EMVCo Publishes New Guidance for Merchants and Issuers on Using FIDO Authentication with EMV® 3-D Secure for Improved Online Payment Experiences

Whitepaper developed in collaboration with FIDO Alliance outlines how use of FIDO Authentication Data in 3DS messages can streamline e-commerce checkout while reducing friction for consumers

1. What is the purpose of the EMVCo 'Use of FIDO Data in 3DS Messages' white paper?

The white paper provides guidance to merchants and card issuers on how FIDO Authentication data can be used to attest that merchant-initiated strong consumer authentication has taken place prior to an EMV® 3DS transaction. This can reduce the need for issuers to authenticate cardholders for every transaction when shopping online and streamline processes for merchants and card issuers.

In many EMV 3DS transactions, the user journey begins with a merchant-initiated authentication. As this authentication precedes the EMV 3DS transaction, there is value in communicating details about the merchant-initiated authentication to the card issuer.

When merchants use strong authentication methods such as FIDO Authentication, the details regarding the authentication can be valuable to the issuer performing authentication of a cardholder for an EMV 3DS transaction. When applying 'risk based decisioning for the transaction, an issuer could leverage the data received about the cardholder or device via a merchant-initiated FIDO authentication. This could provide the issuer with enough data to increase the probability of a frictionless experience for the cardholder.

2. What value does this activity bring to the industry?

The 'Use of FIDO Data in 3DS Messages' white paper is the first guidance to the payment industry of how FIDO Authentication data can be used by issuers to analyse merchant-initiated FIDO authentication as part of their risk evaluations. The functionality to utilise FIDO authentication data with EMV 3DS was first introduced in the EMV 3DS Specification v2.1.0 in 2017.

A key element to the paper is the newly defined FIDO authenticator attestation data. Using this defined data set, merchants can deliver a structured set of data elements and present the card issuer with a consistent set of values for the same user or device along with other data they would receive as part of an EMV 3DS transaction, which reduces the need for repeated consumer authentication.

3. Is the inclusion of FIDO data a new addition to the EMV 3DS Specification?

No. The use of FIDO authentication data in EMV 3DS was first introduced in the EMV 3DS Specification v2.1.0 in 2017. The 'Use of FIDO Data in 3DS Messages' white paper is the first guidance to the payment industry of exactly how the data can be used by card issuers to analyse merchant-initiated FIDO authentication as part of their risk evaluations.

4. Why have EMVCo and FIDO Alliance established a Memorandum of Understanding (MOU)?

In 2016 EMVCo and FIDO Alliance announced they would collaborate to review how FIDO authentication standards can support EMV payment use cases. A key aim of the initiative was to investigate providing simpler and stronger authentication for cardholders making mobile payments using on-device authenticators, such as biometrics, thereby helping to reduce consumer fraud globally while maintaining a good consumer experience.

The collaboration was expanded in 2018 to define in detail how EMV 3DS messages may be used to pass FIDO authenticator attestation data and signatures in a manner that is both scalable and interoperable across the EMV payments ecosystem.

5. What future collaborative efforts do EMVCo and FIDO Alliance have planned in this area?

The use of FIDO Authentication data in EMV 3DS messages is the first of a number of use cases that EMVCo and FIDO Alliance have evaluated for collaboration opportunities. Additional future use cases include receiving additional data from FIDO authentications that issuers could cryptographically verify, and using FIDO Authentication as an EMV 3DS challenge method.

6. What are the key differences between the EMVCo white paper and FIDO Alliance technical brief?

The EMVCo white paper addresses this topic from the perspective of how EMV 3DS components can leverage the FIDO Authentication data to promote a frictionless payment process for consumers and help reduce fraud. The FIDO Alliance technical brief focuses on how FIDO servers and relying parties implementing this data set will be able to do so within the FIDO Alliance framework.

7. Will the use of FIDO Data in 3DS Messages compromise consumer's privacy?

No. The FIDO data that is contained in the 3DS Message is related to the device rather than to the individual user. For example, if a user logs into 'Merchant A' with their device from 'Manufacturer B', the issuer will receive data related to which device the consumer is using, but the FIDO data contains no personally identifying information.