

Programma van Eisen en Wensen

Leeswijzer

Thema	Omschrijving	Pagina nummer	maximaal aantal punten
Thema 1	Producten	Pagina 1 t/m 3	240
Thema 2	Beveiliging, informatie uitwisseling en - verwerking	Pagina 3 t/m 8	169
Thema 3	Technische aspecten	Pagina 8 t/m 12	101
Thema 4	Service en implementatie	Pagina 12 t/m 16	264
Thema 5	Kosten en facturatie	Pagina 16	0
Thema 6	Innovatie en toekomstbestendigheid	Pagina 16 en 17	48
Thema 7	Maatschappelijk Verantwoord Ondernemen	Pagina 17 t/m 19	150

THEMA 1: PRODUCTEN

Inleiding

Via de betaalterminals die zijn aangesloten op een fysieke kassa worden door de Rijksonderdelen de volgende producten afgenomen; debitcards, creditcards en contactloze betalingen. De betaalterminals zijn door verschillend fabrikanten geleverd en enkele jaren oud. De betaalterminals zijn uniform aan te sluiten op de payment service provider. De betaalterminals zijn eigendom van de Rijksonderdelen m.u.v. de betaalterminals van Direct Betalen. Het beheer van de betaalterminal wordt uitgevoerd door de betreffende leverancier. Het beheer van de software aansluiting waarmee de betaalterminal wordt aangesloten op de PSP zal door de PSP worden verzorgd.

De Opdrachtgever stelt de volgende algemene eisen aan de producten die via de betaalterminals geaccepteerd moeten kunnen worden.

Ontvangsten via debitcards en creditcards

Eis 1.1	U dient alle in het Beschrijvend document paragraaf 2.1.4.2. Beschrijving perceel 2 (POS), genoemde betaalmethoden te ondersteunen.
Eis 1.2	U dient betalingen gedaan via een bankpas uiterlijk T+1 op de door het betreffende Rijksonderdeel aangegeven bankrekening over te boeken.
Eis 1.3	U dient de mogelijkheid te bieden om gelden op afroep beschikbaar te stellen aan het betrokken Rijksonderdeel.
Eis 1.4	U dient alle betalingen die u hebt ontvangen van de creditcard maatschappijen bruto direct door te boeken.
Eis 1.5	U dient gelden bestemd voor de Rijksonderdelen, die niet [na verwerking] rechtstreeks op de aangewezen bankrekening van het betreffende Rijksonderdeel worden gestort, aan te houden op een rekening die niet in het vermogen valt van de Inschrijver [bijvoorbeeld door gebruik van een stichting derdengelden] op een manier die is vereist dan wel goed gekeurd door de relevante Toezichthouder.
Eis 1.6	U dient de transacties conform het collecterend model te laten plaatsvinden.
Eis 1.7	U dient via een host to host verbinding minimaal de volgende debit- en creditcards te kunnen verwerken, die worden aangeboden op de betaalautomaten van de Rijksonderdelen: - Maestro - V-Pay

	- Visa - American Express Cards - Mastercard																										
Eis 1.8	U dient zowel verwerking van betaaltransacties op mobiele als een vaste betaalautomaten te ondersteunen.																										
Eis 1.9	U dient POS transacties in het SEPA gebied en in de navolgende landen te kunnen verwerken. Dit betreft transacties in zowel EUR als lokale valuta. - Zwitserland - Noorwegen - Denemarken - Polen - Groot-Brittannië																										
Wens 1.1 <i>Meerkeuze</i>	Diverse Rijksonderdelen hebben ontvangsten via kaarttransacties buiten Nederland. De betaalterminals bevinden zich verspreid over de gehele wereld. In de huidige situatie wordt de betaling ingesteld als een lokale NL-betaling voor Nederlanders in het buitenland met een NL debet - of creditcard. De wens is om de betaling ook als lokale betaling in het gastland aan te kunnen bieden, waarbij lokale klanten en Nederlanders met een lokale bankpas een lokale transactie doen. Door beide mogelijkheden te kunnen aanbieden worden de transactiekosten die berekend worden door de bank van de klant nihil of zo laag mogelijk. U kunt de betreffende Rijksonderdelen ondersteunen in het zoeken naar mogelijkheden om de acceptatie van lokale cards en lokale valuta te gaan accepteren. Kunt u aangeven in welke landen u per direct of op korte termijn deze Dienstverlening kunt bieden. Beoordeling <table border="1"> <thead> <tr> <th>Landen</th><th>Aantal punten</th></tr> </thead> <tbody> <tr><td>Verenigde Staten van Amerika</td><td>7</td></tr> <tr><td>Canada</td><td>7</td></tr> <tr><td>Brazilië</td><td>7</td></tr> <tr><td>Argentinië</td><td>7</td></tr> <tr><td>Mexico</td><td>3</td></tr> <tr><td>Curaçao</td><td>10</td></tr> <tr><td>Caribisch gebied overig (Aruba, Sint Maarten, Bonaire, Sint Eustatius en Saba)</td><td>4</td></tr> <tr><td>India</td><td>3</td></tr> <tr><td>Japan</td><td>3</td></tr> <tr><td>Australië</td><td>3</td></tr> <tr><td>Nieuw Zeeland</td><td>3</td></tr> <tr><td>Zuid Afrika</td><td>3</td></tr> </tbody> </table> 60 punten	Landen	Aantal punten	Verenigde Staten van Amerika	7	Canada	7	Brazilië	7	Argentinië	7	Mexico	3	Curaçao	10	Caribisch gebied overig (Aruba, Sint Maarten, Bonaire, Sint Eustatius en Saba)	4	India	3	Japan	3	Australië	3	Nieuw Zeeland	3	Zuid Afrika	3
Landen	Aantal punten																										
Verenigde Staten van Amerika	7																										
Canada	7																										
Brazilië	7																										
Argentinië	7																										
Mexico	3																										
Curaçao	10																										
Caribisch gebied overig (Aruba, Sint Maarten, Bonaire, Sint Eustatius en Saba)	4																										
India	3																										
Japan	3																										
Australië	3																										
Nieuw Zeeland	3																										
Zuid Afrika	3																										
Wens 1.2 <i>Ja/nee</i>	U kunt voor de betreffende landen zoals genoemd in uw antwoord op wens 1.1 de mogelijkheid bieden dat per terminal ingesteld kan worden dat de kosten in het kader van het omrekenen van lokale valuta naar euro's voor rekening zijn van de betaler of voor rekening van de ontvanger, zowel binnen als buiten de EEA. 60 punten																										
Eis 1.10	U dient retourpinnen op automaatniveau in te kunnen stellen.																										
Eis 1.11	U dient transacties in Europa via NFC (Near Field Communication) te ondersteunen.																										

Wens 1.3 <i>Meerkeuze</i>	Contactloze betalingen buiten Europa op een betaalterminal doormiddel van het gebruik van NFC technologie via een mobiele telefoon, debet of Creditcard zijn wenselijk. U kunt contactloze betalingen op een betaalterminal te ondersteunen buiten Europa. In hoeveel landen kunt u dit? Beoordeling Hoe meer landen, hoe beter. <table border="1"> <thead> <tr> <th>Aantal landen</th><th>Aantal punten</th></tr> </thead> <tbody> <tr> <td>1 t/m 5 landen</td><td>5</td></tr> <tr> <td>6 t/m 10 landen</td><td>10</td></tr> <tr> <td>Meer dan 11 landen</td><td>20</td></tr> </tbody> </table> 20 punten	Aantal landen	Aantal punten	1 t/m 5 landen	5	6 t/m 10 landen	10	Meer dan 11 landen	20
Aantal landen	Aantal punten								
1 t/m 5 landen	5								
6 t/m 10 landen	10								
Meer dan 11 landen	20								
Wens 1.4 <i>Ja/nee</i>	U kunt een standaardproces met betrekking tot chargeback inrichten dat voldoet aan de informatiebehoefte van de Rijksonderdelen. <i>Toelichting</i> Indien een chargeback wordt ingediend, wil het betreffende Rijsonderdeel 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. 20 punten								

Derdenrekening en uitbetaling

Eis 1.12	U dient betalingen die via een derdengeldenrekening verlopen te verwerken onder de eigen naam van het Rijksonderdeel.
Wens 1.5 <i>Ja/nee</i>	U kunt voor de Rijksonderdelen één derdengeldenrekening gebruiken voor POS betalingen. 20 punten
Eis 1.13	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".

QR Code

Wens 1.6 <i>Ja/nee</i>	U kunt transacties verwerken gedaan met de scan van een QR code vanuit China. <i>Toelichting</i> Het ministerie van Buitenlandse Zaken is op dit moment bezig om in China betalingen op de betaalterminal via scan van een QR code mogelijk te maken. 60 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 de Inschrijver 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	Kunt u 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> 30 punten	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																																																											
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. 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-functionaliteit, 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>20</td><td>Maximaal</td></tr><tr><td>B. U beschikt uiterlijk 1 jaar na ingangsdatum over een ISAE3402 type 2 verklaring</td><td>10</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>5</td><td>kwart</td></tr></table> 20 punten	Omschrijving	Antwoord	Punten	A. U beschikt per ingangsdatum over een ISAE3402 type 2 verklaring	20	Maximaal	B. U beschikt uiterlijk 1 jaar na ingangsdatum over een ISAE3402 type 2 verklaring	10	helft	C. U beschikt per ingangsdatum over een ISAE3402 type 1 verklaring (en niet over een type 2 verklaring)	5	kwart
Omschrijving	Antwoord	Punten											
A. U beschikt per ingangsdatum over een ISAE3402 type 2 verklaring	20	Maximaal											
B. U beschikt uiterlijk 1 jaar na ingangsdatum over een ISAE3402 type 2 verklaring	10	helft											
C. U beschikt per ingangsdatum over een ISAE3402 type 1 verklaring (en niet over een type 2 verklaring)	5	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 assuranceverklaring 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. 10 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. 20 punten												

De functionele aspecten van het Portal

Wij verstaan onder een online Portal een dashboard voor bijvoorbeeld het uitlezen van betaalddata, het maken van rapportages en het exporteren van data naar onze administratieve systemen.	
Eis 2.8	U dient een webbrowser onafhankelijk Portal te bieden, zonder gebruik van browser plug ins.
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. 30 punten

Beveiligingsaspecten algemeen van het Portal

Eis 2.9	U dient een Portal ter beschikking te stellen waarbij de verbinding en 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 2.10	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.
----------	---

Vastleggen van acties / 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 2.11	U dient historische loginformatie ten minste 13 maanden beschikbaar te houden.
Wens 2.7	U biedt een koppeling voor de geautomatiseerde uitwisseling van loggegevens.
Ja/nee	10 punten
Wens 2.8	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.
Meerkeuze	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; - indienen van wijzigingen van instellingen en kenmerken van betaalautomaten, indien deze functionaliteit ondersteund wordt; - 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. 28 punten

Opslaan van informatie

Eis 2.12	Het is de Opdrachtnemer (of elke andere partij die namens hem optreedt) uitdrukkelijk verboden om informatie fysiek in een land buiten de Europese Economische Ruimte op te slaan of in cloudoplossingen waarvan de servers zich in een land buiten de Europese Economische Ruimte bevinden, tenzij (i) de Europese Commissie een besluit heeft genomen betreffende de gepastheid van de bescherming van persoonsgegevens in dat specifieke derde land, (ii) de bevoegde toezichthouder (zoals bedoeld in de Voorschriften voor Gegevensverwerking) uitdrukkelijke goedkeuring heeft gegeven aan de Opdrachtnemer ten aanzien van het gebruik van bindende bedrijfsvoorschriften (binding corporate rules) waaraan alle rechtspersonen, entiteiten en andere onderdelen horende bij de groep van de Opdrachtnemer zijn gebonden of (iii) de Aanbestedende Dienst uitdrukkelijk schriftelijk toestemming heeft gegeven voor de opslag van data in dat derde land. De Opdrachtnemer zal alle redelijke inspanningen ondernemen om deze verplichting af te dwingen bij derden die direct of indirect bij de uitvoering van deze Overeenkomst zijn betrokken.
----------	---

THEMA 3: TECHNISCHE ASPECTEN

Portal

Eis 3.1	U dient te voorzien in een web based Portal die beschikt over gebruiksvriendelijke uitgebreide zoek- en sorteermogelijkheden voor het raadplegen van transacties.
Eis 3.2	U dient het mogelijk te maken dat de Rijksonderdelen een serviceverzoek kunnen indienen voor wijzigingen van de instellingen en kenmerken van de betaalautomaat.
Wens 3.1 Ja/nee	U kunt het mogelijk maken dat de Rijksonderdelen een serviceverzoek in de Portal kunnen indienen voor wijzigingen van de instellingen en kenmerken van de betaalautomaat. 10 punten
Eis 3.3	U dient het mogelijk te maken om data uit de Portal eenvoudig te printen of te exporteren naar gangbare kantoorautomatisering bestandsformaten zoals pdf en csv formaat.
Eis 3.4	U dient het mogelijk te maken dat rapportages per dag, per week en per maand opvraagbaar zijn.
Eis 3.5	Uw Portal ondersteunt de Engelse of de Nederlandse taal.
Wens 3.2 Ja/Nee	Uw Portal ondersteunt de Nederlandse taal. 5 punten
Eis 3.6	De Portal dient per Rijksonderdeel minimaal de volgende raadpleeg functionaliteiten te hebben: - real-time inzicht te geven in de status van de transacties per betaalmethode, waarbij bij niet geslaagde betaaltransacties een verwijzing moet zijn naar de reden waarom de transactie is mislukt; - bedrag; - transactienummer; - transactietype; - Transactiedatum en tijdstip; - Transactiekosten; - betaalautomaat-ID; - beschikbare technische apparaat; - locatie informatie; - bankrekeningnummer waarop gelden worden gestort; - opgegeven reconciliatie referentie betaalautomaat.
Wens 3.3 Ja/nee	U kunt vanuit het Portal een overzicht aanbieden waarop de aantallen transacties per maand per betaalmethode automatisch worden gepresenteerd. 5 punten
Eis 3.7	U dient de informatie in het Portal minimaal 13 maanden beschikbaar te stellen.
Eis 3.8	U dient de Portal zo in te richten dat elke gebruiker alleen toegang heeft tot de specifieke informatie en functionaliteiten van zijn/haar Rijksonderdeel en behorende bij zijn/haar gebruikersprofiel.
Eis 3.9	Het ministerie van Buitenlandse Zaken en Direct betalen maken in de huidige situatie gebruik van PayPlaza om ontvangsten gedaan via POS transacties te verwerken in de interne administraties. U dient de mogelijkheid te bieden om de te leveren diensten aan te sluiten op een bestaande infrastructuur. Zie ook Bijlage H Beschrijving organisaties en impressie betalingsverkeer van het Rijk.
Eis 3.10	U dient als onderdeel van het gebruikersbeheer minimaal de volgende functionaliteiten beschikbaar te stellen: - 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.
Eis 3.11	U dient het voor de administrator mogelijk te maken om het gebruikersbeheer geheel digitaal uit te voeren.
Eis 3.12	U dient alle door de administrator uitgevoerde mutaties door middel van een audittrail in een rapportage digitaal beschikbaar te kunnen stellen.
Eis 3.13	U dient administratoraccounts beschikbaar te stellen waarmee uitsluitend gebruikersbeheer van één Rijksonderdeel kan worden uitgevoerd. <i>Toelichting</i> Een deel van de Rijksonderdelen voert het gebruikersbeheer zelfstandig uit. Het resterende deel van de Rijksonderdelen heeft het gebruikersbeheer uitbesteed aan een ander Rijksonderdeel. Uw oplossing voorziet in beide mogelijkheden.
Eis 3.14	U dient administratoraccounts beschikbaar te stellen waarmee gebruikersbeheer van meer dan één Rijksonderdeel kan worden uitgevoerd. <i>Toelichting</i> Een deel van de Rijksonderdelen voert het gebruikersbeheer zelfstandig uit, het resterende deel van de Rijksonderdelen heeft het gebruikersbeheer uitbesteed aan een ander Rijksonderdeel. Uw oplossing voorziet in beide mogelijkheden.
Eis 3.15	U dient het voor administrators onmogelijk te maken om het eigen account te muteren en/of om mutaties aan het eigen account te autoriseren.
Eis 3.16	U dient minimaal 100 gebruikersaccounts beschikbaar te stellen.
Eis 3.17	U dient minimaal 50 administratoraccounts beschikbaar te stellen.
Wens 3.4 Meerkeuze	U kunt voor Gebruikers tenminste de volgende Functieprofielen beschikbaar stellen en deze naar wens van de afzonderlijke Rijksonderdelen door de Administrator aan de Gebruikers laten toekennen: - indienen van wijzigingen van instellingen en kenmerken van betaalautomaten; - raadplegen van derdenrekeningen (indien in gebruik); - aanmelden en wijzigen van serviceverzoeken; - raadplegen van serviceverzoeken; - raadplegen gegevens zoals verwoord in Eis 3.6 thema 3. Beoordeling - Ieder hierboven genoemd Functieprofiel dat geen andere taken bevat levert drie punten op. - Iedere combinatie van één of meer van deze Functieprofielen levert drie punten op. <i>Toelichting</i> De Rijksonderdelen kennen een grote diversiteit op het gebied van organisatorische inrichting. De Rijksonderdelen hebben als gevolg hiervan ieder afzonderlijke wensen met betrekking tot het inrichten van de accounts voor Gebruikers. Zo zijn bij het ene Rijksonderdeel taken gecombineerd, die bij een ander Rijksonderdeel strikt gescheiden zijn. Door taken in logische Functieprofielen onder te brengen, kunnen de Rijksonderdelen het Gebruikersbeheer flexibel en naar wens inrichten.

	15 punten
Wens 3.5 Meerkeuze	U kunt voor Administrators de volgende Functieprofielen beschikbaar stellen en deze naar wens van de afzonderlijke Rijksonderdelen aan de Administrator toekennen: - mutaties met betrekking tot Gebruikersbeheer invoeren (nieuw, wijzigen, beëindigen); - mutaties met betrekking tot Gebruikersbeheer goedkeuren; - raadpleegfunctionaliteit met betrekking tot het gebruikersbeheer; - exporteren van gebruikers, Rechten en Functieprofielen en audittrails in een gangbaar bestandsformaat waarmee verdere bewerking mogelijk is (bijvoorbeeld XLSX of CSV). Beoordeling - Ieder hierboven genoemd Functieprofiel dat geen andere taken bevat levert vier punten op. - Iedere combinatie van één of meer van deze Functieprofielen levert vier punten op. <i>Toelichting</i> De Rijksonderdelen kennen een grote diversiteit op het gebied van organisatorische inrichting. De Rijksonderdelen hebben als gevolg hiervan ieder afzonderlijke wensen met betrekking tot het inrichten van de accounts voor Administrators. Zo zijn bij het ene Rijksonderdeel taken gecombineerd, die bij een ander Rijksonderdeel strikt gescheiden zijn. Door taken in logische Functieprofielen onder te brengen, kunnen de Rijksonderdelen het Gebruikersbeheer flexibel en naar wens inrichten.
Wens 3.6 Ja/nee	U kunt met uw Portal gebruikers voorzien van afzonderlijke functieprofielen per rekening. <i>Toelichting</i> Gebruikers van de afzonderlijke Rijksonderdelen hebben niet voor alle rekeningen dezelfde bevoegdheden. De Rijksonderdelen willen de rechten van de gebruikers kunnen afstemmen op de bevoegdheden per gebruiker per rekening. 16 punten
Wens 3.7 Ja/nee	U kunt met uw Portal de Functieprofielen voor Gebruikers ook aan de Administrator toekennen. 15 punten
	10 punten

Retourinformatie

Eis 3.18	U dient minimaal de volgende transactie informatie mee te sturen bij het doorboeken naar de derdengeldrekening die daarvoor is aangewezen door het betreffende Rijksonderdeel: - datum transactie; - locatie betaalautomaat ; - reconciliatie referentie: door ons opgegeven specifiek nummer per locatie (bijvoorbeeld kostenplaatsnummer).
Wens 3.8 Ja/nee	U kunt ook de volgende transactie informatie meesturen bij het doorboeken naar de rekening die daarvoor is aangewezen door het betreffende Rijksonderdeel: - CT-nummer 5 punten

Piekbelasting en Beschikbaarheid

Eis 3.19	U dient een normale beschikbaarheid van 99.9%, 24*7 aan te bieden, per maand gemeten (doorlopend) exclusief (gepland periodiek) onderhoud van de dienst. Onderhoud van derde partijen telt mee in de beschikbaarheid van de dienst.
----------	--

Eis 3.20	Het ministerie van Defensie heeft dagelijks (op elke werkdag) een forse piekbelasting tussen 11.00 en 14.00 uur. In deze tijd worden er gemiddeld 10.000 transacties aangeboden op de betaalterminals. U dient deze piekbelasting zonder problemen te kunnen verwerken.
Eis 3.21	U dient regulier onderhoud gerelateerd aan het verlenen van de Diensten te verrichten buiten 07.00 uur - 21.00 uur dan wel ervoor zorg te dragen dat dit onderhoud tijdens deze uren geen invloed heeft op de beschikbaarheid, functionaliteit en beveiliging.
Wens 3.9 Ja/nee	U kunt ervoor zorgen dat bij het ministerie van Defensie tussen 11.00 uur en 14.00 uur geen regulier onderhoud plaats vindt. 10 punten
Wens 3.10 Ja/nee	U kunt voor het ministerie van Buitenlandse Zaken het regulier onderhoud, voor de aangesloten betaalterminals welke buiten Nederland werken, laten plaatsvinden op zaterdag tussen 07.00 uur en 12.00 uur. 10 punten

Capaciteit

Eis 3.22	U dient de aangegeven volumes van het Rijk te kunnen verwerken.
----------	---

Testmogelijkheden

Eis 3.23	U dient te allen tijde medewerking te verlenen aan de door de Rijksonderdelen verzochte pennytest in de productieomgeving. Dit door medewerkers ter beschikking te stellen ter ondersteuning en voor analyse- en rapportagedoeleinden.
----------	--

THEMA 4: SERVICE EN IMPLEMENTATIE

Service

Eis 4.1	U dient servicemanagement te leveren bestaande tenminste uit: - een accountmanager; - een servicedesk (eerstelijns); - een tweedelijns ondersteuning; - een implementatiemanager bij projecten.
Eis 4.2	U dient voor de Rijksonderdelen een centrale <u>Servicedesk</u> ter beschikking te hebben waarbij geldt dat: - binnen de Servicedesk voor storingen, overige meldingen en vragen minimaal een aanspreekpunt bereikbaar is op werkdagen van 07:00 uur tot 18:00 uur. - de Servicedesk telefonisch bereikbaar is tegen maximaal lokaal Nederlands tarief; - de Servicedesk eveneens via email bereikbaar is; - de Servicedesk de gang van zaken binnen de Rijksonderdelen kent; - de Servicedesk de beschreven Dienstverlening in de Overeenkomst kent; en - er gecommuniceerd wordt 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 serviceteam voor het Rijk. U kunt een dedicated serviceteam voor het Rijk beschikbaar stellen. 12 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 calamiteiten 24 uur per dag, 7 dagen in de week (24/7) bereikbaar is; - 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	U kunt het <u>accountmanagement</u> dusdanig inrichten 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 de organisatie van de Inschrijver zelf als binnen het vakgebied in het algemeen; - de accountmanager beschikt over een uitgebreid netwerk van contacten met betrekking tot de PSP werkzaamheden. Beschrijf op welke wijze u het accountmanagement concreet gaat inrichten en aan bovenstaande gaat voldoen. 24 punten
Wens 4.3 Ja/nee	U laat toe om in voorkomende gevallen specialisten van de Rijksonderdelen (bijvoorbeeld op het gebied van automatisering) rechtstreeks met de betreffende specialisten van de Opdrachtnemer te laten communiceren. 36 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 per Rijksonderdeel een klachten- en klanteninformatiesysteem inrichten, waarbij op elk gewenst moment een overzicht van openstaande zaken aan het betreffende Rijksonderdeel verstrekken. Tevens kunt u dit via de Portal aanbieden. 36 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 4.5	U dient akkoord te gaan met het gezamenlijk met de Rijksonderdelen overeenkomen en opstellen van Key Performance Indicators (KPI's) op basis van in dit Beschrijvend document gevraagde Dienstverlening.
Eis 4.6	U dient de KPI's periodiek te rapporteren aan en te bespreken met de betreffende Rijksonderdelen, waarbij het Agentschap een kopie ontvangt.

Doorlooptijd vragen Rijksonderdelen

Eis 4.7	U dient akkoord te gaan met de maximale behandel- c.q. oplostijds per activiteit c.q. verzoektype die de Rijksoverheid hieronder stelt.		
	<table> <tr> <td>Actie</td><td>Afhandeling</td></tr> </table>	Actie	Afhandeling
Actie	Afhandeling		

	In behandeling nemen en vastleggen van vragen van Rijksoverheid	Alle Service verzoeken worden zo mogelijk dezelfde dag in behandeling genomen en er wordt een bericht verstuurd met een serviceverzoek identificatienummer.						
	Kennisgeving in geval van technische of andere ernstige problemen ten aanzien van de systemen.	Direct na constatering melden bij de getroffen Rijksonderdelen.						
	Serviceverzoek (niet limitatief)	Behandeltijd (na versturen van het serviceverzoek)						
	Verstrekken van aanvullende informatie met betrekking tot ontvangsten.	4 werkdagen.						
	Opvoeren nieuwe betaalautomaat.	2 werkdagen na ontvangst van de volledige en juiste aangeleverde informatie.						
	Wijzigingen op reeds bekende betaalautomaten.	2 werkdagen na ontvangst van de volledige en juiste aangeleverde informatie.						
	Incidenten en verstoringen	Reactietijd (na eerste melding/bekend worden met het incident of de verstoring)						
	Geen transactie informatie.	Binnen 24 uren de stand van zaken communiceren met de Rijksonderdelen.						
	Systeemstoringen PSP verbinding.	Binnen 2 uren de stand van zaken communiceren met de Rijksonderdelen.						
Wens 4.5	U Kunt nieuwe betaalautomaten zo snel mogelijk opvoeren.							
Meerkeuze	Beoordeling Hoe sneller, hoe hoger uw score. <table><tr><th>Aantal werkdagen</th><th>Aantal punten</th></tr><tr><td>Tussen 0 - 24 uur</td><td>24</td></tr><tr><td>Tussen 24 – 48 uur</td><td>12</td></tr></table>		Aantal werkdagen	Aantal punten	Tussen 0 - 24 uur	24	Tussen 24 – 48 uur	12
Aantal werkdagen	Aantal punten							
Tussen 0 - 24 uur	24							
Tussen 24 – 48 uur	12							
	24 punten							
Wens 4.6	U Kunt wijzigingen op reeds bekende betaalautomaten zo snel mogelijk opvoeren.							
Meerkeuze	Beoordeling Hoe sneller, hoe hoger uw score. <table><tr><th>Aantal werkdagen</th><th>Aantal punten</th></tr><tr><td>Tussen 0 - 24 uur</td><td>36</td></tr><tr><td>Tussen 24 – 48 uur</td><td>16</td></tr></table>		Aantal werkdagen	Aantal punten	Tussen 0 - 24 uur	36	Tussen 24 – 48 uur	16
Aantal werkdagen	Aantal punten							
Tussen 0 - 24 uur	36							
Tussen 24 – 48 uur	16							
	36 punten							

Storing

Eis 4.8	U dient bij het constateren van een storing direct per e-mail of telefonisch contact op te nemen met de contactperso(o)n(en) van Rijksonderdelen die door deze storing worden geraakt.
---------	--

Eis 4.9	U dient indien er in het geval van storing geen verbinding mogelijk is tussen de pinautomaat en de PSP herstelmaatregelen, waaronder back-up en herstelprocedures geïmplementeerd te hebben.
Eis 4.10	U dient de herstelmaatregelen periodiek te testen.
Eis 4.11	U dient te garanderen dat er geen verlies van betalingen of dataverlies van transactie informatie is bij een calamiteit.

Documentatie

Eis 4.12	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.
Wens 4.7 Ja/nee	De documentatie is voor de Rijksonderdelen terug te vinden op een vaste plaats die voor de Rijksonderdelen op gemakkelijke wijze toegankelijk is. 12 punten
Wens 4.8 Ja/nee	De documentatie is: - in de Nederlandse taal beschikbaar; - te raadplegen via het Portal. 12 punten
Wens 4.9 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 12 punten. U kunt voor uw beantwoording zo maximaal 36 punten krijgen. 36 punten

Contacten met derden

Eis 4.13	U dient communicatie met derden voor deze Overeenkomst zoals banken, Creditcard maatschappijen en eventuele onderaannemers, op verzoek van het Rijksonderdeel te verzorgen.
----------	---

Overlegvormen

Eis 4.14	U dient beschikbaar te zijn voor de volgende overleggen en daarvoor de relevante medewerker(s) ter beschikking te stellen: • één keer per zes maanden operationeel overleg per individueel Rijksonderdeel; • één keer per jaar 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 4.15	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 in welke volgorde de activiteiten plaatsvinden, de doorlooptijd [van de activiteiten] en welke inzet van de betreffende Rijksonderdelen nodig is. De Rijksonderdelen willen met u en een afvaardiging van de Rijksonderdelen een stuurgroep vormen. De Rijksonderdelen zullen voor hun onderdeel elk een eigen implementatiemanager aanwijzen.	
Eis 4.16	U dient een implementatiemanager aan te stellen, die verantwoordelijk is voor de implementatie van nieuwe producten, processen of diensten. De implementatiemanager ondersteunt de betreffende Rijksonderdelen bij het implementeren van de Dienstverlening. Per Rijksonderdeel wijst u maximaal één implementatiemanager aan.
Eis 4.17	U dient een implementatiemanager aan te wijzen die verantwoordelijk is voor het overzicht, bewaking van de algehele voortgang en communicatie met het Agentschap.
Eis 4.18	U dient in een globaal implementatieplan aan te geven hoe de migratie van de huidige PSP naar u gaat plaats vinden. Binnen zes weken na gunning dient u een gedetailleerd implementatieplan op te stellen dat gedegen is en onderbouwd en voor het Agentschap een totaaloverzicht van alle implementatieplannen tezamen.
Wens 4.10	De Rijksonderdelen hebben behoefte aan een implementatieplan waarin is aangegeven hoe de migratie van de huidige PSP naar de Dienstverlening door u gaat plaatsvinden.
Open	Ga in uw 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; - de pennytest; - de benodigde inzet en capaciteit van de Rijksonderdelen; - de ondersteuning; - de nazorg; - waar verwacht u dat er knelpunten zullen optreden en hoe gaat u deze knelpunten oplossen? 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. 36 punten

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.
---------	---

Factuur

Eis 5.2	U dient maandelijks te factureren conform Bijlage G – Handreiking basisfactuur Rijk. Het automatisch incasseren van kosten van de (derden)rekening van het Rijksonderdeel is niet toegestaan.
Eis 5.3	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 5.4	U dient de kosten van de transacties maandelijks per factuur in rekening te brengen bij het betreffende Rijksonderdeel.
Eis 5.5	U dient in het geval van een creditfactuur het factuurnummer van de corresponderende debetfactuur te vermelden.
Eis 5.6	U dient op de maandelijkse factuur de vaste en variabele kosten te specificeren per product en geleverde services.
Eis 5.7	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 5.8	U dient geen kosten voor het aanhouden van een derdengeldrekening in rekening te brengen, waaronder eventuele rente kosten.

THEMA 6: INNOVATIE EN TOEKOMSTBESTENDIGHEID

Algemeen

Eis 6.1	U dient alle Rijksonderdelen afzonderlijk en proactief te betrekken bij de ontwikkelingen in [Point of Sale] betaaldienstverlening.
Wens 6.1 Open	De Rijksonderdelen willen regelmatig op de hoogte worden gehouden van functionele en technische ontwikkelingen van bestaande en nieuwe betaalproducten in de landen waar het betreffende Rijksonderdeel actief is. Per Rijksonderdeel zullen er verschillende behoeftes zijn. Hoe informeert u het betreffende Rijksonderdeel actief. 24 punten
Wens 6.2 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. 12 punten
Wens 6.3 Ja/nee	Als er een nieuwe betaalmethode wordt geïntroduceerd in een land waar op het Rijksonderdeel actief is, bent u dan bereid om deze nieuwe betaalmethode ook aan te bieden indien hiertoe behoefte bestaat van één van de Rijksonderdelen. 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.	
<i>Eis 7.1</i>	U dient de verklaring eerbiediging mensenrechten (Bijlage 7) te ondertekenen.
<i>Wens 7.1</i> <i>Open</i>	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
<i>Wens 7.1a</i> <i>Open</i>	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.	
<i>Eis 7.2</i>	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 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?

Open

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 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.

Open

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 Beschrijf op welke wijze u zich inzet voor diversiteit en inclusiviteit.

Open

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