erkennen partijen en diensten. Een ETSI-certificaat 319-411-2 zal doorgaans alleen in bezit zijn van een partij die zich als middelenuitgever en authenticatiedienst wil laten erkennen omdat de uitgifte van een gekwalificeerd certificaat veel overeenkomsten heeft met de uitgifte van een elektronisch identificatiemiddel.* ***De wijze waarop de omvang van de audits voor erkenning bepaald worden door de certificerende conformiteit-beoordelende instantie zijn vergelijkbaar met de wijze waarop dit voor ETSI-audits wordt bepaald.****"*[7]

NotarisID verzoekt u - in lijn met de toelichting bij de AMvB en toezegging - voor de duidelijkheid in de Regeling op te nemen dat partijen die reeds in het bezit zijn van een ETSI 319 411-2 (in combinatie met ETSI 319 411-1 en ETSI 319 401, daar die door middel van inclusie meegenomen zijn in het conformiteitsbeoordelingsverslag van de geaccrediteerde instelling) met het certificaat en de verkregen gekwalificeerde status van Agentschap Telecom aantoonbaar kunnen maken dat ze aan de regels zoals bedoeld onder artikel 9 Wdo voldoen.

Volledigheidshalve verwijst NotarisID hier ook naar het werkdocument[8] van ETSI, in het kader van herziening eIDAS, waarin wordt opgemerkt dat ETSI 319 411-1 en 319 411-2 goede standaarden zijn voor nationale eID-stelsels. Daarin zegt men het volgende over onder meer ETSI 319 411 delen 1 en 2:

> *"[…] The security requirements for the issuing of attribute attestation can use the existing general practices for the security of trust services, in EN 319 401, as well adapt existing standards for issuing of certificates in EN 319 411 parts 1 and 2.* ***These standards could also be adopted as the basis of national schemes issuing electronic identification means.****"*

[5] Zoals gesteld in artikel 3, 4 en 21 en krachtens artikel 5

[6] Besluit identificatiemiddelen voor natuurlijke personen Wdo

[7] Nota van toelichting Besluit identificatiemiddelen Wdo

[8] ETSI SR 019 003

2 Open source

In de Concept-regeling wordt gesuggereerd dat publicatie van de broncode van software de transparantie en het vertrouwen in de gepubliceerde software en betrouwbaarheid van de maker van de software verhoogt. In de beide algemene maatregelen van bestuur is geregeld dat een erkenning slechts wordt verleend indien voor bepaalde bij ministeriële regeling aangewezen componenten software wordt gebruikt die is gepubliceerd[9] onder een open source licentie, of waarvan de broncode is gepubliceerd. NotarisID merkt preliminair op dat in de AMvB en de toelichting de woorden “publiceren”, “open source”, “openbare broncode” en “beschikbaar maken” door elkaar en incorrect worden gebruikt, zonder ogenschijnlijk semantisch en juridisch verschil. Het verdient de aanbeveling dat open source en de daarbij behorende begrippen consistent(er) worden toegepast. Wij verwijzen hierbij ook naar de terechte Kamervragen over de inconsistente terminologie, interpretatie en toepassingen van open source.[10]

De uitwerking van de open source eis is eveneens inconsistent en moeilijk te rijmen met andere belangen, onder andere belangen die voortvloeien uit en samenhangen met de eIDAS-verordening. In antwoord op Kamervragen over de open source eis formuleert de regering het doel als volgt:

> *“De regering ziet zoals gezegd derden die de gepubliceerde broncode kunnen onderzoeken, waardoor de leverancier de code beter kan onderhouden en verbeteren, als een belangrijke aanvullende waarborg voor de veiligheid. Immers, zo wordt gedacht, hoe groter en sterker de gemeenschap hoe groter de kans dat onverhoopte veiligheidsproblemen aan het licht komen voordat kwaadwillenden er gebruik van (kunnen) maken. Het vermeende voordeel van het meer-ogenprincipe, het bereiken van meer veiligheid doordat iedereen kan meekijken, wordt immers groter als de gemeenschap groter is. Andere vermeende voordelen die zich d.m.v. open source manifesteren zijn een groter publiek vertrouwen in het middel, het verlagen van de drempels tot samenwerking en het bevorderen van interoperabiliteit.”*

Allereerst merkt NotarisID op dat in de toelichtingen staat dat het aanwijzen van open source componenten geschiedt op basis van het “open, tenzij”- principe, terwijl relevante belangen worden meegewogen. Echter, NotarisID ziet in de Concept-regeling niet terug welke belangen voor private aanbieders worden meegewogen en derhalve cruciaal kunnen zijn. NotarisID is van mening dat voor een adequaat en coherent open source beleid van belang is dat er specifiek voor identificatiemiddelen een duidelijk kader en open source aanpak is waarin de belangen van private partijen voldoende doorklinken. Thans lijkt in de Concept-regeling een algemene open source eis gesteld te worden die een onvoldoende op maat gesneden open source aanpak weerspiegelt.

---

[9] In deze reactie gebruikt NotarisID “gepubliceerd”. In de AMvB en de toelichting worden “publiceren”, “openbare broncode” en “beschikbaar maken” en gemaakt door elkaar gebruikt, zonder ogenschijnlijk semantisch en juridisch verschil. Het verdient de aanbeveling dat begrippen consequent(er) worden toegepast.

[10] Inbreng verslag van een schriftelijk overleg over toegang, toezicht en eisen inlogmiddelen onder de Wet digitale overheid (Wdo) (o.a. Kamerstuk 35868-17)

Ten tweede is NotarisID van mening dat open source niet per definitie of sec bijdraagt aan de beoogde doelstellingen van transparantie en vertrouwen.[11] Onzes inziens zijn er ook andere manieren om te komen tot transparantie en vertrouwen. Zoals gezegd worden gekwalificeerde vertrouwensdienstverleners na een audit en certificering vertrouwd op basis van een bij Agentschap Telecom ingeleverd positief conformiteitsbeoordelingsverslag en de toekenning van een gekwalificeerde status. Op deze wijze wordt transparantie en vertrouwen (letterlijk) bewerkstelligd en gewaarborgd, via een andere route en wettelijk systeem. NotarisID vraagt u uit te leggen in hoeverre een reeds beschikbaar conformiteitsbeoordelingsverslag kan bijdragen aan de beoogde doelen van transparantie en vertrouwen en hoe een gekwalificeerde status zich verhoudt tot de open source eis.

Ten derde wijst NotarisID erop dat onder de te herziene eIDAS (kort: eIDAS 2.0) naar verwachting een relevante vertrouwensdienst bij komt, genaamd “attributenattestatie”. Door middel van deze attributendienst kan een wallet gevuld worden met attributen. Een attributenattestator lijkt in die zin in belangrijke mate op een exploitant van een eID met erkenning onder Wdo en onderliggende AMvB’s. De gekwalificeerde attributenattestator zal op eenzelfde wijze als andere gekwalificeerde vertrouwensdienstverleners (via ETSI-standaarden) een conformiteitsbeoordelingsverslag en status moeten verkrijgen. ETSI (en het aanverwante TWS en TW4S) stelt (nog) niet dat er sprake moet zijn van open source om *trust worthy systems* te realiseren. NotarisID wenst hierbij vooral op te merken dat er derhalve in de nabije toekomst actoren zullen zijn die actief zijn in het gremium van nationale eID’s, eIDAS genotificeerde eID’s, en gekwalificeerde vertrouwensdiensten waarbij voor de ene actor - door nationale wetgeving - de eis van open source en/of publiceren van broncode geldt, en voor de andere actor niet omdat het valt onder een andere jurisdictie. ***Indien dadelijk elders in EU-wetgeving geen of een beperkte open source eis wordt gesteld zoals thans beoogd door de nationale wetgever dan dreigt er rechtsongelijkheid en rechtsonzekerheid.***

Als laatste merken we op dat verzekerbaarheid een factor is die zich niet tot moeilijk verhoudt tot open source omdat verzekeraars dit als een risico zien en daarvoor geen dekking bieden. Over de verzekerbaarheid gaan we hieronder uitgebreider op in.

3 Verzekerbaarheid

In artikel 2.1 Concept-regeling wordt een verzekeringseis gesteld voor contractuele en wettelijke aansprakelijkheid voor directe en indirecte schade die samenhangt met de activiteiten waarvoor de erkenning wordt aangevraagd. Het is noodzakelijk dat deze eis wordt gesteld. Echter, de ervaring leert dat diensten die samenhangen met elektronische identificatie en vertrouwensdiensten voor de gevraagde verzekerde hoedanigheid welhaast onverzekerbaar blijken te zijn vanwege de risico’s die hiermee samenhangen, onder meer omdat het voor de markt relatief nieuwe diensten zijn. De verzekeringsmarkt blijkt hierop (nog) niet voorbereid te zijn. In een recent gepubliceerd onderzoeksrapport, getiteld “Verzekeraars in een veranderende wereld: Kansen en risico’s in tijden van klimaatverandering, digitalisering en inflatie”, waarschuwt DNB dat onverzekerbaarheid dreigt door

[11] Zie in dit kader het onderzoek van de Europese Commissie “Study about the impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy”, 6 sept 2021

nieuwe ontwikkelingen.[12] Met DNB is NotarisID het eens dat de oorzaken van onverzekerbaarheid zijn: forse potentiële schadelast, asymmetrische informatie en gebrek aan bewustzijn, gebrek aan data voor het inschatten van risico's. Voor het verzekerbaar krijgen van de activiteiten is er onzes inziens nodig dat er anticipatie op steun van de overheid is en dat er een correlatie van risico's gecreëerd kan worden, waardoor schade voor een individuele verzekeraar al snel verzekerbaar wordt.

Wij verzoeken u hierbij alternatieven te geven ingeval onverzekerbaarheid dreigt. NotarisID vraagt u hierbij zowel aandacht te hebben voor de letterlijke onverzekerbaarheid (risico's zijn onbekend of kunnen niet worden ingeschat) als zowel voor praktische onverzekerbaarheid (door bijvoorbeeld te hoge premie en/of hoge en kostbare eisen). Omdat dit risico in de markt (nog) niet verzekerbaar blijkt, geven we de overheid in overweging mee dit risico af te dekken door bepaalde garanties en forfaitaire beperkingen te geven rondom aansprakelijkheid opdat de risico's meer verzekerbaar kunnen geraken.

Een extra uitdaging voor verzekerbaarheid is de open source eis waar NotarisID hierboven aan refereert. Verzekeraars sluiten doorgaans het gebruik van open source uit en geven daarvoor geen dekking. ***De vraag is in hoeverre onderzoek is gedaan naar verzekerbaarheid en/of in hoeverre verzekeraars zijn geraadpleegd/geconsulteerd.***

4 Notificatie eIDAS

In paragraaf 4.4 van de Concept-regeling is geregeld dat een houder van een erkenning in aanmerking kan komen voor een eIDAS-notificatie en kan aansluiten op de infrastructuur en registers, bedoeld in artikel 2.25 alsmede de voorziening, bedoeld in artikel 5, tweede lid, onderdeel a, van de wet, voor zover een notificatie als bedoeld in artikel 4.18 met succes is afgerond met inachtneming van de verplichtingen die aan die notificatie verbonden zijn. Het is onduidelijk onder welke voorwaarden een houder van een erkenning in aanmerking komt voor een eIDAS-notificatie. ***NotarisID verzoekt u omwille van de rechtszekerheid en voorspelbaarheid de voorwaarden te expliciteren waaronder een houder van een erkenning in aanmerking kan komen voor een eIDAS-notificatie.*** Duidelijke regels rondom notificatie in het kader van het eIDAS-stelsel zijn noodzakelijk voor een behoorlijk functioneren van het stelsel. Bij het concipiëren van de nadere eisen/voorwaarden voor notificatie vragen wij u rekening te houden met eIDAS 2.0 waarin private aanbieders meer ruimte krijgen om tot het eIDAS-systeem toe te treden.

5 Conclusie

NotarisID ziet de hierboven besproken thema's als fundamenteel voor het welslagen van een nationaal eID-stelsel. NotarisID verzoekt u bij het verder concipiëren van de Regeling aandacht te hebben voor de genoemde zorg- en knulpunten en een coherente Regeling vorm te geven die tot de vereiste rechtszekerheid en rechtsgelijkheid leidt.

[12] DNB, Verzekeraars in een veranderende wereld Kansen en risico's in tijden van klimaatverandering, digitalisering en inflatie: https://www.dnb.nl/media/elrpseou/dnb-verzekeraars-in-een-veranderende-wereld.pdf

Wij hopen dat u het voorgaande meeneemt in de verdere behandeling van de Concept-regeling. NotarisID is graag bereid tot een nadere toelichting van deze brief.

Hoogachtend,

Evert Jan Nooter
CEO NotarisID