

**Allegato Tecnico E-commerce**

**Istruzioni e regole del servizio 3D Secure**

## Indice

<b>1 - Introduzione</b>	<b>3</b>
<b>2 - Funzionamento del servizio 3D Secure</b>	<b>3</b>
<b>3 - Protocollo 3D-Secure: Verified by Visa/SecureCode MasterCard</b>	<b>5</b>
<b>4 - Liability Shift</b>	<b>7</b>
4.1. - Visa	8
4.2. - MasterCard	10
<b>5 - Glossario</b>	<b>12</b>

## 1 - 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.

## 2 - Funzionamento del servizio 3D Secure

Il servizio **3D Secure** prende il nome di **Verified by Visa (VbV)** per il circuito Visa e di **SecureCode MasterCard (SCM)** 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 **esonero 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 dall'acquirer<sup>1</sup> alla società che ha emesso la carta di credito: un processo denominato **liability shift**.

La **liability shift** viene applicata secondo le regole Visa e MasterCard riassunte a seguire e riportate nei dettagli alle pagine **8,9,10**.

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<sup>2</sup> all'acquirer;
- 2- l'esercente aderisce a VbV, ma la società che ha emesso la carta o il titolare non aderiscono a VbV.

---

<sup>1</sup> Società che fornisce all'esercente il servizio per l'accettazione dei pagamenti con carta di credito

<sup>2</sup> Identificativo univoco generato dalla società che ha emesso la carta per dimostrare che per una determinata carta VISA ha avuto luogo l'autenticazione

Esistono alcune **eccezioni**, a questo secondo caso, per le quali la liability shift non viene applicata.

Queste eccezioni si verificano quando l'**ACS**<sup>3</sup> non è in grado di gestire alcune autenticazioni. Questo può succedere per:

- A) i pagamenti effettuati sui nuovi canali (es. mobile)
- B) le carte aziendali extraeuropee durante le transazioni internazionali
- C) le carte anonime prepagate

### **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 tramite l'inserimento della password personale è avvenuta correttamente; durante la fase di autorizzazione l' esercente ha inoltrato correttamente il Cavv<sup>4</sup> all'acquirer;
- 2- l' esercente aderisce a MSC, ma la società che ha emesso la carta o il titolare non aderiscono a MSC.

A questo 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 processo autorizzativo**.

**I paragrafi successivi** contengono i dettagli delle regole di funzionamento di 3D Secure e delle regole dei circuiti internazionali Visa e MasterCard, le istruzioni tecniche del funzionamento del servizio, le specifiche della liability shift e le eccezioni al servizio attualmente vigenti.

**CartaSi** si riserva la facoltà di modificare tali informazioni in base alle variazioni segnalate di volta in volta dai circuiti internazionali Visa e MasterCard.

In Appendice al documento è presente un **Glossario** che spiega la terminologia tecnica utilizzata.

---

<sup>3</sup> Componente del protocollo 3D Secure, gestita dalla società che ha emesso la carta, che verifica se una carta aderisce al protocollo e ne effettua l'autenticazione

<sup>4</sup> Identificativo univoco generato dalla società che ha emesso la carta per dimostrare che per una determinata carta VISA ha avuto luogo l'autenticazione

### 3 - Protocollo 3D-Secure: Verified by Visa/SecureCode MasterCard

Il seguente schema riassume l'intero processo di una transazione **VbV/SCM**:

#### Step 1

Il titolare della carta di credito effettua un acquisto su un sito **VbV/SCM** e inserisce i dati della propria carta, dando inizio alla transazione

#### Step 2

Il sito dell'esercente si collega, attraverso la componente Merchant Plug-In (**MPI**), al **Directory Server** (di Visa o di MasterCard), inviando un messaggio di tipo **VEReq** contenente il **PAN** della carta;

il **Directory Server** verifica se il **BIN** della carta rientra nella lista dei **BIN** comunicati dai vari Issuer come aderenti al servizio **VbV/SCM** e, in tal caso, contatta l'**ACS** (Access Control Server) dell'**Issuer** che verifica se la singola carta aderisce al servizio.

L'**ACS** risponde con un messaggio **VERes** il cui campo **Pan Authentication Available** indica se un'autenticazione è o non è disponibile per il **PAN** in questione, assumendo di conseguenza uno di questi valori:

**Y** : autenticazione disponibile;

**N** : titolare non partecipante al servizio;

**U** : autenticazione non possibile.

Il messaggio **VERes** è inoltrato al **MPI** dell'esercente.

#### Step 3

Se la carta aderisce al servizio, l'**MPI** invia una richiesta d'autenticazione all'**ACS** attraverso il messaggio **PAReq**.

Resta inteso che, se la carta non aderisce, viene avviato il normale processo autorizzativo e l'**Acquirer** attribuisce **ECI = 6 per Visa, 01 per MasterCard**.

#### Step 4

L'**ACS** effettua la fase d'autenticazione secondo le modalità di validazione del pagamento che l'**Issuer** ha stabilito (tipicamente viene visualizzata sul browser del titolare una pagina per l'inserimento di una password).

#### Step 5

L'**ACS** restituisce all'**MPI** un messaggio **PARes** i cui campi indicano l'esito dell'autenticazione e possono assumere i valori riportati nella tabella a pagina seguente:

Valori	Descrizione	ECI	CAVV valorizzato
Y	L'autenticazione è avvenuta con successo	5 per Visa, 02 per MasterCard	Sì Il merchant/acquirer deve inoltrarlo nell'autorizzazione
N	L'autenticazione è fallita	-	-
A	Il titolare non è iscritto al servizio. Questo caso si verifica se l'Issuer ha deciso di adottare l' <i>Attempt functionality</i> che gli consente di generare una prova dell'avvenuto tentativo da parte del merchant d'autenticazione del titolare indipendentemente dal fatto che il titolare aderisca o meno al servizio VbV/SCM <sup>5</sup>	6 per Visa, 01 per MasterCard	Valorizzato o meno a discrezione dell'Issuer. Per le carte del circuito Visa se l'ACS genera il CAVV il merchant/acquirer deve inoltrarlo nell'autorizzazione, per le carte del circuito MasterCard il merchant/acquirer NON deve inoltrare il CAVV nell'autorizzazione.
U	Non è stato possibile eseguire l'autenticazione	-	-

### Step 6/7

Il Merchant Server Plug-in verifica la risposta dell'ACS e decide proseguire o meno con il normale processo autorizzativo.

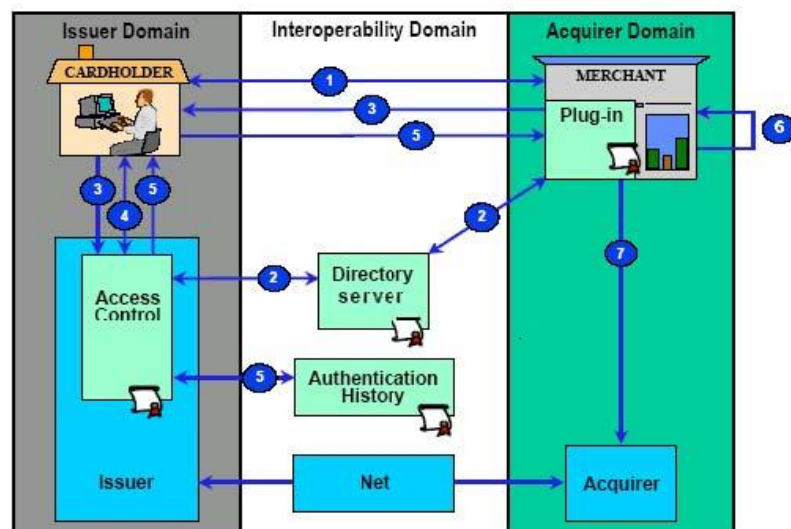


Figura 1: processo d'acquisto con protocollo VbV/SCM

<sup>5</sup> Tale funzionalità è prevista solo per gli esercenti VbV/SCM con versione 1.02 e non si applica alle precedenti versioni.

## 4 - Liability Shift

La **liability shift** è il **passaggio della responsabilità** della transazione dall'acquirer alla società che ha emesso la carta di credito.

Le **tabelle successive** riassumono le regole dei circuiti internazionali Visa e MasterCard per l'applicazione della liability shift in funzione della gestione del servizio **3D Secure**.

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 prescrizioni e le normative dei circuiti, CartaSi esonera l'esercente da qualsiasi responsabilità in caso di disconoscimento della transazione da parte dei titolari quando i circuiti garantiscono la liability shift.

Nelle pagine seguenti sono indicati i casi nei quali si applica la liability shift per le transazioni Verified by Visa e SecureCode MasterCard.

#### 4.1. - Visa

La seguente tabella indica in quali casi si applica la liability shift per una transazione **Verified by Visa**.

Autenticazione	VERes <sup>6</sup>	PARes <sup>7</sup>			autorizzazione		Liability shift
		Stato	ECI	CAVV	CAVV in BASE I <sup>8</sup>	VisaNet ECI <sup>9</sup>	
<b>Autenticazione positiva</b> Issuer aderente, titolare aderente, autenticazione conclusa con successo	Y	Y	5	Si	Si	5	Si
					No	7	No
				No	No	5	Si
<b>Autenticazione negativa</b> Issuer aderente, titolare aderente, autenticazione fallita (il titolare non è stato in grado di fornire la password corretta)	Y	N	N/A	No	N/A	N/A (l'autorizzazione non deve essere inoltrata)	No
<b>Non adesione al VbV</b> 1. Issuer non aderente 2. Issuer aderente ma BIN non registrato sui circuiti 3. Issuer aderente, ma titolare non aderente	N	none	N/A	No	N/A	6	Si
<b>Attempts</b> Issuer aderente che si avvale di un ACS con funzionalità "Attempt"	Y	A	6	Si	Si	6	Si
					No	7	No
				No	No	6	Si
<b>Impossibile autenticare (a)</b> Issuer aderente, titolare aderente, l'ACS ha risposto al messaggio VEReq, ma non al messaggio PAReq (transazione incompleta)	Y	none	N/A	No	N/A	7	No
<b>Impossibile autenticare (b)</b> Issuer aderente, titolare aderente, si sono verificati dei problemi che non hanno consentito l'autenticazione	Y	U	N/A	No	N/A	7	No
<b>Impossibile autenticare (c)</b> 1. Issuer aderente, si sono verificati problemi oppure il tipo di carta o di canale non è supportato 2. titolare sta effettuando l'acquisto su un merchant con versioni VbV precedenti alla 1.02 e l'issuer si è avvalso dell'Attempt functionality.	U	Nessuna	N/A	No	N/A	7	No

<sup>6</sup> Messaggio inviato dall'ACS per comunicare al merchant se il titolare aderisce o meno al servizio VbV.

<sup>7</sup> Messaggio inviato dall'ACS per comunicare al merchant l'esito della fase d'autenticazione.

<sup>8</sup> Valore CAVV inoltrato nell'autorizzazione dal merchant/acquirer.

<sup>9</sup> ECI che dovrebbe essere inoltrato nell'autorizzazione dal merchant/acquirer.

## Eccezioni

In generale l' esercente è protetto dalla liability shift nei seguenti casi:

### **transazione con ECI = 5**

Se l'autenticazione è avvenuta con successo e nel rispetto del protocollo 3D Secure, l'Issuer non può fare il chargeback

### **transazione con ECI = 6**

Se il merchant ha effettuato un tentativo d'autenticazione nel rispetto del protocollo 3D Secure, l'Issuer non può fare il chargeback in caso di disconoscimento della transazione..

In particolare, per essere protetto dalla liability shift, il merchant/acquirer **deve** inoltrare, nell'autorizzazione, il CAVV se generato dall'Issuer.

Tuttavia, a tali regole generali **fanno eccezione i seguenti casi**, nei quali le transazioni vengono processate con ECI=7 (nel caso in cui, le transazioni vengano erroneamente processate con ECI=6 l'Issuer mantiene comunque il diritto di effettuare il charge back):

- nuovi canali (es. mobile): l'ACS dell'Issuer potrebbe non gestire messaggi non-HTML;
- carte aziendali extraeuropee: la gestione dell'autenticazione per le carte aziendali (nei casi in cui più persone possono utilizzare una stessa carta) può non essere gestita dall'ACS; questa eccezione si applica solo per le transazioni inter-regional;
- carte anonime prepagate: la gestione dell'autenticazione per titolari anonimi potrebbe non essere gestita dall'ACS.

Tali eccezioni NON si applicano per le transazioni con ECI=5

#### 4.2. - MasterCard

La seguente tabella indica in quali casi si applica la liability shift per una transazione SecureCode MasterCard:

Fase d'autenticazione							Fase d'Autorizzazione	
Autenticazione	VEReq inviato?	VERes	PAREq inviato?	PAREs			Inoltro? <sup>10</sup>	Liability shift
				Stato	ECI	AAV		
Autenticato con successo	Si	Y	Si	Y	02	Si	Si	Si
Autenticato con successo (senza AAV)	Si	Y	Si	Y	02	No	Si	Si*
Autenticazione fallita (Secure code errato)	Si	Y	Si	N	-	No	No	No
Autenticazione fallita (verifica della firma del PAREs fallita)	Si	Y	Si	Tutti	Tutti	Tutti	No	No
Impossibile autenticare	Si	Y	Si	U	-	No	opzionale	Si*
Attempt	Si	Y	Si	A	01	Si	Si	Si*
Attempt senza AAV	Si	Y	Si	A	01	No	Si	Si*
Titolare non aderente	Si	N	No	-	-	-	Si	Si*
Impossibile autenticare	Si	U	No	-	-	-	Si	Si*
Titolare non aderente (via directory cache)	No	-	-	-	-	-	Si	Si*
Errore nella Directory Server	No	-	-	-	-	-	Si	Si*
Errore nel VEReq	Errore	-	No	-	-	-	opzionale	Si*
Errore nel VERes	Si	Errore	No	-	-	-	opzionale	Si*
Errore nel PAREs	Si	Y	Si	Errore			opzionale	Si*
Esercente non aderente al SecureCode	-	-	-	-	-	-	Si	No

\* Ad eccezione delle transazioni extra europee effettuate da carte aziendali.

#### Eccezioni

In generale l' esercente è protetto dalla liability shift nei seguenti casi:

##### transazione con ECI = 5

Se l'autenticazione è avvenuta con successo e nel rispetto del protocollo 3D Secure, l'Issuer non può fare il chargeback

##### transazione con ECI = 6

Se il merchant ha effettuato un tentativo d'autenticazione nel rispetto del protocollo 3D Secure, l'Issuer non può fare il chargeback in caso di disconoscimento della transazione.

In particolare, per essere protetto dalla liability shift, il merchant/acquirer **deve** inoltrare, nell'autorizzazione, il CAVV se generato dall'Issuer.

Tuttavia, a tali regole generali **fa eccezione il seguente caso**, nel quale le transazioni vengono processate con ECI=7 (nel caso in cui, le transazioni

<sup>10</sup> Questa colonna indica come dovrebbe comportarsi il merchant/acquirer per l'inoltro dell'autorizzazione in base all'esito della fase d'autenticazione.

vengano erroneamente processate con ECI=6 l'Issuer mantiene comunque il diritto di effettuare il charge back):

- carte aziendali: la gestione dell'autenticazione per le carte aziendali (nei casi in cui più persone possono utilizzare una stessa carta) può non essere gestita dall'ACS; questa eccezione si applica solo per le transazioni inter-regional.

Tale eccezione NON si applica per le transazioni con ECI=5

## 5 - 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
ECI Electronic Commerce Indicator	Indica il livello di sicurezza utilizzato in una transazione e-commerce. La sua valorizzazione è obbligatoria per l'Acquirer, l'Issuer deve poterlo ricevere e includerlo in tutti i processi relativi ad eventuali dispute. L'ECI può essere generato dall'ACS se l'Issuer aderisce oppure dall'Acquirer.
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
PAReq Payer Authentication Request	Messaggio del protocollo 3D Secure, inviato dall'MPI per richiedere l'autenticazione del titolare
PARes Payer Authentication Response	Messaggio del protocollo 3D Secure, inviato come risposta al messaggio PAReq. Contiene l'esito della fase d'autenticazione del titolare.
SecureCode	Nome del protocollo 3D Secure di MasterCard.
UCAF Universal Cardholder Authentication Field	Campo utilizzato da Issuers MasterCard per inviare l'AAV
VbV Verified by Visa	Nome del protocollo 3D Secure di Visa
VEReq Verify Enrolment Request	Messaggio del protocollo 3D Secure inviato dall'MPI alla Directory Server per verificare se la carta partecipa al VbV o al SecureCode.
VERes Verify Enrolment Response	Messaggio del protocollo 3D Secure inviato in risposta al messaggio VEReq. Indica se la carta partecipa al VbV o al SecureCode
XID	Identificativo univoco della transazione.