

Deze bijzondere voorwaarden zijn een aanvulling op de algemene voorwaarden voor acceptatie van de American Express Kaart (hierna: **Algemene Voorwaarden**) bij aanvaarding van de Kaart voor online Transacties met SafeKey. Zij maken desgevallend deel uit van de overeenkomst tussen de Merchant en Alpha Card Merchant Services (hierin ook aangeduid als **ACMS**).

SafeKey wordt enkel aangeboden aan de Merchant onder voorwaarde van acceptatie van deze SafeKey bijzondere voorwaarden voor de Merchant.

Door SafeKey aan te vragen, te implementeren respectievelijk te (blijven) gebruiken, aanvaardt de Merchant deze SafeKey bijzondere voorwaarden voor de Merchant.

Deze SafeKey bijzondere voorwaarden voor de Merchant en eventuele wijzigingen worden gepubliceerd op www.americanexpress.be (hierna: de **Website**).

1. SAFEKEY

American Express SafeKey® (hierna: **SafeKey**) is een authenticatiemethode ontwikkeld door het American Express betaalschema gebaseerd op het 3D Secure protocol. Wanneer SafeKey wordt toegepast, verhoogt dat de beveiliging van online Transacties.

SafeKey wordt desgevallend toegepast naast en samen met andere risicobeheersings-, beveiligings-, authenticatie- en autorisatiemethoden. Wanneer een transactie niet doorgaat dan kan dit het gevolg zijn van een of meerdere van deze methoden.

ACMS biedt SafeKey, zoals aangeboden door American Express, aan voor alle Merchants die in aanmerking komen.

2. TOEPASSINGSGBIED

SafeKey wordt gebruikt bij online Transacties.

SafeKey is in principe van toepassing op alle American Express Kaarten. Evenwel zijn kaarten waar de Kaarhouder of de gebruiker van de Kaart anoniem is uitgesloten van het SafeKey proces (hierna **Uitgesloten Kaarten**). Het gaat daarbij bijvoorbeeld om prepaid kaarten, Business Travel Accounts en Travel Agency Accounts. Welke kaarten al dan niet uitgesloten zijn, wordt uitiem bepaald door American Express (zie o.a. SafeKey Implementation Guide).

Aan de kant van de Handelaar vereist SafeKey dat deze bepaalde software – de zogenaamde Merchant Plug-In – implementeert. SafeKey wordt toegepast bij Handelaars die die implementatie hebben gedaan (hierna **Participerende Merchant**).

3. AANVRAAG

Een Merchant kan deelname aan SafeKey aanvragen via het formulier dat beschikbaar is gesteld via de website <http://www.americanexpress.be/beperkfraude>.

Daarbij dient een Merchant de SafeKey voorwaarden van American Express en de privacy verklaring te aanvaarden. De aanvraag omvat m.a.w. de aanvaarding van de inhoud van deze documenten.

De Merchant dient "Alpha Card Merchant Services" (mogelijk afgekort als "Alpha Card") aan te duiden als "acquiring bank". Daarmee wordt de contractuele relatie met ACMS bevestigd. ACMS wordt verwittigd van de aanvraag van de Merchant.

De keuze van de "Merchant Plug-In Service Provider" houdt minstens in dat die partij daarvan wordt verwittigd. Mogelijk houdt dat een aanvraag in tot contact of zelfs opdracht tot het implementeren van de Merchant Plug-In. De Merchant wordt aangeraden om vooraf contact op te nemen met de Merchant Plug-In Service Provider die hij wenst te kiezen om de gevolgen van de aanduiding te kennen en desgevallend een offerte te vragen dan wel een contract aan te gaan.

Elk (persoons)gegeven dat wordt ingegeven in het formulier wordt in eerste instantie doorgegeven aan en verwerkt door American Express, desgevallend in het buitenland. Dat betekent onder meer dat de gegevens soms worden doorgegeven naar landen waar de juridische bescherming van de persoonsgegevens niet equivalent is aan deze in de Europese Unie. Voor het overige wordt verwezen naar de privacyverklaring.

4. PARTICIPATIEVOORWAARDEN

Om deel te nemen aan SafeKey moet de Merchant (cumulatief):

- gebruik maken van een Merchant Plug-In die via de door de Merchant gekozen Service Provider ter beschikking wordt gesteld en door American Express werd gecertificeerd of bij implementatie van een eigen Merchant Plug-In, de SafeKey Implementation Guide naleven, die beschikbaar kan worden gemaakt voorafgaand aan de technische certificering
- de vereiste SafeKey technische certificering verkrijgen
- de certificering hebben verkregen voor alle middelen voor fraudepreventie die beschikbaar zijn in de markt van de Merchant, zoals beschreven in de Algemene Voorwaarden of andere onderdelen van de overeenkomst tussen de Merchant en ACMS
- de SafeKey vereisten en instructies inzake het gebruik van de American Express merken en logo's naleven (zie "kenbaar maken")
- een fraude-tot-verkoopratio van minder dan 1% (in principe over 6 opeenvolgende maanden) aanhouden met betrekking tot Transacties die SafeKey gegevens bevatten;
- een fraude-ratio aanhouden van minder dan drie (3) unieke Kaartrekeningen betrokken in frauduleuze Transacties die SafeKey gegevens bevatten (in principe over 6 opeenvolgende maanden);
- een goede relatie met American Express en ACMS te onderhouden, wat op redelijke wijze door ACMS bepaald wordt,
- elke andere vereiste naleven die American Express of ACMS redelijkerwijs van tijd tot tijd introduceren of wijzigen, na daarvan in kennis te zijn gesteld.

Deze voorwaarden worden de **Participatievoorwaarden** genoemd.

5. KENBAAR MAKEN

De Participerende Merchant dient in zijn aankoopproces (onder meer in zijn "aankoopmandje") het logo voorgeschreven door American Express bij gebruik van SafeKey (hierin: **SafeKey Logo**) volgens de instructies van American Express (hierin: de **Logo**

Guidelines) duidelijk kenbaar te maken zodat de Kaarthouders weten dat SafeKey toegepast wordt. De Logo Guidelines zijn beschikbaar via de website van American Express www.amexsafekey.com.

Een Participerende Merchant kan het SafeKey Logo en de bijhorende instructies van American Express opvragen via de website van American Express http://network.americanexpress.com/be/en/safekey/merchants_and_acquirers.aspx. Daarbij dient de Merchant de gebruiksvoorwaarden van American Express voor het Logo te aanvaarden. De aanvraag en het gebruik van het Logo omvat m.a.w. de aanvaarding van die voorwaarden.

6. MERCHANT PLUG-IN

De **Merchant Plug-In** is de software(aanpassing) die nodig is om aan de kant van de Merchant SafeKey in diens online aankoopproces te integreren.

American Express heeft enkele geselecteerde partners (**Merchant Plug-In Service Providers**) die de toelating hebben gekregen om de Merchant Plug-In te installeren. Een Merchant die SafeKey wenst toe te passen dient in principe een Merchant Plug-In Service Provider aan te stellen. De installatie van de Merchant Plug-In is een zaak waar ACMS niet in tussenkomt en die geregeld moet worden tussen de Merchant en de Merchant Plug-In Service Provider.

7. VERWERKING VAN TRANSACTIES

Bij de verwerking van SafeKey Transacties moet de Merchant:

- een enkel authenticatieverzoek per Transactie doorsturen
- zich onthouden van het hergebruik van authenticatie data buiten de betrokken SafeKey Transactie.

8. SAFEKEY CHARGE BACK VRIJSTELLING

ACMS zal haar Chargeback rechten niet uitoefenen ten aanzien van Transacties die voldoen aan de Transactiecriteria indien (cumulatief)

- de Merchant voldoet aan de Participatievoorwaarden
- de Transactie voldoet aan de Transactiecriteria
- de Transactie enkel wordt betwist op basis van fraude of onrechtmatig gebruik van de Kaart en niet voor een andere reden

De criteria waaraan een Transactie moet voldoen om in aanmerking tot komen (hier: **Transactiecriteria**) zijn (cumulatief):

- de Transactie valt onder de overeenkomst tussen de Participerende Merchant en ACMS
- de Transactie is een Transactie waarbij voor de betaling van goederen of diensten betalingsgegevens van de Kaart worden ontvangen via een internetpagina voor betalingen, het internet, intranet, extranet of een ander digitaal betaalnetaalnetwerk voor goederen of diensten
- de Transactie wordt verricht met een daarvoor in aanmerking komende Kaart (zie "toepassingsgebied")
- de Transactie wordt verricht bij afwezigheid van de kaart
- de Transactie geeft weer dat deze volledig SafeKey geauthentiseerd was of dat een SafeKey authenticatie is geprobeerd te verkrijgen

- de toepasselijke SafeKey authenticatie gegevens zijn verschaft in het verzoek tot Autorisatie alsmede bij het aanbieden van de Transactie
- de Kaarthouder betwist de Transactie als frauduleus of onrechtmatig

9. INFORMEREN VAN MISBRUIK

De Participerende Merchant die merkt of vermoedt dat SafeKey onrechtmatig of frauduleus wordt gebruikt, dient ACMS onmiddellijk te verwittigen.

10. BLOKKERING

Een Transactie kan door SafeKey worden gestopt en een kaarthouder kan door SafeKey worden geblokkeerd bij mogelijke problemen met de beveiliging of autorisatie van Transacties. ACMS is ook niet gehouden tot dergelijke blokkering.

De Merchant kan ACMS niet aanspreken op basis van zo'n blokkering (bijv. omwille van een gemiste verkoopmogelijkheid) noch op basis van het gebrek aan blokkering.

11. VERANTWOORDELIJKHEID

Met uitzondering van expliciete afwijking in deze bijzondere voorwaarden, wijzigt het gebruik van SafeKey niets aan de regeling van verantwoordelijkheden in de Algemene Voorwaarden.

Hoewel SafeKey de veiligheid van online betaling verhoogt, garandeert Alpha Card niet dat online aankopen – zelfs niet met SafeKey – volledig zonder risico zijn. Daarvoor zijn er te veel factoren die buiten elke redelijke controle liggen.

Dat een Merchant SafeKey gebruikt, houdt geen aanbeveling van of voorkeur voor de betrokken Merchant in. De Merchant mag dat ook zo niet presenteren aan Kaarthouders.

De Merchant aanvaardt dat bepaalde (online) Transacties omwille van SafeKey niet of niet meteen zullen kunnen doorgaan. De Merchant kan geen enkele vordering inroepen gebaseerd op het niet (tijdig) doorgaan van de Transactie.

De Merchant draagt het risico voor zaken die buiten de controle van Alpha Card zijn, zoals:

- het naleven van deze SafeKey bijzondere voorwaarden voor de Merchant
- de relatie met de Merchant Plug-In Service Provider, inclusief de eventueel daaraan verbonden voorwaarden en kosten
- de implementatie van de Merchant Plug-In
- de beveiliging (incl. infectie door virussen en andere malware) van
 - de toestellen waarop de Merchant Plug-In is geïmplementeerd
 - het toestel, de platformen en de toepassingen waarmee de Merchant toegang neemt tot SafeKey of berichten ontvangt met betrekking tot SafeKey
- kosten die eventueel door derden (bijv. telecomoperatoren) worden aangerekend voor de implementatie en het onderhoud van SafeKey
- de gevolgen van een blokkering van SafeKey

12. WIJZIGINGEN

ACMS kan de SafeKey bijzondere voorwaarden voor de Merchant te allen tijde en – tenzij dwingende wetgeving anders voorschrijft - met onmiddellijke ingang wijzigen, in het bijzonder in geval van wijzigingen die doorgevoerd worden door American Express als aanbieder van SafeKey. Wijzigingen zullen worden meegedeeld door vervanging van de gepubliceerde

versie op de Website. Wijzigingen met een belangrijke impact zullen de Participerende Merchant ter kennis worden gebracht, bijvoorbeeld via email (op het email-adres doorgegeven voor SafeKey of een andere email adres gekend in de systemen).

American Express en ACMS kunnen SafeKey (als proces) te allen tijde en – tenzij dwingende wetgeving anders voorschrijft - met onmiddellijke ingang wijzigen, zonder dat daarvoor kennisgeving aan de Participerende Merchant vereist is.

ACMS is niet aansprakelijk en heeft geen verplichtingen jegens de Merchant indien ACMS SafeKey of de SafeKey bijzondere voorwaarden voor de Merchant aanpast.

Als de Participerende Merchant na de wijziging aan de SafeKey bijzondere voorwaarden voor de Merchant verder gebruik maakt van SafeKey dan wordt hij geacht de gewijzigde SafeKey bijzondere voorwaarden voor de Merchant te aanvaarden.

13. NIET LANGER VOLDOEN AAN VEREISTEN

Indien de Merchant op enig moment niet voldoet aan de vereiste Participatievoorwaarden of indien ACMS een onevenredige hoeveelheid Betwiste Transacties of een groot aantal fraudegevallen ontvangt dan geldt dat

- ACMS naar eigen goeddunken de deelname van de Participerende Merchant aan SafeKey kan wijzigen of beëindigen en
- de Participerende Merchant verplicht is om met ACMS mee te werken om de hoeveelheid Betwiste Transacties bij de Participerende Merchant te verminderen.

14. BEËINDIGING

ACMS kan te allen tijde SafeKey schorsen of stopzetten. Dit is zeker het geval als American Express SafeKey schorst of stopzet.

Een Participerende Merchant kan te allen tijde SafeKey stoppen. De Participerende Merchant moet daarvan ACMS en de Merchant Plug-In Service Provider schriftelijk in kennis stellen.

In geval SafeKey (bij een Participerend Merchant) wordt beëindigd, dient de (voormalig) Participerende Merchant

- de SafeKey certificatie status in te leveren en
- alle vertrouwelijke informatie met betrekking tot SafeKey die aan de Participerende Merchant ter beschikking is gesteld, terug te geven aan ACMS of te vernietigen en dit schriftelijk te bevestigen ten aanzien van ACMS

15. VERPLICHTING

ACMS kan de implementatie van SafeKey verplicht maken voor de Merchant. Het niet implementeren of stopzetten van SafeKey kan dan aanleiding geven tot een beëindiging met onmiddellijk effect van de overeenkomst tussen ACMS en de Merchant.