Samenvatting Marktconsultatie Creditcards Rijksoverheid

Inleiding

In het kader van de voorbereiding op de nieuwe aanbesteding voor zakelijke creditcards ten behoeve van de Rijksoverheid is een brede marktconsultatie uitgevoerd. Het doel van deze consultatie is om actueel inzicht te verkrijgen in de marktstandaarden, technische mogelijkheden, beveiligingskaders, integratie-opties en innovaties op het gebied van corporate betaalkaarten en virtuele betaaloplossingen.

Onderstaande tabel bevat een geanonimiseerde synthese van de reacties van de deelnemende marktpartijen op de gestelde vragen binnen de thema's 1 tot en met 9 (vragen 1a t/m 9f). Alle herleidbare partijnamen, specifieke handelsmerken en merknamen zijn geanonimiseerd om een objectief en overzichtelijk beeld te geven van de marktcapaciteit en -bereidheid.

Overzicht Beantwoording Marktconsultatie (Vragen 1a t/m 9f)

Vraag	Samenvatting
Thema 1: Online portaal en functionaliteiten	
1a. Online omgeving voor kaarthouders en beheerders	De marktpartijen bieden een beveiligd online beheerportaal en mobiele apps (iOS/Android) voor zowel individuele kaarthouders als (programma)beheerders. Kaarthouders hebben direct inzicht in actuele transacties, bestedingsruimte, pincodes en rekeningoverzichten. Beheerders hebben overkoepelend inzicht, kunnen programma's en gebruikers beheren, limieten direct operationeel wijzigen en managementrapportages genereren.
1b. Inlogmethoden en internationale bereikbaarheid	Toegang wordt beveiligd via sterke meervoudige authenticatie (MFA/2FA) met e-mail, PIN, biometrie en eenmalige verificatiecodes (SMS-OTP). Voor gebruikers in het buitenland bij wie SMS-aflevering hapert, voorzien aanbieders in alternatieven zoals pushnotificaties via de eigen app, telefonische spraakoproepen, eID-oplossingen of 24/7 ondersteuning via de servicedesk.
1c. Autorisatieniveaus binnen het portaal	Binnen de beheeromgevingen zijn gedifferentieerde autorisatieniveaus beschikbaar. Er wordt strikt onderscheid gemaakt tussen kaarthouders (alleen inzage in eigen data), programmabeheerders (volledige operationele en administratieve beheerrechten) en raadplegers/auditoren (uitsluitend lees- en rapportagerechten zonder wijzigingsbevoegdheid).
1d. Periodieke digitale totaaloverzichten	Beheerders kunnen periodiek en ad-hoc overkoepelende uitgavenoverzichten genereren en downloaden, uitgesplitst per kaart, afdeling of entiteit. Deze overzichten bevatten gedetailleerde transactiedata (datum, omschrijving, valuta, bedrag) en kunnen worden geëxporteerd naar Excel (xlsx), CSV en PDF, of via geautomatiseerde datafeeds worden aangeleverd.
1e. Logging- en auditmogelijkheden	De platformen beschikken over uitgebreide audit- en logging functionaliteiten ter ondersteuning van interne en externe controles. Mutaties, roltoewijzingen, autorisaties en transactiestromen worden traceerbaar vastgelegd (inclusief gebruikers-ID's en tijdstempels) en kunnen via specifieke auditrapporten worden geëxporteerd.

Vraag	Samenvatting
1f. Koppelingen met ERP- en boekhoudsystemen	Aanbieders ondersteunen geautomatiseerde bestands- en systeemkoppelingen met alle gangbare ERP-, boekhoud- en onkostenbeheersystemen (waaronder SAP, Oracle, Exact en meer dan 60–75 andere platforms). Gegevensoverdracht vindt plaats via beveiligde datafeeds en protocollen zoals SFTP, EBICS en standaard exportformaten (zoals CDF3, VCF4, CSV en TXT).
Thema 2: Declaratieproces en reconciliatie	
2a. Digitalisering van het declaratieproces	De marktpartijen ondersteunen een volledig digitaal proces door transactiedata geautomatiseerd aan te leveren aan externe declaratiesystemen (Expense Management Systems), of bieden optioneel een eigen geïntegreerde onkostentool aan. Kaarthouders kunnen bonnen en facturen fotograferen via de mobiele app (met OCR-herkenning), waarna fiattering en goedkeuring binnen de gekoppelde workflowsoftware plaatsvinden.
2b. Automatische reconciliatie met bonnetjes en grootboek	Transactiedata wordt verrijkt met bonnetjes en facturen aangeleverd als dagelijkse niet-gefactureerde datastroom aan het declaratie- of ERP-systeem van de opdrachtgever. De daadwerkelijke matching met grootboekrekeningen en journaalpostvorming vindt plaats binnen de financiële systemen van de Rijksoverheid.
2c. Real-time inlezen en matchen van transacties	Transacties en autorisaties zijn real-time inzichtelijk binnen de mobiele app en het beheerportaal. De formele doorlevering van verwerkte en goedgekeurde transactiedata naar externe ERP- en declaratiesystemen geschiedt standaard via dagelijkse geautomatiseerde batchfeeds conform de afwikkelingsketen van de kaartnetwerken.
2d. Dynamic FX conversion en uitsplitsing zakelijk/privé	Dynamic Currency Conversion (DCC) wordt afgeraden of niet aangeboden, omdat afrekening in lokale valuta via het reguliere netwerk aanzienlijk lagere wisselkoerskosten oplevert. Zakelijke creditcards zijn conform Europese bancaire kaders uitsluitend bestemd voor beroepsmatige uitgaven; privé-uitgaven worden contractueel en beleidsmatig uitgesloten, al kan binnen bepaalde apps optioneel een annotatie worden toegevoegd.
Thema 3: Facturatie	
3a. Factureringsmogelijkheden	Aanbieders ondersteunen zowel centrale facturatie (één verzamelfactuur per ministerie/programma) als individuele facturatie (per creditcard). Betaling kan plaatsvinden via automatische incasso of handmatige overboeking. Er zijn flexibele maandelijkse facturatiecycli instelbaar (zoals de 2e, 9e, 17e of 26e dag van de maand).
3b. Betalingsvoorwaarden	Betalingscondities kunnen flexibel op maat worden overeengekomen. Standaard zakelijke kaders hanteren betaaltermijnen van 21 kalenderdagen na factuurdatum. Bij maatwerkafspraken zijn termijnen mogelijk van 10 tot 28 dagen via automatische incasso, of tot 30 dagen bij handmatige bankoverboeking.
3c. Terugbetalingen en creditsaldi (ook bij opgeheven kaarten)	Terugbetalingen worden rechtstreeks teruggestort op de oorspronkelijke kaart. Indien de kaart inmiddels is opgeheven, wordt het bedrag automatisch overgeboekt naar het centrale account van het programma, verrekend met de eerstvolgende verzamelfactuur, of via de servicedesk teruggestort op de bankrekening van de betreffende entiteit.

Vraag	Samenvatting
3d. Gevolgen van betalingsachterstand	Bij overschrijding van de betalingstermijn wordt de organisatie in gebreke gesteld en kunnen vertragingskosten in rekening worden gebracht. Achterstanden worden gerapporteerd in de portal en proactief opgevolgd door accountmanagement. Bij aanhoudende achterstand (tot circa 3 maanden) volgt tijdelijke opschorting of blokkade van de kaarten binnen het programma.
Thema 4: Bestedingslimiet	
4a. Maximale bestedingslimiet per creditcard	Aanbieders hanteren in principe geen vastgesteld plafond per kaart; de opdrachtgever bepaalt de individuele limieten zelf. Op organisatieniveau wordt een totale kredietlimiet (Group Exposure Limit) vastgesteld op basis van het verwachte uitgavenvolume. Binnen dit kader kunnen maandlimieten (bijv. standaard € 20.000 of incidenteel tot € 1 miljoen+), daglimieten en transactielimieten flexibel worden ingesteld.
4b. Instellen van limieten per kaart of bedrijfsonderdeel	Bestedingslimieten kunnen modulair worden geconfigureerd per ministerie, dienstonderdeel, gebruikersgroep of individuele kaart. Beheerders voeren deze instellingen zelfstandig en digitaal door via het online portaal of de beheer-app.
4c. Tijdelijke en permanente limietaanpassingen	Geautoriseerde beheerders kunnen bestedingslimieten 24/7 via het portaal aanpassen. Zowel tijdelijke als permanente wijzigingen worden real-time verwerkt en zijn per direct operationeel, zolang deze binnen de totale overeengekomen bedrijfskredietruimte vallen.
4d. Bevoegdheid tot wijzigen van de bestedingslimiet	Het wijzigen van limieten is strikt voorbehouden aan geautoriseerde programmabeheerders of officiële tekenbevoegden via het portaal. Individuele kaarthouders hebben geen bevoegdheid om hun eigen bestedingslimiet aan te passen (tenzij de organisatie expliciet en optioneel kiest voor ingekaderde selfservice).
Thema 5: Beveiliging	
5a. Naleving van PCI DSS v4.0.1 Level 1	De marktpartijen borgen dat de verwerking, overdracht en opslag van kaartdata voldoen aan de strikte vereisten van PCI DSS Level 1 en PSD2. Maatregelen omvatten Chip & PIN, Strong Customer Authentication (SCA), 3D Secure, data-encryptie en ISO 27001-gecertificeerde Information Security Management Systemen (ISMS) met dataopslag binnen de EU.
5b. Aansluiting bij BIO2 v1.3	Aanbieders geven aan dat hun beveiligingsmaatregelen, risicomanagement en governancestructuur nauw aansluiten bij de Baseline Informatiebeveiliging Overheid 2 (BIO2 v1.3), aangezien hun systemen zijn gebaseerd op ISO/IEC 27001/27002, strikte AVG/GDPR-naleving en wetgeving zoals DORA en NIS2. Zij hebben ruime ervaring met overheden en defensie-instanties.
5c. Detectie en preventie van fraude	Fraude wordt 24/7/365 bewaakt via een gelaagd stelsel: real-time transactiescoring, AI/rule-based monitoringsystemen, EMV-chiptechnologie, 3DS-authenticatie, directe kaartblokkades en gespecialiseerde antifraudeteams die bij verdachte transacties direct contact opnemen.
5d. Scheiding van post- en correspondentieadressen	Alle marktpartijen bevestigen dat het postadres voor fysieke kaartlevering aan de individuele kaarthouder structureel kan worden gescheiden van het correspondentie- of facturatieadres van de programmabeheerder en het ministerie.

Vraag	Samenvatting
Thema 6: Dekking	
6a. Beschikbare kaartmerken en wereldwijde inzetbaarheid	Aanbieders leveren zakelijke creditcards via de twee wereldwijd leidende netwerken (Mastercard en/of Visa). Sommige partijen bieden beide merken aan, terwijl andere zich vanuit efficiency en schaalgrootte richten op één van beide platforms met wereldwijde dekking bij meer dan 150 tot 200 miljoen acceptatiepunten.
6b. Regionale acceptatiebeperkingen	Hoewel de netwerken wereldwijd opereren, kan 100% acceptatie niet universeel worden gegarandeerd. Beperkingen gelden primair in landen onder internationale sancties en embargo's. Daarnaast kunnen lokale merchantvoorkeuren of infrastructurele beperkingen optreden in specifieke regio's in Zuidoost-Azië, Afrika en Zuid-Amerika; wereldwijde toegang tot geldautomaten biedt hierbij een contant alternatief.
6c. Landspecifieke diensten en lokale kaartuitgifte	Internationale creditcards functioneren overal waar het netwerk wordt ondersteund. Bij lokale gesloten betaalsystemen (zoals specifieke laadpalen of lokale betaallinks zonder internationaal kaartlogo) kunnen beperkingen optreden. Aanbieders opereren onder Europese banklicenties en geven geen separate lokale buitenlandse creditcards uit; voor specifieke regio's kunnen eventueel lokale partnerbanken worden geraadpleegd.
Thema 7: Levering	
7a. Aanvraag- en beëindigingsproces van creditcards	Aanvragen verlopen volledig digitaal via bulk-upload (Excel), individuele invoer door de beheerder of online selfservice door medewerkers via intranet met beheerder-goedkeuring. Beëindiging en blokkering kunnen door beheerders 24/7 direct of op een toekomstige datum worden ingepland via het portaal, of via de 24/7 servicedesk.
7b. Leveringstermijnen (standaard, spoed en vervanging)	• **Standaard:** Fysieke levering binnen 2 tot 5 werkdagen (48–120 uur) na KYC-validatie; digitale kaarten zijn per direct (0 uur) beschikbaar in de app. • **Spoed:** Binnen 48 uur geleverd (mogelijk met additionele koerierskosten). • **Vervanging (diefstal/verlies):** Direct digitaal beschikbaar en fysieke verzending binnen 24–120 uur. Vervanging is kosteloos of tegen een vaste administratieve vergoeding (€ 7,50 – € 9,00).
Thema 8: Gebruiksmogelijkheden	
8a. Gehanteerde bestedingscategorieën	Bestedingen worden geclassificeerd op basis van internationale Merchant Category Codes (MCC) en transactiecategorieën (zoals reizen, verblijf, restaurants, retail, tanken en contante opnames), ondersteund door geautomatiseerde spend-analyse in het portaal.
8b. Blokkeren van specifieke categorieën	Het is technisch mogelijk om specifieke MCC-categorieën en branches (zoals gokken, juweliers, warenhuizen of volwassenenentertainment) structureel uit te sluiten of te blokkeren op programma-, account- of individueel kaartniveau.
8c. Inrichting per kaarthouder (contant geld en contactloos)	Functionaliteiten kunnen per kaarthouder op maat worden geconfigureerd. Contant geld opnemen bij geldautomaten kan per individuele kaart of afdeling eenvoudig worden in- of uitgeschakeld. Contactloos betalen is standaard actief en kan

Vraag	Samenvatting
	bij sommige aanbieders via een technisch script op verzoek worden gedeactiveerd.
8d. Meerdere transacties per dag	Creditcards mogen onbeperkt meerdere keren per dag worden gebruikt, zolang de ingestelde bestedingslimieten, daglimieten en fraudepreventieparameters niet worden overschreden. Het maximum aantal dagelijkse transacties kan per kaart flexibel worden geconfigureerd.
Thema 9: Product en innovaties	
9a. Verwachte productontwikkelingen en innovaties	De markt richt zich op verregaande digitalisering, geautomatiseerde API-integraties met ERP/Inkoopsystemen (zoals Coupa, SAP, Oracle), uitbreiding van virtuele creditcards met voorafgaande goedkeuringsworkflows, spend controls, tokenization en Virtual Card to Wallet-technologie voor fysiek mobiel betalen.
9b. Virtuele creditcards en digitale wallets	Aanbieders ondersteunen virtuele creditcards voor online inkopen en leveranciersbetalingen (B2B), instelbaar met strikte voorwaarden vooraf (bedrag, geldigheid, MCC). Er wordt actief gewerkt aan of reeds ondersteuning geboden voor tokenization naar wallets zoals Apple Pay en Google Pay via beveiligde protocollen.
9c. Prepaid creditcards	Aanbieders leveren geen prepaid creditcards. Zij adviseren virtuele creditcards met voorafgaande fiattering (pre-approval) en dynamische bestedingslimieten als superieur alternatief, waarmee maximale grip wordt geboden zonder de administratieve last en liquiditeitsbeslag van pre-funding.
9d. Prepaid debitcards	Prepaid debitcards worden momenteel niet aangeboden en zijn niet voorzien op de korte termijn. Voor gecontroleerde uitgaven wordt verwezen naar virtuele kaarten met koppelingen naar declaratie- en ERP-systemen.
9e. Niet-persoonsgebonden en anonieme creditcards	Volledig anonieme kaarten zijn wettelijk niet toegestaan onder de Europese anti-witwaswetgeving (Wwft/AMLD). Reguliere kaarten zijn persoonsgebonden (na identificatie). Wel kunnen virtuele creditcards en centrale betaalaccounts functioneel worden ingezet op afdelings- of leveranciersniveau zonder koppeling aan een fysieke individuele kaarthouder.
9f. Serviceorganisatie en 24/7 ondersteuning	Alle marktpartijen beschikken over een meertalige, professionele helpdesk en customer support die 24 uur per dag, 7 dagen per week bereikbaar is voor kaarthouders en programmabeheerders voor acute assistentie, PIN-vragen, transactieonderzoek en directe kaartblokkades bij calamiteiten.

Conclusie en Kernbevindingen

Uit de marktconsultatie blijkt dat de markt voor zakelijke creditcards volwassen, technologisch geavanceerd en compliant is met de strenge Europese wet- en regelgeving:

1. **Beheer en Integratie:** Alle aanbieders bieden krachtige online portalen, mobiele apps en flexibele datafeeds naar gangbare ERP- en declaratiesystemen.
2. **Beveiliging en Autorisatie:** Er wordt voldaan aan hoge beveiligingsstandaarden (PCI DSS Level 1, ISO 27001, PSD2 SCA en BIO2-aansluiting), met strikte scheiding van autorisaties tussen beheerders en kaarthouders.

3. **Innovatie:** Virtuele kaarten met voorafgaande fiattering, tokenization naar mobiele wallets en verfijnde limiet- en categorierestricties (MCC) vormen de standaard voor gecontroleerde overheidsuitgaven.