Customer Advisory

To: CA Transaction Manager Customers
From: The CA Technologies Digital Payments Product Team
Subject: Update to 3D Secure Protocol
Date: November 17, 2014

A recent online article in the Independent news reported that Visa and MasterCard are working on a new protocol for improving the security of online transactions[1]. Please note that this is not a new protocol, but an update to the existing 3-D Secure (3DS) protocol. The article and accompanying comments further indicate that issuers may be encouraged or mandated to move away from using static passwords. The sophistication of fraud and the desire for an improved customer experience has already led a significant number of CA Technologies customers to choose CA "Zero-Touch" authentication and move away from the use of static passwords. Those customers that continue to use the static password have a number of alternatives from CA Technologies covered below.

CA Technologies welcomes the enhancements to the 3DS protocol that are being considered and expects that this will accelerate the adoption with issuers and merchants globally. We are working closely with Visa and MasterCard on updates to the protocol. This collaboration is under strict NDA – with Visa/MasterCard offering details to card issuers and merchants at appropriate points along the evolution lifecycle.

CA Technologies is a leading provider of solutions that are compliant with 3DS. Our 3DS service is used by over 13,500 portfolios and has over 150 million active cardholders. The 3DS protocol (currently in version 1.0.2) enables online merchants to request the issuer to authenticate the cardholder during an online transaction providing greater assurance to the cardholder and improved security against CNP fraud.

What does this mean for current CA Technologies 3D Secure Customers?

The 3DS protocol was intended to be a counter to online fraud and continues to be a great weapon in the issuer's arsenal to mitigate fraud. No other option gives issuers access to a rich set of environmental factors (device, location, etc.) of the online transaction and allows issuers to participate in the decision making at the point of purchase.

CA Technologies will upgrade both its SaaS offering and on-premise software so that issuers, merchants and cardholders can benefit from improvements to the 3DS protocol. Consistent with past protocol updates, CA Technologies' upgraded software will be available for issuers to start supporting the new protocol before the Visa/MasterCard mandates are in effect. We will share the milestone timeline with you as soon as the new specifications are published.

3D Secure protocol milestones:

- Draft of new specifications made available for review
- Specifications revised based on 3DS community feedback

- Final specifications released
- CA Technologies develops software upgrades to support the new specifications
- Visa/MasterCard certify the software upgrades for compliance with new specifications
- Software upgrades are deployed in production according to a sequence for upgrading card brand software (DS), issuer software (ACS) and merchant software (MPI)
- Once all systems are stable and running on new version, the older version is discontinued for use

CA Technologies Options for Frictionless Customer Authentication Experience

- CA Risk Analytics provides advanced statistical predictive models and rules to assess the potential risk of each transaction and appropriately deny or allow each transaction. Issuers can opt for this **"Zero-Touch"** authentication with no explicit cardholder interruption to the checkout process.
- CA Risk Analytics also offers the ability to allow a transaction and in parallel alert the cardholder for confirmation of the transaction. Using **"auto-resolution"** these transactions can be validated instantaneously by cardholders to allow them continued use of the card.
- Issuers can augment CA Risk Analytics with CA Strong Authentication providing simple, intuitive and dynamic authentication schemes. These include a dynamic one-time-password (OTP) delivered over SMS, email or voice call; CA Mobile OTP generator for the mobile device; and CA two-way notification service for cardholders to confirm their transaction on their mobile device.
- In addition, CA Technologies is working closely with partners to deliver biometric based authentication options.

What's next?

We will work with you to advise on CA Technologies' current "Zero-Touch" authentication options and help you prepare for the change to the 3DS protocol. The benefits are significant improvements to the customer experience and protection against CNP fraud. For further information, CA Technologies customers can contact Technical Support or their account representative.

[1]Mastercard and Visa to kill off password authentication

Sophie Curtis
Independent.IE

Published 13/11/2014 | 13:09

Mastercard and Visa have announced plans to ditch the need to enter passwords as a means of confirming user identity.

Current systems MasterCard SecureCode and Verified by Visa are both based on the 3D Secure protocol, which was developed by Visa to reduce fraudulent credit and debit card transactions online.

It works by forcing people to enter a password into a pop-up window, enabling the card issuer to confirm their identity before the transaction completes.

Retailers have been encouraged to adopt the protocol as it reduces the number of fraudulent chargebacks – money returned to the consumer from the merchant due to a fraudulent card transaction.

However, it is unpopular with online shoppers, because it requires them to use complex passwords that are easy to forget, and it can be difficult to tell whether the pop-ups are legitimate or fraudulent.

Static passwords are also inherently vulnerable, as they are repeatedly used for authentication and can often be discovered via social media or other means, rendering the consumer subject to fraudulent transactions.

A new invisible authentication system aims to tackle some of these issues by reducing the reliance on passwords as a means of verifying identity.

In the event that authentication is needed, cardholders will be able to identify themselves with the likes of one-time passwords or fingerprint biometrics, rather than committing static passwords to memory.

Mastercard is also piloting commercial tests for facial and voice recognition apps to authenticate cardholders, and conducting trials of a wristband which authenticates a cardholder through their unique cardiac rhythm.

“All of us want a payment experience that is safe as well as simple, not one or the other," said Ajay Bhalla, president of enterprise security solutions at MasterCard.

"We want to identify people for who they are, not what they remember. We have too many passwords to remember and this is creates extra problems for consumers and businesses."

The new protocol could be adopted in 2015 and will gradually replace the current 3D Secure protocol.