



Marktconsultatie eID: privaat inlogmiddel of –middelen

Opdrachtgever:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Uitvoerder:

Centrum voor Facilitaire Dienstverlening
Inkoopuitvoeringscentrum Belastingdienst
John. F. Kennedylaan 8
7314 PS Apeldoorn

Datum : 4 oktober 2017

INHOUDSOPGAVE

| | |
|---|-----------|
| HOOFDSTUK 1: ALGEMEEN | 2 |
| 1.1 AANLEIDING | 2 |
| 1.2 DOELSTELLING MARKTCONSULTATIE | 2 |
| 1.3 OPDRACHTGEVER..... | 2 |
| 1.4 UITVOERDER MARKTCONSULTATIE | 3 |
| 1.5 RANDVOORWAARDEN MARKTCONSULTATIE | 3 |
| 1.6 LEESWIJZER..... | 3 |
| HOOFDSTUK 2: DE TE VOLGEN PROCEDURE | 4 |
| 2.1 ALGEMEEN | 4 |
| 2.2 AANKONDIGING | 4 |
| 2.3 MARKTCONSULTATIE..... | 4 |
| 2.4 AANLEVEREN GEGEVENS MARKTCONSULTATIE | 4 |
| 2.5 COMMUNICATIE TIJDENS DE MARKTCONSULTATIE | 4 |
| 2.6 UITERSTE DATUM VOOR AANLEVERING VAN DE BEANTWOORDING | 4 |
| 2.7 VOORWAARDEN AAN DE BEANTWOORDING | 5 |
| 2.8 VERTROUWELIJKHEID | 5 |
| 2.9 PLANNING | 5 |
| HOOFDSTUK 3: ACHTERGROND | 6 |
| 3.1 WAAROM ZOEKT DE OVERHEID EEN ALTERNATIEF NAAST DIGID OP HET NIVEAU SUBSTANTIEEL? | 6 |
| 3.2 WET GDI EN DE TE STELLEN EISEN | 6 |
| 3.3 PILOTS | 7 |
| HOOFDSTUK 4: VERTREK PUNT VOOR EISEN..... | 8 |
| HOOFDSTUK 5: VRAGEN AAN DE MARKT | 20 |
| HOOFDSTUK 6: BIJLAGEN..... | 21 |
| BIJLAGE 1: BEGRIPPENLIJST | 21 |
| BIJLAGE 2: RELEVANTE DOCUMENTEN EN WETGEVING | 22 |
| BIJLAGE 3: RELEVANTE TWEDE KAMERSTUKKEN | 23 |

HOOFDSTUK 1: ALGEMEEN

1.1 Aanleiding

De dienstverlening door overheidsorganisaties geschiedt steeds meer digitaal. Om zaken te kunnen doen met de overheid moet de burger inloggen en zich identificeren en authenticeren. Tot nu toe geschiedt het inloggen met het publieke middel DigiD.

Voor online identificeren en authenticeren is het programma eID gestart (elektronische identiteit). De centrale doelstellingen van het programma eID zijn:

- het verhogen van het betrouwbaarheidsniveau van de toegang tot digitale overheidsdienstverlening;
- het waarborgen van de continuïteit van het stelsel van elektronische identificatie en authenticatie.

Betrouwbaarheidsniveau

De overheid ontwikkelt publieke eID-middelen op hogere betrouwbaarheidsniveaus. Ook kunnen één of meerdere private eID-middelen voor gebruik in de (semi)publieke sector worden toegelaten.

Continuïteit

Met de toename van de digitale dienstverlening neemt ook het belang van stabiele beschikbaarheid toe van een stelsel voor identificatie en authenticatie voor alle burgers en voor alle dienstverleners in de (semi)publieke sector. Maatregelen zijn nodig om de risico's te beperken van langdurige uitval van DigiD of wanneer de betrouwbaarheid of veiligheid niet meer kan worden gewaarborgd.

Om de continuïteit te waarborgen is het wenselijk dat zo snel mogelijk één of meerdere betaalbare alternatieven voor het huidige DigiD breed beschikbaar komen op betrouwbaarheidsniveau Substantieel; thans wordt in deze marktconsultatie niet gevraagd naar een alternatief op betrouwbaarheidsniveau Hoog. De genoemde alternatieven op betrouwbaarheidsniveau Substantieel zijn enkel bedoeld voor burgers en niet voor bedrijven.

1.2 Doelstelling marktconsultatie

De doelstellingen van deze marktconsultatie zijn:

1. Inventariseren of de markt inlogmiddelen kan leveren die voldoen aan onze toekomstige eisen;
2. Het toetsen en aanscherpen van de doelstellingen en de eisen van een mogelijk vervolgtraject, onder andere gericht op technische haalbaarheid, wenselijkheid en gebruik makend van alle mogelijkheden waarop aan de eisen kan worden voldaan. De doelstellingen vindt u in paragraaf 1.1. Een vertrekpunt voor de eisen is opgenomen in hoofdstuk 4.

Voor de markt biedt deze consultatie dus de mogelijkheid om voorafgaand aan een mogelijk vervolgtraject invloed uit te oefenen op de doelstellingen en de eisen die daarin gesteld worden.

1.3 Opdrachtgever

Opdrachtgever voor deze Marktconsultatie is de Staat der Nederlanden gevestigd te 's-Gravenhage, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK).

ICT Categoriemanagement

Ter ondersteuning van (generieke) bedrijfsprocessen zet de Rijksoverheid ICT-oplossingen in die vanuit de ICT-categorieën worden verworven. De ICT-categoriemanager kent de markt en de relevante ontwikkelingen, specialiseert zich in de inkoop en het contracteren van de ICT-oplossingen, weet wat wenselijke voorwaarden zijn, ook naar de toekomst toe, waar aandachtspunten zitten en hoe afspraken passend gemaakt kunnen worden. Ook het managen van de tot stand gebrachte (raam)overeenkomsten, valt onder de verantwoordelijkheid van de ICT-categoriemanager.

1.4 Uitvoerder marktconsultatie

Namens BZK coördineert het IUC van de Belastingdienst/Centrum voor Facilitaire Dienstverlening deze marktconsultatie. Het IUC Belastingdienst heeft ten aanzien van dit traject een onafhankelijke rol, en is dus onafhankelijk van de Belastingdienst in de rol van dienstaanbieder die gebruik zal maken van authenticaties met eID-middelen.

Inkoopuitvoeringscentrum Belastingdienst

Het IUC Belastingdienst is onderdeel van Belastingdienst/Centrum voor facilitaire dienstverlening (B/CFD) en verricht generieke inkoopactiviteiten voor de bij haar ondergebrachte Rijkscategorieën en daarnaast zorgt zij voor de specifieke inkoop van de Belastingdienst en Domeinen Roerende Zaken. Zie voor meer informatie over de organisatie van de Belastingdienst de internetsites www.belastingdienst.nl en www.rijksoverheid.nl/ministeries/fin.

1.5 Randvoorwaarden marktconsultatie

Deze marktconsultatie dient uitdrukkelijk niet om een voorselectie te maken van gegadigden in het kader van een eventueel uit te voeren vervolgtraject. Evenmin zullen bij de marktconsultatie betrokken partijen op enige wijze worden uitgesloten van eventuele participatie in een mogelijk vervolgtraject.

Marktpartijen komen door deel te nemen aan de marktverkenning niet in een bevoordeelde of benadeelde positie op het moment van een mogelijk vervolgtraject.

Deelnemers aan de marktconsultatie kunnen geen rechten ontlenen aan deelname aan de marktconsultatie of aan enige informatie die tijdens de marktconsultatie wordt verstrekt. Marktpartijen kunnen geen rekening sturen of anderszins aanspraak maken op een (geldelijke of andere) vergoeding voor hun bijdrage aan de consultatie.

De informatie uit de marktconsultatie zal gebruikt worden om de doelstellingen en eisen aan te scherpen van een mogelijk vervolgtraject.

1.6 Leeswijzer

In hoofdstuk 2 is aangegeven welke procedure gevolgd wordt bij deze marktconsultatie. Hoofdstuk 3 schetst de achtergrond van de doelstellingen van het programma eID en deze marktconsultatie. Hoofdstuk 4 bevat een vertrekpunt voor de eisen aan een eID-middel en de aanbieder. Hoofdstuk 5 bevat vragen van BZK aan de markt. Hoofdstuk 6 bevat een overzicht van begrippen en bijlagen.

HOOFDSTUK 2: DE TE VOLGEN PROCEDURE

2.1 Algemeen

De aanvragende dienst is:
Belastingdienst/Centrum voor facilitaire dienstverlening (B/CFD)
Inkoopuitvoeringscentrum Belastingdienst.

Contactpersoon:

De heer R.R. Kalksma (Senior Inkoopspecialist ICT IUC Belastingdienst)
Contact via de berichtenfunctie op TenderNed.

2.2 Aankondiging

Deze marktconsultatie wordt via www.TenderNed.nl gepubliceerd.

2.3 Marktconsultatie

Deze marktconsultatie bestaat uit een schriftelijke vragenlijst die door marktpartijen beantwoord kunnen worden (hoofdstuk 5) en een gesprekkenronde met partijen die zich hiervoor aanmelden.

De gesprekkenronde start en eindigt voordat de schriftelijke beantwoording ingediend moet zijn, en heeft als doel om meer diepgang en inhoud te geven aan de marktconsultatie.

De (individuele) gesprekken zullen verlopen aan de hand van een vooraf vastgestelde agenda die bij elk gesprek gehanteerd zal worden. Van de gesprekken wordt een gespreksverslag gemaakt. Iedere marktpartij krijgt het gespreksverslag van zijn eigen gesprek ter informatie toegestuurd. Eventuele opmerkingen en aanvullingen kunnen binnen twee werkdagen worden ingediend.

Indien partijen waarde hechten aan een individueel gesprek dienen zij dit uiterlijk 18 oktober 2017 aan te geven via de contactpersoon voor deze marktconsultatie.

Indien er na het indienen van de schriftelijke beantwoording aanvullende vragen zijn, zullen deze worden toegestuurd aan alle partijen die hebben deelgenomen aan de marktconsultatie. BZK behoudt zich het recht voor een mondelinge toelichting te vragen naar aanleiding van de ingediende beantwoording.

2.4 Aanleveren gegevens marktconsultatie

Wij verzoeken u de beantwoording in de Nederlandse taal te doen.

2.5 Communicatie tijdens de marktconsultatie

Tijdens de marktconsultatie verloopt alle communicatie met betrekking tot dit onderwerp via de berichtenmodule in TenderNed.

2.6 Uiterste datum voor aanlevering van de beantwoording

Wij verzoeken u de beantwoording uiterlijk, digitaal via TenderNed, aan te leveren op vrijdag 1 december 2017, 16:00 uur.

Wijze van aanlevering van de beantwoording

- Via TenderNed;
- Alle documentatie mag als PDF-bestand worden aangeleverd.

2.7 Voorwaarden aan de beantwoording

Het deelnemen aan de marktconsultatie is voor zowel deelnemers, als de Staat der Nederlanden, vrijblijvend. Partijen (inclusief partijen die niet deelnemen aan de marktconsultatie) kunnen aan deze marktconsultatie geen (wederzijdse) verplichtingen of rechten jegens de Staat der Nederlanden ontleen.

Voor de beantwoording en de daarvoor uit te voeren werkzaamheden en te verstrekken materialen kunnen aan de Staat der Nederlanden geen kosten in rekening worden gebracht.

2.8 Vertrouwelijkheid

Conform artikel 10, eerste lid, onderdeel c, van de Wet openbaarheid van bestuur behandelt BZK alle informatie die in het kader van deze marktconsultatie door marktpartijen wordt verstrekt als vertrouwelijk, tenzij de marktpartij zelf aangeeft dat (een deel van) die informatie openbaar gemaakt kan worden.

2.9 Planning

| Activiteit | Datum |
|---|----------------------------|
| Publiceren Marktconsultatie | 4 oktober |
| Indienen vragen over consultatie door marktpartijen & aanmelden voor de gesprekkenronde | 18 oktober 2017 |
| Vragen van marktpartijen beantwoord | 25 oktober 2017 |
| Einde gesprekkenronde | 17 november 2017 |
| Schriftelijke reactie marktpartijen | 1 december 2017, 16:00 uur |

HOOFDSTUK 3: ACHTERGROND

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

Inloggen door burgers op de digitale dienstverlening van de Nederlandse overheid geschiedt met het middel DigiD. DigiD wordt gebruikt door ca. 13,6 miljoen Nederlanders, die in 2016 zo'n 280 miljoen keer inlogden bij overheidsdienstverleners.

Het huidige DigiD kent het betrouwbaarheidsniveau Laag: DigiD Basis (inlognaam en wachtwoord) en DigiD Midden (2-factorauthenticatie met SMS of App). 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. Een link naar deze verordening vindt u in hoofdstuk 6.

Met DigiD als enige beschikbare inlogmiddel, is het huidige stelsel van identificatie en authenticatie bij de overheid kwetsbaar voor storingen, hacks en inbraak. Korter of langer durende uitval is niet uitgesloten. Indien DigiD door een ernstige storing of inbraak in het informatiesysteem (tijdelijk) niet gebruikt kan worden, lopen bepaalde vormen van digitale dienstverlening aan burgers vast, met alle maatschappelijke gevolgen van dien.

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. BZK streeft om bovenstaande redenen naar een zo snel als mogelijke marktintroductie, uiterlijk eind 2018.

3.2 Wet GDI en de te stellen Eisen

De Wet Generieke Digitale Infrastructuur (Wet GDI) zal in de toekomst de wettelijke grondslag vormen voor online identificatie en authenticatie bij de overheid. De Wet GDI wordt op dit moment ontworpen.

Een eerdere versie van de Wet GDI is inclusief de toenmalige Uniforme Set van Eisen in 2016 gepubliceerd op www.internetconsultatie.nl. U vindt een link naar de internetconsultatie in hoofdstuk 6. Eén van de keuzes naar aanleiding van de internetconsultatie is om – naast het doorontwikkelde publieke middel DigiD – één of meer alternatieve middelen toe te laten tot het publieke domein. Er wordt dus niet meer voorzien in een regulier vergunningstelsel (waarbij alle partijen worden toegelaten die aan de criteria voldoen).

De belangrijkste wijzigingen naar aanleiding van de internetconsultatie zijn in juni 2017 gemeld in de brief aan de Tweede Kamer (zie hoofdstuk 6, bijlage 3). De reacties zijn verwerkt in een bijgestelde versie van de Wet GDI die op 29 augustus 2017 voor advies is voorgelegd aan de Autoriteit Persoonsgegevens (zie de link in hoofdstuk 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. In deze marktconsultatie wordt een vertrekpunt voor eisen aan private eID-middelen en -aanbieders gepresenteerd (hoofdstuk 4), bedoeld om met de markt in gesprek te gaan.

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. Deze pilots zijn geëvalueerd onder regie van de commissie Kuipers (augustus 2016; zie hoofdstuk 6, bijlage 3).

HOOFDSTUK 4: VERTREKPUNT VOOR EISEN

De eisen die in dit hoofdstuk zijn genoemd, vormen een vertrekpunt om te komen tot een set van eisen voor een mogelijk vervolgtraject.

| | |
|------|---|
| | Algemeen |
| AG 1 | De Aanbieder levert diensten op het betrouwbaarheidsniveau 'substantieel' zoals bedoeld is in de eIDAS-verordening 910 / 2014 en de daaraan gekoppelde uitvoeringsverordeningen 2015 / 1501 en 2015 / 1502. |
| AG 2 | <p>De Aanbieder voldoet aan de betreffende Europese regelgeving, in het bijzonder de eIDAS Uitvoeringsverordening 2015 / 1502 inzake de inrichting van de betrouwbaarheidsniveaus van authenticatiemiddelen en de wettelijke verplichtingen inzake privacywaarborgen voor Gebruikers.</p> <p>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.</p> |
| | Privacy |
| PV1 | <p>BZK stelt nadere eisen inzake naleving van de relevante privacyregelgeving zodat het voor BZK controleerbaar wordt dat de Aanbieder adequate waarborgen heeft geïmplementeerd om de dienstverlening te laten voldoen aan de privacyregelgeving. De nadere eisen betreffen in elk geval:</p> <ol style="list-style-type: none"> 1. De verwerking van persoonsgegevens binnen de vastgestelde doelen en bewaartermijnen; 2. Verwerking van persoonsgegevens, waaronder scheiding, van gebruikersinformatie en gebruiksinformatie; 3. Het management van de geïmplementeerde privacywaarborgen waaronder uitvoeren van analyses en opvolging van bevindingen; 4. De toepassing van privacybevorderende technologieën; |

| | |
|--|---|
| | Communicatie |
| CM1 | <p>De Aanbieder waarborgt dat zijn communicatie-uitingen over het wettelijke kader voor het gebruik van zijn authenticatiemiddelen voldoen aan de nadere richtlijnen die BZK daarover stelt. De Aanbieder moet bij communicatie-uitingen in elk geval zich:</p> <ol style="list-style-type: none"> 1. onthouden van uitingen die het vertrouwen van Gebruikers in authenticatiemiddelen ondermijnen; 2. onthouden van uitingen die een vergelijk maken tussen publieke middelen en het aangeboden middel in de zin van 'veiliger of minder veilig'; 3. conformeren aan de richtlijnen van BZK. In elk geval vereist massacommunicatie goedkeuring van BZK. |
| CM2 | <p>De Aanbieder waarborgt dat hij zich conformeert aan de nader te stellen richtlijnen van BZK over de communicatie en de organisatie daarvan in geval van gebeurtenissen die naar hun ernst publieke communicatie vereisen. In elk geval verlopen de perscontacten in deze gevallen via BZK of met goedkeuring van BZK.</p> |
| CM3 | <p>De Aanbieder waarborgt dat het inlog-keuzescherf dat de Gebruiker te zien krijgt als hij inlogt bij een Dienstverlener voldoet aan de nader te stellen richtlijnen van BZK.</p> |
| CM4 | <p>De Aanbieder waarborgt dat hij in zijn algemene communicatie over zijn aangeboden middel ook verwijst naar de door BZK aangewezen informatie op de website 'rijksoverheid.nl'. Dit betreft zowel de communicatie op de websites van de Aanbieder als de communicatie via andere media. De kosten voor communicatie over het aangeboden middel komen in principe voor rekening van de Aanbieder.</p> |
| Aanvulling op eIDAS 2015 / 1502 | Betrouwbaarheidsniveaus |
| <i>eIDAS 2.1.1.</i> | <i>Aanvraag en registratie</i> |
| AR1 | <p>De Aanbieder waarborgt dat de Gebruiker bekend is gemaakt met de wettelijke- en andere door BZK nog nader te bepalen voorwaarden voor het gebruik van zijn middel. De voorwaarden bevatten in elk geval de verplichting voor de Gebruiker om zijn middel veilig te beheren en gebruiken en om vermoedens van misbruik te melden aan de Aanbieder.</p> |

| | |
|--------------------|---|
| AR2 | <p>De Aanbieder waarborgt ten behoeve van de uitgifte van het middel de registratie van de juiste persoonsidentificatiegegevens van de Gebruiker.</p> <p>In elk geval moeten worden geregistreerd*):</p> <ol style="list-style-type: none"> 1. Voorletters of Voornamen 2. Achternaam 3. Geboortedatum 4. Burger Service Nummer**) <p>De persoonsidentificatiegegevens worden overgenomen uit een gezaghebbende bron waaronder een Wettelijk Identiteitsbewijs (WID) en eventuele andere voorzieningen die door BZK beschikbaar worden gesteld.</p> <p>*) De Aanbieder waarborgt dat als zijn authenticatiemiddel in andere EU-lidstaten bruikbaar moet zijn dat de set van te verstrekken persoonsgegevens bij een authenticatie voldoet aan de Europese uitvoeringsverordening 2015/1501.</p> <p>***) Na verwerking mag het BSN niet worden gearchiveerd tenzij er andere wettelijke kaders dan de wet GDI zijn die archivering vereisen.</p> |
| AR3 | <p>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.</p> |
| AR4 | <p>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.</p> |
| <i>eIDAS 2.1.2</i> | <i>Bewijs en verificatie van identificatie</i> |
| BI1 | <p>De Aanbieder waarborgt dat hij de persoonsidentificatiegegevens die hij ontvangt verifieert aan een gezaghebbende bron*).</p> <p>*) Als gezaghebbend gelden hier het Wettelijk Identificatie Document van de aanvrager en eventuele voorzieningen die BZK daarvoor ter beschikking stelt.</p> |

| | |
|------------------------|--|
| BI2 | <p>De Aanbieder waarborgt dat de identiteit van de aanvrager overeenkomt met de persoonsidentificatiegegevens die de aanvrager verstrekt.</p> <p>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.</p> |
| BI3 | <p>De Aanbieder waarborgt dat hij beschikt over adequaat opgeleid personeel en faciliteiten (zie ook 2.4.5) om het risico te mitigeren dat een middel onder andere wordt uitgegeven:</p> <ol style="list-style-type: none"> 1. Op basis van een vals identiteitsbewijs 2. Op basis van een ongeldig identiteitsbewijs 3. Als gevolg van persoonsverwisseling |
| <i>eIDAS 2.2.1</i> | <i>Kenmerken en ontwerp van authenticatiemiddelen</i> |
| KO1 | De Aanbieder waarborgt dat een eenmaal uitgegeven middel NIET aan een andere identiteit wordt gekoppeld. |
| <i>eIDAS 2.2.2</i> | <i>Uitgifte, uitreiking en activering</i> |
| UA1 | De Aanbieder waarborgt dat de Gebruiker in staat is om afwijkingen te ontdekken in het proces voor uitgifte, uitreiking en activering. |
| UA2 | De Aanbieder waarborgt dat de Gebruiker over afwijkingen in het proces van uitgifte, uitreiking en activering tijdig en laagdrempelig in contact kan treden met de Aanbieder. |
| UA3 | <p>De Aanbieder waarborgt dat:</p> <ol style="list-style-type: none"> 1. Authenticatiefactoren via gescheiden kanalen en gescheiden in tijd worden verstrekt; 2. Persoonlijke contactgegevens worden gebruikt voor de verstrekking; 3. De bruikbare periode van activatiecodes is beperkt; 4. Het gebruik van het middel noodzakelijk is voor de activatie ervan. 5. De status van de abonneerrelatie wordt geregistreerd bij een nader te bepalen centrale voorziening van BZK |

| | |
|-----------------------|---|
| <i>eIDAS</i> 2.2.3 | <i>Schorsing, Herroeping en Reactivering</i> |
| SR1 | De Aanbieder waarborgt dat hij authenticatiemiddelen kan intrekken en kan schorsen: <ol style="list-style-type: none"> 1. Op initiatief van de Gebruiker; 2. Op initiatief van de Aanbieder; 3. Op initiatief van een daartoe bevoegde instantie, waaronder BZK. |
| SR2 | De Aanbieder waarborgt dat hij bij gereede vermoedens van misbruik het middel intrekt of schorst. |
| SR3 | De Aanbieder waarborgt dat hij bij de omgang met verzoeken tot schorsing en intrekking van middelen in elk geval aansluit bij de eisen voor reactie- en behandeltermijnen bij verzoeken tot intrekking van gekwalificeerde certificaten (ETSI EN 319411-1 paragraaf 6.2.4). |
| <i>eIDAS</i> 2.2.4 | <i>Verlenging en vervanging</i> |
| 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. In voorkomende gevallen moet dit kunnen leiden tot vervanging van het middel. |
| 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. |
| <i>eIDAS</i> 2.3.1 | <i>Authenticatiemechanisme</i> |
| AM1 | De Aanbieder waarborgt dat zowel de identificatie, het gebruikte authenticatiemiddel, als het proces van de authenticatie minimaal het door de Dienstverlener gevraagde betrouwbaarheidsniveau heeft. |

| | |
|------------------------------|--|
| AM2 | <p>De Aanbieder waarborgt dat de Gebruiker wordt geïnformeerd over zijn inlog op een specifieke dienst en Dienstverlener. De Gebruiker moet in staat worden gesteld met deze informatie een door hem niet gewenste inlogactiviteit af te breken en met de Aanbieder in contact te treden over afwijkingen.</p> <p>De informatie van de Aanbieder moet voldoende betrouwbaar zijn, ook als applicatie voor het aanloggen of het platform waarop deze applicatie actief is, gecorrumpereerd is.</p> |
| AM3 | <p>De Aanbieder waarborgt dat hij een reeds uitgevoerde authenticatie niet opnieuw gebruikt voor een her-authenticatie bij dezelfde online Dienstverlener of voor het aanloggen bij een andere online Dienstverlener.</p> |
| AM4 | <p>De Aanbieder waarborgt dat het correct functioneren van het authenticatiemechanisme weerstand biedt tegen fysieke en logische manipulatie door een aanvaller met een 'gematigd aanvalspotentieel' (moderate attacker potential). Aanvalspotentieel wordt opgevat in de zin van de Common Criteria (ISO 15408-3) en de bijbehorende evaluatienorm (ISO/IEC 18045 Annex B):</p> <ol style="list-style-type: none"> 1. Weerstand tegen een gematigd aanvalspotentieel betekent o.a. weerstand tegen de dreiging van een Man-in-the-Browser aanval; 2. De weerstand tegen het aanvalspotentieel moet worden bevestigd door een deskundige en onafhankelijke beoordelende instantie; 3. Er zullen nadere eisen worden gesteld aan deze beoordelende instantie en de frequentie waarmee de weerstand moet worden aangetoond. |
| Beheer en organisatie | |
| <i>eIDAS 2.4.1</i> | <i>Algemene bepalingen</i> |
| AB 1 | <p>De Aanbieder waarborgt ingeval van beëindiging van de dienstverlening - ongeacht de oorzaak of intentie van de beëindiging - dat wordt voldaan aan de nadere richtlijnen van BZK inzake de omgang met gebruikersgegevens en gebruiksgegevens en overige relevante loggings. De nadere richtlijnen dienen als waarborg voor in elk geval:</p> <ol style="list-style-type: none"> 1. de continuering van de inzage van gebruikersgegevens en gebruiksgegevens door Gebruikers; 2. van de veiligheid en integriteit van de bedoelde gegevens; 3. de naleving van privacyregelgeving; 4. de effectiviteit van misbruikbestrijding. |

| | |
|-----------------------|---|
| <i>eIDAS</i> 2.4.2 | <i>Informatie voor Gebruikers</i> |
| IG1 | <p>De Aanbieder waarborgt dat Gebruiker de rechtmatigheid van de uitgifte van een authenticatiemiddel op zijn identiteit kan controleren in een door BZK gefaciliteerde voorziening*).</p> <p>BZK stelt nadere eisen over hoe de Aanbieder zijn bijdrage aan de bedoelde centrale voorziening levert.</p> <p><i>*) Deze eis maakt onderdeel uit van het vernieuwde concept van de wet GDI en betekent dat de Gebruiker in staat wordt gesteld de uitgifte van zowel de publieke als private middelen in één register te controleren.</i></p> |
| IG2 | <p>De Aanbieder waarborgt dat de Gebruiker met gebruikmaking van een geldig authenticatiemiddel*) inzage heeft in de door de Aanbieder vastgelegde gegevens over:</p> <ol style="list-style-type: none"> 1. de identiteit van de Gebruiker en; 2. het gebruik van het authenticatiemiddel dat door de Aanbieder is verstrekt. <p><i>*) Geldige middelen betreffen in elk geval de authenticatiemiddelen die door de Aanbieder zelf zijn uitgegeven en betreffen bijvoorkeur ook de geldige publieke middelen.</i></p> |
| IG3 | <p>De Aanbieder waarborgt dat de Gebruiker op laagdrempelige, betrouwbare wijze in staat wordt gesteld om tijdig in contact te treden met de Aanbieder over vermoedens van fouten en misbruik ten aanzien van de hierboven genoemde gegevens.</p> |
| <i>eIDAS</i> 2.4.3 | <i>Informatiebeveiliging</i> |
| IB1 | <p>De Aanbieder waarborgt dat de dienstverlening die hij aanbiedt is ondergebracht in zijn managementsysteem voor informatiebeveiliging.</p> <p>Voor de opzet en het functioneren van het managementsysteem geldt als referentie de internationale standaard ISO 27001:2013</p> |
| IB2 | <p>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.</p> |

| | |
|-----------------------|--|
| IB3 | <p>De Aanbieder waarborgt dat gebeurtenissen laagdrempelig en betrouwbaar gemeld en afgehandeld kunnen worden. Het betreft het proactief melden en behandelen van nader te omschrijven gebeurtenissen op het gebied van beveiliging en het misbruik van middelen. Het proces van melding en afhandeling moet in elk geval de volgende scenario's omvatten:</p> <ol style="list-style-type: none"> 1. Meldingen door de Gebruiker aan de Aanbieder; 2. Meldingen door de Aanbieder aan de Gebruiker; 3. Meldingen door de Aanbieder aan door BZK nader te omschrijven centrale functie; 4. Meldingen door de Dienstverlener aan de Aanbieder. |
| IB4 | <p>De Aanbieder waarborgt dat hij de behandeling van calamiteiten en crises inzake de dienstverlening ordelijk organiseert en afhandelt in afstemming met BZK.</p> |
| <i>eIDAS</i> 2.4.4 | <i>Bijhouden van Administratie</i> |
| BA 1 | <p>De Aanbieder waarborgt de archivering van de gegevens en de bijbehorende bewaartermijnen die door BZK met nadere richtlijnen worden vast gesteld.</p> <p>Dit betekent dat de Aanbieder in elk geval:</p> <ol style="list-style-type: none"> 1. de naleving in van de richtlijnen controleerbaar maakt; 2. de mogelijkheid tot het doen van navraag door de Gebruiker waarborgt; 3. de integriteit van de gearchiveerde gegevens waarborgt; 4. de misbruikbestrijding ondersteunt. |
| <i>eIDAS</i> 2.4.5 | <i>Faciliteiten en personeel</i> |
| FP1 | <p>De Aanbieder waarborgt in continuïteit en de integriteit van het bij de dienstverlening betrokken personeel.</p> |
| FP2 | <p>De Aanbieder waarborgt dat het personeel dat identificatiewerkzaamheden doet in het kader van uitgifte van middelen adequaat is opgeleid voor deze taak.</p> <p>Als referentie voor de kwaliteit van de opleiding voor uitvoering van de identificatie geldt het proces voor uitgifte van paspoorten en rijbewijzen.</p> |

| | |
|-----------------------|---|
| <i>eIDAS</i> 2.4.6 | <i>Technische Controles</i> |
| TC1 | <p>De Aanbieder waarborgt dat hij effectieve technische beheersmaatregelen neemt voor de gegevensverwerkende systemen die de dienstverlening ondersteunen. Deze maatregelen betreffen in elk geval:</p> <ol style="list-style-type: none"> 1. Beheersing van de toegang tot de gegevensverwerkende systemen; 2. Controleerbaarheid van handelingen en integere gegevensverwerking in de systemen; 3. Waarborgen voor de beschikbaarheid van de dienstverlening; 4. Bescherming tegen aanvallen en inbreuken op de dienstverlening en onderliggende gegevensverwerkende systemen en infrastructuren; 5. Maatregelen tegen het door medewerkers creëren van fictieve identiteiten of valse middelen op bestaande identiteiten. |
| TC2 | <p>De Aanbieder waarborgt dat de periodieke beoordeling van de werking en de relevantie van de hierboven bedoelde technische beheersmaatregelen is ondergebracht binnen het managementsysteem voor informatiebeveiliging.</p> |
| <i>eIDAS</i> 2.4.7 | <i>Compliance en Audit</i> |
| CA1 | <p>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.</p> |
| CA2 | <p>De Aanbieder waarborgt de naleving van de door BZK vast te stellen nadere richtlijnen over de <u>wijze</u> waarop de Aanbieder aantoont dat hij voldoet aan alle in CA1 bedoelde eisen. De nadere richtlijnen bevatten o.a. betrokkenheid van:</p> <ol style="list-style-type: none"> 1. Een Certificerende Instelling; 2. Een Toezichthouder namens BZK; 3. BZK zelf. |

| | Techniek en functionaliteit |
|-----|--|
| | <i>Privacy: functies en -techniek</i> |
| PT1 | <p><i>Doelstelling: Privacy by Design</i></p> <p>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.</p> |
| PT2 | <p><i>Proportionele verwerking van het BSN</i></p> <p>De Aanbieder waarborgt de inzet van een nader te omschrijven voorziening van BZK zodat alleen die Dienstverleners het Burgerservicenummer (BSN) ontvangen, die daarvoor over de wettelijke grondslag beschikken.</p> |
| PT3 | <p><i>Ondersteuning pseudoniemen</i></p> <p>De Aanbieder waarborgt dat naast identiteit (BSN) ook alléén een pseudoniem kan worden geleverd aan Dienstverleners</p> |
| PT4 | <p><i>Conform pseudoniemen Autoriteit Persoonsgegevens</i></p> <p>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.</p> |
| PT5 | <p><i>Randomisering van pseudoniemen</i></p> <p>De Aanbieder waarborgt dat het pseudoniem dat hij aan Dienstverleners verstrekt steeds gelijk is voor dezelfde Gebruiker, ongeacht het gebruikte geldige authenticatiemiddel*).</p> <p>*) Geldige middelen betreffen hier niet alleen de authenticatiemiddelen die door de Aanbieder zelf zijn uitgegeven.</p> |
| PT6 | <p><i>Scheiding gebruikersinformatie en gebruiksinformatie (security-in-depth)</i></p> <p>De Aanbieder waarborgt dat het niet mogelijk is om uit één gecompromitteerde database zowel de identificatie data van de Gebruiker en zijn bezoeken aan Dienstverleners te lekken.</p> |
| PT7 | <p>Het BSN mag geen persistent onderdeel zijn van de opgeslagen met betrekking tot de identiteit van de Gebruiker.</p> |

| | |
|-----|--|
| | <i>Waarborg Gebruiksvriendelijkheid voor Gebruikers en Dienstverleners</i> |
| WG1 | <p><i>Compatibele pseudoniemen</i></p> <p>De Aanbieder waarborgt dat de door hem gebruikte pseudoniemen compatibel zijn met de gebruikte pseudoniemen van de Publieke middelen.</p> |
| WG2 | <p><i>Europese interoperabiliteit: unieke identificatiecode</i></p> <p>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.]</p> |
| WG3 | <p><i>Interoperabiliteit met Publieke diensten voor vertegenwoordiging en attribuutverstrekking.</i></p> <p>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.</p> <p>BZK stelt nadere eisen aan de wijze waarop deze interoperabiliteit vorm gegeven wordt.</p> <p>Toelichting op genoemde publieke diensten:</p> <p>Vertegenwoordiging: De voorziening die het mogelijk maakt dat een burger met zijn authenticatiemiddel gebruik maakt van een machtiging die hem is verstrekt.</p> <p>Attribuutverstrekking: De voorziening die bij het inloggen additionele attributen over de Gebruiker levert aan een Dienstverlener.</p> <p>Routeringsdienst: De voorziening die zowel de publieke als private authenticatiemiddelen ontsluit ter ontzorging van de Dienstverleners die daar voor kiezen.</p> |
| | <i>Bescherming tegen misbruik</i> |
| BS1 | <p>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.</p> |

REFERENTIES Functionaliteit en techniek

| # | Document |
|------|--|
| [1.] | Pseudonimisering risicoverevening, College Bescherming Persoonsgegevens, 6 maart 2007 (kenmerk: z2006-1382). |
| [2.] | UITVOERINGSVERORDENING (EU) 2015/1501 VAN DE COMMISSIE van 8 september 2015 betreffende het interoperabiliteitskader bedoeld in artikel 12, lid 8, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt |

HOOFDSTUK 5: VRAGEN AAN DE MARKT

Dit hoofdstuk bevat de vragen waar BZK graag van u, als marktpartij, een antwoord op krijgt. Gedachte hierachter is dat u de gelegenheid heeft mee te denken over, en invloed uit te oefenen op, de mogelijke inzet van private elektronische inlogmiddelen door de overheid.

1. Beschrijf het inlogmiddel dat u voor ogen heeft.
Wilt u in uw beschrijving aangeven:
 - a. op welke wijze dit geschikt is of geschikt te maken is voor de doelstellingen van BZK;
 - b. hoe u het tijdpad met daarin de marktintroductie en uitrol (inclusief de omvang van het aantal actieve gebruikers) ziet, tot het moment dat alle huidige DigiD-gebruikers actief gebruiker zijn van uw inlogmiddel. Indien uw oplossing alleen bedoeld is voor een specifieke doelgroep, dan vragen wij u deze doelgroep en hetzelfde tijdpad met betrekking tot deze doelgroep te beschrijven;
 - c. hoe het gebruikersgemak en de –support eruit ziet van uw oplossing voor alle gebruikersdoelgroepen (burgers) in Nederland;
 - d. hoe u de continuïteit van uw oplossing organiseert?

De vragen 2 tot en met 4 betreffen hoofdstuk 4. Dit hoofdstuk geeft een indicatie van de eisen voor een eventueel vervolgtraject. Met de volgende vragen nodigt BZK u uit mee te denken over, en te reageren op, dit vertrekpunt voor eisen.

2. BZK heeft extra interesse in uw reactie op een aantal specifieke eisen. Wilt u daarom onderstaande vragen beantwoorden:
 - a. Geef aan hoe u, als marktpartij, aantoont dat u voldoet aan eis CA2?
 - b. Geef aan op welke manier u voldoet aan de eisen AM4, IG2, IG3, PT1, PT4, PT5, WG1, WG2 en BS1?
3. In hoofdstuk 4 geeft BZK een paar keer aan dat ze 'nadere eisen' wil gaan formuleren. Wat is uw voorstel om invulling te geven aan deze 'nadere eisen' ?
4. Aan welke eisen kunt u niet voldoen en kunt u hierbij een toelichting geven, eventueel voorzien van uw voorstel voor een aanpassing?
5. Hoe kunt u zowel bij de start als gedurende de samenwerking (contract) bewijzen dat uw oplossing (en uw dienstverlening) aantoonbaar voldoet en blijft voldoen aan de doelstellingen en eisen van BZK?
6. Hoe adviseert u ons het verrekeningsmodel (financieel of anderszins) voor uw oplossing in te richten? Kunt u daarbij een indicatie geven van de prijs/verrekening die u vraagt voor uw oplossing?
7. Als u BZK was, welke overige eisen en criteria zou u hanteren en wat zou u verder nog vragen aan de (toekomstige) opdrachtnemer(s)?
8. Welke zaken zijn niet in het voorgaande aan de orde gekomen, maar wilt u ons ter aanvulling meegeven?

HOOFDSTUK 6: BIJLAGEN

Bijlage 1: Begrippenlijst

- *aangewezen organisaties/dienstverleners*: organisaties als bedoeld in artikel 3, tweede lid van de Wet GDI. Onder deze noemer vallen de overheidsorganisaties op rijksniveau(inclusief de ZBO's), provinciaal en gemeentelijk niveau, waterschappen, alsmede vanuit de wet aan te wijzen semi-publieke instellingen zoals scholen, zorginstellingen, zorgverzekeraars en pensioenfondsen.
- *authenticatie*: elektronisch proces voor de verificatie en bevestiging van de identiteit van een natuurlijke persoon of rechtspersoon;
- *identificatiemiddel*: methode voor de authenticatie van een natuurlijke persoon of rechtspersoon die deze toegang biedt tot elektronische dienstverlening;
- *betrouwbaarheidsniveau substantieel*: de mate waarin vertrouwen kan worden gesteld in de elektronische dienstverlening of het identificatiemiddel en waarbij wordt voldaan aan de bij of krachtens de eIDAS-verordening gestelde criteria aan het betrouwbaarheidsniveau substantieel;
- *elektronische dienstverlening*: verlening van openbare elektronische diensten door een bestuursorgaan als bedoeld in artikel 1:1, eerste lid, onderdeel a, van de Algemene wet bestuursrecht of aangewezen organisatie aan natuurlijke personen of rechtspersonen, waarvoor-authenticatie op betrouwbaarheidsniveau substantieel vereist is;
- *erkend identificatiemiddel*: een bedrijfs- en organisatiemiddel dat is erkend ingevolge de Wet GDI (artikel 9);
- *privaat identificatiemiddel*: niet door BZK uitgegeven aan een natuurlijke persoon verstrekt identificatiemiddel dat toegang geeft tot elektronische dienstverlening;
- *publiek identificatiemiddel*: door BZK uitgegeven aan een natuurlijke persoon verstrekt identificatiemiddel dat toegang geeft tot elektronische dienstverlening;
- *toegelaten identificatiemiddel*: een identificatiemiddel voor een natuurlijke persoon dat is aangewezen ingevolge artikel 7 van de wet GDI;
- *de eIDAS-verordening*: Verordening (EU) Nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (Pb EU 2014, L 257/73) en de krachtens deze verordening vastgestelde uitvoeringshandelingen.
- *Aanbieder*: Bedrijf dat een privaat identificatiemiddel aanbiedt;
- *Gebruiker*: Een natuurlijke persoon (burger) in het bezit van een BSN;
- *Opdrachtgever*: het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties;
- *BSN*: Het Burger Servicenummer;
- *BSNk*: Het BSN koppelregister is een register waarmee een pseudoniem van een gebruiker kan worden gekoppeld aan een burgerservicenummer.
- *AVG*: Algemene verordening gegevensbescherming (deze vervangt, tezamen met de in voorbereiding zijnde Uitvoeringswet AVG, de wet bescherming persoonsgegevens);

Bijlage 2: Relevante documenten en wetgeving

eIDAS

EU verordening nr. 910/2014 van het Europees Parlement en de Raad (23 juli 2014)

<http://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX%3A32014R0910>

Uitvoeringsverordening EU 2015/1501

<http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32015R1501>

EU 2015/1502 (8 september 2015) betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.

<http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32015R1502>

Wet GDI en de Uniforme Set van Eisen

Consultatie van de Wet GDI versie 22 december 2016:

<https://www.internetconsultatie.nl/wetgdi/details>

Uniforme Set van Eisen

Consultatie van de Uniforme Set van Eisen versie 22 december 2016:

<https://www.rijksoverheid.nl/actueel/nieuws/2016/12/22/overheid-en-zorg-starten-in-2017-met-nieuwe-manieren-van-inloggen>

Concept Wet GDI versie 29 augustus 2017

<https://www.rijksoverheid.nl/ministeries/ministerie-van-binnenlandse-zaken-en-koninkrijksrelaties/documenten/publicaties/2017/08/30/wetsontwerp-generieke-digitale-infrastructuur-gdi>

Wet bescherming persoonsgegevens

<http://wetten.overheid.nl/BWBR0011468/2017-07-01>

Algemene Verordening gegevensbescherming

<http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32016R0679>

Bijlage 3: Relevante Tweede Kamerstukken

Tweede Kamer stukken zijn te vinden op de volgende website door intikken van dossiernummer en ondernummer (bijvoorbeeld 26643 / 481):

https://zoek.officielebekendmakingen.nl/zoeken/parlementaire_documenten

20170706 TK 26 643 nr 481 Aanbieding Gegevensbeschermingseffectbeoordeling (PIA) eID stelsel

* Bijlage Gegevensbeschermingseffectbeoordeling eid stelsel

20170623 TK 26 643 nr 476 Voortgangsrapportage programma eID

20170407 TK 26 643 nr 456 Risicobeheersing Impuls eID

20170307 TK 26 643 nr 452 Aanbiedingsbrief Evaluatie pilots in de zorg

* Bijlage Evaluatie pilots in de zorg blg-801586

20170118 TK 26 643 nr 443 Verslag van het AO Digitale Infrastructuur eID op 18 januari 2017

20161221 TK 26 643 nr 437 Voortgang programma eID

* Bijlage uniforme-set-van-eisen

20161109 TK 26 643 nr 425 Brief Geactualiseerde businesscase Inloggen in het BSN domein

* Bijlage Geactualiseerde businesscase Inloggen in het BSN domein

20160929 TK 26 643 nr 423 Verslag van het AO van 29 september 2016 over eID

20160908 TK 26 643 nr 421 Brief ARK Rapport Vernieuwing stelsel voor digitale identificatie en authenticatie (eID)

* Bijlage ARK Rapport Vernieuwing stelsel voor digitale identificatie en authenticatie (eID)

20160825 TK 26 643 nr 419 Brief Impuls eID

* Deze brief kent zes bijlagen (I t/m VI), waarvan bijlage IV de rapporten van de commissie Kuipers bevat (weer 5 bijlagen). Zie voor een overzicht van bijlagen het aparte Word document:

20160825 TK 26 643 nr 419 Overzicht bijlagen bij de brief Impuls eID van 25 augustus 2016

20160617 TK 26 643 nr 414 Kamerbrief-inzake-bureau-ict-toetsing-bit-advies-programma-eid

* Bijlage afschrift-brief-advisering-bit-inzake-programma-eid