Reactie op internetconsultatie Besluit bedrijfs- en organisatiemiddel

Geachte heer Knops,

Hierbij ontvangt u namens de huidige erkende leveranciers van eHerkenning een gezamenlijke reactie op het ter consultatie voorgelegde Ontwerpbesluit bedrijfs- en organisatiemiddel Wdo.

Met vriendelijke groeten,

Frank Jonker
Voorzitter leveranciersoverleg eTD

Inleiding

Als erkende leveranciers van eHerkenning vinden wij het zeer positief te noemen dat de gestelde regels/eisen in lijn zijn met de Uitvoeringsverordening eIDAS en het huidige afsprakenstelsel (elektronische Toegangsdiensten) voor eHerkenning. Wij voldoen al aan de hierin gestelde eisen en sinds 6 juni 2019 ligt Europese notificatie van de eHerkenningsmiddelen op niveau substantieel en hoog in het verschiet, naar aanleiding van het positieve oordeel van het eIDAS coöperatie netwerk.

Er zijn wel zorgen over de impact van het certificerings-/auditregime. De beweging richting het regime, zoals dit momenteel al van toepassing is op de vertrouwensdiensten (PKI), zien we niet als onlogisch, echter maken wij ons dan wel zorgen over de gevolgen voor de kostprijs van een middel en/of machtiging. De kostprijs van een PKI Overheid certificaat ligt flink hoger dan die van een eHerkenningsmiddel. Een factor die hierin mee speelt is de zwaarte van het certificerings-/auditregime en de kosten die daarmee gemoeid zijn. Zodra op het bedrijfs- en organisatiemiddel een vergelijkbaar regime van toepassing gaat zijn, is de verwachting dat de kostprijs (flink) zal stijgen. Wij roepen er toe op om zoveel mogelijk bestaande certificeringen te erkennen en geen dubbele audits uit te voeren.

Ook willen wij het belang benadrukken om naast deze beschrijving van de eisen aan erkende diensten (middels dit besluit), ook een beschrijving te geven van de verantwoordelijkheden en plichten van de publieke deelnemers aan dit stelsel (waaronder BSNk en de eIDAS-infrastructuur), en hun rol in de uitvoering/realisatie. Zonder deze publieke deelnemers kunnen erkende diensten immers niet leveren. Het besluit is wat dit betreft naar onze mening te eenzijdig gericht op de eisen aan private partijen.

Op dit moment bieden de eHerkenningsleveranciers overigens niet alleen publieke dienstverlening, maar ook private. Het voorgenomen besluit en nog overige uit te werken regelgeving, moeten niet beperkend of schadelijk voor deze markt zijn.

Wij juichen het verder toe dat er op veel punten wordt uitgegaan van de bewezen zelfregulering van het stelsel en er geen onnodige inhoudelijke voorschriften genoemd worden terwijl wel de mogelijkheid geborgd wordt om dit indien nodig te corrigeren.

Artikelsgewijs

Artikel 1 Begripsbepalingen

- De gebruikte terminologie binnen het eTD-stelsel en binnen deze documentatie als het gaat om de certificeringsaudit en de technische toets. Hierbij lijken een aantal termen erg op elkaar, terwijl er verschillende dingen bedoeld worden en dat zou verwarrend kunnen werken. Voor de certificeringsaudit wordt gesproken over een "certificaat van conformiteit" of "conformiteitsverklaring", terwijl in het huidige afsprakenstelsel gesproken wordt over een conformiteitsbeoordeling of conformiteitstoets, maar dan gaat het juist over de technische toets op het authenticatiemechanisme en/of het -middel. In deze documentatie wordt dan gesproken over "technische beveiligingstoets".
  Advies: definieer de terminologie zodanig dat het onderscheid tussen het certificaat van conformiteit/conformiteitsverklaring en de technische beveiligingstoets/conformiteitsbeoordeling of -toets duidelijk is.

Artikel 3 Aanvullende eisen erkende diensten

- Hier wordt aangehaald dat erkende diensten aan regels gebonden kunnen worden. Het is wenselijk dat er ook eisen worden gesteld o.a. aan de beschikbaarheid van generieke publieke voorzieningen waar het stelsel van afhankelijk is (o.a. BSNk, EB, BRPk).
- Onder het eerste lid, a, wordt aangehaald dat bij ministeriële regeling aanvullende eisen kunnen worden gesteld met betrekking tot de bestrijding van misbruik. De, op pagina 7 van de Nota van Toelichting (NvT), beschreven mogelijke maatregelen kunnen potentieel enorm kostenverhogend werken. Ons advies is om vooral centraal maatregelen te nemen om misbruik te voorkomen.

Artikel 4 Eisen erkende middelenuitgever

- Onder lid 2 wordt gesproken over het zorgen voor een kenbaar proces van schorsing óf intrekking. Echter, in de NvT staat dat conform de Uitvoeringsverordening schorsing én intrekking van een middel mogelijk moet zijn. Dit is naar onze mening te scherp gesteld. Uit deze formulering zou je kunnen lezen dat ook schorsen verplicht is, terwijl dit binnen eIDAS optioneel is, zie Verordening (EU) nr. 910/2014, onder (53). Intrekken is wel verplicht. Schorsing is bovendien complex (hoe te bepalen wel/niet schorsen én wel/niet (her)activeren middelen) en daarmee kostbaar (hoge ontwikkelkosten). En hoe regel je schorsing binnen het stelsel. Een persoon kan meerdere middelen hebben over verschillende erkende aanbieders. Het advies is om schorsing optioneel op te laten nemen.

  NB. Schorsing op middel heeft ook een hoge impact, geen van de machtigingen is nog bruikbaar, ook wanneer deze voor meerdere organisaties zijn geregistreerd en gekoppeld zijn aan één middel.

Artikel 6 Eisen erkende ontsluitende dienst

- Artikel 6, derde lid: "Een erkende ontsluitende dienst informeert de overige erkende diensten over de bestuursorganen of aangewezen organisaties waarmee hij een overeenkomst als bedoeld in het eerste lid heeft gesloten." In de NvT staat dat het aan de ontsluitende dienst is om dit vorm te geven en dat het enkel om de namen van de dienstverleners gaat. Hiermee lijkt een systeem als de huidige dienstencatalogus van het ETD-stelsel te worden bedoeld. De specifieke diensten hierin zijn mogelijk nog relevanter als de dienstverlenersnamen. Zonder generieke specificaties voor alle ontsluitende diensten, is er bovendien een risico dat iedere ontsluitende dienst een eigen formaat, kanaal en wijze van bericht hiervoor hanteert.

Artikel 10 Aanwijzingen

- Wenselijk is dat in dit artikel wordt opgenomen dat oplostermijnen voor aanwijzingen realistisch en in overleg tussen toezichthouder en leveranciers worden gemaakt. Oplostermijnen voor incidenten en bevindingen zijn in het verleden niet altijd realistisch en haalbaar gebleken.

Artikel 12 Certificaat van conformiteit

- Om de twee jaar opnieuw certificeren is kostbaar en de procedures en systemen zullen niet met een dergelijk hoge frequentie wijzigen. Wij willen voorstellen om de frequentie van ISO 27001 aan te houden, te weten een certificeringsaudit gevolgd door twee onderhoudsaudits. Verder ontbreekt een soort van meldplicht voor grote wijzigingen in de procedures en systemen. Overigens wordt in de NvT hoofdstuk 3 (De erkenning), gerefereerd aan een onderhoudsaudit in het tussenliggende jaar, maar in artikel 12 van het ontwerpbesluit staat hier niets over beschreven.

Artikel 13 Aangewezen conformiteitsbeoordelingsinstantie en Artikel 14 Intrekken aanwijzing conformiteitsbeoordelingsinstantie

- We maken ons zorgen over de mogelijke situatie waarin er slechts 1 CBI wordt benoemd. Dit vraagt om waarborgen tegen het ontstaan van een SPOF of SPOK (Single Point of Failure of Single Point of Knowledge). Ook ontbreekt een beschrijving van een situatie waarin de accreditatie of aanwijzing van een CBI ingetrokken wordt. Volgens de huidige tekst is het Certificaat van Conformiteit dan niet meer geldig. Hoeveel tijd krijgen erkende diensten bijvoorbeeld om bij een andere geaccrediteerde CBI een Certificaat van Conformiteit te behalen? Wat zijn dan de gevolgen voor de bestaande dienstverlening?

Nota van Toelichting

Specifiek ten aanzien van de Nota van Toelichting (NvT) geven wij het volgende mee:

- In de NvT staat dat de opzet van certificering analoog is aan de wijze waarop dit voor 'trustservices' in het kader van de eIDAS-verordening is geregeld. Betekent dat hiervoor (deels) de ETSI-normering wordt overgenomen?
- Op pagina 5 wordt in de derde alinea ten onrechte naar ETSI 319 403 verwezen. Dit is de ETSI norm voor Certificerende Instellingen die ETSI audits uitvoeren bij TSP's en dus geen ETSI certificering die een marktpartij kan verkrijgen (en dus kostenverlagend kan werken voor een marktpartij). Hier wordt zeer waarschijnlijk ETSI 319 411-2 bedoeld, zoals in een alinea eronder wel terecht staat.
- Op pagina 5 wordt aangegeven: "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." Naar onze mening wordt hier ten onrechte alleen de operationele infrastructuur genoemd. We kunnen ons goed voorstellen dat er ook voor generieke auditobjecten/processen als fysieke toegang, HR processen, financiële stabiliteit van een organisatie, gebruik van bepaalde soft- en/of hardware etc. ook gesteund kan worden op het ETSI certificaat, mits aangetoond kan worden dat die in scope zaten van de betreffende ETSI audit.
- Op pagina 5 wordt aangegeven dat een Technische beveiligingstoets plusminus 25.000 euro zal bedragen. Het is niet duidelijk waar dit bedrag op gebaseerd is en of dit richtinggevend is.