DirectLink con 3-D Secure

ingenico
ePayments

Tabella dei contenuti

1. 3-D Secure v1.0

1.1 Introduzione

Il protocollo 3-D Secure permette di identificare il titolare della carta durante la procedura d'acquisto. Il titolare della carta deve essere connesso a Internet durante la procedura di identificazione. 3-D Secure non funziona per i call center o per i pagamenti ricorrenti.

Visa ha implementato il protocollo 3-D Secure con il nome Verified By Visa, MasterCard con il nome SecureCode, JCB con il nome J-Secure e American Express con il nome SafeKey.

Lo scopo dell'integrazione di DirectLink con 3-D Secure è di avviare un pagamento in modalità DirectLink e terminarlo in modalità e-Commerce, se è necessaria l'autenticazione del titolare della carta.

Nel presente documento viene spiegata l'integrazione del protocollo 3-D Secure in DirectLink. Per maggiori informazioni relative a DirectLink o e-Commerce, visitare la pagina DirectLink o la documentazione di e-Commerce.

1.2 Flusso della transazione 3-D mediante DirectLink

Il flusso della transazione comprende i seguenti passaggi:

1. Ci inviate una richiesta di transazione DirectLink contenente una serie di parametri aggiuntivi (cfr. Parametri di richiesta aggiuntivi).
2. Il sistema riceve il numero di carta contenuto nella richiesta e controlla online se la carta è registrata nella directory VISA/MasterCard /JCB/AmEx (per registrata si intende che il numero di carta può essere identificato, quindi che la carta è una carta 3-D Secure).
3. Se il titolare della carta è registrato, la risposta alla richiesta di DirectLink contiene uno stato di pagamento specifico e un codice html, da restituire al cliente per avviare il processo di identificazione (cfr. Campi restituiti aggiuntivi). Il blocco di codice html avvia automaticamente il processo di identificazione tra il titolare della carta (cliente) e la banca emittente.
4. Il titolare della carta si identifica sulla pagina della banca emittente.
5. Il nostro sistema riceve dall'emittente una risposta sull'identificazione.
6. Se l'identificazione viene superata, il sistema invia all'acquirente la transazione finanziaria effettiva.
7. Il risultato dell'identificazione globale e del processo di autorizzazione online viene inviato tramite i canali di feedback della modalità e-Commerce.

Commenti:

- l'eventuale applicabilità del passaggio della responsabilità della transazione dipende dal contratto dell'acquirente. Si consiglia pertanto di verificare i termini e le condizioni con l'acquirente.
- Se il titolare della carta non è registrato (nel passaggio 3), riceve la risposta XML standard di DirectLink con il risultato del processo di autorizzazione online.
- Per ricevere lo stato esatto del pagamento e i codici errore (nel passaggio 7), è necessario implementare il feedback post-vendita online o offline, seguendo le istruzioni fornite nella e-Commercedocumentazione.

1.2.1 Parametri di richiesta aggiuntivi

Oltre ai parametri standard di DirectLink, è necessario inviare i seguenti dati:

Campo	Descrizione
FLAG3D	Valore fisso: 'Y' Indica il nostro sistema come eseguire un'identificazione 3-D Secure, se necessario.

Campo	Descrizione
HTTP_ACCEPT	Campo richiesta-intestazione Accetto nel browser del titolare della carta, utilizzato per specificare alcuni tipi di supporti accettati per la risposta. Questo valore è utilizzato dall'emittente per controllare se il browser del titolare della carta è compatibile con il sistema di identificazione dell'emittente. Ad esempio: Accetto: */*
HTTP_USER_AGENT	Campo richiesta-intestazione Utente-Agente nel browser del titolare della carta, contenente informazioni sull'agente utente che genera la richiesta. Questo valore è utilizzato dall'emittente per controllare se il browser del titolare della carta è compatibile con il sistema di identificazione dell'emittente. Ad esempio: Agente utente: Mozilla/4.0 (compatibile, MSIE 6.0, Windows NT 5.0)
WIN3DS	Un modo per mostrare al cliente la pagina di identificazione. Valori possibili: • MAINW: consente di visualizzare la pagina di identificazione nella finestra principale (valore predefinito). • POPUP: consente di visualizzare la pagina di identificazione nella finestra di popup e alla fine di tornare alla finestra principale. • POPIX: consente di visualizzare la pagina di identificazione nella finestra di popup e di rimanere nella finestra di popup.
ACCEPTURL	URL della pagina Web da mostrare al cliente quando il pagamento è stato autorizzato (o è in attesa di autorizzazione).
DECLINEURL	URL al quale viene reindirizzato il cliente al raggiungimento del numero massimo di tentativi di autorizzazione falliti (10 per impostazione predefinita, sebbene il valore possa essere modificato nella pagina Technical Information, nella sezione "Payment retry" della scheda "Global transaction parameters").
EXCEPTIONURL	URL della pagina Web da mostrare al cliente se il risultato del pagamento è incerto.
PARAMPLUS	Campo in cui inserire vari parametri e i relativi valori che si desidera ricevere nella richiesta post vendita o nel reindirizzamento finale.
COMPLUS	Campo in cui inserire un valore che si desidera ricevere nella richiesta post vendita o nell'output.
LANGUAGE	Lingua del cliente, ad esempio: “en_US”
Facoltativo	
TP	Per modificare il layout della pagina "order_A3DS", è possibile inviare un URL/nome di modello con questo parametro. (vedere e-Commerce: Modello dinamico).

Per maggiori informazioni, vedere Feedback sulla transazione.

1.2.2 Campi restituiti aggiuntivi

Se il titolare della carta non è registrato, viene restituita la normale risposta di DirectLink. Se il titolare della carta è registrato, vengono restituiti i seguenti campi (aggiuntivi):

Campo	Descrizione
STATUS	Nuovo valore: “46” (in attesa di identificazione)
HTML_ANSWER	Codice html con codifica BASE64 da aggiungere alla pagina html restituita al cliente.

Campo	Descrizione
	Il tag viene aggiunto come elemento secondario del tag XML globale <ncresponse>. Il campo HTML_Answer contiene un codice HTML da aggiungere alla pagina html restituita al browser del cliente. Il codice carica automaticamente la pagina identificativa della banca emittente in un popup nella finestra principale, in base al valore del parametro WIN3DS. Per evitare interferenze tra i tag html inclusi nel contenuto del tag XML HTML_ANSWER, insieme al resto del codice XML restituito come risposta alla richiesta di DirectLink, il contenuto HTML_ANSWER viene codificato con BASE64 dal sistema prima che venga restituita la risposta. Di conseguenza, questo deve essere decodificato con BASE64 prima di essere incluso nella pagina html inviata al titolare della carta.

1.2.3 Commenti

Carte di prova

È possibile usare le seguenti carte di prova per simulare una carta registrata 3-D Secure nel nostro ambiente di prova:

Marchio	Numero carta	Data di scadenza	Password
VISA	4000000000000002	Qualsiasi data futura	11111
MasterCard	5300000000000006	Qualsiasi data futura	11111
American Express	371449635311004	Qualsiasi data futura	11111

Identificazione errata

Se una transazione è bloccata a causa di un errore di identificazione, il risultato della transazione sarà:

STATUS = 0

NCSTATUS = 5

NCERROR = 40001134

2. 3-D Secure v2.1 (Disponibile in TEST)

2.1 Introduction

In 2013, la Commissione Europea ha pubblicato una proposta per la versione rivisitata della Direttiva sui servizi di pagamento, nota come PSD2 per semplificare l'elaborazione dei pagamenti e creare le regole e i regolamenti dei servizi di pagamento nell'UE e da allora è nata la necessità di una nuova versione di 3-D Secure, v2.1.

La modifica maggiore consiste nel richiedere ai commercianti di condividere un maggior numero di dati: gli emittenti hanno bisogno di punti dati per migliorare la precisione delle loro decisioni e giungere a uno scenario privo di attriti. Ma siete voi quelli in prima linea nella cattura dei dati. L'approccio di 3DS v2 alla valutazione del rischio è più efficace, ma richiede la modifica dell'intero ecosistema per poter inviare i dati fino all'emittente.

Con l'introduzione di queste nuove regole, i principali reti di carte de pagamento hanno aggiornato il loro logo 3DS. Se sei integrato in DirectLink, significa che gestisci la tua pagina di pagamento, e per questo assicurati di implementare questi nuovi loghi (Visa / Mastercard / JCB /...).

2.2 Flusso della transazione 3-D mediante DirectLink

Il flusso delle transazioni implica i passi seguenti:

1. Si invia la richiesta DirectLink della transazione, contenente un certo numero di parametri aggiuntivi.

Tali parametri sono organizzati in tre gruppi:

a. Parametri obbligatori da catturare nella pagina di pagamento in cui il titolare della carta sta inserendo i dettagli della carta.

Parametri	Descrizione	Format	Obbligante
browserAcceptHeader	Il contenuto esatto dell'HTTP accetta intestazioni come inviate al commerciante dal browser del titolare di carta di credito. *	Tipo dati: String Lunghezza: Variabile, massimo 2.048 caratteri Valore accettato: Se la lunghezza totale dell'intestazione inviata dal browser supera i 2.048 caratteri, il server 3DS tronca la porzione in eccesso.	Sì
browserColorDepth	Valore che rappresenta la profondità in bit della palette di colori per le immagini, in bit per pixel. Ottenuto dal browser del titolare di carta di credito usando la proprietà di profondità del colore dello schermo.	Tipo dati: Stringa Valori accettati: 1 = 1 bit 4 = 4 bit 8 = 8 bit 15 = 15 bit 16 = 16 bit 24 = 24 bit 32 = 32 bit 48 = 48 bit	Sì
browserJavaEnabled	Booleano che rappresenta la capacità del browser del titolare di carta di credito di eseguire Java. Il valore è restituito dalla proprietà di abilitazione	Tipo dati: Booleano Valori accettati: true	Sì

Parametri	Descrizione	Format	Obbligante
	Java del navigatore.	false	
browserLanguage	Valore che rappresenta la lingua del browser, come definita nel codice IETF BCP47. Restituito dalla proprietà della lingua del navigatore.	Tipo dati: Stringa Lunghezza: Variabile, 1-8 caratteri	Sì
browserScreenHeight	Altezza totale dello schermo del titolare di carta di credito in pixel. Il valore è restituito dalla proprietà dell'altezza dello schermo.	Tipo dati: Int Tra 0 e 999999	Sì
browserScreenWidth	Larghezza totale dello schermo del titolare di carta di credito in pixel. Il valore è restituito dalla proprietà della larghezza dello schermo.	Tipo dati: Int Tra 0 e 999999	Sì
browserTimeZone	Differenza oraria tra l'orario UTC e l'ora locale del browser del titolare di carta di credito, in minuti.	Tipo dati: Int Tra -720 e 840	Sì
browserUserAgent	Contenuto esatto dell'intestazione user-agent HTTP. *	Tipo dati: Stringa Lunghezza: Variabile, massimo 2.048 caratteri Nota: se la lunghezza totale dell'user-agent inviato dal browser supera i 2.048 caratteri, il server 3DS tronca la porzione in eccesso.	Sì

*HTTP_ACCEPT e HTTP_USER_AGENT non devono essere inviati con browserAcceptHeader e browserUserAgent; diversamente, lo compileremo con i parametri del browser.

Nota: non dimenticare di calcolare i parametri nella firma SHA.

Di seguito è disponibile un esempio di codice Javascript per l'acquisizione di tali parametri.

```
<script type="text/javascript" language="javascript">

function createHiddenInput(form, name, value)
{
var input = document.createElement("input");
input.setAttribute("type", "hidden");
input.setAttribute("name", name);
input.setAttribute("value", value);
form.appendChild(input);
}

var myCCForms = document.getElementsByName("MyForm");
if (myCCForms != null && myCCForms.length > 0)
{
var myCCForm = myCCForms[0];
createHiddenInput(myCCForm, "browserColorDepth", screen.colorDepth);
```

createHiddenInput(myCCForm, "browserJavaEnabled", navigator.javaEnabled());
createHiddenInput(myCCForm, "browserLanguage", navigator.language);
createHiddenInput(myCCForm, "browserScreenHeight", screen.height);
createHiddenInput(myCCForm, "browserScreenWidth", screen.width);
createHiddenInput(myCCForm, "browserTimeZone", new Date().getTimezoneOffset());
}
</script>

b. Parametri aggiuntivi necessari (cfr. Parametri di richiesta aggiuntivi).

c. Parametri opzionali ma consigliati (elenco di parametri) che se inviati avranno influenza positiva sulle velocità di conversione della transazione. In base alle informazioni contenute in tali parametri si potrebbe generare un possibile flusso di autenticazione senza attriti, in cui il titolare della carta non avrà più bisogno di autenticarsi e perciò ci si aspetta un completamento più veloce della transazione. In caso contrario, se non si fornisce nessuno di tali parametri avrà luogo il reindirizzamento relativo alla normale autenticazione.

Il sistema riceve il numero di carta contenuto nella richiesta e controlla online se la carta è registrata nella directory VISA/MasterCard /JCB/AmEx (per registrata si intende che il numero di carta può essere identificato, quindi che la carta è una carta 3-D Secure).

2. In base alla risposta della directory degli schemi, se il titolare della carta è registrato in 3-D Secure e in caso siano stati forniti i parametri aggiuntivi **1.c (Parametri opzionali ma consigliati-elenco di parametri) precedenti si potranno avere due possibili flussi:**

2.1. Flusso senza attriti: Il titolare della carta non ha fisicamente bisogno di autenticarsi perché l'autenticazione è avvenuta in background senza il loro contributo. In questo caso, lo spostamento di responsabilità è sulla banca emittente.

2.2. Flusso difficile: Il titolare della carta dovrà autenticarsi ulteriormente.

i. La risposta alla richiesta di DirectLine contiene lo stato di pagamento specifico e il codice html che deve essere fatto tornare al cliente per iniziare il processo di identificazione (vedi i campi aggiuntivi di ritorno). Il blocco del codice html inizia automaticamente il processo di identificazione tra il titolare della carta (il cliente) e la sua banca emittente.

ii. Il titolare della carta si identifica sulla pagina della banca emittente.

iii. Il nostro sistema riceve dall'emittente una risposta sull'identificazione.

iv. Se l'identificazione viene superata, il sistema invia all'acquirente la transazione finanziaria effettiva.

3. Il risultato dell'identificazione globale e del processo di autorizzazione online viene inviato tramite i canali di feedback della modalità e-Commerce.

2.2.1 Parametri di richiesta aggiuntivi

Oltre ai parametri standard di DirectLink, è necessario inviare i seguenti dati:

Campo	Descrizione
FLAG3D	Valore fisso: 'Y' Indica il nostro sistema come eseguire un'identificazione 3-D Secure, se necessario.
HTTP_ACCEPT	Campo richiesta-intestazione Accetto nel browser del titolare della carta, utilizzato per specificare alcuni tipi di supporti accettati per la risposta. Questo valore è utilizzato dall'emittente per controllare se il browser del titolare della carta è compatibile con il sistema di identificazione dell'emittente. *

Campo	Descrizione
	Ad esempio: Accetto: */*
HTTP_USER_AGENT	Campo richiesta-intestazione Utente-Agente nel browser del titolare della carta, contenente informazioni sull'agente utente che genera la richiesta. Questo valore è utilizzato dall'emittente per controllare se il browser del titolare della carta è compatibile con il sistema di identificazione dell'emittente. * Ad esempio: Agente utente: Mozilla/4.0 (compatibile, MSIE 6.0, Windows NT 5.0)
WIN3DS	Un modo per mostrare al cliente la pagina di identificazione. Valori possibili: • MAINW: consente di visualizzare la pagina di identificazione nella finestra principale (valore predefinito). • POPUP: consente di visualizzare la pagina di identificazione nella finestra di popup e alla fine di tornare alla finestra principale. • POPIX: consente di visualizzare la pagina di identificazione nella finestra di popup e di rimanere nella finestra di popup.
ACCEPTURL	URL della pagina Web da mostrare al cliente quando il pagamento è stato autorizzato (o è in attesa di autorizzazione).
DECLINEURL	URL al quale viene reindirizzato il cliente al raggiungimento del numero massimo di tentativi di autorizzazione falliti (10 per impostazione predefinita, sebbene il valore possa essere modificato nella pagina Technical Information, nella sezione "Payment retry" della scheda "Global transaction parameters").
EXCEPTIONURL	URL della pagina Web da mostrare al cliente se il risultato del pagamento è incerto.
PARAMPLUS	Campo in cui inserire vari parametri e i relativi valori che si desidera ricevere nella richiesta post vendita o nel reindirizzamento finale.
COMPLUS	Campo in cui inserire un valore che si desidera ricevere nella richiesta post vendita o nell'output.
LANGUAGE	Lingua del cliente, ad esempio: “en_US”
Facoltativo	
TP	Per modificare il layout della pagina "order_A3DS", è possibile inviare un URL/nome di modello con questo parametro. (vedere e-Commerce: Modello dinamico).

*HTTP_ACCEPT e HTTP_USER_AGENT non dovranno essere inviati se vengono inviati browserAcceptHeader e browserUserAgent.

Per maggiori informazioni, vedere Feedback sulla transazione.

2.2.2 Campi restituiti aggiuntivi

Se il titolare della carta non è registrato, viene restituita la normale risposta di DirectLink. Se il titolare della carta è registrato, vengono restituiti i seguenti campi (aggiuntivi):

Campo	Descrizione
STATUS	Nuovo valore: “46” (in attesa di identificazione)
HTML_ANSWER	Codice html con codifica BASE64 da aggiungere alla pagina html restituita al cliente.

Campo	Descrizione
	Il tag viene aggiunto come elemento secondario del tag XML globale <ncresponse>. Il campo HTML_Answer contiene un codice HTML da aggiungere alla pagina html restituita al browser del cliente. Il codice carica automaticamente la pagina identificativa della banca emittente in un popup nella finestra principale, in base al valore del parametro WIN3DS. Per evitare interferenze tra i tag html inclusi nel contenuto del tag XML HTML_ANSWER, insieme al resto del codice XML restituito come risposta alla richiesta di DirectLink, il contenuto HTML_ANSWER viene codificato con BASE64 dal sistema prima che venga restituita la risposta. Di conseguenza, questo deve essere decodificato con BASE64 prima di essere incluso nella pagina html inviata al titolare della carta.

2.2.3 Commenti

Carte di prova

È possibile usare le seguenti carte di prova per simulare una carta registrata 3-D Secure nel nostro ambiente di prova:

Flusso senza attriti Marchio	Numero carta	Data di scadenza
VISA	4186455175836497	Qualsiasi data futura
Mastercard	5137009801943438	Qualsiasi data futura
American Express	375418081197346	Qualsiasi data futura

Flusso difficile Marchio	Numero carta	Data di scadenza
VISA	4874970686672022	Qualsiasi data futura
Mastercard	5130257474533310	Qualsiasi data futura
American Express	379764422997381	Qualsiasi data futura

Nota: è possibile scaricare più numeri di schede di prova qui.

Identificazione errata

Se una transazione è bloccata a causa di un errore di identificazione, il risultato della transazione sarà:

STATUS = 0

NCSTATUS = 5

NCERROR = 40001134

2.3 Esclusioni ed esenzioni del 3DSv2

2.3.1 3DSv2 ed esclusioni

Con l'introduzione del 3DSv2, l'autenticazione del titolare della carta diventerà obbligatoria per tutti, come definito dalla Seconda direttiva sui servizi di pagamento (2015/2366 PSD2) dell'UE . Tuttavia alcune transazioni sono escluse da questa regola, in presenza dei casi seguenti:

- Ordini per posta/ordini telefonici
- Il PSP del beneficiario (ovvero l'acquirente del commerciante) o il PSP del pagatore (ovvero l'emittente del metodo di pagamento dell'acquirente) si trova fuori dalla zona SEE (Spazio Economico Europeo)
- Carte di pagamento prepagate anonime fino a 150 € (articolo 63)
- MIT - Merchant Initiated Transactions

2.3.2 SCA e Flusso frictionless / challenge del 3DS

La SCA (Strong Customer Authentication, richiesta di autenticazione forte) fa parte di questo nuovo regolamento. Questa implica la possibilità che l'emittente (la banca del titolare della carta) richieda ulteriori informazioni al titolare della carta. In questo caso il processo di autenticazione condurrà al Flusso challenge (procedura che richiede al titolare della carta di autenticarsi attivamente) invece che al Flusso frictionless (procedura senza autenticazione del titolare della carta).
Ma ai nostri commercianti consentiamo di indicare il flusso preferito. Per far ciò, si inviano parametri aggiuntivi che saranno utilizzati dall'emittente per la valutazione del rischio. In base alla decisione dell'emittente, si potrà eseguire il Flusso frictionless. In alcuni casi, se si applicano specifiche esenzioni si potrebbe anche saltare completamente il 3DS.

2.3.3 Indicazione del flusso preferito

Per indicare la preferenza del Flusso frictionless durante la richiesta di autenticazione, il commerciante potrà inviare il parametro aggiuntivo Mpi.threeDSRequestorChallengeIndicator. In base alla valutazione del commerciante sui rischi di frode, si potranno inviare gli specifici valori (per es. valutazione di basso rischio: 02, rischio di frode aumentato: 03)

Parametro	Valori	Obbligatorio / Opzionale
Mpi.threeDSRequestorChallengeIndicator	01 = Nessuna preferenza 02 = Nessuna verifica richiesta 03 = Verifica richiesta: preferenza del commerciante 04 = Verifica richiesta: Autorizzazione	Obbligatorio (nel caso di una preferenza per un flusso specifico)

Il commerciante può aumentare ancora la possibilità del rapporto Flusso frictionless / conversione, inviando altri campi opzionali.

2.3.4 Esenzioni di 3DS

In alcune transazioni il commerciante potrebbe saltare il 3DS (permettendo il Flusso frictionless) e passare direttamente all'autorizzazione. Questo processo è limitato alle transazioni che sono escluse dalla SCA (come descritto precedentemente) o che possono beneficiare di specifiche esenzioni. Tali esenzioni devono far parte di un accordo tra il commerciante e il suo acquirente. In questi casi, il commerciante indicherà di saltare il processo di autenticazione inviando questi parametri aggiuntivi:

Parametro	Valori	Obbligatorio / Opzionale

FLAG3DS	N = Salto del processo di autenticazione 3DS	Obbligatorio (in caso di salto del 3DS)
3DS_EXEMPTION_INDICATOR	Fornire giustificazioni al salto del 3DS. I valori numerici sono applicabili in base alla transazione 03 = TRA* emittente 04 = esenzione per bassi importi 05 = TRA* Commerciante / Acquirente 06 = Whitelisting 07 = Corporate 08 = Spedizione ritardata 09 = Autenticazione ritardata (portafoglio certificato)	Obbligatorio (in caso di salto del 3DS)

* Analisi rischio della transazione

Ma sarà sempre l’emittente a decidere se si dovrà eseguire il processo di autenticazione. Se l’emittente insiste sul 3DS, la transazione viene rifiutata.