

Programma van Eisen en Wensen

Leeswijzer

Thema	Omschrijving	Pagina nummer	maximaal aantal punten
Thema 1	Producten	Pagina 1 t/m 4	229
Thema 2	Beveiliging, informatie uitwisseling en - verwerking	Pagina 4 t/m 10	143
Thema 3	Technische aspecten	Pagina 10 t/m 12	98
Thema 4	Service en implementatie	Pagina 12 t/m 15	270
Thema 5	Kosten en facturatie	Pagina 15	0
Thema 6	Innovatie en toekomstbestendigheid	Pagina 15 en 16	140
Thema 7	Maatschappelijk Verantwoord Ondernemen	Pagina 17 t/m 19	150

THEMA 1: PRODUCTEN

Algemeen

Eis 1.1	U dient in ieder geval de volgende betaalmethoden te ondersteunen: • iDEAL; • iDEAL QR; • Bancontact; • Sofort; • Giropay; • Digitaal Incasso Machtigen; • Mastercard; • Visa; • PayPal.												
Wens 1.1 Meerkeuze	U kunt aangeven of u uw Dienstverlening afhankelijk van de betaalmethode zowel distribuerend als collecterend voor onderstaande betaalmethoden kunt aanbieden, waarbij de ontvangsten altijd via de derden bankrekening verlopen. <i>Toelichting</i> De Rijksonderdelen zijn voornemens om diverse betaalmethoden te gaan gebruiken. Bij de betaalmethoden waarbij dit mogelijk is, bijvoorbeeld iDEAL, willen de Rijksonderdelen gebruik maken van het distribuerend model. Beoordeling Hoe meer distribuerend, hoe hoger uw score. <table><tr><th>Betaalmethode</th><th>Distribuerend</th><th>Collecterend</th></tr><tr><td>Bancontact</td><td>10</td><td>0</td></tr><tr><td>Sofort</td><td>10</td><td>0</td></tr><tr><td>Giropay</td><td>10</td><td>0</td></tr></table> 30 punten	Betaalmethode	Distribuerend	Collecterend	Bancontact	10	0	Sofort	10	0	Giropay	10	0
Betaalmethode	Distribuerend	Collecterend											
Bancontact	10	0											
Sofort	10	0											
Giropay	10	0											
Wens 1.2 Ja/nee	U kunt de volgende Creditcard schemes ondersteunen: • American Express; • China Union Pay; • JCB; • Diners Club.												

	Beoordeling Hoe meer u kunt aanbieden, hoe hoger uw score. <table border="1"> <thead> <tr> <th>Creditcard schemes</th><th>Aantal punten</th></tr> </thead> <tbody> <tr> <td>American Express</td><td>5</td></tr> <tr> <td>China Union Pay</td><td>1</td></tr> <tr> <td>JCB</td><td>1</td></tr> <tr> <td>Diners Club</td><td>1</td></tr> <tr> <td>..... zelf toevoegen</td><td>1</td></tr> </tbody> </table> 9 punten	Creditcard schemes	Aantal punten	American Express	5	China Union Pay	1	JCB	1	Diners Club	1	 zelf toevoegen	1
Creditcard schemes	Aantal punten												
American Express	5												
China Union Pay	1												
JCB	1												
Diners Club	1												
..... zelf toevoegen	1												
Eis 1.2	U dient het inkomende online Betalingsverkeer van de Rijksonderdelen te verwerken conform geldende wet- en regelgeving.												
Eis 1.3	U dient bijschrijvingen op de rekening(en) van het betreffende Rijksonderdeel uitsluitend in Euro's te laten plaats vinden. <i>Toelichting</i> Alle vorderingen van de Rijksonderdelen luiden zonder uitzonderingen in EUR. De Rijksonderdelen gaan ervan uit dat de betalingen in de aangegeven valuta EUR zal plaatsvinden. Bij een beperkt aantal betaalmethode is het niet uit te sluiten dat een betaler toch in lokale valuta betaalt.												
Wens 1.3 Ja/nee	U kunt zorgdragen voor bijschrijven van het oorspronkelijke te betalen bedrag in EUR waarbij de kosten voor het omrekenen van de lokale valuta niet ten laste van het Rijksonderdeel komt. 30 punten												
Eis 1.4	U dient het mogelijk te maken om bovenstaande online betaalmethoden te ontsluiten via een digitale Mijn omgeving, een website en/of een betaallink.												

Nationaal Archief

Wens 1.4 Ja/nee	Het Nationaal Archief wil graag aansluiten bij deze aanbesteding. Zij maken gebruik van een website geschreven in Drupal. Voor de aansluiting op de PSP maakt zij hiervoor gebruik van standaard modules die onderhouden worden onder toezicht van de security advisory board van Drupal. Op het moment dat u kunt aansluiten op de standaard module binnen een website die in Drupal is geschreven en wordt onderhouden onder toezicht van het security advisory board van Drupal, zal Nationaal Archief aansluiten bij deze aanbesteding. Lukt u dat niet, dan sluiten zij niet aan. U kunt aansluiten op de standaard modules binnen een website die in Drupal is geschreven en wordt onderhouden onder toezicht van het security advisory board van Drupal. 10 punten
--------------------	--

iDEAL

Eis 1.5	U dient de ontvangst uit een iDEAL transactie per Rijksonderdeel conform het distribuerend model dagelijks bij te laten schrijven. De bijschrijving van de transactie op de bankrekening van het Rijksonderdeel vindt plaats via onze huisbank. De verwerking van de transactie, het acquiring gedeelte, wordt door u uitgevoerd. <i>Toelichting</i> Wij verwachten dat gedurende de nieuwe contractperiode het product iDEAL Instant Payment beschikbaar zal komen. U dient, ontvangsten via iDEAL Instant Payment direct na ontvangst door Opdrachtnemer door te boeken op de gekoppelde rekeningen.
Eis 1.6	U dient, in geval van een gecomprimeerde bijschrijving, een specificatie aan te leveren.

	<i>Toelichting</i> De ontvangsten uit iDEAL transacties kunnen zowel gecompriemd als post voor post worden bijgeschreven op de relevante bankrekening(en).
Eis 1.7	U dient iDEAL transacties aan verschillende bankrekeningen van de Rijksonderdelen te koppelen. <i>Toelichting</i> Elk Rijksonderdeel gebruikt per wettelijke regeling een andere bankrekening.
Eis 1.8	U dient ervoor te zorgen dat de ontvangsten uit iDEAL transacties op werkdagen, en in het weekend en op feestdagen uiterlijk de volgende werkdag bij worden geschreven. <i>Toelichting</i> Onder verwijzing naar de toelichting bij Eis 1.5 over de introductie van iDEAL Instant Payment zal bovengenoemde Eis per datum ingebruikname van dit product komen te vervallen. Deze datum zal/kan per Rijksonderdeel verschillen.
Eis 1.9	U dient ervoor te zorgen dat de ontvangsten uit iDEAL transacties per Rijksonderdeel met een vast format (vaste volgorde transactie informatie) worden bijgeschreven.
<i>Wens 1.5</i> <i>Ja/nee</i>	U kunt het betalingskenmerk van het Rijksonderdeel als eerste onderdeel in dit vaste format (vaste volgorde transactie informatie) plaatsen? 20 punten
Eis 1.10	De Rijksonderdelen gebruiken voor de reconciliatie het door het Rijksonderdeel bepaalde betalingskenmerk van de iDEAL transactie. Deze moet worden teruggemeld in het dagafschrift/de rekeninginformatie. Het moet mogelijk zijn om een betalingskenmerk te hanteren van minimaal 16 karakters. Elk Rijksonderdeel heeft zijn eigen unieke betalingskenmerk(en). U dient bovenstaande te ondersteunen waarbij het door het Rijksonderdeel vooraf aangegeven kenmerk zichtbaar moet zijn op de afschriften van de betaler en de begunstigde Rijksonderdelen.
Eis 1.11	U dient het mogelijk te maken dat bij niet volledig uitvoeren van een iDEAL betaling, de transactie opnieuw kan worden uitgevoerd met hetzelfde betalingskenmerk.
<i>Wens 1.6</i> <i>Ja/nee</i>	U kunt het mogelijk maken dat, zolang de definitieve autorisatie van de betaler niet is gegeven, de betaler binnen zijn betaalomgeving kan switchen (zowel van rekeningnummer binnen een bank als naar een andere bank) zonder dat er wordt teruggeschakeld naar het systeem van het Rijksonderdeel. 20 punten

iDEAL QR

Eis 1.12	U dient iDEAL QR codes te kunnen aanmaken voor een Rijksonderdeel. Deze iDEAL QR codes kunnen door het Rijksonderdeel op een fysieke aanschrijving worden geplaatst of worden aangeboden in de digitale omgeving van het Rijksonderdeel.
----------	---

Digitale SEPA Incasso Machtigen

Eis 1.13	U dient, indien het Rijksonderdeel daarom verzoekt, de Digitale SEPA Incasso Machtigingen op te slaan voor het Rijksonderdeel en de machtiging voor het Rijksonderdeel beschikbaar te stellen.
----------	---

Derdengeldenrekening en uitbetaling

Dit onderdeel geldt alleen voor het ontvangen van gelden voor betaalmethoden die niet distribuerend kunnen worden uitgevoerd.	
--	--

Wens 1.7 Ja/nee	U kunt gelden voor de Rijksonderdelen die door u moeten worden aangehouden ten behoeve van het betaalproces, plaatsen op een aparte derdengeldrekeningen inzake het Rijksonderdeel. 30 punten
Eis 1.14	U dient de derdengeldenrekening alleen te gebruiken voor het ontvangen van online betalingen en voor het doorstorten van deze betalingen naar de Rijksonderdelen.
Eis 1.15	U dient bij Inschrijving en gedurende de contractperiode de derdengeldrekening aan te houden bij een bank die beschikt over voldoende kredietwaardigheid tot uitdrukking komend in minimaal twee van de drie navolgende long-term debt ratings: • een long-term debt rating van A- toegekend door de rating agency "Standard & Poor's"; • een long-term debt rating van A- toegekend door de rating agency "Fitch"; • een long-term debt rating van A3 toegekend door de rating agency "Moody's".
Eis 1.16	U dient betalingen die via een derdengeldenrekening verlopen aan de betaler terug te melden en de eigen naam van het Rijksonderdeel toe te voegen.
Eis 1.17	U dient de betalingen die via de derdengeldenrekening lopen, na verevening, automatisch door te storten naar de bankrekening die daarvoor door het Rijksonderdeel is aangewezen.
Wens 1.8 Ja/nee	U kunt ervoor zorgen dat het betaalde bedrag Franco op de rekening van de Rijksonderdelen wordt bijgeschreven. 30 punten
Eis 1.18	U dient bij gecoprimeerde bijschrijving (per bankrekening) een specificatie van de uitbetaling aan te leveren in tenminste CSV en XML formaat, waarop minimaal de volgende informatie staat: naam betaler, bedrag, betalingskenmerk, datum betaling, transactiesoort en rekeningnummer begunstigde.
Wens 1.9 Ja/nee	U kunt, indien een Rijksonderdeel daarom verzoekt, de ontvangen bedragen op de derdengeldenrekening één op één (dus per transactie) overboeken naar de gekoppelde rekening(en) van het Rijksonderdeel onder vermelding van het betalingskenmerk van de betreffende online transactie. <i>Toelichting</i> De Rijksonderdelen laten de online betaaltransacties na tussenkomst van de derden bankrekening bij voorkeur rechtstreeks bijschrijven op één of meerdere rekeningen van het Rijksonderdeel. Voor sommige online betaalproducten zoals Bancontact en Creditcard is rechtstreekse bijschrijving vooralsnog waarschijnlijk niet mogelijk en worden deze bedragen periodiek in één totaalbedrag via de derdengeldenrekening overgeboekt naar de gekoppelde rekening(en) van het Rijksonderdeel. 30 punten

Creditcard

Eis 1.19	U dient 3D-secure beveiligingen bij betalingen aan te bieden in landen waar 3D-secure gangbaar is.
Wens 1.10 Ja/nee	U kunt een standaardproces met betrekking tot chargeback inrichten die voldoet aan de informatiebehoefte van de Rijksonderdelen. <i>Toelichting</i> Indien een chargeback wordt ingediend, wil het betreffende Rijksonderdeel hierover binnen 24 uur na indiening geïnformeerd worden. De melding naar het Rijksonderdeel dient geautomatiseerd plaats te vinden en in de melding dienen minimaal het rekeningnummer, de issuer en de reden

	van de chargeback opgenomen te worden. Het moment van indienen is het first presentment door de card schemes. 20 punten
--	---

THEMA 2: BEVEILIGING, INFORMATIE UITWISSELING EN -VERWERKING

Informatie uitwisseling en -verwerking algemeen

Voor een efficiënte inrichting van haar Betalingsverkeer is het voor de Rijksonderdelen essentieel dat de werkprocessen zoveel mogelijk zonder handmatige interventie verlopen. Uitvoering en Beheersing van deze werkprocessen dient ingericht te zijn volgens de beveiligingseisen van de Rijksoverheid.

Informatiebeveiliging algemeen

Voor de Dienstverlening in het kader van deze Opdracht onderkennen we de volgende relevante frameworks en/of standaarden¹ ten aanzien van het veilig uitwisselen en verwerken van informatie:

1. De Nederlandse wet- en regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG) en het Voorschrift Informatiebeveiliging Rijk (VIR).
2. De Baseline Informatiebeveiliging Overheid. De BIO is samengesteld volgens NEN/ISO 27001:2017 bijlage A en ISO 27002:2017, aangevuld met specifieke Overheidsmaatregelen (O-maatregelen). De meest actuele versie van de ISO-standaard geldt als uitgangspunt, aangevuld met de van toepassing zijnde O-maatregelen. De BIO onderscheidt drie basisbeveiligingsniveaus (BBN's). Ieder BBN bestaat uit een aantal controls, een aantal verplichte overheidsmaatregelen en een verantwoordings- en toezichtregime. In het kader van deze Aanbesteding is BBN2 van toepassing. Dit betekent dat zowel de relevante controls van BBN1 als BBN2 dienen te worden doorlopen en de relevante overheidsmaatregelen van zowel BBN1 als BBN2 nodig zijn.
3. PCI-DSS (Payment Card Industry Data Security Standard) versie 3.2.1 (mei 2018)
4. ISO 27017 (Aanvullende beveiligingseisen voor cloud computing) en ISO 27018 (Aanvullende privacy eisen voor cloud computing)
5. De European Banking Authority (EBA) richtsnoeren met betrekking tot de veiligheid van internetbetalingen: EBA Guidelines EBA/GL/2014/12 on the security of internet payments, published on 19th December 2014
6. Open Standaarden voor de uitwisseling van digitale gegevens tussen overheden onderling en tussen de overheid, bedrijven en burgers. De standaarden zijn een mix van de pas-toe-of-leg-uit lijst en de lijst aanbevolen standaarden. Forum Standaardisatie is hoeder van de complete set Open Standaarden. Alle relevante Open Standaarden voor deze aanbesteding zijn voorzien van een toepassingsgebied.

Wij hanteren de volgende spelregels in geval van verschillen van inzicht of tegenstellingen in de verschillende aangedragen richtlijnen:

- a. Nederlandse wet- en regelgeving (op het gebied van IT-voorzieningen en data zoals de AVG) is altijd leidend, gevolgd door ISO-normen (c.q. BIO), gevolgd door Open Standaarden en richtlijnen en tot slot PCI-DSS en (eigen)beleid van de inschrijver.
- b. De richtlijnen in de BIO, Open standaarden en PCI-DSS hebben betrekking op die delen van de beheerorganisatie/ICT-infrastructuur van u als Inschrijver die van belang zijn voor de Rijksonderdelen. Dus ook delen van de ICT en beheerorganisatie die wij als Rijksonderdelen delen met andere klanten van u.
- c. De richtsnoeren van de European Banking Authority (EBA) gelden voor het internet betalingsverkeer.

Eis 2.1	U dient beveiligingsoplossingen te bieden die voldoen aan de geschetste frameworks en standaarden nummer 1 t/m 5.
---------	---

¹ De Aanbestedende dienst heeft ervoor gekozen voor de frameworks en/of standaarden geen links naar websites op te nemen, omdat deze snel (kunnen) wijzigen. De Aanbestedende dienst gaat ervan uit dat u zelf de meest actuele versie van de betreffende frameworks en/of standaarden kan vinden.

Eis 2.2	Open Standaarden (nummer 6) draagt effectief bij aan het voorkomen van cybercriminaliteit en zijn zonder veel kosten of moeite in te zetten. U dient met de door u aangeboden oplossing te voldoen aan de volgende relevante Open Standaarden norm 1 t/m 9. <table><tr><th>Norm</th><th>Naam</th><th>Toepassing</th></tr><tr><td>1</td><td>AES</td><td>Versleutelingstechniek</td></tr><tr><td>2</td><td>DNSSEC</td><td>Domeinnaambeveiliging</td></tr><tr><td>3</td><td>HTTPS en HSTS</td><td>Beveiligde websiteverbinding</td></tr><tr><td>4</td><td>IPv6 en IPv4</td><td>Adressering van ICT-systemen binnen een netwerk</td></tr><tr><td>5</td><td>NTP</td><td>Synchroniseren van tijd</td></tr><tr><td>6</td><td>SHA-2</td><td>Authenticatie en integriteitscontrole</td></tr><tr><td>7</td><td>TLS</td><td>Beveiligde internetverbinding</td></tr><tr><td>8</td><td>X509</td><td>Authenticatie (PKI Certificaten)</td></tr><tr><td>9</td><td>Beveiligings-richtlijnen voor Webapplicaties van het NCSC (versie 1-09-2015)</td><td>Bouwvoorschriften voor webapplicaties</td></tr></table>	Norm	Naam	Toepassing	1	AES	Versleutelingstechniek	2	DNSSEC	Domeinnaambeveiliging	3	HTTPS en HSTS	Beveiligde websiteverbinding	4	IPv6 en IPv4	Adressering van ICT-systemen binnen een netwerk	5	NTP	Synchroniseren van tijd	6	SHA-2	Authenticatie en integriteitscontrole	7	TLS	Beveiligde internetverbinding	8	X509	Authenticatie (PKI Certificaten)	9	Beveiligings-richtlijnen voor Webapplicaties van het NCSC (versie 1-09-2015)	Bouwvoorschriften voor webapplicaties																														
Norm	Naam	Toepassing																																																											
1	AES	Versleutelingstechniek																																																											
2	DNSSEC	Domeinnaambeveiliging																																																											
3	HTTPS en HSTS	Beveiligde websiteverbinding																																																											
4	IPv6 en IPv4	Adressering van ICT-systemen binnen een netwerk																																																											
5	NTP	Synchroniseren van tijd																																																											
6	SHA-2	Authenticatie en integriteitscontrole																																																											
7	TLS	Beveiligde internetverbinding																																																											
8	X509	Authenticatie (PKI Certificaten)																																																											
9	Beveiligings-richtlijnen voor Webapplicaties van het NCSC (versie 1-09-2015)	Bouwvoorschriften voor webapplicaties																																																											
Wens 2.1 Open	U kunt beschrijven in hoeverre het toepassen van Open standaarden in uw oplossing bijdraagt aan het effectief voorkomen van cyber criminaliteit. Besteedt in uw antwoord aandacht aan: • de mate waarin u onderstaande Open standaarden toepast; • indien u bepaalde Open standaarden niet toepast, waarom u die niet toepast; • hoe leidt uw toepassing tot het effectief voorkomen van cybercriminaliteit. <table><tr><th>Norm</th><th>Naam</th><th>Toepassing</th></tr><tr><td>1</td><td>Ades Baseline Profiles</td><td>Geavanceerde en gekwalificeerde digitale handtekeningen</td></tr><tr><td>2</td><td>ASN.1</td><td>Data structuren</td></tr><tr><td>3</td><td>CAA</td><td>Controle over uitgifte van digitale certificaten</td></tr><tr><td>4</td><td>Digikoppeling</td><td>Veilige berichtenuitwisseling</td></tr><tr><td>5</td><td>DKIM</td><td>Bescherming tegen e-mailphishing</td></tr><tr><td>6</td><td>DMARC</td><td>Bescherming tegen e-mailphishing</td></tr><tr><td>7</td><td>ETSI TS 119 312</td><td>Digitale handtekening</td></tr><tr><td>8</td><td>IP Sec</td><td>Beveiligde IP verbindingen</td></tr><tr><td>9</td><td>LDAP</td><td>Netwerkprotocol</td></tr><tr><td>10</td><td>OAuth</td><td>API Autorisatiestandaard</td></tr><tr><td>11</td><td>RPKI</td><td>Beveiligen van de routing infrastructuur</td></tr><tr><td>12</td><td>S/MIME</td><td>E-mail beveiliging</td></tr><tr><td>13</td><td>Secure Software Development</td><td>Ontwikkelen veilige software</td></tr><tr><td>14</td><td>SAML</td><td>Authenticatie en autorisatie</td></tr><tr><td>15</td><td>SPF</td><td>Bescherming tegen e-mailphishing</td></tr><tr><td>16</td><td>SSH-2</td><td>Versleuteld inloggen</td></tr><tr><td>17</td><td>STARTTLS en DANE</td><td>Beveiligde verbinding tussen mailservers</td></tr><tr><td>18</td><td>STIX en TAXII</td><td>Uitwisseling van cyberdreigings-informatie</td></tr><tr><td>19</td><td>TOTP</td><td>Wachtwoord generatie</td></tr></table>	Norm	Naam	Toepassing	1	Ades Baseline Profiles	Geavanceerde en gekwalificeerde digitale handtekeningen	2	ASN.1	Data structuren	3	CAA	Controle over uitgifte van digitale certificaten	4	Digikoppeling	Veilige berichtenuitwisseling	5	DKIM	Bescherming tegen e-mailphishing	6	DMARC	Bescherming tegen e-mailphishing	7	ETSI TS 119 312	Digitale handtekening	8	IP Sec	Beveiligde IP verbindingen	9	LDAP	Netwerkprotocol	10	OAuth	API Autorisatiestandaard	11	RPKI	Beveiligen van de routing infrastructuur	12	S/MIME	E-mail beveiliging	13	Secure Software Development	Ontwikkelen veilige software	14	SAML	Authenticatie en autorisatie	15	SPF	Bescherming tegen e-mailphishing	16	SSH-2	Versleuteld inloggen	17	STARTTLS en DANE	Beveiligde verbinding tussen mailservers	18	STIX en TAXII	Uitwisseling van cyberdreigings-informatie	19	TOTP	Wachtwoord generatie
Norm	Naam	Toepassing																																																											
1	Ades Baseline Profiles	Geavanceerde en gekwalificeerde digitale handtekeningen																																																											
2	ASN.1	Data structuren																																																											
3	CAA	Controle over uitgifte van digitale certificaten																																																											
4	Digikoppeling	Veilige berichtenuitwisseling																																																											
5	DKIM	Bescherming tegen e-mailphishing																																																											
6	DMARC	Bescherming tegen e-mailphishing																																																											
7	ETSI TS 119 312	Digitale handtekening																																																											
8	IP Sec	Beveiligde IP verbindingen																																																											
9	LDAP	Netwerkprotocol																																																											
10	OAuth	API Autorisatiestandaard																																																											
11	RPKI	Beveiligen van de routing infrastructuur																																																											
12	S/MIME	E-mail beveiliging																																																											
13	Secure Software Development	Ontwikkelen veilige software																																																											
14	SAML	Authenticatie en autorisatie																																																											
15	SPF	Bescherming tegen e-mailphishing																																																											
16	SSH-2	Versleuteld inloggen																																																											
17	STARTTLS en DANE	Beveiligde verbinding tussen mailservers																																																											
18	STIX en TAXII	Uitwisseling van cyberdreigings-informatie																																																											
19	TOTP	Wachtwoord generatie																																																											

24 punten

Eis 2.3	U dient gedurende de looptijd van de Overeenkomst in elk geval aanpassingen in frameworks en/of Open Standaarden zoals beschreven in Eis 2.1 en 2.2 binnen één jaar te implementeren.
Eis 2.4	U dient ervoor te zorgen dat een medewerker van de Rijksonderdelen zich unconnected identificeert. Met andere woorden dat de medewerker bij multifactor authenticatie geen USB-device of andere digitale gegevensdrager aan een lokaal werkstation hoeft te koppelen.

Het testen van de beveiliging

Eis 2.5	U dient de beveiliging van de door u geboden oplossing jaarlijks te testen.																
Wens 2.2 Ja/nee	Graag krijgen wij nader inzicht in de mate waarin u uw beveiliging test. Wij vragen u daarom de ja/nee vragen uit onderstaande tabel te beantwoorden. <table border="1"> <thead> <tr> <th>Vraag</th><th>Antwoord</th></tr> </thead> <tbody> <tr> <td>1. U geeft gedurende de looptijd van de Overeenkomst op verzoek van Opdrachtgever inzage in testverslagen met openstaande beveiligingsrisico's van de uitgevoerde beveiligingstesten.</td><td>Ja/Nee</td></tr> <tr> <td>2. U voert ieder half jaar of vaker een penetratietest uit.</td><td>Ja/Nee</td></tr> <tr> <td>3. U lost bevindingen uit de beveiligingstesten (geautomatiseerd of handmatig) met de classificatie 'hoog' binnen één maand op.</td><td>Ja/Nee</td></tr> <tr> <td>4. U voert beveiligingstesten uit volgens procedures ontleend aan industriebrede standaarden zoals de Penetration Testing Execution Standard en de Open Source Security Testing Methodology Manual of gelijkwaardige standaarden.</td><td>Ja/Nee</td></tr> <tr> <td>5. De personen die de beveiligingstest uitvoeren zijn minimaal CEH (Certified Ethical Hacker) of vergelijkbaar gecertificeerd.</td><td>Ja/Nee</td></tr> <tr> <td>6. De personen die de beveiligingstest uitvoeren staan onafhankelijk ten opzichte van het te onderzoeken object.</td><td>Ja/Nee</td></tr> <tr> <td>7. De personen die de beveiligingstest uitvoeren hebben aantoonbare eerdere ervaringen hiermee.</td><td>Ja/Nee</td></tr> </tbody> </table> Beoordeling Voor iedere (sub)vraag waarop uw antwoord 'ja' is, krijgt u 3 punten. U kunt voor uw beantwoording zo maximaal 21 punten krijgen. 21 punten	Vraag	Antwoord	1. U geeft gedurende de looptijd van de Overeenkomst op verzoek van Opdrachtgever inzage in testverslagen met openstaande beveiligingsrisico's van de uitgevoerde beveiligingstesten.	Ja/Nee	2. U voert ieder half jaar of vaker een penetratietest uit.	Ja/Nee	3. U lost bevindingen uit de beveiligingstesten (geautomatiseerd of handmatig) met de classificatie 'hoog' binnen één maand op.	Ja/Nee	4. U voert beveiligingstesten uit volgens procedures ontleend aan industriebrede standaarden zoals de Penetration Testing Execution Standard en de Open Source Security Testing Methodology Manual of gelijkwaardige standaarden.	Ja/Nee	5. De personen die de beveiligingstest uitvoeren zijn minimaal CEH (Certified Ethical Hacker) of vergelijkbaar gecertificeerd.	Ja/Nee	6. De personen die de beveiligingstest uitvoeren staan onafhankelijk ten opzichte van het te onderzoeken object.	Ja/Nee	7. De personen die de beveiligingstest uitvoeren hebben aantoonbare eerdere ervaringen hiermee.	Ja/Nee
Vraag	Antwoord																
1. U geeft gedurende de looptijd van de Overeenkomst op verzoek van Opdrachtgever inzage in testverslagen met openstaande beveiligingsrisico's van de uitgevoerde beveiligingstesten.	Ja/Nee																
2. U voert ieder half jaar of vaker een penetratietest uit.	Ja/Nee																
3. U lost bevindingen uit de beveiligingstesten (geautomatiseerd of handmatig) met de classificatie 'hoog' binnen één maand op.	Ja/Nee																
4. U voert beveiligingstesten uit volgens procedures ontleend aan industriebrede standaarden zoals de Penetration Testing Execution Standard en de Open Source Security Testing Methodology Manual of gelijkwaardige standaarden.	Ja/Nee																
5. De personen die de beveiligingstest uitvoeren zijn minimaal CEH (Certified Ethical Hacker) of vergelijkbaar gecertificeerd.	Ja/Nee																
6. De personen die de beveiligingstest uitvoeren staan onafhankelijk ten opzichte van het te onderzoeken object.	Ja/Nee																
7. De personen die de beveiligingstest uitvoeren hebben aantoonbare eerdere ervaringen hiermee.	Ja/Nee																

Assurance en audits

Eis 2.6	U dient uiterlijk één jaar na ingang van de Overeenkomst in bezit te zijn van een ISAE 3402 type 1 verklaring en uiterlijk twee jaar na ingang van de Overeenkomst in bezit te zijn van een ISAE 3402 type 2. Daarna dient de ISAE 3402 type 2 verklaring gedurende de looptijd van de Overeenkomst jaarlijks behaald te worden. De onderwerpen van de ISAE 3402 verklaringen hebben betrekking op de beveiliging van de datacommunicatieverbinding en het dashboard, de kwaliteit van de ICT-infrastructuur, de gegevensverwerking, datatransport, dataopslag en de afhandeling van het betalingsverkeer.
Wens 2.3 Meerkeuze	Wij vragen u: A. Aan te geven of u per ingangsdatum beschikt over een ISAE 3402 type 2 verklaring met betrekking tot de beveiliging van de datacommunicatieverbinding en EB-functionaliiteit, de kwaliteit van de ICT-infrastructuur, de gegevensverwerking, datatransport, dataopslag en de afhandeling van het betalingsverkeer.

	B. Aan te geven, indien u niet beschikt over een ISAE 3402 type 2 verklaring per ingangsdatum overeenkomst, of het voor u haalbaar is om één jaar na ingang van de Overeenkomst te beschikken over een verklaring type 2 (= opzet, bestaan en werking.) C. Aan te geven, indien u <u>niet</u> beschikt over een ISAE 3402 type 2 verklaring per ingangsdatum overeenkomst, of het voor u haalbaar is om per ingangsdatum over een verklaring type 1 te beschikken (= opzet en bestaan). Beoordeling De punten worden verdeeld volgens onderstaande tabel. Geef aan wat voor u van toepassing is. U geeft dit aan door in onderstaande tabel achter het antwoord dat voor u van toepassing is een kruisje te zetten in de antwoordkolom. U kruist maximaal één antwoord aan, meerdere kruisjes resulteert in een score van 0 punten. <table><tr><th>Omschrijving</th><th>Antwoord</th><th>Punten</th></tr><tr><td>A. U beschikt per ingangsdatum over een ISAE3402 type 2 verklaring</td><td>16</td><td>Maximaal</td></tr><tr><td>B. U beschikt uiterlijk 1 jaar na ingangsdatum over een ISAE3402 type 2 verklaring</td><td>8</td><td>helft</td></tr><tr><td>C. U beschikt per ingangsdatum over een ISAE3402 type 1 verklaring (en niet over een type 2 verklaring)</td><td>4</td><td>kwart</td></tr></table> 16 punten	Omschrijving	Antwoord	Punten	A. U beschikt per ingangsdatum over een ISAE3402 type 2 verklaring	16	Maximaal	B. U beschikt uiterlijk 1 jaar na ingangsdatum over een ISAE3402 type 2 verklaring	8	helft	C. U beschikt per ingangsdatum over een ISAE3402 type 1 verklaring (en niet over een type 2 verklaring)	4	kwart
Omschrijving	Antwoord	Punten											
A. U beschikt per ingangsdatum over een ISAE3402 type 2 verklaring	16	Maximaal											
B. U beschikt uiterlijk 1 jaar na ingangsdatum over een ISAE3402 type 2 verklaring	8	helft											
C. U beschikt per ingangsdatum over een ISAE3402 type 1 verklaring (en niet over een type 2 verklaring)	4	kwart											
Eis 2.7	U dient te borgen dat data met betrekking tot het betalingsverkeer van een Rijksonderdeel alleen verstrekt wordt aan derden (inclusief de andere Rijksonderdelen) nadat het betreffende Rijksonderdeel hiervoor schriftelijk toestemming heeft gegeven.												
Wens 2.4 Ja/nee	U kunt ons toestaan het right to review van het auditdossier met betrekking tot de jaarlijkse Assurance verklaring te gebruiken, zodat inzicht kan worden verworven in de kwaliteit van de gehanteerde controls en de hiervoor verzamelde onderbouwing zoals overeengekomen tussen u en de Rijksonderdelen. 8 punten												
Wens 2.5 Ja/nee	U kunt verklaren dat uiterlijk één jaar na ingang van de Overeenkomst onderzoeksrapporten en een dossier toegankelijk zijn over de kwaliteit van de van toepassing zijnde ISO-norm c.q. BIO-maatregelen. 16 punten												

De functionele aspecten van de datacommunicatieverbinding

Eis 2.8	U dient als datacommunicatieverbinding een beveiligde verbinding met de Rijksonderdelen ter beschikking te stellen waarbij de slaagkans op een succesvolle eerste poging tot gegevensuitwisseling minimaal 99,50% * bedraagt. <i>* Toelichting</i> Dit betekent dat maximaal 1 op de 200 eerste pogingen tot gegevensuitwisseling mag mislukken. Na gunning maken wij afspraken over de gewenste uitwisselmomenten en monitoring.
Eis 2.9	U dient een datacommunicatieverbinding met de Rijksonderdelen ter beschikking te stellen welke voldoet aan de navolgende prestatie-eis: Indien een webservice geboden wordt dient deze een responstijd te hebben van maximaal 5 seconden.
Eis 2.10	U dient er zorg voor te dragen dat datacommunicatie met de Rijksonderdelen, zonder uitdrukkelijke toestemming, niet verloopt via een andere partij dan Opdrachtnemer.

Eis 2.11	U dient voor de datacommunicatieverbinding op werkdagen tussen 08:00 uur en 17:00 uur ondersteuning (incident- en probleemmanagement) te bieden.
----------	--

De functionele aspecten van het Portal

Wij verstaan onder een online portal een dashboard, binnen de beveiligde internetomgeving van u als Inschrijver, voor bijvoorbeeld het uitlezen van betaalddata, het maken van rapportages en het exporteren van data naar onze administratieve systemen.	
Eis 2.12	U dient een Portal ter beschikking te stellen dat als webapplicatie middels een webbrowser wordt benaderd.
Eis 2.13	U dient een webbrowser onafhankelijk Portal te bieden zonder gebruik van browser plug ins.
Eis 2.14	U dient ervoor te zorgen dat Portals alleen toegankelijk zijn voor geautoriseerde vertegenwoordigers van de Opdrachtgever.
Wens 2.6 Ja/nee	De Rijksonderdelen kunnen geen software installeren op de werkplekken. U kunt een Portal bieden met een 'zero footprint' op de werkplek. 24 punten

Beveiligingsaspecten algemeen van het Portal

Eis 2.15	U dient een Portal ter beschikking te stellen waarbij de verbinding voor het transport van de data (van en naar u als Inschrijver) beveiligd is door middel van encryptie. De functionele eisen inzake de encryptie-oplossing zijn: • authenticatie van u als Inschrijver en de gebruiker; • integriteit van de transacties.
----------	--

Authenticatie voor portal

Eis 2.16	U dient een Portal ter beschikking te stellen waarbij een gebruiker (natuurlijk persoon) wordt geauthentiseerd via twee (of meer) factor authenticatie, ook wel twee (of meer) stappen verificatie genoemd.
----------	---

Functionele Logging

Acties van gebruikers en medewerkers (ook die van uw eigen organisatie) dienen vastgelegd te worden (logging). Met onderstaande wens krijgen wij nader inzicht in de mogelijkheden om logging te bewaren en te delen (BIO 12.4.1).	
Eis 2.17	U dient historische logininformatie ten minste 13 maanden beschikbaar te houden.
Wens 2.7 Ja/nee	U biedt een koppeling voor de geautomatiseerde uitwisseling van loggegevens. 8 punten
Wens 2.8 Meerkeuze	De Rijksonderdelen hebben een voorkeur voor een Portal dat de gebeurtenissen in de Portal logt voor tenminste 13 maanden, waarbij de logging gegevens door de administrator te raadplegen en te downloaden zijn. Welke van onderstaande gebeurtenissen worden gelogd: - opvoeren, wijzigen, afvoeren van gebruikersaccounts; - activeren en deactiveren van middelen waarmee toegang tot de Portal kan worden verkregen; - opvoeren, wijzigen en verwijderen van functieprofielen; - toevoegen van rechten en functieprofielen aan gebruikersaccounts; - verwijderen van rechten en functieprofielen bij gebruikersaccounts;

	- aanmelden en wijzigen van serviceverzoeken, indien deze functionaliteit ondersteund wordt. Beoordeling Voor ieder van de genoemde gebeurtenissen waarvoor u aan de wens kunt voldoen scoort u 4 punten. 24 punten
--	--

Opslaan van informatie

Eis 2.18	U dient informatie alleen op te slaan in een land binnen de Europese Economische Ruimte of op cloudoplossing waarvan de servers zich in een land binnen de Europese Economische Ruimte bevinden. U levert daarnaast redelijke inspanningen om deze verplichting af te dwingen aan derden die, direct of indirect, betrokken zijn bij de uitvoering van deze Overeenkomst.
----------	---

THEMA 3: TECHNISCHE ASPECTEN

Berichtenverkeer

Eis 3.1	U dient te voldoen aan de technische eisen die voor de Rijksonderdelen gelden voor de geautomatiseerde oplossing van gegevensuitwisseling van het berichtenverkeer.
Wens 3.1 Ja/nee	U kunt voor de geautomatiseerde oplossing van gegevensuitwisseling van het berichtenverkeer een uniform standaard format aanleveren voor alle gebruikte betaalmethoden. 21 punten
Eis 3.2	U dient in het berichtenverkeer tussen u en de Rijksonderdelen te voldoen aan de application programming interface (API) online betalingen.
Eis 3.3	U dient voor terugmeldingen (ook wel 'pushnotificaties' of 'pushberichten' genoemd) naar Rijksonderdelen aan te sluiten op het beveiligde net van het betreffende Rijksonderdeel. Specifieke minimale eis hier is 'two-way SSL' op basis van certificaten.
Eis 3.4	U dient voor terugmeldingen naar het front-end naast beveiligd transport ook ondertekening van het bericht te ondersteunen.

Beschikbaarheid betaalmethode

Eis 3.5	U dient een normale beschikbaarheid van de betaalmethode van 99.9%, 24*7 aan te bieden, per maand gemeten (doorlopend) exclusief (gepland periodiek) onderhoud van de Dienstverlening. Onderhoud van derde partijen telt mee in de beschikbaarheid van de dienst.
---------	---

Back-up

Eis 3.6	U dient te beschikken over een aantoonbaar werkende back-up van het platform waarmee de Dienstverlening zo spoedig mogelijk, maar in ieder geval binnen 4 uur, hersteld kan worden.
Eis 3.7	U dient de back-up en herstel procedure minimaal eenmaal per jaar te testen. De resultaten van deze test aangevuld met eventuele aanbevelingen deelt u met de Rijksonderdelen.

Business continuity

Wens 3.2 Ja/nee	U heeft, voor op het moment dat uw productieomgeving langer dan 4 uur uitvalt, de beschikking over een uitwijkomgeving met een exacte kopie van uw productieomgeving. Deze uitwijkomgeving moet continu gesynchroniseerd zijn met uw productieomgeving.
--------------------	---

21 punten

Wijzigingen

Eis 3.8	U dient wijzigingen/nieuwe releases tenminste zes maanden voor uitvoering/implementatie te communiceren naar de Rijksonderdelen. Indien tevens een wijziging aan de zijde van de Rijksonderdelen benodigd is, dienen de wijzigingen tenminste negen maanden voor de uitvoering/implementatie te worden gecommuniceerd. Gedurende deze periode dient u zowel de oude als de nieuwe omgeving te ondersteunen.
Eis 3.9	U dient releasenotes van aankomende wijzigingen te leveren.
Eis 3.10	U dient minimaal zestig dagen voor het verlopen van een certificaat bij de Rijksonderdelen hiervan melding te maken bij de contactperso(n)en van de Rijksonderdelen.
Eis 3.11	U dient de beschikking te hebben over een testomgeving waarin wijzigingen/nieuwe releases door de Rijksonderdelen kunnen worden getest voordat deze wijziging(en)/nieuwe releases door de Opdrachtnemer in de productieomgeving worden gezet. Deze testomgeving dient volledig gescheiden te zijn van de productieomgeving.
Wens 3.3 Ja/nee	U kunt bij een door de Rijksonderdelen gevraagde wijziging binnen een redelijke termijn, maar uiterlijk binnen drie maanden na melding, starten met de implementatie van deze wijziging. <i>Toelichting</i> Hiermee wordt onder andere bedoeld: - Het aansluiten van een nieuwe betaalmethode; - Het opleveren van een nieuwe rapportage. 21 punten

Portal

Eis 3.12	U dient ervoor te zorgen dat uw Portal de Nederlandse en/of Engelse taal ondersteunt.
Wens 3.4 Ja/Nee	Uw Portal ondersteunt de Nederlandse taal. 7 punten
Eis 3.13	U dient per Rijksonderdeel real-time inzicht te geven in de status van de transacties per betaalmethode.
Eis 3.14	Uw portal geeft voor ieder afzonderlijk Rijksonderdeel transactie informatie per betaalmethode weer, waarbij minimaal de volgende transactie informatie genest kan worden geraadpleegd: hoofd- en sub account, betaalmethode/transactietype, naam betaler, bedrag, transactienummer en betalingskenmerk. De informatie moet opvraagbaar zijn per dag, per week en per maand.
Eis 3.15	U dient uw portal zodanig in te richten dat per betaalmethode inzicht wordt verstrekt in de geslaagde en niet geslaagde betaaltransacties. Bij niet geslaagde betaaltransacties moet een verwijzing worden opgenomen naar de reden waarom de transactie is mislukt.
Wens 3.5 Ja/nee	U kunt vanuit uw portal een overzicht aanbieden waarop de aantallen transacties per maand per betaalmethode automatisch worden gepresenteerd. 14 punten
Eis 3.16	Uw portal dient per Rijksonderdeel te beschikken over uitgebreide zoek- en sorteermogelijkheden, minimaal op account (per hoofd- en sub account per Rijksonderdeel), datum en bedrag. Tevens dient het mogelijk te zijn om deze data eenvoudig te printen of te exporteren naar gangbare kantoorautomatisering bestandsformaten zoals PDF, Excel en CSV formaat. De rapportages moeten per dag, per week en per maand opvraagbaar zijn.

Eis 3.17	U dient de informatie in het portal minimaal 13 maanden beschikbaar te houden.								
Wens 3.6 Meerkeuze	U kunt de informatie in het portal langer dan 13 maanden beschikbaar houden. Beoordeling Hoe langer, hoe hoger uw score. <table border="1"> <thead> <tr> <th>Aantal maanden</th><th>Aantal punten</th></tr> </thead> <tbody> <tr> <td>14 t/m 24 maanden</td><td>4</td></tr> <tr> <td>25 t/m 36 maanden</td><td>8</td></tr> <tr> <td>37 t/m 84 maanden</td><td>14</td></tr> </tbody> </table> 14 punten	Aantal maanden	Aantal punten	14 t/m 24 maanden	4	25 t/m 36 maanden	8	37 t/m 84 maanden	14
Aantal maanden	Aantal punten								
14 t/m 24 maanden	4								
25 t/m 36 maanden	8								
37 t/m 84 maanden	14								
Eis 3.18	U dient in uw Portal de mogelijkheid te bieden aan de Rijksonderdelen zelf om gebruikers toe te voegen dan wel te verwijderen.								
Eis 3.19	U dient minimaal de rollen administrator, beheer en raadplegen te ondersteunen.								

Capaciteit

Eis 3.20	U dient de aangegeven volumes van het Rijk te kunnen verwerken.
----------	---

THEMA 4: SERVICE EN IMPLEMENTATIE

Service

Eis 4.1	U dient servicemanagement te leveren bestaande uit tenminste: - Een accountmanager; - Een Servicedesk (eerstelijns); - Een tweedelijns ondersteuning; - Een implementatiemanager bij projecten.
Eis 4.2	U dient voor de Rijksonderdelen een <u>Servicedesk</u> ter beschikking te hebben waarbij geldt dat: - de Servicedesk voor storingen, overige meldingen en vragen bereikbaar is op werkdagen van 08:00 uur tot 17:00 uur; - de Servicedesk dient telefonisch bereikbaar te zijn tegen maximaal lokaal Nederlands tarief; - de Servicedesk dient eveneens via email bereikbaar te zijn; - de Servicedesk bemanning kent de gang van zaken binnen de Rijksonderdelen; - de Servicedesk is op de hoogte van de actuele verstoringen van zowel uw eigen dienstverlening als die van de onderaannemers en is daarnaast op de hoogte van de verstoringen van de aangeboden betaalproducten van derden; - de Servicedesk kent de beschreven Dienstverleningsovereenkomst; - de Servicedesk communiceert in de Nederlandse taal tenminste op het niveau B2.2 van het Europees Referentiekader talen.
Wens 4.1 Ja/nee	De Rijksonderdelen geven de voorkeur aan een dedicated Servicedesk voor de Rijksonderdelen. U kunt een dedicated Servicedesk voor het Rijk beschikbaar stellen. 15 punten
Eis 4.3	U dient het <u>accountmanagement</u> zodanig in te richten dat er een accountmanager voor de Rijksonderdelen bereikbaar is, waarbij geldt dat: - de accountmanager tijdens werkdagen van 08.00 uur tot 18.00 uur bereikbaar is;

	- de accountmanager of de betreffende achtervang bij incidenten van het Prio 1 niveau 24*7*365 bereikbaar te zijn; - er een ervaren accountmanager is voor beleidsmatige en operationele zaken; - er 100% achtervang van deze accountmanager is; - er wordt gecommuniceerd in de Nederlandse taal op het niveau B2.2 van het Europees Referentiekader talen; en - de accountmanager en diens achtervang een Verklaring Omtrent Gedrag bezitten.
Wens 4.2 Open	De Rijksonderdelen vinden het belangrijk dat het <u>accountmanagement</u> dusdanig is ingericht dat: - de accountmanager direct en proactief actie onderneemt bij calamiteiten; dit geldt ook voor calamiteiten die buiten zijn/haar directe invloedssfeer optreden; - de accountmanager geïnformeerd is over toekomstige ontwikkelingen, zowel binnen uw organisatie zelf als binnen het online betalingsverkeer in het algemeen; - de accountmanager beschikt over een uitgebreid netwerk van contacten met betrekking tot het bank- en betalingsverkeer. Beschrijf op welke wijze u het accountmanagement concreet gaat inrichten en aan bovenstaande gaat voldoen. 45 punten
Wens 4.3 Ja/nee	U kunt in voorkomende gevallen specialisten van de Rijksonderdelen (bijvoorbeeld op het gebied van automatisering) rechtstreeks met de betreffende specialisten van de Opdrachtnemer laten communiceren. 45 punten
Eis 4.4	U dient ervoor zorg te dragen dat uw medewerkers van de tweedelijnsondersteuning kunnen communiceren in de Nederlandse taal op niveau B2.2 van het Europees Referentiekader talen of op niveau B2.2 in het Engels.
Wens 4.4 Ja/nee	U kunt tweedelijnsondersteuning verschaffen in de Nederlandse taal op niveau B2.2 van het Europees Referentiekader talen. 15 punten
Eis 4.5	U dient binnen uw Servicedesk alle meldingen met een uniek meldingsnummer te registreren en terug te koppelen.
Wens 4.5 Ja/nee	U kunt via het Portal de geregistreerde vragen, klachten en incidenten met daarbij status en verwachte oplostijd online ontsluiten voor de Rijksonderdelen. 45 punten
Eis 4.6	U dient ervoor te zorgen dat de Servicedesk actief het betrokken Rijksonderdeel op de hoogte houdt van de status van de gemelde incidenten.
Wens 4.6 Ja/nee	U kunt ieder Rijksonderdeel ondersteunen bij hun rapportage verplichting t.a.v. PCI-DSS bij het voldoen aan de compliance verplichtingen door middel van: 1. een rapport van een extern gekwalificeerde beveiligings auditor en/of; 2. d.m.v. ondersteuning bij het invullen van een compliance rapportage (self-assessment questionnaire) en/of; 3. het aanbieden van een beveiligingssysteem dat een geïntegreerde beveiligings en compliance oplossing biedt dat helpt om gevoelige data te beveiligen en te voldoen aan informatie beveiligings en privacy standaarden. Beoordeling Voor iedere (sub)vraag waarop uw antwoord 'ja' is, krijgt u 15 punten. U kunt voor uw beantwoording zo maximaal 45 punten krijgen. 45 punten

Performance measurement

De Rijksonderdelen wensen na definitieve gunning gezamenlijk met u KPI's overeen te komen, ter monitoring van de door u geleverde prestaties en het kunnen opstellen van wederzijdse verbeterpunten. De KPI's worden vastgelegd in de Service Niveau Overeenkomst.

Eis 4.7	U dient akkoord te gaan met het gezamenlijk met de Rijksonderdelen overeenkomen en opstellen van Key Performance Indicators (KPI's) op basis van in het Beschrijvend document gevraagde Dienstverlening.
Eis 4.8	U dient de KPI's periodiek te rapporteren aan en te bespreken met de Rijksonderdelen.

Storing

Eis 4.9	U dient bij het constateren van een storing direct per telefoon of e-mail contact op te nemen met de contactperso(n)en(en) van Rijksonderdelen die door deze storing worden geraakt.
---------	--

Documentatie

Eis 4.10	U dient technische documentatie en handleidingen die voor de Rijksonderdelen van belang zijn in de Nederlandse taal op niveau B2.2 van het Europees Referentiekader talen of op niveau B2.2 in het Engels digitaal toegankelijk te maken voor de Rijksonderdelen.
<i>Wens 4.7</i> <i>Ja/nee</i>	De documentatie is: - in de Nederlandse taal beschikbaar; - te raadplegen via het Portal. 15 punten

Contacten met derden

Eis 4.11	U dient communicatie met derden op het gebied van online betaalmethoden en zoals Creditcard maatschappijen en eventuele Onderaannemers, te verzorgen, tenzij de online betaalmethode direct contact met de Rijksonderdelen vereist.
----------	---

Overlegvormen

Eis 4.12	U dient beschikbaar te zijn voor de volgende overleggen en daarvoor de relevante medewerker(s) ter beschikking te stellen: • één keer per twee maanden operationeel overleg per individueel Rijksonderdeel; • één keer per zes maanden strategisch overleg met alle Rijksonderdelen gezamenlijk; • ad hoc per individueel Rijksonderdeel. In het operationeel overleg worden in ieder geval de ontwikkelingen van de betaalproducten besproken.
----------	--

Managementrapportage

Eis 4.13	U dient managementrapportages beschikbaar te stellen t.b.v. de diverse overlegvormen waarin u rapporteert over relevante aspecten van uw Dienstverlening welke nader worden uitgewerkt in de Service Niveau Overeenkomst.
----------	---

Implementatie

De Rijksonderdelen willen graag weten hoe u de implementatie na definitieve gunning gaat vormgeven. In een plan van aanpak moet onder andere aangegeven worden welke volgorde van activiteiten plaatsvinden, de doorlooptijd en welke inzet van de Opdrachtgever nodig is. Het Rijk wil met u en een afvaardiging van de

Rijksonderdelen een stuurgroep vormen. De Rijksonderdelen zullen voor hun onderdeel elk een eigen implementatiemanager aanwijzen.	
Eis 4.14	U dient een implementatiemanager(s) aan te stellen die verantwoordelijk is voor de implementatie van nieuwe producten, processen of diensten. De implementatiemanager(s) ondersteunt de betreffende Rijksonderdelen bij het implementeren van de Dienstverlening. Per Rijksonderdeel wijst u maximaal één implementatiemanager aan.
Eis 4.15	U dient een implementatiemanager aan te wijzen die verantwoordelijk is voor het overzicht, bewaking van de algehele voortgang en communicatie met het Agentschap.
Wens 4.8 Open	De Rijksonderdelen hebben behoefte aan een implementatieplan waarin is aangegeven hoe de migratie van de huidige Dienstverlener naar u gaat plaatsvinden. Ga bij de beantwoording in op de volgende aspecten: - de verschillende stappen en mijlpalen in het migratieproces; - de volgorde waarin deze stappen worden uitgevoerd; - de invulling van het implementatieteam; - de doorlooptijd van de implementatie; - de testfase; de wijze waarop de Rijksonderdelen van een testomgeving gebruik kunnen maken; - de benodigde inzet en capaciteit van de Rijksonderdelen; - de geboden ondersteuning aan de Rijksonderdelen; - de geboden nazorg aan de Rijksonderdelen; - waar u verwacht dat er knelpunten zullen optreden en hoe u deze knelpunten gaat (helpen) oplossen; - geef tevens aan wat de ervaringen zijn met verschillende financiële systemen. Beoordeling Punten zullen worden toegekend voor: • volledigheid (of alle activiteiten vermeld in deze wens zijn vervuld en hoe activiteiten kwalitatief worden geïnterpreteerd); • doelmatige aanpak en methoden; • uitvoerbaarheid; en • hoe cohesie tussen de verschillende componenten/doelstellingen van deze wens is gegarandeerd. 45 punten
Eis 4.16	U dient zes weken na gunning per Rijksonderdeel een gedetailleerd implementatieplan op te stellen dat gedegen is en onderbouwd en voor het Agentschap een totaaloverzicht van alle implementatieplannen tezamen.

THEMA 5: KOSTEN EN FACTURATIE

Facturatie

Eis 5.1	U dient voor deze Inschrijving tarieven aan te bieden die vast staan voor de gehele duur van de overeenkomst.
Eis 5.2	U dient de geleverde Diensten na afloop van iedere maand te factureren bij alle verschillende Rijksonderdelen afzonderlijk.
Eis 5.3	U dient op de factuur de transactiekosten in rekening te brengen per verschillende online betaalmethode waarbij het aantal transacties per betaalmethode wordt aangegeven.

Eis 5.4	U dient bij bovenstaande Eis onderscheid te maken tussen vaste en variabele kosten te specificeren per product en geleverde services.
Eis 5.5	U dient in het geval van een creditfactuur het factuurnummer van de corresponderende debetfactuur te vermelden.
Eis 5.6	U dient de kosten voor creditcard acquiring niet in rekening te brengen op de creditcard transactie. Deze kosten moeten apart op de maandelijkse factuur in rekening worden gebracht.
Eis 5.7	U dient te factureren conform het format in Bijlage G – Handreiking basisfactuur Rijk. Het automatisch incasseren van kosten van de (derdengelden)rekening van het Rijksonderdeel is niet toegestaan.
Eis 5.8	Implementatiekosten zijn kosten die u moet maken gedurende de implementatieperiode voor de overgang van de dienstverlening op de PSP en de implementatiekosten bij de introductie van een nieuw betaalproduct. U dient geen implementatiekosten in rekening te brengen.
Eis 5.9	U dient geen kosten voor het aanhouden van een derdengeldrekening in rekening te brengen, waaronder eventuele rentekosten.

THEMA 6: INNOVATIE EN TOEKOMSTBESTENDIGHEID

Algemeen

Eis 6.1	De Rijksonderdelen proberen de markt- en productontwikkelingen op de voet te volgen. De Rijksonderdelen vinden het belangrijk dat u de Rijksonderdelen periodiek informeert over nieuwe marktontwikkelingen en nieuwe betaalproducten. U dient alle Rijksonderdelen afzonderlijk en proactief te betrekken bij de Europese- en Wereldwijde ontwikkelingen in betaaldienstverlening.
Wens 6.1	De Rijksonderdelen zijn continu op zoek naar innovatieve betaalmethode, zowel nationaal als internationaal.
Open	Hoe kunt u de Rijksonderdelen voorzien in informatie met betrekking tot de toepasbaarheid van huidige en toekomstige betaalproducten. Beoordeling Punten zullen worden toegekend voor: • volledigheid (of alle activiteiten vermeld in deze wens zijn vervuld en hoe activiteiten kwalitatief worden geïnterpreteerd); • doelmatige aanpak en methoden; • toepasbaarheid; en • de wijze waarop de oplossing aansluit bij de betaalprocessen van de Rijksoverheid. 36 punten
Wens 6.2	U kunt een online betaalmethode aanbieden waarbij het mogelijk is om een betaling in de toekomst in te plannen.
Ja/nee	36 punten
Wens 6.3	U kunt een online betaalmethode aanbieden waarbij het mogelijk is om een betaling periodiek in de toekomst in te plannen.
Ja/nee	12 punten
Wens 6.4	De herziene Europese wetgeving ten aanzien van de Payment Services Directive (PSD2) biedt mogelijkheden voor derde partijen om toegang te krijgen tot rekeninginformatie van bankklanten

Open	(Account Information services/AIS of Payment Initiation services/PIS), mits klanten hiervoor akkoord geven en de derde partij een licentie van de toezichthouder krijgt. Hierdoor komen er aanbieders met nieuwe betaal- en informatiediensten op de markt. • Heeft u een licentie voor AIS en/of PIS in uw bezit? • Heeft u de intentie om deze in de (nabije) toekomst aan te vragen? Zo ja, wanneer denkt u dit te realiseren? Welke toepassingsmogelijkheden voor de Rijksonderdelen ziet u? 24 punten																										
Wens 6.5 Open	In de markt ontstaan steeds meer mogelijkheden om bij online betaalproducten de betaling via een QR Code te laten uitvoeren. U kunt de QR Code ondersteunen bij het gebruik van online betaalproducten. Geef aan bij welke betaalproducten u dit nu en in de toekomst denkt te gaan ondersteunen. <table border="1"> <thead> <tr> <th>Betaalproduct</th><th>Aantal punten</th></tr> </thead> <tbody> <tr><td>iDEAL</td><td>2</td></tr> <tr><td>iDEAL QR</td><td>2</td></tr> <tr><td>Bancontact</td><td>2</td></tr> <tr><td>Sofort</td><td>2</td></tr> <tr><td>Giropay</td><td>2</td></tr> <tr><td>Mastercard</td><td>2</td></tr> <tr><td>Visacard</td><td>2</td></tr> <tr><td>Paypal</td><td>2</td></tr> <tr><td>American Express</td><td>1</td></tr> <tr><td>China Union Pay</td><td>1</td></tr> <tr><td>JCB</td><td>1</td></tr> <tr><td>Diners</td><td>1</td></tr> </tbody> </table> 20 punten	Betaalproduct	Aantal punten	iDEAL	2	iDEAL QR	2	Bancontact	2	Sofort	2	Giropay	2	Mastercard	2	Visacard	2	Paypal	2	American Express	1	China Union Pay	1	JCB	1	Diners	1
Betaalproduct	Aantal punten																										
iDEAL	2																										
iDEAL QR	2																										
Bancontact	2																										
Sofort	2																										
Giropay	2																										
Mastercard	2																										
Visacard	2																										
Paypal	2																										
American Express	1																										
China Union Pay	1																										
JCB	1																										
Diners	1																										
Wens 6.6 Open	U kunt de Rijksonderdelen adviseren en ondersteunen bij het aansluiten op online betalingen (waaronder E-Wallets) en ontvangsten in het buitenland (mogelijk via uw contacten met lokale aanbieders). <i>Toelichting</i> Het Ministerie van Buitenlandse zaken wil in de toekomst haar buitenlandse posten en vertegenwoordigingen, waar mogelijk, gebruik laten maken van online betaalsystemen voor het doen van online betalingen. Beoordeling Mate van ondersteuning en het aantal contacten bepaalt de score. 12 punten																										

THEMA 7: MAATSCHAPPELIJK VERANTWOORD ONDERNEMEN (MVO)

Eerbiediging mensenrechten

De Staat bevordert de eerbiediging van mensenrechten door het bedrijfsleven. Het doel is om mensenrechtenschendingen door bedrijven, rechtstreeks of indirect via productieketens, te voorkomen. Bedrijven hebben een maatschappelijke verantwoordelijkheid voor wat speelt in hun productieketen inclusief werk met fatsoenlijke arbeidsvoorwaarden. Om schendingen in hun productieketen op het gebied van mensenrechten zoveel mogelijk te voorkomen verwacht het kabinet dat bedrijven handelen volgens de United Nation's Guiding Principles on Business and Human Rights en de OESO-richtlijnen. Met betrekking tot arbeid verwacht de Staat dat bedrijven de ILO core conventions als minimum-standaard hanteren.

Eis 7.1	U dient de verklaring eerbiediging mensenrechten (Bijlage 7) te ondertekenen.
Wens 7.1 Open	Beschrijf welke risico's u onderkent in relatie tot mensenrechtenschendingen. Geef daarbij aan hoe u in uw organisatie invulling geeft aan het waarborgen van mensenrechten (denk bijvoorbeeld bij dienstverlening, productie of uitbesteding in lagelonenlanden aan arbeidsomstandigheden en leefbaar loon). Beoordeling In uw antwoord dienen in ieder geval de volgende aspecten terug te komen: • uw beleid ten aanzien van aanbestedingen en uitbestedingen; • uw beleid ten aanzien van stakeholderengagement (denk aan gesprekken met de klant en uw werknemers, en het hebben van een klachtenmechanisme); • het effect van de door u genomen maatregelen en de wijze waarop u hierover naar buiten communiceert. 20 punten
Wens 7.1a Open	Beschrijf uw beleid in den brede om te voorkomen dat reputatieschade kan ontstaan als gevolg van activiteiten en handelingen van bedrijven waaraan u diensten verleent. Geef in elk geval aan welke (beoogde) klanten of klantgroepen u als verhoogd risico beschouwt (zoals gokbranche, adult entertainmentbranche, cryptovalutabedrijven, trustkantoren en bedrijven uit landen die door de FATF als verhoogd risico worden beschouwd), het aandeel transacties (per jaar) dat u met klanten of klantgroepen met een verhoogd risicoprofiel realiseert en de maatregelen die u neemt om de verhoogde risico's van dergelijke klanten of klantgroepen te beheersen. Beoordeling In uw antwoord dient in ieder geval het volgende aspect terug te komen: • uw beleid ten aanzien van beoordeling van informatie die naar voren komt als onderdeel van de customer due diligence, in het bijzonder de mate waarin u bent blootgesteld aan klanten of klantgroepen met een verhoogd risicoprofiel, de mitigerende maatregelen die u treft en in hoeverre deze mitigerende maatregelen adequaat zijn om het risico te beheersen. 50 punten

Verbod op clustermunitie

Voor in Nederland gevestigde financiële ondernemingen is het verboden om te investeren in ondernemingen die clustermunitie, of cruciale onderdelen daarvan, produceren, verkopen of distribueren.

Financiële ondernemingen moeten adequate maatregelen treffen om te voorkomen dat ze: transacties (laat) uitvoeren in, leningen verstrekt aan of niet-vrij verhandelbare deelnemingen neemt in deze bedrijven.

Eis 7.2	U dient de verklaring clustermunitie (bijlage 8) te ondertekenen.
---------	---

Beloningsbeleid

Wij streven naar een duurzame en aan de burger dienstbare financiële sector waarin geen excessen voorkomen. Wij hechten daarom aan een beheerst beloningsbeleid waarin perverse prikkels worden voorkomen en stakeholders worden betrokken.

Wens 7.2 Open	Beschrijf welke risico's u onderkent in relatie tot een beheerst beloningsbeleid en geef aan hoe u binnen uw organisatie invulling geeft aan een beheerst beloningsbeleid? Beoordeling In uw antwoord dienen in ieder geval de volgende aspecten terug te komen: • de maatregelen die u heeft getroffen voor een beheerst beloningsbeleid ter voorkoming van perverse prikkels en de wijze waarop u stakeholders heeft betrokken;
------------------	--

	• het effect van de door u genomen maatregelen en de manier waarop u dit naar buiten communiceert. 25 punten
--	---

Duurzaamheid

Door middel van onze inkoop stimuleren wij duurzaamheid. Dat wil zeggen dat wij het belangrijk vinden dat onze opdrachtnemers bij de totstandkoming van door ons ingekochte goederen of diensten een negatieve impact op bijvoorbeeld het klimaat, voorkomen of minimaliseren, dan wel een positieve bijdrage leveren.	
Wens 7.3 Open	Beschrijf op welke wijze en in welke mate u bijdraagt aan het behalen van de doelstelling van het Klimaatakkoord zoals op 28 juni 2019 door de Nederlandse regering is gepresenteerd. Beoordeling In uw antwoord dienen in ieder geval de volgende aspecten terug te komen: • Uw beleid bij uw eigen bedrijfsvoering ten aanzien van: - o de klimaatimpact en energie-efficiency van uw eigen bedrijfsvoering en de wijze waarop u deze meet; - o de wijze waarop u transparant bent over de klimaatimpact en energie-efficiency van uw bedrijfsvoering en werkt aan continue verbetering; - o de wijze waarop u ons over ontwikkelingen in bovenstaande informeert gedurende de uitvoering van de opdracht. • Het effect van de door u genomen maatregelen en de manier waarop u dit naar buiten communiceert. 25 punten

Diversiteit en inclusiviteit

Wij vinden het belangrijk dat onze opdrachtnemers oog hebben voor diversiteit en inclusiviteit. Daarom hechten wij waarde aan een intern beleid dat diversiteit en inclusiviteit bevordert, bijvoorbeeld ten aanzien van leeftijd, levensfase, functieverblijfsduur, geslacht, herkomst of seksuele oriëntatie. Diversiteit en inclusiviteit kunnen daarnaast een relevant thema zijn in uw bedrijfsactiviteiten, als u bijvoorbeeld financiële inclusie bevordert door betaaldiensten toegankelijker te maken voor verschillende groepen in de samenleving.	
Wens 7.4 Open	Beschrijf op welke wijze u zich inzet voor diversiteit en inclusiviteit. Beoordeling In uw antwoord dienen in ieder geval de volgende aspecten terug te komen: • Het beleid dat u heeft ten aanzien van diversiteit en inclusiviteit binnen uw bedrijf; • Indien van toepassing, welke rol deze thema's spelen in uw bedrijfsactiviteiten; • Het effect van de door u genomen maatregelen en de manier waarop u dit naar buiten communiceert. 15 punten

Social return

U kunt zich in deze aanbesteding onderscheiden op het gebied van social return. Wij zien het als onze taak om mensen met een afstand tot de arbeidsmarkt te ondersteunen, zodat iedereen zoveel mogelijk meedoet in de samenleving en uitzicht houdt op werk en inkomen.	
Wens 7.5 Open	Beschrijf, indien van toepassing, op welke wijze u mensen met een afstand tot de arbeidsmarkt ondersteunt. Beoordeling In uw antwoord dienen in ieder geval de volgende aspecten terug te komen: • Het beleid dat u heeft ten aanzien van social return;

	• De wijze waarop u dit beleid ten uitvoer brengt. Denk daarbij aan het aantrekken van mensen met een afstand tot de arbeidsmarkt en de vorm van de begeleiding; • De controleerbaarheid van uw maatregelen; • Het effect van de door u genomen maatregelen en de manier waarop u dit naar buiten communiceert. 15 punten
--	--