Beantwoording op vragen marktconsultatie middel eID

25 oktober 2017

1. Wat is de verhouding van deze marktconsultatie tot de eisen die BZK stelt aan private middelen vooruitlopend op de inwerkingtreding van de wet GDI?

Deze marktconsultatie biedt marktpartijen de mogelijkheid mee te denken over de doelstellingen en eisen die BZK zal stellen in een mogelijk toekomstig vervolgtraject. Deze consultatie dient tegen het licht van dat vervolgtraject te worden benaderd. Voor het geval dat het vervolgtraject en de toelating van een privaat middel in de aanloop naar inwerkingtreding van de wet GDI zijn beslag krijgt, voorziet de wet GDI in overgangsrecht terzake de bij overeenkomst gestelde eisen.

2. Waarom wordt alleen niveau substantieel uitgevraagd, terwijl niveau hoog ook wordt onderkend in het herontwerp van de wet GDI?

BZK heeft in deze fase geen behoefte aan een of meer alternatieve middelen op niveau hoog.

3. Wat verwacht BZK (in de toekomst) van eID-middelen gerelateerd aan gekwalificeerde elektronische handtekeningen (mede gezien de verwijzing bij SR3)?

Volgens het Forum Standaardisatie is een elektronische handtekening een set gegevens die geassocieerd is met het ondertekende document of de ondertekende gegevens. Zij geeft de identiteit van de ondertekenaar weer en de authenticiteit van het ondertekende document of de ondertekende gegevens.

Het ligt in de lijn der verwachtingen dat er ondertekendiensten kunnen ontstaan die het authenticatieresultaat dat geleverd wordt door het private middel, gebruikt voor deze elektronische handtekening (dus de associatie van het authenticatieresultaat met de wilsuiting/het document verzorgt). De gevraagde dienst van de authenticatiedienst verandert hiermee niet.

4. Voor welke periode geldt toelating van een eID middel tot het overheidsdomein door BZK? Kan een eID middel op een willekeurig moment worden toegelaten?

Start van de uitrol van een privaat middel(en) is voorzien per eind 2018. Toelating zoals beoogd door deze marktconsultatie dient vanzelfsprekend daarvoor plaats te vinden. In het gesprek kan een meer gedetailleerde planning worden besproken.

5. Gelden alle in dit document genoemde eisen ook voor de publieke middelen?

In het beleid van BZK gelden voor private en publieke middelen op een groot aantal punten dezelfde eisen ontleent aan eIDAS en toepasbaar gemaakt voor de Nederlandse situatie. De technische uitwerkingen hiervan kunnen verschillen van elkaar.

6. Staat BZK open voor de toepassing van nieuwe technologieën (zoals bijvoorbeeld blockchain bij het toepassen van bijvoorbeeld attribuut verstrekking)?

BZK staat in beginsel open voor alle oplossingen die passen binnen de doelstellingen, zoals genoemd in het consultatiedocument, paragraaf 1.1.

7. Wat is het vervolg op de markt consultatie? Volgt hierop een Europese aanbesteding of volgt er bijvoorbeeld een onderhandse aanbesteding?

Dat is onder andere afhankelijk van de uitkomsten op de marktconsultatie. Hier is op dit moment nog geen duidelijk antwoord op te geven.

8. CM1/CM2. Het middel wat Gegadigde voor ogen heeft zal ook voor private toepassingen gebruikt gaan worden, en naast gebruik bij overheids(gerelateerde)-toepassingen ook voor private toepassingen als inlogmiddel worden gebruikt. In hoeverre wil BZK een rol spelen cq. is BZK verantwoordelijk bij massacommunicatie over toepassingen van hetzelfde inlogmiddel in het private domein?

BZK is in principe niet verantwoordelijk voor de communicatie over het gebruik van het inlogmiddel in het private domein. Het zou wel kunnen zijn dat er in de (massa)communicatie door BZK aandacht wordt besteed aan de mogelijkheden die het inlogmiddel (nog meer) biedt. Dit wordt, indien aan de orde, bekeken en met de leverancier afgestemd. Verder vindt BZK het van belang dat de communicatie-uitingen van een private leverancier het vertrouwen van burgers in het publieke inlogmiddel niet schaden. De communicatie van de marktpartij met de consument over gebruik buiten het BSN-domein, is overigens een zaak van de marktpartij zelf. Uiteraard binnen de algemene regels die daarvoor gelden.

9. UA3.5. Wat wordt hier bedoeld met abonneerelatie? Kunt u hier een voorbeeld van geven?

De Aanbieder waarborgt dat de status van de abonneerelatie wordt geregistreerd bij een nader te bepalen centrale inzagevoorziening van BZK

De abonneerelatie is de klantrelatie van de eindgebruiker met de aanbieder. De betekenis van de status van deze relatie is of het authenticatiemiddel 'actief' is, ingetrokken of geschorst etc. Het registreren hiervan is nodig om de gebruiker inzicht te geven in welke middelen op diens naam actief zijn.

10. BI1. Wat zijn de voorzieningen die BZK ter beschikking stelt bij BI1?

11. BI1. Zal BZK toestaan dat voor identiteitsvaststelling van een persoon (uitsluitend) gebruik wordt gemaakt van elektronische identificatie gebaseerd op een publiek eID middel of reeds toegelaten privaat eID middel (van minimaal hetzelfde betrouwbaarheidsniveau)

12. VV1. Waarom is de periode voor 'her verificatie' op maximaal 3 jaar gesteld? (Dit wijkt af van de geldigheid van wID documenten)

13. VV1 en Algemeen: In welke mate is BZK bereid om (proactief) bij wijzigingen in status van (de persoonsgegevens van) een persoon (zoals bijvoorbeeld bij overlijden) Aanbieders hiervan op de hoogte te stellen?

Antwoord op vraag 10 t/m 13.

BZK biedt het BSN koppelregister. Daarnaast levert BZK de routeringsvoorziening ten behoeve van één koppelvlak naar dienstverleners.

Eén keer in de drie jaar dienen de persoonsgegevens te worden vergeleken met een authentieke bron waarvoor BZK het BSN koppelregister ter beschikking stelt.

Ten aanzien van vraag 13: hiervoor staat nog geen beslissing vast, en suggesties ten aanzien van dit thema kunnen desgewenst door marktpartijen worden ingebracht in de gesprekkenronde en/of schriftelijke ronde van deze marktconsultatie.

14. IG2. Indien wij de selfcare van het middel hiervoor gebruiken, mogen dan de publieke middelen ook gebruikt worden om op de selfcare van het middel in te loggen?

Dit belangrijke vraagstuk kan tijdens de consultatie door de marktpartij worden ingebracht.

15. FP2 De genoemde referentie lijkt betrekking te hebben op een uitgifteproces op (eIDAS) niveau hoog, terwijl de consultatie betrekking heeft op niveau substantieel. Voor bijvoorbeeld geautomatiseerde verwerking identiteitsvaststellingen en afgeleide identificaties zal het proces (sterk) afwijken van het proces dat voor uitgifte van paspoorten en rijbewijzen wordt toegepast. In hoeverre bedoeld BZK hier af te wijken van de eisen voor eIDAS Substantieel?

BZK wijkt niet af van de eisen voor eIDAS substantieel. De eis voor substantieel stelt dat er geverifieerd moet worden dat de persoon in het bezit is van een erkend bewijs, welk gecontroleerd is op echtheid en er maatregelen zijn getroffen die aantonen dat persoon en het bewijs bij elkaar horen. Hiertoe kunnen maatregelen voor identificatie op afstand behoren. Substantieel vereist geen identificatieproces met daadwerkelijk fysieke gezichtsherkenning. eIDAS hoog – evenals de uitgifte van het paspoort, NIK en Rijbewijs – vereisen dit wel. Zo moet de lijn van BZK worden gelezen.

16. H5, vraag 1d. Welke continuïteit wordt hier bedoeld? (wordt hier bijvoorbeeld bedoeld beschikbaarheid van de dienst, of technische-, commerciële-of business continuïteit?)

BZK is geïnteresseerd in de technische continuïteit (beschikbaarheid), maar ook in de business continuïteit.

17. We begrijpen dat jullie, naast DigiD, een gecertificeerde en bestaande oplossing voor identificatie / authenticatie willen. Is dat correct?

BZK staat in beginsel open voor alle oplossingen die passen binnen de doelstellingen, zoals genoemd in het consultatiedocument, paragraaf 1.1.

18. Overwegen jullie na deze marktconsultatie om eventueel bestaande elektronische methodes van DigiD aan te vullen / te vervangen?

Ja, momenteel onderzoekt BZK alternatieve technieken voor DigiD ten behoeve van bepaalde doelgroepen.

19. Moet de nieuwe identiteit provider opereren als een privaat bedrijf gecertificeerd bij de overheid, privaat publiek partnerschap in naam van de overheid, of uit naam van de overheid?

Hierover staat nog geen besluit vast. Marktpartijen die hier suggesties voor hebben, worden van harte uitgenodigd deze te delen in de gesprekken en/of de schriftelijke ronde van deze consultatie.

20. Moet deze nieuwe identiteitsaanbieder officieel worden aangemeld op EU-niveau en ook gebruikt worden als een toegangspoort voor EIDAS?

Dit is optioneel.

21. Wij begrijpen dat DigiD momenteel beheerd wordt door Logius. Is het de bedoeling dat de nieuwe oplossing beheerd wordt door Logius als een second sourcing?

Het vertrekpunt is dat het private middel wordt geëxploiteerd voor rekening en risico van de private partij. Beheer door Logius past hier niet bij.

22. De marktconsultatie is openbaar gekomen, terwijl er 2 pilots lopen met iDen en Idensys. Hoe zien jullie deze pilots in de context van de marktconsultatie.

Indien er een vervolgtraject komt, naar aanleiding van de consultatie, dan hebben alle marktpartijen in het vervolgtraject evenveel kans. Marktpartijen die participeren in iDIN of Idensys zijn niet bij voorbaat toegelaten of uitgesloten tot het vervolgtraject.
Deelname aan een pilot is irrelevant voor het vervolgtraject.

23. Wat is de voortgang op de wet, bedoeld voor de eIDAS 2015/1502? En waar kunnen wij een draft versie vinden?

Op 30 augustus 2017 zijn het voorstel voor de Wet generieke digitale infrastructuur (GDI) en de bijbehorende memorie van toelichting voor advies naar de Autoriteit Persoonsgegevens gezonden. Deze documenten zijn gepubliceerd op www.rijksoverheid.nl. Inwerkingtreding van het wetsvoorstel is gepland op 1 januari 2019.

24. Vanaf september 2018 moeten alle landen binnen de EU een ID gateway live hebben, waardoor inwoners van andere Europese landen toegang hebben tot de publieke website, gebruikmakende van de methodiek aangeleverd van het land. Hoe gaat Nederland dit verzorgen? Met een voorkeur voor een private op publieke oplossing toegang?

Ook Nederland heeft een gateway en dit is een publieke oplossing.

25. Door te verklaren dat de dienst van de identiteitsaanbieder moet voldoen aan eIDAS 2015/1501, zijn jullie ook van plan de eIDAS interop format intern te gaan gebruiken binnen Nederland? Oftewel, moet de identiteitsaanbieder ook dienen als toegangspoort?

Nee de dienst hoeft niet te gaan dienen als toegangspoort voor burgers uit andere EU lidstaten. Hiervoor wordt momenteel een infrastructuur geimplementeerd.

26. Begrijpen wij goed dat de identiteitsaanbieder alleen de LOA niveau substantieel hoeft aan te leveren? En waarom zouden niet de Niveau's laag en middel?

eIDAS kent de betrouwbaarheidniveau's Laag, Substantieel en Hoog. Niveau Laag wordt niet uitgevraagd in deze consultatie omdat het de ambitie van BZK is om naar hogere niveaus van betrouwbaarheid te gaan. Niveau Laag wordt zo spoedig mogelijk uitgefaseerd voor diensten waarvoor substantieel vereist is. Ook het publieke middel wordt zodanig doorontwikkeld.

27. Hoe kijken jullie naar identificatie en registratie gebaseerd op video identificatie voor het LOA niveau substantieel? Wordt dit omschreven in de lokale wet voor eIDAS 2015/1502?

Video identificatie zou een manier kunnen zijn om gezichtsherkenning uit te voeren.

28. Wat is jullie visie over biometrische registratie, inschrijving en authenticatie?

BZK staat in beginsel open voor alle oplossingen die passen binnen de doelstellingen, zoals genoemd in het consultatiedocument, paragraaf 1.1.

29. Wat is het plan / protocol wat er gebruikt gaat worden in de communicatie tussen service providers en identiteitsaanbieders in Nederland?

Indien de vraag is gericht op architectuur, dan is het antwoord als volgt:
In 2016 zijn de protocollen en koppelvlakspecificaties volledig uitgeschreven in de Uniforme Set van Eisen. Naar aanleiding van de formele internetconsultatie is er besloten duidelijker te specificeren wat de functionele behoefte is, en meer vrijheid te laten aan de (technische) invulling hiervan, mits dit functioneert in het federatieve systeem. In de marktconsultatie is BZK dus geïnteresseerd in de manier waarop aanbieder hierin voorziet. Het concept Routeringsvoorziening (concept wet GDI, artikel 5, lid 1, onderdeel c) maakt dit makkelijker. Deze routeringsvoorziening biedt aan de ene kant dienstverleners één koppelvlak en aan de andere kant ontsluit deze de diverse authenticatieoplossingen. Het aansluiten op deze voorziening is niet verplicht voor dienstverleners, maar zou wel kunnen ontzorgen.

30. Wat is de motivatie voor de beschreven twee-factor authenticatie om aparte kanalen te gebruiken voor elke factor die ook qua tijd gescheiden is? Is er een specificatie beschikbaar?

De gewenste scheiding heeft betrekking op het uitgifteproces van het authenticatiemiddel. Het mag bekend worden verondersteld dat bij multifactorauthenticatie de twee authenticatiefactoren niet gelijktijdig en via hetzelfde kanaal mogen worden verstrekt omdat het tegendeel onvoldoende zekerheid biedt dat het middel daadwerkelijk in handen komt van de juiste persoon.

31. Eis AM4 stelt dat de authenticatie methodiek weerbaar moet zijn volgens norm EAL3. Betekent dit dat het authenticatiemechanisme of de factoren ervan formeel moeten worden gecertificeerd aan de hand van de gebruikelijke criteria?

De wijze waarop aanbieders moeten aantonen dat de te leveren dienst aan alle eisen voldoet ligt nog niet vast. BZK beraadt zich nog over de wijze waarop dit wordt vormgegeven. Hoofdstuk 5 vraag 5 vraagt de aanbieder om met ideeën te komen die BZK voldoende zekerheid bieden dat voldaan wordt aan de eisen.

32. "Section: 3.1 / Paragraph 2 /Pag 6

DigiD wordt op dit moment doorontwikkeld naar het hogere betrouwbaarheidsniveau Substantieel en naar het niveau Hoog. De betrouwbaarheidsniveaus Substantieel en Hoog zijn gebaseerd op de eIDAS verordening 2015/1502.

Worden onderstaande vier parameters volgens DigID toegepast voor het kwalificeren van het betrouwbaarheidsniveau eIDAS:

1. Identity Verification Method

2. Technology used / Procedure for using identity

3. Parties involved issuing the identity

4. Use of the identity?

Deze verduidelijking is relevant om te begrijpen welke criteria zijn toegepast om kunnen opereren onder DigID betrouwbaarheidsniveau's."

Aanbieder wordt geacht te voldoen aan de eIDAS betrouwbaarheidsniveaus en de set van eisen die daarvoor geldt. Ook DigiD zal zich aan die eisen conformeren. De techniek die DigiD gebruikt is niet het uitgangspunt, maar wel de genoemde eIDAS criteria die ruimte geven voor nadere invulling.

33. "Section: 3.1 / Paragraph 4 / Pag 6

Teneinde de kwetsbaarheid te verminderen en de continuïteit van de dienstverlening te waarborgen is het gewenst dat er – naast de publieke eID-middelen – één of meer alternatieve inlogmiddelen op het betrouwbaarheidsniveau Substantieel beschikbaar komen.

Wat is de scope van deze uitvraag in relatie tot DigID:

1. De creatie van een complete nieuwe infrastructuur naast de DigiD oplossing?

a. Als dit het geval is, van welke marktpenetratie zal hier dan sprake zijn?

i. Welke marktpenetratie heeft dan DigID (100% = 13 mill)?

2. Als alternatief van DigID

a. Gebruik maken van dezelfde infrastructuur als DigID (Logius)?

b. Een oplossing die aan Logius geleverd wordt die vervolgens door Logius gemanged wordt gelijk DigID?

c. Een oplossing die gebruik maakt van het DigiD netwerk maar extern door een provider(s) gemanged wordt?"

Het alternatief (of alternatieven) voor DigiD dient een zelfstandig functionerende infrastructuur te hebben, zodat deze infrastructuur inzetbaar is bij ernstige compromittering of technische beperkingen bij het DigiD inlogmiddel. De huidige penetratie is ruim 13 mln. Er is op dit moment geen beeld te geven van de toekomstige marktpenetratie van DigiD. Het vertrekpunt is dat het private middel wordt geëxploiteerd voor rekening en risico van de private partij. Beheer door Logius past hier niet bij.

34. "Section: 3.2 / Paragraph 4 / Pag 6

Via de internetconsultatie heeft de markt ook gereageerd op de Uniforme Set van Eisen. Op basis van deze reacties is besloten dat de eisen als zodanig (nog) niet voldoen, en opnieuw moeten worden bezien.

De huidige concept GDI wettekst laat een beperkte aanpassing naar aanleiding van de marktconsultatie zien. Aangenomen dat er werkelijk een "DigiD" vanuit de markt beschikbaar moet komen dan is het van belang dat we de impact binnen het BSN-K waarbij private oplossingen toegang krijgen tot het BSN beter begrijpen.

Het kan namelijk ertoe leiden dat buitenlandse private ondernemingen via DigiD kunnen authentiseren (aangenomen dat de overheid DigiD als eIDAS middel kwalificeert), maar een NL private onderneming dit niet mag vanwege "BSN beperkingen"."

Het is voor BZK onduidelijk welke vraag wordt gesteld.

35. "Section: 3.2/Paragraph 4/Pag 7

Sinds 2016 nemen de marktpartijen iDIN…

Wat betekenen deze pilots voor deze marktconsultatie? Zijn dit alternatieven die meedingen naast de aan te bieden alternatieven in deze marktconsultatie?

De commissie Kuipers focust enkel op bruikbaarheid en ergonomie, waarbij de kosten (geld & business case) en aansprakelijkheid (juridisch aspect) buiten beeld blijven. Is hier rekening mee gehouden, gezien het feit dat de business case en juridische aspecten een belangrijke rol spelen?"

Indien er een vervolgtraject komt, naar aanleiding van de consultatie, dan hebben alle marktpartijen in het vervolgtraject evenveel kans. Marktpartijen die participeren in iDIN of Idensys zijn niet bij voorbaat toegelaten of uitgesloten tot het vervolgtraject. Deelname aan een pilot is irrelevant voor het vervolgtraject.