Come funziona l’autenticazione forte del cliente (Strong Customer Authentication) introdotta dalla Direttiva PSD2

Author : Pier Luigi Rotondo

Date : 20 Novembre 2019

La direttiva europea PSD2 (2015/2366/UE) ha recentemente introdotto il tema dell’**autenticazione forte del cliente**, in inglese *Strong Customer Authentication* o semplicemente SCA.

La *Strong Customer Authentication* impone che tutte le operazioni di pagamento elettronico, e alcune altre operazioni a distanza che comportino un rischio di frode, vengano confermate e autorizzate combinando *due o più fattori* di autenticazione, scelti tra qualcosa che solo chi effettua l’operazione conosce (ad esempio un PIN o una password), qualcosa che solo chi effettua l’operazione possiede (un’app su un dispositivo mobile o una chiave che genera codici OTP), oppure un elemento di inerenza, cioè qualcosa che contraddistingue univocamente l’utente (l’impronta digitale, la geometria del volto, o un’altra caratteristica biometrica).

I fattori scelti devono essere **mutuamente indipendenti**, in modo che la violazione di uno dei fattori non comprometta l’affidabilità degli altri.

Questo al fine di garantire servizi di pagamento elettronici basati su tecnologie in grado di garantire l'autenticazione sicura dell'utente e ridurre il rischio di frode

Questo articolo esamina tutti i più diffusi metodi di autenticazione, e la loro accettabilità con i requisiti della SCA, secondo le precisazioni della European Banking Authority (EBA).

Elementi di conoscenza

Un elemento di conoscenza, secondo la PSD2, contraddistingue qualcosa che *solo l’utente conosce*. La conoscenza è un elemento statico che deve già esistere prima della transazione elettronica.

Un PIN, una password o *passphrase*, oppure la risposta a una domanda di sicurezza sono elementi di conoscenza ai quali siamo già abituati, e certamente validi nel contesto della

autenticazione forte del cliente. Anche un *pattern* disegnato sullo schermo, come il codice di sblocco del cellulare, costituisce un elemento di conoscenza, anche se decisamente poco robusto in quanto visibile da una persona vicina, e facilmente replicabile.

Elementi a cui altri possono, anche occasionalmente, avere accesso non rappresentano un valido elemento di conoscenza per la PSD2. Un chiaro esempio sono i dettagli stampati su una carta di pagamento (numero, data di scadenza, codice di sicurezza CVV) in quanto leggibili del commerciante a cui affidiamo la carta per effettuare il pagamento in un negozio. Per contrasto, un numero di carta di credito che cambia dinamicamente, ad esempio generato prima di ogni acquisto, è un valido elemento di conoscenza.

Elementi di possesso

La PSD2 definisce il possesso come *qualcosa che solo l'utente possiede*.

Il possesso va oltre il mero possesso fisico di un oggetto e si estende anche al possesso di qualcosa di immateriale, come un'app su uno smartphone, oppure una sessione Internet. L'app sul dispositivo mobile necessita tuttavia di una operazione preliminare di registrazione del dispositivo, detta *enrollment*, e che serve a creare un collegamento univoco tra il servizio remoto, il dispositivo mobile e l'utente che lo possiede. Nel caso della sessione Internet, la scansione di un QR code presentato a schermo tramite un dispositivo mobile consente di associare univocamente la sessione all'utente presente davanti al computer.

All'atto pratico, nella fase di *enrollment*, viene scambiata una chiave univoca che permetterà di contraddistinguere in futuro questa istanza dell'app oppure la specifica sessione del browser. Un'app installata sullo smartphone che non sia stata sottoposta ad enrollment non soddisfa invece i requisiti di Strong Customer Authentication.

Una chiave che genera token OTP è ancora un valido elemento di autenticazione secondo la PSD2, ma questo approccio diventa sempre meno diffuso in favore di app per smartphone che generano codici OTP, e che consentono di portare a termine una transazione utilizzando un solo dispositivo.

Elementi di inerenza

La PSD2 definisce l'inerenza come *qualcosa che l'utente è,* e si riferisce sia alle caratteristiche fisiche che comportamentali che contraddistinguono l'utente che effettua il pagamento. Per caratteristiche fisiche intendiamo caratteristiche che non cambiano nel tempo, come ad esempio l'impronta digitale, le caratteristiche geometriche del volto o della mano lette da una telecamera, e negli approcci più sofisticati la scansione della retina o dell'iride. Esempi di caratteristiche comportamentali sono invece elementi come l'andatura durante una camminata, l'inclinazione con cui teniamo lo smartphone, oppure la velocità di movimento su una tastiera, o il battito cardiaco.

Il **riconoscimento biometrico** è indubbiamente il settore più innovativo e con lo sviluppo più

veloce. Tra le aree di frontiera rientra anche l'autenticazione continua, permessa dai dispositivi *wearable* (ad esempio gli smart watch o gli occhiali per visione aumentata) e rimangono a contatto con il corpo per un periodo di tempo prolungato. Dopo una prima fase di autenticazione complessa, il dispositivo può rimanere autenticato fintanto che rimane fisicamente a contatto con il corpo.

Su quest'area si continueranno a vedere progressi nel prossimo futuro. Il nuovo protocollo 3-D Secure v2.0, usato per autorizzare transazioni remote con carte di pagamento, almeno nelle implementazioni attualmente sul mercato, non permette la trasmissione di caratteristiche biometriche.

Un'opportunità per il commercio online

Il volume transato con carte di credito in Italia nel 2018 ha superato gli 80 miliardi di euro, con circa 15 milioni di carte di credito attive.

Secondo i dati più recenti disponibili, nel corso del solo 2016 il valore totale delle transazioni fraudolente condotte utilizzando carte di pagamento emesse all'interno dell'area SEPA ha toccato gli 1,8 miliardi, e in termini percentuali ha rappresentato lo 0.041% del valore totale delle transazioni.

Il 73% delle frodi in valore, per un totale di 1,32 miliardi di euro è avvenuto sui pagamenti da remoto di tipo *card-not-present* (CNP), ad esempio tramite Internet o telefono, dove i dettagli della carta vengono comunicati in remoto, e la carta non viene fisicamente inserita o avvicinata al lettore al momento del pagamento. Per questo tipo di transazione il rischio di frode è chiaramente più alto, in quanto non c'è incontro fisico tra titolare e commerciante, e su queste transazioni l'autenticazione forte del cliente porterà i maggiori benefici [6]. Le frodi al terminale POS rappresentano circa il 19% del totale, mentre quelle su prelievo di contante su macchine ATM ammontano a circa l'8% del valore. Il 47% di queste due ultime categorie è avvenuto con carte smarrite o rubate.

I numeri indicano un continuo spostamento nel corso degli ultimi anni dalle **frodi** *card-present* (CP) a quelle di tipo *card-not-present* (CNP). Tuttavia il mercato sta sviluppando proprio per questa modalità, una moltitudine di soluzioni anti-frode (protocollo 3-D Secure, risk-based authentication).

Tra le pieghe della *Strong Customer Authentication* si cela una pratica che, più di altre, potrebbe imprimere al mercato una **spinta virtuosa**. Uno scenario di esenzione dalla SCA è relativo ai pagamenti elettronici gestiti da fornitori che dimostrano un tasso di frode particolarmente basso. L'importo della transazione esente dipende in maniera diretta dal tasso di frode del fornitore, e raggiunge fino a €500 nel caso di pagamenti elettronici il cui fornitore di servizi di pagamento mantenga un tasso di frode inferiore allo 0,01%, un obiettivo ambizioso e decisamente inferiore all'attuale tasso di frode medio nell'area SEPA.

Questo spingerà tutti gli attori del sistema dei pagamenti a migliorare costantemente il proprio tasso di frode, potendo così offrire soglie di esenzione crescenti e attraendo di conseguenza un

numero sempre maggiore di clienti.

Riferimenti

[1] Pier Luigi Rotondo, *Multifactor Authentication Delivers the Convenience and Security Online Shoppers Demand,* SecurityIntelligence.com, January 2019

[2] *Directive (EU) 2015/2366 of the European Parliament and of the Council,* Official Journal of the European Union, November 2015

[3] *Fifth report on card fraud,* European Central Bank – Eurosystem, September 2018

[4] Pier Luigi Rotondo, *How Will Strong Customer Authentication Impact the Security of Electronic Payments?,* SecurityIntelligence.com, September 2019

Articolo a cura di **Pier Luigi Rotondo**