FEDERAL RESERVE BANK OF BOSTON™

Payment Strategies

BRIEF

Why 3-Domain Secure should be adopted in the U.S.

January 17, 2017

By Susan Pandy, Ph.D., Director, Payment Strategies

The broad adoption of smartphones in the U.S. and increased willingness of consumers to use their mobile phones to make e-commerce purchases has incented merchants to expand their online card-not-present (CNP)[1] businesses to the mobile channel.[2,3] At the same time, U.S. issuers and merchants are migrating to EMV chip cards at POS to reduce counterfeit card fraud, which is driving fraud to the less secure online and mobile channels. All of these factors together emphasize the need for stronger security controls to manage the growing CNP fraud. Tools exist today to address some CNP risks, particularly around authentication, which has been a long-standing primary challenge to the industry. This brief discusses the pros and cons of one tool – the 3-Domain Secure (3DS) authentication messaging protocol, comparing the initial 3DS version 1.0 to the new 3DS 2.0 version, and why the time is right for the U.S. issuers and merchants to adopt it.

What is 3-Domain Secure?

3-Domain Secure (1.0) was created fifteen years ago to accelerate the growth of e-commerce and reduce fraudulent use of credit and debit transactions by preventing unauthorized use of cards online. It requires issuers to authenticate cardholders using a PIN or password entered into a pop-up screen during an online purchase, removing the need for the user to enter his payment credentials directly on a merchant website. This additional layer of security also protects merchants from exposure to fraud-related chargebacks. Three major U.S. card networks support their own branded versions of 3DS, Visa *Verified by Visa*, MasterCard *SecureCode*, and American Express *SafeKey*.[4] The three domain structure supports the protocol that includes the merchant/acquirer domain, issuer domain, and interoperability domain.[5]

EMVCo developed the new version of 3DS (2.0), which it released in October 2016.[6] 3DS 2.0 is more robust than 3DS 1.0 and provides global interoperability and a consistent consumer experience across major e-commerce channels and connected devices, including mobile in-app purchases. 3DS 2.0 can function separately and in parallel with version 1.0, which Visa will continue to own but begin to phase out as 3DS 2.0 matures.

---

[1] Card-not-present payment occurs when a cardholder/card is not physically present when making a purchase, preventing the merchant from validating the cardholder as the card owner. Examples of CNP payments include internet (via mobile or PC/laptop), telephone, or mail order.

[2] For more information on mobile CNP fraud, see Crowe et al. (2016, Nov.) *Getting Ahead of the Curve: Assessing Card-Not-Present Fraud in the Mobile Payments Environment.* Available at https://www.bostonfed.org/publications/mobile-payments-industry-workgroup/getting-ahead-of-the-curve-assessing-card-not-present-fraud-in-the-mobile-payments-environment.aspx.

[3] Between 2011 and 2016, consumer use of the mobile browser to make online purchases doubled and the availability of mobile apps to make online purchases is adding to that trend. Javelin Strategy & Research. (2016, October.) *Mobile Online Retail Payments 2016*.

[4] JCB International also offers 3DS as *J/Secure.*

[5] The interoperability domain includes the Internet and interfaces to the access control server (ACS), merchant plug-in (MPI), or any other software provider. GPayments (2016, Nov. 29) *About 3D Secure 2.0 by EMVCo.* Retrieved from https://www.gpayments.com/About/3DSecure2.aspx.

[6] EMVCo (2016, Oct). *EMV 3-D Secure–Protocol and Core Functions Specification v2.0.0.* Available for download at https://www.emvco.com/specifications.aspx?id=299.

Challenges of 3DS 1.0

Adoption of 3-Domain Secure 1.0 in the U.S. was very low as it was not user-friendly; requiring merchant, cardholder, and card issuer to all participate in the authentication process. Consumers were required to enroll with a password, creating a negative shopping experience. The pop-up window often confused consumers because it was difficult to determine if it was the legitimate card network requesting authentication or a fraudulent phishing website. Furthermore, it interrupted every consumer online transaction with additional checks, requiring the consumer to authenticate for each transaction invoked by a merchant. This created customer friction and resulted in higher levels of shopping cart abandonment during checkout, which led to low merchant adoption of 3DS in the U.S., where it was not mandated.[7] Despite adoption of 3DS 1.0 in other countries (where it was mandated in some cases), there was a need to improve on the existing specification, which only supported cardholder authentication for online browser-based transactions, not newer CNP channels such as mobile in-app or mobile and digital wallets.

Benefits of 3DS 2.0

Online shopping continues to increase with the growth in smartphone adoption as more consumers make purchases via a mobile browser or a mobile app. Innovation in mobile technologies is driving the need to enhance the 3DS protocol in order to fully support and optimize these developments. With changes to how consumers pay online (e.g., mobile) and availability of other security tools such as payment tokenization,[8] the card networks looked at the overall shopping experience and tasked EMVCo[9] to develop the new, risk-based 3DS 2.0 version.

EMVCo's objectives for 3DS 2.0 were to: (1) reduce friction in the transaction process by providing better integration with a merchant's offering; (2) make authentication flows that accommodate all connected device purchases across mobile platforms (e.g., mobile in-app, non-browser based e-commerce transactions); (3) future proof the technology with support for digital wallets and other forms of digital payments; (4) align to country specific and regulatory requirements; (5) move from static authentication (passwords) to dynamic authentication (one-time passcodes (OTPs)) when necessary; (6) improve the challenge response process to avoid disruption of the merchant checkout experience; and (7) facilitate a cleaner experience without sacrificing security.

The 3DS 2.0 specification incorporates knowledge- and risk-based authentication (RBA) elements and delivers expanded capabilities in terms of technology, security (e.g., tokenization), performance, user experience, and flexibility. Merchants decide if stepped-up authentication (e.g., OTPs, biometrics, out-of-band authentication) is needed for a higher risk transaction; for example, a mobile device or laptop does not match one that the customer used before, and can invoke 3DS.[10] When a merchant invokes 3DS during online checkout, the purchase information, along with device data and other details, is sent to the issuer to authenticate the cardholder and confirm the purchase.[11] The issuer may passively authenticate the cardholder using RBA, or, based on the risk profile, use stepped-up authentication by asking the cardholder to either enter an OTP or respond to a customer service representative call.

---

[7] In 2013, only about 3 percent of U.S. merchants were using 3DS and currently, adoption is around 10 percent.[7] U.S. Congressional Research Service (n.d.). *The EMV chip card transition: Background, status, and issues for Congress.* Retrieved from https://www.fas.org/sgp/crs/misc/R43925.pdf.

[8] For more information on tokenization, see Crowe et al. (2015, June). *Is Payment Tokenization Ready for Primetime: Perspectives from Industry Stakeholders on the Tokenization Landscape?*

[9] EMVCo is a consortium that manages the security specifications for chip-based payment cards (EMV), including payments tokenization and advancements on the next generation of the 3DS protocol and related certification program. It is jointly owned by American Express, Discover, Visa, MasterCard, JCB, and Union Pay. EMVCo's mission is to facilitate the worldwide interoperability and acceptance of secure payment transactions by managing and evolving the EMV specifications and related testing processes.

[10] 3DS 2.0 risk engine will only challenge transactions that merchants deem medium to high risk.

[11] 3DS 2.0 allows issuers and merchants to exchange additional risk data, such as device ID and geolocation, at both the issuer identification and verification (ID&V) and transactional levels.

3DS 2.0 is more flexible than the original version because it can be customized for issuers as well as merchants. The goal is to enable merchants to have more control over when to invoke 3DS. However, issuers will maintain control of the authentication stream because they will still own the liability for all 3DS-initiated transactions that they approve. Merchants will supply more data (e.g., email address, mobile phone number, shipping, billing and IP addresses) to help issuers make authorization decisions. Merchant benefits from 3DS include reduced fraudulent transactions and a shift in fraud liability to the issuer, whether the issuer supports the 3DS request through risk assessment or stepped-up authentication prompts.

Conclusion

Since the 3DS 2.0 specification was only recently released, developers (payments technology providers, payment processors and gateways, etc.) need time to create and market solutions based on the new specification. For example, the 3DS protocol requires an Access Control Server (ACS) on the issuer side, which verifies whether a 3DS authentication is available for a particular primary account number (PAN), and manages cardholder authentication for a specific transaction. Most financial institutions outsource the ACS to third party providers.[12] Additionally, the card networks (Visa and MasterCard) do not allow merchants to send requests to their directory servers, but isolate the servers by licensing software providers known as merchant plug-ins (MPIs)[13] to perform this function.[14] Merchants and issuers will need to update their internal systems to support 3DS 2.0. In this way, the specification serves as a tool box to industry stakeholders that seek to develop and implement 3DS 2.0 compliant products and services that are globally interoperable and promote a unified international payments framework.

The enhanced 3DS 2.0 has many positive features. It recognizes newer payment channels that are increasing in popularity and addresses vital industry security concerns by incorporating a dynamic authentication system to keep up with the evolving threats. It also eliminates the earlier issues with adoption of 3DS 1.0 by making use of richer data and a risk-based approach that allows merchants to decide for each transaction whether passive or stepped-up authentication is needed. This process is designed to reduce fraud and mitigate disruption to the consumer shopping experience, shopping cart abandonment, and unauthorized chargebacks. And, if a transaction is fraudulent, liability rests with the issuer responsible for the 3DS authentication.

Consumer convenience increases with 3DS 2.0. When making CNP purchases they get improved security (without needing to remember passwords) and a seamless shopping experience that only requires further action by the consumer if the purchase is high risk or suspicious – a win-win.

Reducing shopping cart abandonment can increase revenue for both merchants and issuers. For the issuer, a positive experience using a card can make that card "top of wallet" for the customer. For the merchant, a positive customer experience is a priority for building customer loyalty and brand reputation.

Adoption trends are difficult to forecast, since the first, live transactions are not expected until mid to late 2017. Once we begin to see the growth of 3DS 2.0 transactions, we can begin to assess implementations, merchant integration, and evaluate the effect on consumer experience. In the meantime, the payments industry should embrace 3DS 2.0 as a welcome addition to enhancing the security of the mobile and digital commerce online payments environment, particularly as the CNP channel becomes a more likely target than the POS for fraud.

[12] Well-known ACS providers include: Arcot Systems, ACI Worldwide, GPayments, and SIA.
[13] A merchant plug-in is a software module that connects the card network and merchant servers.
[14] Visa keeps a full list of compliant software vendors including MPI and ACS providers.