FAQ

Visa 3-D Secure 2.0

Visa Confidential

OVERVIEW

- Over 15 years ago, Visa developed 3-D Secure (3DS) to provide merchants and issuers a way to authenticate the cardholder for eCommerce payments.
- EMVCo, in collaboration with Visa and industry stakeholders, updated the standard, which is referred to as 3-D Secure 2.0 (3DS 2.0). EMVCo released the specification in October 2016, with an updated version, 2.1.0, published in October 2017.
- 3DS 2.0 addresses industry concerns over poor user experience and shopping cart abandonment (i.e. friction from cardholders forgetting their static passwords or poor integration of the standard into the merchant shopping experience) associated with the original standard. The new specification focuses on a more seamless and integrated consumer experience across a variety of devices, including mobile and in-app.
- In addition, the new standard includes enhancements that promote greater data exchange between stakeholders to better manage fraud and maximize authenticated transactions. Enhanced data enables stronger risk-based authentication – issuers can be more confident in approving the transaction and request additional verification from the cardholder for only the riskiest transactions.
- Visa's 3-D Secure program governs how stakeholders use 3DS for Visa transactions. Among other rules and policies, the program provides merchants with fraud-related chargeback protection on eCommerce transactions, which takes effect on the applicable activation date by region.
- Visa is developing an updated program that will govern Visa transactions using 3DS 2.0. This program will have staged activation dates for different regions, with Europe starting on 12 April 2019, at which time the current Visa liability policy for 3DS 1.0 will extend to 3DS 2.0 transactions. Prior to the applicable activation date, only transactions where both the merchant *and* the issuer participate in 3DS 2.0 will be fully subject to the updated program, such as the liability shift rules.
- As the industry prepares for 3-D Secure 2.0 and as 3-D Secure solution providers are introducing certified solutions, merchants and issuers should work with their vendors to assess their current eCommerce authentication capabilities and identify migration opportunities.
- Clients working to enable 3-D Secure 2.0 should take advantage of the available data in 3DS 1.0 to perform risk-based authentication to prepare for the migration to 3DS 2.0.

- All clients need to enable risk-based or dynamic authentication to prepare for the removal of static passwords for 3-D Secure, starting from 14 April 2018.

Q&A

About 3-D Secure

1. **What is 3-D Secure?**

   Visa created the Three-Domain Secure (3-D Secure) messaging protocol in 1999 to give merchants and issuers a way to authenticate cardholders as they shop online. This additional layer of security helps prevent unauthorized use of cards and protects eCommerce merchants and issuers from exposure to fraud.

   The merchant, issuer, and the payment brand-governed 3-D Secure infrastructure comprise the "three domains". 3-D Secure 2.0 constitutes the same three domains as 3-D Secure 1.0, but with improved capability of authenticating a Cardholder during an electronic commerce (eCommerce) transaction or to provide identity verification and account confirmation.

2. **What is Visa's 3-D Secure Program? How does it work?**

   Visa's 3-D Secure Program is Visa's program that governs Visa transactions using the 3-D Secure standard. The program provides the rules and policies merchants and issuers must follow to invoke authentication for eCommerce transactions, enabling verification of the cardholder's identity before the transaction is sent for authorization.

   Additional information may be required from consumers to confirm identity. Historically, this was a password request. However, 3DS 2.0 authentication often works behind the scenes, with many issuers using risk-based authentication to evaluate transactions in real-time, so that additional cardholder verification is rarely needed.

3-D Secure Version 2.0

3. **What is 3-D Secure 2.0? How is it different from 3-D Secure 1.0?**

   When Visa first created the 3-D Secure standard, personal computers were the only channel available for consumers to shop online. Thus, the first version (3-D Secure 1.0) was designed for browser-based authentication. The rapid proliferation of mobile devices, such as smartphones, tablets, and other connected devices, has changed how consumers shop online. Furthermore, 3-D Secure 1.0 used static passwords to enroll customers into the service, which created a clumsy user experience that led to shopping cart abandonment as well as increased operational costs for issuers (due to customer calls requesting password resets). Pain-points such as these created demand for an enhanced version – 3-D Secure 2.0, which also provides the following incremental benefits:

- Flexible Device & Channel Support. Promotes a smoother and more consistent user-experience across multiple payment channels, including mobile web, in-app, and digital wallet payments.

- Improved User Experience. Gives merchants the capability to better integrate the authentication process into the shopping experience, providing cardholders with a fast, simple, and convenient authentication experience, while maintaining security.

- Enhanced Data Exchange to Manage Fraud and Reduce Friction. Opens additional data fields to enable enhanced risk-based authentication (RBA). When used effectively, risk-based authentication can provide protection against fraud, minimize cardholder friction, increase completed sales, and lead to a better experience for all stakeholders.

4. What is risk-based authentication?

Risk-based authentication, which is provided by Access Control Servers (ACS), is the evaluation of a transaction's risk profile that typically involves analyzing:

- Contextual data from the merchant
- Cardholder/merchant transaction history
- Transaction characteristics such as amount, device ID, and location

A risk score model and/or risk rules can be used to determine if:

- Authentication is successful
- Additional cardholder information is required
- Authentication failed

Risk-based authentication allows the issuers to authenticate its cardholders without asking for any additional information on the majority of the transactions, performing step-up authentication only on the riskiest transactions. Less than 5% of transactions are expected to be stepped-up for additional verification, such as a one-time-passcode. When used effectively, risk-based authentication can provide protection against fraud, increase completed sales, and lead to a better experience for all stakeholders.

5. Will 3-D Secure 2.0 remove the use of passwords from online authentication?

The 3-D Secure standard allows the issuer to authenticate the cardholder through a dedicated secure channel. The issuer will still have the flexibility to choose the method used to authenticate the cardholder through this secure channel.

To strengthen security and improve the consumer experience of 3-D Secure transactions, Visa eliminated the use of Verified by Visa-specific static passwords and its related enrollment processes beginning in 2018, unless required by regulatory mandates where applicable. This was announced in a VBN released in all regions except Europe on August 25, 2016, and in Europe on November 3, 2016.

Eliminating static passwords for VbV will drive the industry towards alternate forms of authentication, which is expected to improve the consumer experience and reduce shopping cart abandonment.

6. **Are any changes needed in authorization to support 3DS 2.0?**

Issuers can continue to use their existing CAVV keys as long as they are using the same ACS provider. Visa is requiring all Verified by Visa transactions to contain a Consumer Authentication Verification Value (CAVV) where the electronic commerce indicator (ECI) is one of the following:

- ECI 05 – Fully Authenticated Transaction
- ECI 06 – Attempted Authentication Transaction

Effective dates:
14 April 2018 - AP, Canada, LAC, and U.S.
13 October 2018 – CEMEA and Europe

Per these dates, acquirers must include the CAVV (Field 126.9) in the VisaNet authorization request when it is generated by an issuer's access control server (ACS) or attempts access control server (AACS) for a Verified by Visa transaction. Failure to do so will result in the ECI being reclassified to an ECI 07 in the VisaNet authorization system.

Additionally, Visa is providing an optional subfield, 3DS Indicator in field 126.20 (refer to VisaNet Business Enhancements published in December 2017). CAVV subfield values in Field 126.9 allow the issuer's 3DS 2.0 ACS and attempts server to include the 3DS 2.0 authentication method used in their CAVV. As a result, issuers can get this information from CAVV or the optional data field.

Visa 3-D Secure 2.0 Program

7. **When will Visa support 3-D Secure 2.0?**

Visa's 3DS 2.0 platform is now live and ready to process 3DS 2.0 authentication requests. Prior to participating in the 2.0 program, ACS and 3DS Server service providers must complete testing with both EMVCo and Visa. Providers may begin testing with Visa only after receiving a letter of approval that certifies successful completion of testing with EMVCo.

To ensure that stakeholders have a reasonable amount of time to implement 3-D Secure 2.0, the full set of program rules will not take effect until the program activation date as specified below:

- **April 2019:** Action date for Europe
- **August 2019:** Activation date for Canada, LAC, & US
- **April 2020:** Activation date for AP and CEMEA

8. **Will the Visa 3-D Secure 2.0 program provide the same rules and policies for 3-D Secure 2.0 as it does for 3-D Secure 1.0?**

   Merchants that authenticate transactions using 3-D Secure 1.0 are generally protected from issuer eCommerce fraud-related chargeback claims (chargeback reason codes 75 and 83) -- *market-specific program exceptions may apply*. This rule will fully extend to Visa 3-D Secure 2.0 transactions after the program activation date.

   - **Prior to the Visa 3-D Secure 2.0 program activation date**, merchants will not receive fraud-related chargeback protection for merchant-attempted 3-D Secure 2.0 authentication transactions (i.e. issuer BIN does not yet support 3-D Secure 2.0).

     Merchants will only receive fraud-related chargeback protection for issuer-authenticated 3-D Secure 2.0 transactions.
   - **As of the program activation date**, merchants will have fraud-related chargeback protection on merchant-attempted 3-D Secure 2.0 authentication transactions. Full program rules and policies, including pricing for Visa 3-D Secure 2.0, will be communicated later.
   - Merchants will continue to receive protection from issuer fraud-related chargeback claims for 3-D Secure 1.0 transactions.

9. **Will 3-D Secure 1.0 continue to be supported?**

   Visa will continue to own, manage, and support the 3-D Secure 1.0 specification, and will do so until a future sunset date is announced.

10. **When will 3-D Secure 2.0 implementation guides and rules be available to stakeholders?**

    The Visa 3-D Secure 2.0 Merchant/Acquirer Implementation Guide and the Visa 3-D Secure 2.0 Issuer Implementation Guide are available on VOL. These guides include additional rules governing the Visa 3-D Secure 2.0 program.

Impact to Stakeholders

11. **What are the impacts of 3-D Secure 2.0 to consumers?**

    Generally, a consumer will not know if authentication is conducted using 3-D Secure 1.0 or 3-D Secure 2.0. The new specification includes enhancements that seek to improve the consumer checkout experience by reducing friction for a more seamless checkout experience.

    Issuers should update existing risk models to take advantage of the additional data that 3-D Secure 2.0 messages provide, in order to improve decision-making.

    Merchants should: 1) Work on collecting and passing the additional data per specification and Visa's program rules, and 2) Integrate solutions into their mobile apps.

12. How will the specification be adopted by the payment systems and other payments stakeholders?

EMVCo is responsible for the development of the specifications and management of the testing platform for 3-D Secure 2.0.

Payment brands and vendors, including issuer access control server (ACS) providers[1] and merchant 3DS Server providers[2] will use the specifications to develop commercial products and services to meet market needs.

Vendors participating in the Visa 3-D Secure 2.0 program will perform Visa product testing with Visa for 3-D Secure 2.0, as with the 3-D Secure 1.0 protocol.

13. What will be Visa's role going forward for 3-D Secure 1.0? For 3-D Secure 2.0?

Working with EMVCo's other member-owners, Visa is contributing its knowledge and experience to develop and continuously enhance the EMV 3-D Secure specification version 2.0 for the benefit of the entire payments industry.

Visa will maintain sole ownership and management of the 3-D Secure version 1.0 specification. EMVCo owns the 3-D Secure version 2.0 specifications, which are available royalty-free. EMVCo is currently working to support the functional testing and certification of 3DS solutions to ensure compliance of the 3-D Secure 2.0 specification.

14. Will there be other versions of the 3-D Secure protocol from EMVCo?

EMVCo will continue to revise the 3-D Secure protocol based on technology advancement and market feedback. For the most up-to-date version of the specification, please refer to the EMVCo website.

15. Will Visa continue to test and approve 3-D Secure 1.0 products? If so, for how long?

There are no changes to the Verified by Visa compliance testing for 3-D Secure 1.0 at this time. Visa will continue to own, manage, and support the 3-D Secure 1.0 specification. Visa's existing 3-D Secure 1.0 testing and approval requirements and procedures will continue to apply.

16. How does 3-D Secure 2.0 impact existing users of Verified by Visa?

---

[1]Access Control Server (ACS) provider is the issuer server hardware/software entity that supports 3-D Secure 2.0 authentication and other functions. The issuer or the issuer's processor operates the ACS. The ACS verifies that the individual card account number is eligible for authentication, receives authentication requests from merchants, authenticates the cardholder during online purchases, and provides authentication response messages that are digitally signed.

[2]Merchant 3DS Server provider is the merchant software necessary to support 3-D Secure 2.0. Merchants may develop and implement their own 3DS Server or may obtain technology products and consulting services (including software integration into the merchant's commerce environment) from a technology provider.

Visa is committed to supporting the industry in transitioning from 3-D Secure 1.0 to 3-D Secure 2.0. Visa recommends that issuers and merchants support both specifications, as the two versions were designed to exist independently and be maintained in parallel, with no backwards compatibility.

Supporting both versions will ensure that stakeholders can initiate and respond to either authentication message version and maximize authenticated transactions.

Implementation

17. How can issuers and merchants participate in 3-D Secure 2.0?

Issuers will need an Access Control Server (ACS) to participate in 3DS. Merchants will need a 3DS Server (formerly known as Merchant Plugin, or MPI, for 3DS 1.0). There are several way issuers and merchants can obtain this software:

- Use a third-party hosted solution that minimizes infrastructure investment.
- Develop own software, which needs to be first certified by EMVCo and then tested with Visa, before it can be part of Visa's 3-D Secure 2.0 program.
- Purchase an ACS solution, in which case it should have already been certified by EMVCo. All you need to do is to come to Visa to test with Visa's 3-D Secure 2.0 program. A list of approved vendors will be available on the Visa Technology Partners website.

18. As an issuer, what do I need to do to implement 3-D Secure 2.0?

Issuers should consult their 3-D Secure solution providers for information on product availability.

Issuer development and implementation effort will vary depending on existing authentication capabilities:

- Issuers with existing risk-based authentication solutions will transition to 3-D Secure 2.0 by ingesting new data elements and optimizing risk-based models and rules.
- Issuers seeking to deploy a risk-based authentication approach but currently having limited risk-based capabilities, or currently relying on static authentication methods, will need to work with their ACS provider to prepare for a more significant upgrade effort.
- Issuers who already support 3DS 1.0 should:

  1. Register their BINs & URLs for the 3DS 2.0 platform with Visa
  2. Refer to the implementation guides to support field 126.9

3. Work with ACS providers to make sure 3DS 2.0 is supported, and set up rules that reflect updated policies to take advantage of the new and increased data sharing for improved decision-making

- Issuers who are new to 3-D Secure should:
  1. Work with an ACS provider
  2. Fill out the Client Information Questionnaire (CIQ) form to register BINS with URLs for the 2.0 platform.

19. As a merchant, what do I need to do to implement 3-D Secure 2.0?

Merchants and their providers will need to focus on several key areas for implementation:

- Integration of the mobile channel to support 3-D Secure
- Delivery of new data elements to strengthen authentication
- Management of coexisting 3-D secure message versions (1.0 and 2.0). Specifically:
  - Merchants already supporting 3-D Secure 1.0 will need to work with their 3DS server provider to make sure 2.0 is supported
  - Merchants new to 3-D Secure will need to work with a 3DS Server provider to ensure support for 3-D Secure 2.0

20. Can Visa help me select an issuer ACS or a merchant 3DS Server provider?

Yes, Visa offers an ACS service called VCAS through its subsidiary CardinalCommerce. CardinalCommerce serves merchants, acquirers, and issuers with authentication solutions that help to secure eCommerce transactions from fraud. Offering both a Merchant 3DS Server, previously known as a "merchant plug-in" (MPI), and an "access control server" (ACS), Visa and CardinalCommerce are able to connect merchants to issuers using 3-D Secure for all network brands.

Additionally, a list of Visa-approved service providers can be found on the Visa Technology Partner 3DS 2.0 Library page.

21. Does CyberSource offer a product for 3-D Secure 2.0?

CyberSource currently supports 3-D Secure 2.0 except where tokens are involved. For more information, contact your CyberSource representative.

22. Does Visa provide any pre-production test environment for merchants and issuers?

No, merchants and issuers should work with their 3DS server providers and ACS providers respectively to test before going into production.

23. Should clients continue to support 1.0 after implementing 2.0?

The 3-D Secure server determines which version of the protocol to use. The 3-D Secure server will know which issuer BINs support which version of the protocol. Some hosted 3DS server providers are doing this already based on which issuer BINs currently deploy risk-based authentication.

Prior to the Visa 3-D Secure 2.0's program activation date, the AACS (attempts access control server) will not be responding for non-participating BINs. The AACS will only respond for participating BINs as a backup in the rare case the issuer's 2.0 ACS is down due to technical difficulties.

Questions about interoperability with other products

24. How does 3-D Secure 2.0 work with Visa Token Service (VTS)?

3-D Secure 2.0 allows for interoperability with Visa Token Service. The Directory Server (DS) will map tokens back to the corresponding Primary Account Number (PAN). As a result, ACS providers and 3DS Server providers have minimal work to do to integrate with VTS.

25. How does 3-D Secure 2.0 impact VISA Checkout?

Visa Checkout is integrated with the 3DS Server solution offered by CardinalCommerce, so that Visa Checkout can enable 3DS 2.0 on behalf of the merchant for eCommerce transactions. Merchants should work with their 3DS Server providers to identify which transactions should be authenticated using 3-D Secure.

26. How do 3-D Secure and Visa Direct work together?

3DS can be used for the initial funds load, it cannot be used for the Original Credit Transaction (OCT).