Marktconsultatie eID: privaat inlogmiddel of –middelen

HOOFDSTUK 1
Continuïteit
Om de continuïteit te waarborgen is het wenselijk dat zo snel mogelijk één of meerdere betaalbare alternatieven voor de huidige DigiD beschikbaar komen.
Vraag 1:
Wat vind u betaalbaar in relatie tot de kwaliteit van het middel voor een termijn van 10 jaar?

Eén van de vragen in deze marktconsultatie betreft een mogelijk voorstel van marktpartijen voor een verrekeningsmodel. Voor BZK is het daarom nu geen geschikt moment om uw vraag over betaalbaarheid te beantwoorden.

Substantieel; thans wordt in deze marktconsultatie niet gevraagd naar een alternatief op betrouwbaarheidsniveau Hoog.
Vraag 2:
Wanneer komt betrouwbaarheidsniveau "Hoog" aan de orde? Worden we niet gedwongen snel het hoogste beveiligingsniveau als norm te nemen? Deze marktconsultatie gaat over een oplossing voor minimaal de komende tien jaar. Zoals de technische ontwikkelingen nu gaan worden we hoogstwaarschijnlijk binnen vijf jaar al gedwongen om het hoogste beveiligingsniveau tot norm te verheffen. Is het dan niet veel beter en veel goedkoper om daar nu mee te beginnen? (-zie onder andere de aanbevelingen vanuit het ministerie van VWS voor het middel "Hoog")

Hiervoor verwijzen we u naar de beantwoording van de vragen van de andere marktpartijen. Deze is te vinden op TenderNed.

De genoemde alternatieven op betrouwbaarheidsniveau Substantieel zijn enkel bedoeld voor burgers en niet voor bedrijven.
Vraag 3:
Voor burgers alleen in het publieke domein?
Dienen bedrijven ook niet in te loggen op beveiligingsniveau "Substantieel"?

Deze marktconsultatie is gericht op een middel waarmee burgers kunnen inloggen in het publieke domein. Het staat u vrij om tijdens deze consultatie voorstellen te doen voor bredere inzetbaarheid van een toe te laten middel.

1.2 Doelstelling marktconsultatie
De doelstellingen van deze marktconsultatie zijn:
1. Inventariseren of de markt inlogmiddelen kan leveren die voldoen aan onze toekomstige eisen;

Vraag 4:
Kunt u een roadmap aangeven betreffende de verwachte toekomstige eisen?

Deze marktconsultatie heeft als doel een beslissing te kunnen nemen over een mogelijk vervolgtraject, inclusief bijbehorende eisen.

2.3 Markt consultatie
een gesprekken ronde met partijen die zich hiervoor aanmelden.
Vraag 5:
Wij melden ons bij deze graag aan voor een gespreksronde

Deze afspraak is inmiddels gemaakt.

3.1 Waarom zoekt de overheid een alternatief naast DigiD op het niveau Substantieel?

DigiD wordt op dit moment doorontwikkeld naar het hogere betrouwbaarheidsniveau Substantieel en naar het niveau Hoog.
Vraag 6:
Op basis van de PIA van DigiD "Substantieel" kan niet anders worden geconcludeerd dan dat het huidige fundament van DigiD niet toereikend is om hier op voort te bouwen voor de beveiligingsniveaus "Substantieel" en "Hoog". Om nu al een pad naar de toekomst veilig te stellen dient het fundament optimaal te zijn. De state-of-the-art uit 2003 kan in 2017 nauwelijks de basis zijn voor de komende tien jaar tot 2027. Er dient een nieuw fundament te komen. Het opwaarderen van het huidige, al te kort schietende fundament is geen Privacy by Design. Kunt u zich in deze zienswijze vinden?

Nee

3.2 Wet GDI en de te stellen Eisen

De Wet Generieke Digitale Infrastructuur (Wet GDI)
Vraag 7:
In dit document wordt naar de Wet GDI verwezen terwijl die wet nog niet bestaat. Hoe moeten we daarmee om gaan?
In het voorstel van de wet GDI wordt pseudonimisering van het ID verplicht gesteld, terwijl dit door PKI-overheid verboden wordt om als common name een pseudoniem te gebruiken.
Het gebruik van een PKI-overheid certificaat is toegestaan in het wetsvoorstel GDI.
Wij zijn is zeer gebaat bij een goede oplossing, omdat een XX een PKI certificaat is, wat ons betreft een PKI-overheid certificaat, als de wet GDI dit niet tegenhoudt.
Op welke manier en wanneer gaat BZK dit oplossen?

Op rijksoverheid.nl is het wetsontwerp gepubliceerd. Het wetsvoorstel voorziet in een publiekrechtelijke grondslag voor de toelating van een privaat authenticatiemiddel ten behoeve van gebruik in het publieke domein en de (daaraan verbonden) nader te stellen eisen. De technische wijze waarop privacy wordt gewaarborgd zal niet in het wetsvoorstel zelf worden vastgelegd. Dit zal deel uitmaken van de eisen, die in het vervolgproces na de markconsultatie worden gesteld. BZK eist op het niveau substantieel geen uitgifte van een middel met PKI-overheid certificaat.

3.3 Pilots

Sinds 2016 nemen de marktpartijen iDIN (het inlogmiddel van de bankensector) en Idensys (een publiek-private samenwerkingsconstructie tussen het ministerie van Economische Zaken en een aantal private partijen) als uitkomst van een aanbesteding deel aan pilots voor identificatie en authenticatie in de (semi)publieke sector.
Vraag 8:
Wij willen dit jaar pilots starten in samenwerking met VWS. Is BZK bereid met ons in gesprek te gaan om te bepalen op welke manier er omgegaan wordt met het BSN?

Er worden geen nieuwe pilots gestart. BZK zal de koppeling met het BSNk voor de lopende pilots nog wel blijven ondersteunen tot uiterlijk eind 2018.

HOOFDSTUK 4

Algemeen

AG 2
BZK stelt op onderdelen van de hierboven bedoelde regelgeving nadere eisen of zal nadere eisen stellen. De eisen in de paragraaf 'Betrouwbaarheidsniveaus' zijn nadere aanvullingen op de eIDAS uitvoeringsverordening 2015 / 1502.
Vraag 9:
Zijn de hierna genoemde nadere eisen volledig of kunnen we nog aanvullingen verwachten? Is hier een roadmap voor ?

Zie vraag 4.

Privacy
PV1
4. De toepassing van privacy bevorderende technologieën;
Vraag 10:
Aan welke technologieën denkt u hierbij ?

De vraag is aan welke technologieën de aanbieder daarbij denkt.

Communicatie
CM 1
2. onthouden van uitingen die een vergelijk maken tussen publieke middelen en het aangeboden middel in de zin van 'veiliger of minder veilig';
Vraag 11:
Wat is de achtergrond van deze eis?

BZK staat geen negatieve vergelijkende reclame toe over het inlogmiddel DigiD ten faveure van het eigen inlogmiddel. Deze eis draagt bij aan het krijgen en behouden van vertrouwen van mensen in het inloggen bij de overheid.

3. conformeren aan de richtlijnen van BZK. In elk geval vereist massacommunicatie goedkeuring van BZK
Vraag 12:
Wat zijn de publiciteitsrichtlijnen, waar zijn deze te vinden ?

De richtlijnen zijn er nog niet. Als ze er zijn of komen, moet de aanbieder zich daar aan houden, zoals de eis dat vergelijkende reclameover gebruik in het BSN-domein goedkeuring vereist van BZK.

CM3

De Aanbieder waarborgt dat het inlog-keuzescherm dat de Gebruiker te zien krijgt als hij inlogt bij een Dienstverlener voldoet aan de nader te stellen richtlijnen van BZK.
Vraag 13:
Deze richtlijnen zijn wel essentieel en kunnen invloed hebben op betrouwbaarheid van de verbinding met de Dienstverlener. Wanneer worden deze richtlijnen bekend gemaakt.

Dat is nog niet bekend.

Aanvulling op eIDAS 2015 / 1502 Betrouwbaarheidsniveaus
AR2
De persoonsidentificatiegegevens worden overgenomen uit een gezaghebbende bron waaronder een Wettelijk Identiteitsbewijs (WID) en eventuele andere voorzieningen die door BZK beschikbaar worden gesteld.
UIT eIDAS:
"Er is geverifieerd dat de persoon in het bezit is van het bewijs dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat dit de opgegeven identiteit vertegenwoordigt en het bewijs is gecontroleerd op de echtheid ervan; of het bestaan ervan volgens een gezaghebbend bron bekend is en het betrekking
heeft op een werkelijk bestaand persoon en er maatregelen getroffen zijn om het risico te minimaliseren dat de identiteit van de persoon niet met de opgegeven identiteit overeenstemt, rekening houdend met bijvoorbeeld het risico dat het bewijsstuk verloren, gestolen, geschorst, ingetrokken of verlopen is".
In de PIA wordt aangegeven dat de gezaghebbende bron het BRP is.
Vraag 14:

Wat wordt er bedoeld met eventuele andere voorzieningen die door BZK beschikbaar worden gesteld?

Hiervoor verwijzen we u naar de beantwoording van de vragen van de andere marktpartijen. Deze is te vinden op TenderNed.

AR 3
De Aanbieder waarborgt dat de verplichte set persoonsidentificatiegegevens aan de centrale voorziening (BSNk) van BZK worden gezonden als extra waarborg van de juistheid, de identiteit en de integriteit van de persoonsgegevens.
Vraag 15:
In ons geval controleert XX de verplichte set persoonsidentificatie-gegevens in het BRP. Het BSNk is voor ons overbodig. Is dit met BZK bespreekbaar?

Het BSNk is essentieel als centrale registratie van de activering die noodzakelijk is voor de inzagefunctie t.b.v. de gebruiker (via MijnOverheid) en om periodieke verificatie van de gegevens mogelijk te maken.

AR 4
De Aanbieder waarborgt dat hij voldoende betrouwbaar in contact kan treden met de Gebruiker. Het kanaal waarover de communicatie verloopt moet in verband met mogelijk misbruik of verlies onafhankelijk zijn van het gebruik van het middel van de Gebruiker.
Vraag 16:
Twee communicatiekanalen kunnen op 'logisch' niveau gescheiden worden, waardoor twee kanalen fysiek eindigen in één device. Is deze oplossing voor BZK acceptabel? Waarom wel / niet?

De eis geeft juist aan dat: 1) Als voor het contact met de gebruiker - in geval van verlies - geen alternatief is behalve het betreffende device dat ook het middel bevat, wordt niet voldaan aan de betreffende eis. 2) Ook wanneer bijvoorbeeld een smartphone-device waarop het middel is geïmplementeerd gecorrumpeerd raakt moet nog steeds betrouwbaar contact met de Gebruiker mogelijk zijn. Een daadwerkelijk persoonlijk telefoongesprek of brief ligt dan meer voor de hand dan bijvoorbeeld een SMS- of Whatsapcommunicatie.

Bewijs en verificatie van identificatie

BI1
De Aanbieder waarborgt dat hij de persoonsidentificatiegegevens die hij ontvangt verifieert aan een gezaghebbende bron*).
*) Als gezaghebbend gelden hier het Wettelijk Identificatie Document van de aanvrager en eventuele voorzieningen die BZK daarvoor ter beschikking stelt.
Vraag 17:
De gezaghebbende bron is toch het BRP, zoals o.a. gesteld in de PIA van DigiD "Substantieel"?

Het WID wordt beschouwd als een voldoende betrouwbare afgeleide van de brongegevens in de BRP. In het gehele verificatieproces van de gegevens is voorzien dat ook andere van de BRP afgeleide gezaghebbende bronnen een rol kunnen spelen.

BI2
Een vorm van 'identificatie op afstand' kan worden toegestaan mits de kwaliteit daarvan in een door BZK te bepalen mate overeenkomt met een daadwerkelijk fysieke identificatie.
Vraag 18:
Wanneer zijn de sterke standaarden hiervoor beschikbaar

Het is aan de Aanbieder om faciliteiten in te richten om in het verificatieproces de echtheid en geldigheid van identiteitsbewijzen adequaat te controleren en om personen (al dan niet fysiek) te identificeren. BZK zal in dit stadium geen specificaties geven waarmee identificatie op afstand

gelijkwaardig is aan fysieke identificatie.

eIDAS 2.2.2 Uitgifte, uitreiking en activering
UA1
De Aanbieder waarborgt dat de Gebruiker in staat is om afwijkingen te ontdekken in het proces voor uitgifte, uitreiking en activering.
Vraag 19:
De Gebruiker heeft geen notie van het technische proces, kunt u aangeven welke afwijkingen ontdekt moeten kunnen worden?

Deze eis doelt niet op achterliggende technische processen. Bedoeld is dat de gebruiker op de hoogte is gebracht van wat hij kan verwachten bij aanvraag, uitreiking en activering van het middel en daarmee dus in staat is om afwijkingen te constateren.

UA3
Authenticatiefactoren via gescheiden kanalen en gescheiden in tijd worden verstrekt;
Vraag 20:
Welke kanaal scheiding is voldoende?

De kanaalscheiding heeft hier betrekking op de procedure voor de uitreiking van het middel. Gescheiden kanaal betekent dat minimaal twee verschillende wegen worden gebruikt waarmee de authenticatie-factoren worden verstrekt. Het versturen van een smartcard via de post en een week later ook de pin versturen via de post voldoet - behoudens ten aanzien van enkele bijzondere/specifieke groepen personen - dus niet. Dergelijke uitgifteprocessen zijn te voorspelbaar te manipuleren.

De status van de abonneerelatie wordt geregistreerd bij een nader te bepalen centrale voorziening van BZK
Vraag 21:
Kunnen wij nadere uitleg ontvangen over welke voorziening hier bedoeld wordt?

Hiervoor verwijzen we u naar de beantwoording van de vragen van de andere marktpartijen. Deze is te vinden op TenderNed.

eIDAS 2.2.3 Schorsing, Herroeping en Reactivering
SR2
De Aanbieder waarborgt dat hij bij gerede vermoedens van misbruik het middel intrekt of schorst.
Vraag 22:
Kunt u "gerede vermoedens" vastleggen om te voorkomen dat de Aanbieder het risico loopt van te vroeg dan wel te laat in te grijpen?

Nee, de Aanbieder richt zelf zijn eigen doeltreffende detectiefaciliteiten in, die zijn afgestemd op zijn eigen specifieke technische oplossing en omgeving. De aanbieder hanteert voor de beoordeling een daarop afgestemd eigen afwegingskader. Het beleid van BZK rond de Aanbieder overstijgende misbruikbestrijding is in ontwikkeling en naar verwachting bij een mogelijk vervolgtraject bekend.

eIDAS 2.2.4 Verlenging en vervanging
VV1
De Aanbieder waarborgt dat minimaal 1 maal per 3 jaar opnieuw de geregistreerde persoonsidentificatiegegevens van de Gebruiker aan een betrouwbare bron (zie 2.1.2) worden geverifieerd.
Vraag 23:
Wat is de reden hiervan? Zou dit ook gelden bij een middel op niveau "Hoog"?

Het koppelen van geldigheid van een middel aan een specifieke technische levensduur is vanuit het

oogpunt van de regelgever weinig zinvol, omdat de technische levensduur van diverse mogelijke middelen zeer uiteen kan lopen. De essentie, de geldigheid van een middel, is daarom gekoppeld aan een geldigheidsduur van een identificatie. Dit houdt meer rekening met de diverse zogenaamde levensgebeurtenissen (life-events) zoals naamsveranderingen en overlijden.

VV2

De Aanbieder waarborgt dat als hij één enkele authenticatiefactor van het middel vervangt, de uitgifte van deze authenticatiefactor met dezelfde betrouwbaarheid plaatsvindt als de initiële uitgifte van die authenticatiefactor. De vervanging van één enkele authenticatiefactor mag de betrouwbaarheid van het uitgegeven middel in elk geval niet aantasten.

Vraag 24:

Hoe kijkt u naar het in zijn geheel vervangen van het middel? Vanuit ons denken wij dat een middel met verschillende authenticatiefactoren niet gaat werken, alleen al omdat de historie van eenzelfde middel met verschillende authenticatiefactoren verwarring geeft.

Bent u bereid dit in uw overweging mee te nemen en zeker niet verplicht te stellen? Een XX middel kan alleen vervangen worden en niet worden aangepast.

Het beleid voor het eventueel vervangen van een volledig middel is aan de Aanbieder. Bij geheel vervangen van een middel wordt ook voldaan aan de betreffende eis. De achtergrond van de eis is dat met deze vrijheidsgraad de kosten van vervanging beperkt kunnen worden wanneer slechts enkel een wachtwoord of PIN door de gebruiker is vergeten of een smartcard wordt vermist.

eIDAS 2.3.1 Authenticatiemechanisme

AM2

De informatie van de Aanbieder moet voldoende betrouwbaar zijn, ook als applicatie voor het aanloggen of het platform waarop deze applicatie actief is, gecorrumpeerd is.

Vraag 25:

Graag nadere uitleg wat hiermee voorgesteld wordt?

Voorbeeld: Indien met een Browser op een PC of 'smart-device' wordt ingelogd bij de Belastingdienst om de belastingaangifte in te vullen, moet de gebruiker worden bericht dat hij op het punt staat om bij de Belastingdienst in te loggen om zijn aangifte te doen. Deze berichtgeving moet voldoende betrouwbaar zijn, ook als de browser op de PC of smart-device is gecorrumpeerd. Het bericht moet dus in zekere mate beschermd zijn tegen manipulatie.

eIDAS 2.4.2 Informatie voor Gebruikers

IG1

De Aanbieder waarborgt dat Gebruiker de rechtmatigheid van de uitgifte van een authenticatiemiddel op zijn identiteit kan controleren in een door BZK gefaciliteerde voorziening*).

Vraag 26:

Mag dat ook een voorziening van de Aanbieder zijn, welk onderdeel is van de audit ?

Nee, de Aanbieder wordt niet gevraagd om de bedoelde BZK-voorziening te leveren. Maar zie IG2: ook de Aanbieder moet aan de Gebruiker gegevens kunnen tonen met betrekking tot het middel dat de Aanbieder aan de gebruiker heeft uitgegeven.

BZK stelt nadere eisen over hoe de Aanbieder zijn bijdrage aan de bedoelde centrale voorziening levert.

Vraag 27:

Wanneer komen deze eisen beschikbaar?

Zie vraag 4.

eIDAS 2.4.3 Informatiebeveiliging

IB2

De Aanbieder waarborgt dat hij risico's mitigeert die relevant zijn voor de diensten die hij aanbiedt. De Aanbieder geeft aan welke risicogebieden hij relevant acht voor zijn dienstverlening.

Vraag 28:
Kunt u een minimale lijst van risicogebieden aangeven?

De vraag betreft het geven van inzicht aan BZK over de risicogebieden die de Aanbieder zelf relevant acht voor zijn oplossing.

IB3
Meldingen door de Aanbieder aan door BZK nader te omschrijven centrale functie;
Vraag 29:
Wat wordt hier mee bedoeld?

Hiervoor verwijzen we u naar de beantwoording van de vragen van de andere marktpartijen. Deze is te vinden op TenderNed.

eIDAS 2.4.4 Bijhouden van Administratie
BA1
De Aanbieder waarborgt de archivering van de gegevens en de bijbehorende bewaartermijnen die door BZK met nadere richtlijnen worden vast gesteld.
Vraag 30:
Welke gegevens vallen onder de archiveringswet?
Wordt de bewaar termijn van loggegevens blijvend gesteld op 5 jaar? Dit geeft een enorme opslagbehoefte en vergroot het risico op profiling?

Het beleid van BZK rond archivering en bewaartermijnen rond de thema's navraag, beslechten van geschillen en misbruikbestrijding is naar verwachting bij de start van het eventuele vervolgtraject beschikbaar.

eIDAS 2.4.5 Faciliteiten en personeel

FP1
De Aanbieder waarborgt in continuïteit de integriteit van het bij de dienstverlening betrokken personeel.
Vraag 31:
Continuïteit dienstverlening kan verlangd worden, maar van personeel is dit niet reëel, kunt u dit beter omschrijven?

Nee. Met de term 'in continuïteit' wordt bedoeld 'bij voortduring'. Het afleggen van een 'eed' is of 'VOG' is een eenmalige momentopname en dus niet voldoende als continue waarborg van personele integriteit.

FP2
Als referentie voor de kwaliteit van de opleiding voor uitvoering van de identificatie geldt het proces voor uitgifte van paspoorten en rijbewijzen.
Vraag 32:
Op welke manier kunnen wij deze beschrijving ontvangen?

De Nederlandse Vereniging voor Burgerzaken kan als bron worden gebruikt. De Aanbieder dient aan te tonen dat de kwaliteit van de opleiding die zijn personeel heeft genoten in dit kader gelijkwaardig is.

eIDAS 2.4.7 Compliance en Audit
CA1
De Aanbieder waarborgt dat hij aantoonbaar voldoet aan alle gestelde eisen. Dit betreft zowel de naleving van de in paragraaf Algemeen genoemde eIDAS-verordeningen als de naleving van de nadere eisen die door BZK zijn gesteld en nog worden gesteld.
Vraag 33:
Wanneer worden deze openbaar? In welke richting(en) gaan uw gedachten?

Zie vraag 4.

CA2
De nadere richtlijnen bevatten o.a. betrokkenheid van:
1. Een Certificerende Instelling;
2. Een Toezichthouder namens BZK;
3. BZK zelf.
Vraag 34:
Wanneer worden de nadere richtlijnen bekend?
Aan welke certificering dient voldaan te worden?
Wie wordt de toezichthouder?

Zie vraag 4.

Techniek en functionaliteit
Doelstelling: Privacy by Design
PT1
De Aanbieder waarborgt de toepassing van de AVG-beginselen, onder andere het beginsel van 'privacy by design' inzake het ontwerp en de implementatie van de gevraagde diensten en de toepassing van het principe van dataminimalisatie op controleerbare wijze is toegepast.
Vraag 35:
Draagt BZK er zorg voor dat ook bij PKI-overheid dataminimalisatie wordt doorgevoerd, eenzijdige data minimalisatie heeft geen zin

De Aanbieder toont aan dat hij de bedoelde beginselen heeft gehanteerd en die verplichting omvat tevens de relevante toeleveranciers indien de Aanbieder daar gebruik van maakt.

Ondersteuning pseudoniemen
PT3
De Aanbieder waarborgt dat naast identiteit (BSN) ook alléén een pseudoniem kan worden geleverd aan Dienstverleners.
Vraag 36:
Wordt dit door de Dienstverlener gevraagd of is dit een generieke dienst voor vooraf bepaalde Dienstverleners?

De uitvraag wordt gedaan door de Dienstverlener of een faciliterende tussenpartij.

PT4

De Aanbieder waarborgt dat de door hem gebruikte pseudoniemen mede voldoen aan de richtlijnen van de Autoriteit Persoonsgegevens [1.]. Dit betekent onder meer dat een pseudoniem Dienstverlener specifiek moet zijn en alleen bekend is bij de betreffende Dienstverlener.
Vraag 37:
Hoe kunnen we in bezit komen van de AP richtlijnen?

Het AP publiceert ze op zijn website; een referentie staat in het marktconsultatiedocument.

PT7
Het BSN mag geen persistent onderdeel zijn van de opgeslagen met betrekking tot de identiteit van de Gebruiker.
Vraag 38:
Onduidelijke zin, graag nadere uitleg?

Weggevallen zinsdeel: …van de opgeslagen “gegevens”…

Waarborg Gebruiksvriendelijkheid voor Gebruikers en Dienstverleners
WG1

Compatibele pseudoniemen
De Aanbieder waarborgt dat de door hem gebruikte pseudoniemen compatibel zijn met de gebruikte pseudoniemen van de Publieke middelen.
Vraag 39:
Welke pseudoniemen worden hier bedoeld? Zijn deze beschikbaar?

Hierover volgen nadere uitspraken in een mogelijk vervolgtraject.

WG2
Europese interoperabiliteit: unieke identificatiecode
De Aanbieder waarborgt dat in het geval zijn middelen in andere Europese lidstaten bruikbaar zijn, hij zich conformeert aan de Nederlandse standaarden voor het genereren van een 'unieke identificatiecode' voor Gebruikers in de zin van [2.]
Vraag 40:
Wordt hiermee de onder punt 2 beschreven methode (in welke document) bedoeld? Wat zijn de Nederlandse standaarden?

[2.] is een referentie naar een bron in hetzelfde document.

WG3
Interoperabiliteit met Publieke diensten voor vertegenwoordiging en attribuutverstrekking.
De Aanbieder waarborgt dat een Gebruiker met zijn middel gebruik kan maken van de Publieke diensten voor 'vertegenwoordiging', 'attribuutverstrekking' en via een 'routeringsdienst' kan inloggen op online diensten van Dienstverleners. BZK draagt zorg voor voorzieningen die de naleving van deze eis ondersteunen. BZK stelt nadere eisen aan de wijze waarop deze interoperabiliteit vorm gegeven wordt.
Vraag 41:
Welke voorzieningen wil BZK hiervoor inrichten? Wellicht zijn die voor ons niet nodig?

Hiervoor verwijzen we u naar de beantwoording van de vragen van de andere marktpartijen. Deze is te vinden op TenderNed.

Routeringsdienst: De voorziening die zowel de publieke als private authenticatiemiddelen ontsluit ter ontzorging van de Dienstverleners die daar voor kiezen.
Vraag 42:
Is Routeringsdienst hier de inlogknop met de diverse mogelijkheden van inlog? Valt het koppelvlak hierbuiten?

De routeringsdienst is er ter ontzorging van, met name, de Dienstverlener. Voor de Aanbieder als Authenticatiedienst is dit voor het overgrote deel transparant.

Bescherming tegen misbruik
BS1
De Aanbieder waarborgt in samenwerking met door BZK aan te wijzen beheerders van de publieke middelen dat, het management van misbruik over de keten (identiteitsfraude en fraude over ketens heen) kan worden georganiseerd.
Vraag 43:
Hier wordt toch de *bestrijding* van misbruik over de keten bedoeld?

Het primaire doel van de bestrijding van misbruik over de keten heen is het bescherming van Gebruikers en Dienstverleners.