Bijlage III: Uniforme set van eisen inloggen in het BSN-domein

Deze bijlage bevat de uitwerking van de onderwerpen in de uniforme set van eisen voor inloggen in het BSN-domein, zoals gevraagd in de motie De Caluwé[1].

Uitgangspunt: eIDAS als basis voor Uniforme Set van Eisen

Voor het opstellen van de uniforme eisen is de EU eIDAS verordening als uitgangspunt genomen. De eisen krijgen hun nationale basis in de voorgenomen wet Generieke Digitale Infrastructuur[2] en uitvoeringsregelgeving daarbij. In de bijlage bij de brief van 14 december 2015[3] is een eerste schets gegeven van de te reguleren onderwerpen.

De eIDAS verordening brengt mee, dat elke lidstaat nationale middelen met bijbehorende authenticatiemechanismen aan de Europese Commissie kan notificeren wanneer deze voldoen aan de gestelde eisen. Burgers en bedrijven hebben er recht op met een genotificeerd en vervolgens toegelaten middel uit een EU lidstaat toegang te krijgen tot het publieke domein in andere lidstaten. Het ligt in de rede dat Nederland dezelfde eisen hanteert. Als Nederland lagere eisen zou stellen zouden Nederlandse middelen niet bruikbaar zijn in het publieke domein in andere lidstaten. De eIDAS verordening laat ruimte aan de lidstaten om eigen procedures en regelgeving te hanteren. Ook laat de verordening ruimte om de eigen architectuur (functionaliteit en techniek) te ontwerpen. De eIDAS verordening beschrijft niet gedetailleerd hoe conformiteit met de eisen moet worden aangetoond, hoe de toelating tot het nationale publieke domein plaatsvindt en hoe toezicht moet worden ingericht. Bij de uitwerking moet een balans worden gevonden tussen duidelijkheid, rechtszekerheid en flexibiliteit. Daarom geldt als uitgangspunt dat het operationele detail wordt gezocht als er een expliciete noodzaak is om een risico op uniforme wijze te mitigeren. Ook worden invulling en aanvulling van de Europese eisen gedefinieerd als te bereiken *doelstellingen* en door de normadressaat *te mitigeren risico's* te benoemen. De wijze waarop aan deze eisen wordt voldaan kan daarmee variëren.

De onderwerpen die in wet- en regelgeving worden vastgelegd, worden hieronder weergegeven.

1.Beheer

Algemene bepalingen
Betreft kaders waaraan de organisaties in de authenticatieketen moeten voldoen.

Informatie voor gebruikers
Betreft de vereisten voor informatie aan gebruikers over processen, producten en procedures voor het informeren over wijzigingen van uitgifte/intrekkingsprocessen en leveringsvoorwaarden. Regelt informatieplicht aan gebruikers.

[1] Kamerstuk 26 643, nr. 374.
[2] Zie Brief over Uitgangspunten Wetgeving GDI, Kamerstuk 26 643, nr. 373.
[3] Kamerstuk 26 643, nr. 379

Bijhouden van de administratie
Betreft de vereisten aan de diverse administraties waaronder zakelijke overeenkomsten, registraties van identiteitsgegevens, loggings van berichtenverkeer etc. Dit met het oog op nationale regelgeving inzake financiële controle, privacy en onderzoek van beveiligingsinbreuken en misbruik van identiteiten en fraude.

Faciliteiten en personeel
Betreft de vereisten aan de competentie van ingezet personeel en beperking van toegang tot persoonsgegevens en cryptografische gegevens en andere gevoelige gegevens.

2.Techniek en functionaliteit

Als onderdeel van de eisen zal een aangepast systeemontwerp worden bijgevoegd, dat een oplossing biedt voor de bevindingen in de eerdere Privacy Impact Assessment (PIA)[4]. Dit ontwerp biedt betere mogelijkheden voor privacybescherming, zonder adequate misbruikbestrijding uit te sluiten. In het nieuwe ontwerp wordt *privacy by design* doorgevoerd. Naast het ontwerp omvatten de eisen ook specificaties. Er wordt er een PIA uitgevoerd op het ontwerp (gereed: september 2016). Bij de te stellen technische eisen wordt er, conform staand kabinetsbeleid, zoveel mogelijk gebruik gemaakt van open standaarden. Daarbij is het streven om zo min mogelijk koppelvlakken te introduceren. Beide principes dragen bij aan het borgen en vergroten van de interoperabiliteit van de toegangsdiensten, terwijl deze aanpak tegelijkertijd ruimte laat voor doorontwikkeling en innovatie.

3.Informatiebeveiliging

Dit betreft de vereisten voor een beheerssysteem voor informatiebeveiligingsrisico's en specificaties en controles ter waarborging van de betrouwbaarheid van authenticatiemiddelen, beveiliging van bestanden, berichten en het berichtenverkeer.

[4] Zie voor de PIA https://www.idensys.nl/fileadmin/bestanden/idensys/documenten/basisdocumentatie/pia/31072015_PIA_Introductieplateau_eIDv1_final.pdf

4.Privacybescherming

Inschrijving:
Aanvraag en Registratie (natuurlijke persoon)
Betreft de vereisten voor registratie van de natuurlijke persoon die voor zichzelf een authenticatiemiddel aanvraagt en gebruiksvoorwaarden.

Bewijs en verificatie identiteit
Betreft de vereisten voor de verificatie van aangeleverde identiteitsinformatie.

Bewijs en verificatie identiteit (rechtspersoon)
Betreft de vereisten voor identificatie van rechtspersonen en verificatie van aangeleverde gegevens. Onderdeel hiervan is de identificatie van de natuurlijke personen die de rechtspersoon vertegenwoordigen.

Koppeling tussen elektronische identificatiemiddelen van natuurlijke personen en rechtspersonen.
Betreft de uitgifte van bedrijfsmiddelen aan medewerkers.

Beheer elektronische identificatiemiddelen:
Kenmerken en ontwerp van elektronische Identificatiemiddelen
Betreft specificaties voor het ontwerp van middelen in relatie tot het gebruik op elke betrouwbaarheidsniveau

Uitgifte, uitreiking en activering
Betreft de vereisen voor de manier waarop de gebruiker zijn middel in bezit krijgt.

Schorsing, Herroeping en Reactivering
Betreft de vereisten voor het schorsen, verzoeken voor intrekking en reactivering van authenticatiemiddelen.

Verlenging en vervanging
Betreft de vereisten voor de levensduur van middelen, de levensduur van de identificatie en vervanging/verlenging van middelen

Authenticatie:
Authenticatiemechanisme
Betreft de vereisten voor de betrouwbaarheid van alle handelingen die de gebruiker moet verrichten met zijn middel om in te kunnen loggen bij een dienstverlener en de elektronische communicatie tussen het middel en de authenticatiedienst.

5. Toelating en toezicht

Toelating van authenticatiemiddelen, ongeacht of deze worden uitgegeven door publieke of private authenticatiediensten, geschiedt als volgt. Individuele partijen doen een verzoek tot toelating bij de minister van BZK. Deze wordt bij zijn beoordeling ondersteund door de toezichthouder. Een geaccrediteerde partij voert een conformiteitstoets uit en levert de uitkomsten aan bij de toezichthouder. Deze vormt zich een oordeel mede op basis van de conformititeitstoets en adviseert de minister van BZK. De minister betrekt de beschikbare documentatie bij zijn besluit tot toelating.

Regulier interbestuurlijk toezicht is in dit verband niet onverkort bruikbaar, omdat dit ziet op naleving door overheidsorganen. In casu is sprake van publieke en private partijen die authenticatiemiddelen aanbieden voor gebruik in het publieke domein. Een specifiek toezichtsregime is daarom gerechtvaardigd.

Toezicht op de naleving van de eisen wordt opgedragen aan een externe toezichthouder. Overwogen wordt het Agentschap Telecom aan te wijzen, die informatie verzamelt en aan oordeelsvorming en interventie doet. Een besluit tot intrekking van een toelating kan alleen door de minister van BZK worden genomen. De toezichthouder kan wel advies uitbrengen aan de minister om al dan niet over te gaan tot een intrekking. Deze rol is passend omdat de toezichthouder beschikt over actuele informatie over de mate van normnaleving.

Tussen de betrokken toezichthouders - immers: ook De Nederlandse Bank en de Autoriteit Persoonsgegevens hebben een rol - zullen werkafspraken worden gemaakt om dubbel toezicht en/of overlap van toezicht te voorkomen.