INTRODUZIONE

Questo documento contiene le istruzioni, le regole e le specifiche tecniche del servizio 3D Secure, il sistema di sicurezza per l'e-commerce progettato dai circuiti internazionali Visa e MasterCard.
Il prossimo paragrafo spiega il funzionamento di 3D Secure; quelli successivi, di carattere più tecnico, contengono le regole, le istruzioni e le specifiche tecniche per l'attivazione del servizio.

FUNZIONAMENTO DEL SERVIZIO 3D SECURE

Il servizio 3D Secure prende il nome di Verified by Visa (VbV) per il circuito Visa e di MasterCard SecureCode (MSC) per il circuito MasterCard.
3D Secure assicura una maggiore tutela sugli acquisti in internet poiché richiede l'autenticazione del pagamento da parte del titolare della carta di credito, che deve inserire una password personale.
La password personale viene richiesta durante ogni acquisto effettuato presso un esercente che aderisce al servizio.
L'esercente che aderisce a 3D Secure viene esonerato da qualsiasi responsabilità sulla base delle regole stabilite dai circuiti internazionali: infatti, nel caso in cui il titolare della carta di credito dovesse disconoscere una spesa, la responsabilità della transazione passa alla società che ha emesso la carta di pagamento: un processo denominato liability shift.

LIABILITY SHIFT

La liability shift è il passaggio della responsabilità della transazione dall'acquirer alla società che ha emesso la carta di pagamento.
L'applicazione di tali regole è subordinata al rispetto delle regole del protocollo 3D Secure da parte dell'esercente/gestore terminali per la tratta di sua competenza. In conformità con le regole applicative della liability shift dei circuiti Visa e Mastercard, T.P@Y esonera l'esercente da qualsiasi responsabilità in caso di disconoscimento della transazione da parte dei titolari quando i circuiti garantiscono la liability shift.
Di seguito sono riassunte le regole dei circuiti internazionali Visa (Verified by Visa) e MasterCard (SecureCode MasterCard) per l'applicazione della liability shift in funzione della gestione del servizio 3D Secure.

Per Visa la liability shift viene applicata nei seguenti due casi:
1) l'esercente, la società che ha emesso la carta, il titolare della carta di credito, aderiscono tutti a 3D Secure (VbV); l'autenticazione del titolare tramite l'inserimento della password personale è avvenuta correttamente; durante la fase di autorizzazione l'esercente ha inoltrato correttamente il Cavv all'acquirer;
2) l'esercente aderisce a VbV, ma la società che ha emesso la carta o il titolare non aderiscono a VbV.
Per il secondo caso esistono alcune eccezioni per le quali la liability shift non viene applicata. Queste eccezioni si verificano quando l'ACS non è in grado di gestire alcune autenticazioni. Questo può succedere per a) i pagamenti effettuati su nuovi canali (es. mobile); b) le carte aziendali extraeuropee in caso di transazioni internazionali; c) le carte prepagate anonime.

Per Mastercard la liability shift viene applicata nei seguenti due casi:
1) l'esercente, la società che ha emesso la carta, il titolare della carta di credito, aderiscono tutti a 3D Secure (MSC); l'autenticazione del titolare è avvenuta correttamente tramite l'inserimento della password personale; l'esercente ha inoltrato correttamente il Cavv4 all'acquirer durante la fase di autorizzazione;
2) l'esercente aderisce a MSC, ma la società che ha emesso la carta o il titolare non aderiscono a MSC.
Per il secondo caso esiste una sola eccezione per la quale la liability shift non viene applicata: le transazioni extra europee effettuate da carte aziendali.

Sia per le carte Visa, sia per le carte MasterCard, una volta completata la fase d'autenticazione tramite password, la transazione prosegue nel normale iter autorizzativo.
T.P@Y si riserva la facoltà di modificare tali informazioni in base alle variazioni segnalate di volta in volta dai circuiti internazionali Visa e MasterCard.

GLOSSARIO

Directory Server	Componente del protocollo 3D Secure gestita da Visa e MasterCard che determina se l'issuer e la carta partecipano al servizio e in caso positivo restituisce al merchant l'URL dell'ACS da contattare per effettuare la fase d'autenticazione
AAV Accountholder Authentication Value	Identificativo univoco generato dall'Issuer per dimostrare che per una determinata carta MasterCard ha avuto luogo l'autenticazione
ACS Access Control Server	Componente del protocollo 3D Secure gestita dall'Issuer che verifica se una carta aderisce al protocollo e ne effettua l'autenticazione
Acquirer	Società che fornisce all'esercente il servizio per l'accettazione dei pagamenti con carta di credito
BIN	Prime 6 cifre del numero Carta, identificano l'Issuer della carta
CAVV Cardholder Authentication Verification Value	Identificativo univoco generato dall'Issuer per dimostrare che per una determinata carta VISA ha avuto luogo l'autenticazione
Issuer	Società che emette la carta di credito
Liability shift	Trasferimento della responsabilità e passività di una transazione dall'Acquirer all'Issuer
Merchant	Esercente
MPI Merchant Plug-in	Componente del protocollo 3D Secure che consente al merchant di collegarsi con i circuiti e con l'ACS per effettuare la fase d'autenticazione
SecureCode	Nome del protocollo 3D Secure di MasterCard
VbV Verified by Visa	Nome del protocollo 3D Secure di Visa
XID	Identificativo univoco della transazione