CA Viewpoint

Summary of 3D Secure 2.0 and How CA Can Help

EMVCo, the global technical body that manages security specifications for chip-based payment cards, is working on making advancements to the next generation of the 3D Secure protocol. EMVCo is collectively owned by American Express, Discover, JCB, MasterCard, UnionPay, Visa and is currently responsible for the developments of the EMV 3D Secure 2.0 (3DS 2.0) specification and associated certification program.

Understanding the Objectives of 3D Secure 2.0 and Actions That Must Be Taken

EMVCo's new development will utilize richer cardholder [and device] data during the transaction which will result in far fewer password interruptions as stated in this MasterCard press release. One of the biggest changes that cardholders will notice immediately is that the onerous registration process (seen in the traditional 3D Secure protocol) will be eliminated, providing a pleasant online shopping experience for online shoppers. As the card-not-present (CNP) and 3D Secure transaction volumes increase, the importance of a standardized and seamless customer experience has never been more important. According to the press releases by EMVCo, it can be concluded that 3DS 2.0 will aim to help make online shopping safer and more convenient for cardholders by removing the necessity of having to authenticate via static passwords, (EMVCo press release 2015).

The initial 3D Secure protocol, co-written by Visa and Arcot (now CA Technologies), enabled secure online shopping by providing "3 Domain" communication between the issuer, merchant and cardholder and facilitated an authentication dialog between the cardholder and the issuer. The primary goal then was to improve security for online shopping and 3D Secure delivered. Over time, transaction abandonment became an issue which made it clear that creating a better user experience for online shopping was necessary. Industry leaders, like CA Technologies, developed solutions that focused on improving the cardholder payment experience for 3D Secure transactions by doing a risk assessment of the transaction to help determine if it was initiated by the legitimate cardholder. If the transaction was low risk, authentication could be bypassed which helped reduce transaction abandonment.

Now, new consumer devices, such as smartphones and in-app purchases, have changed how consumers interact and shop online. These innovative technologies spawned the need to enhance the 3D Secure protocol in order to fully support and optimize them.

Objectives of 3D Secure 2.0

1. Support authentication based on data elements shared through the protocol with focus on a frictionless shopping experience for the cardholder.
2. Make the message interface and authentication flows amenable to mobile platforms (multi-device, device agnostic, multi-channel, etc.).
3. Make the technology future proof with support for digital wallets and other forms of digital payments.
4. Align to country specific and regulatory requirements.
5. Move from static authentication to dynamic authentication when necessary.

As a Technical Associate of EMVCo, CA Technologies is lending our experience to provide input and comment on the protocol as it's being developed. Being a Technical Associate provides CA the ability to adapt product offerings to fully support 3DS 2.0 from day one, providing issuers a seamless migration. In addition, once 3DS 2.0 becomes officially available, both versions of the protocol (3DS 1.x and 3DS 2.0) are said to run simultaneously, as stated publicly in EMVCo's press release. This is good news for issuers who are currently investing, or that have already invested, in the current version of the protocol as it will continue to be supported in the future.

One of the main highlights that came from the EMVCo announcement is that 3DS 2.0 provides additional data which will enhance the ability for risk-based authentication solutions to identify cardholder and device behavior. The fundamental premise of 3DS 2.0 is similar to our implementation of 3DS 1.0 with CA Risk Analytics—to use the additional authentication data elements that are available at the time of the transaction so that both the merchant and the issuer can make a more informed and precise decision as whether or not to complete or deny a card-not-present transaction. The data available includes transaction related information as well as details about the device being used for the transaction. CA Risk Analytics will also use this additional data in 3DS 2.0 to enhance the entire decisioning process.

How CA Technologies Payment Security Products Help Ease the Migration to 3DS 2.0

How can CA Technologies help when 3D Secure 2.0 is officially launched?

1. CA can help to improve and maintain the cardholder's online shopping experience across additional devices and form factors to reduce shopping cart abandonment.
2. CA can help simplify the use of additional available transaction data to add intelligence to our models and rules infrastructure, allowing cardholders to complete a majority of transactions without friction-filled authentication.
3. CA adds support for in-app purchases to satisfy the demand for a seamless mobile cardholder shopping experience.
4. CA can help to build the foundation for additional ID&V (Identity and Verification) flows outside of traditional online payment transactions, like wallet and mobile payment provisioning.

CA Technologies has been providing a zero-touch authentication experience for cardholders and has been delivering technology to accomplish that goal while simultaneously reducing the risk of fraud. The formulation of EMVCo by payment industry leaders embraces the need for a frictionless customer experience and the requirement for data and analytics to verify that the transactions are being made by genuine cardholders. CA Technologies is a Technical Associate[1] of EMVCo and supports its effort in introducing 3DS 2.0 to overcome the struggle consumers, merchants and issuers all face with online payment authentication.

CA Transaction Manager is designed specifically for issuers to reduce the risk of CNP fraud, protect cardholders and provide an uninterrupted, dynamic and personalized online shopping experience via a comprehensive implementation of 3D Secure™. By partnering with CA Technologies, issuers can be assured that our software will continue to work as desired even after the official launch of 3DS 2.0. CA possesses the expertise necessary to properly guide issuers through setting up successful rules and business policies for the best cardholder experience possible. Furthermore, issuers can expect CA to facilitate changes, if any, to the cardholder experience once the migration starts to 3DS 2.0.

The flexible software-as-a-service (SaaS) architecture facilitates integration with existing card issuer systems including home banking and other card not present (CNP) fraud management systems. It provides full 3DS compliance with Verified by VISA, MasterCard SecureCode, JCB J/Secure, American Express SafeKey and Discover/Diners ProtectBuy cardholder authentication programs.

CA Risk Analytics is a zero-touch authentication cloud service that uses advanced statistical predictive models and dynamic rules to assess the potential risk of each transaction and instantaneously deny, alert, allow or require additional authentication for each transaction appropriately. With the release of 3D Secure 2.0, a risk-based approach can be built directly into the protocol to simplify processes.

By partnering with CA Technologies, issuers can build a foundation that will open up the door to numerous authentication opportunities, including additional ID&V flows outside of traditional online payment transactions like wallet provisioning. For example, CA Risk Analytics can help utilize transaction data to add intelligence to the models and rules infrastructure, significantly reducing the friction-filled experience cardholders must endure during online transactions.

CA Strong Authentication for Payments provides simple, intuitive and dynamic authentication for scenarios where a cardholder cannot be accurately identified. In the event a transaction is deemed risky based on the richer set of data, convenient methods of strong authentication can be used to accurately identify the cardholder in real-time. CA Strong Authentication for Payments provides an alert for the cardholder to confirm their valid transaction via several mobile authentication options including push notifications, OTP via SMS/email and a mobile OTP app. Issuers have the freedom to choose whichever method of strong authentication they would like to employ, depending on what is necessary and practical for their cardholders.

What steps should be taken to prepare for 3D Secure 2.0?

As a leading provider of 3D Secure solutions, CA Technologies is the ideal partner to help issuers migrate to 3DS 2.0. With the current 3DS payment security solutions from CA Technologies, issuers can achieve a powerful CNP payments foundation, create a seamless customer experience as well as confidently prepare themselves for 3DS 2.0. In addition, CA will continue to support both the current and new 3DS protocols so that issuers can easily accept transactions from all merchants, regardless of which version of 3DS they are using. Here are some recommendations that should be considered when preparing for 3DS 2.0:

Prepare for a consistent customer journey. It is expected that 3D Secure 1.0 and 3D Secure 2.0 will run in parallel for some time. It is highly likely that cardholders will experience existing 3D Secure transaction flows at one merchant and 3DS 2.0 transaction flows at another merchant. It will be important for issuers to make a decision about how they can provide a consistent journey and a more seamless experience between the two transaction types. This is crucial given that issuers will not have control over the rate of 3DS 2.0 adoption. CA Technologies would recommend Issuers adopt a risk-based authentication solution for existing 3D Secure transactions. This will provide immediate benefits by optimizing the existing customer journey while providing a more consistent journey as more and more 3DS 2.0 transactions are seen in the real world.

Adopt an analytics driven approach to risk-based authentication. It is expected that 3DS 2.0 transactions will mandate a risk-based authentication approach. It is also expected that merchants will be afforded greater control in the authentication flow with the rate of challenge likely to be more closely scrutinized by both schemes and merchants. In addition, the risk-based decision will be based on a standardized and extended set of data elements. This will consequently increase the importance of using an analytics driven approach to risk-based authentication. CA Technologies recommends that issuers look for the highest granularity of control over the risk decision using the most sophisticated analytical techniques.

Adopt one-time-password methods for stronger authentication. Static or partial passwords are still prevalent in existing 3D Secure transactions. Due to the risk-based authentication approach that is expected in 3DS 2.0, issuers using static or partial passwords should consider the unlikelihood that cardholders will remember their passwords if these are only used for 3D Secure and are infrequently requested. This would lead to a far greater abandonment and failure rate. CA Technologies recommends issuers look to build their strategy for introducing stronger/one-time-password methods for authentication (OTP's delivered by SMS, two-way notification) and ideally rationalize the proposed method of authentication across banking channels. As issuers consider their authentication strategy for the bank's own platforms (mobile apps, online banking portals, etc.), it is also worth considering the need for stronger forms of authentication in other transaction types such as wallets.

CA can help with defining business policies and rules to ensure that the frictionless customer experience is maintained when migrating to 3DS 2.0. To learn more about CA Technologies payment security products, head to www.ca.com/payment-security or send an email to paymentsecurity@ca.com to connect with a product expert. CA Technologies customers can contact their account representative for a detailed assessment on how our payment security solutions can ease their specific migration to 3D Secure 2.0.

For more information, please visit **ca.com/payment-security**

1 Technical Associate - participation at this level enables organizations to provide input and receive feedback on detailed technical and operational issues connected to the EMV Specifications and related processes. Technical Associates engage with all nine of EMVCo's technical Working Groups to receive updates/provide input on their activities.

CS200-181828_0316