IDENTITY & ACCESS FORUM

Powered by SECURE TECHNOLOGY ALLIANCE

AN IDENTITY & ACCESS FORUM WHITE PAPER

Device Identification and Authentication Methods for Payments

Version 1.0

Publication Date: July 2024

Identity & Access Forum
544 Hillside Road
Redwood City, CA 94062

www.securetechalliance.org

About the Identity and Access Forum

The Identity and Access Forum is a cooperative, cross-industry body dedicated to developing, advancing, and adopting secure identity technologies, including physical and logical access. Through the collaborative efforts of a diverse group of stakeholders, the Forum advocates for market adoption of trusted, user-centric, and interoperable digital identities to ensure safe and seamless access to services across all interactions. The organization operates within the Secure Technology Alliance, an association that encompasses all aspects of secure digital technologies.

Executive Summary

In today's connected environment, consumers use a variety of devices (e.g., computers, tablets, mobile phones) to transact online. The consistent and reliable identification of a consumer's device and association of that device to the legitimate consumer are key tools in creating a more secure environment for online commerce. For example, when an attempt is made to purchase from a device that has been previously used with a given merchant, and that device has a known track record of valid, approved transactions, the merchant may assign a high degree of confidence that the person attempting the purchase is truly the customer of record with the merchant. This white paper provides an overview of the data that can be collected to identify a device, the challenges of collecting that data, and methods for authenticating the consumer with EMV® 3-D Secure and network tokenization use cases.

EMV 3-D Secure (3DS) is an authentication model that leverages three domains to exchange device, transaction, and cardholder data and perform consumer authentication. The three domains are the merchant/acquirer domain, the issuer domain, and the interoperability domain. These domains exchange data and perform authentication through a set of request and response messages. The device data collected will depend on whether the transaction is performed using a browser or conducted in-app. In addition to the data collected, 3-D Secure also allows the issuer to present a challenge where the consumer may enter a one-time passcode, provide a biometric, or perform another form of authentication.

Approximately a dozen primary device data elements are collected for authentication performed in a browser, including a "Device ID."[1] However, the Device ID may not be consistent for all transactions with the same device. For example, if two merchants use different vendors, those vendors may generate different IDs for the same device. EMVCo has defined a set of over 150 data elements that can be collected for in-app authentication. The data elements collected will vary by operating system, and as there are multiple versions of the specification, the data elements collected can vary among implementations. Additionally, even when using the same device, the Device ID for browser-based transactions will differ from the Device ID for app-based transactions.

Network tokenization replaces a payment card's sensitive primary account number (PAN) with a surrogate value. The underlying PAN cannot be reverse engineered from the token as there is no mathematical or logical relationship between the PAN and the token. Multiple techniques (such as cryptogram validation and domain restrictions) are used in combination to prevent the provisioning of a token to, and the use of a token by, an unauthorized party. Issuer validation and approval can help ensure tokens are only provisioned for legitimate cardholders. Network tokenization supports a number of use cases such as device tokens, card-on-file tokens, and browser tokens. Similar to EMV 3DS, the device information that can be collected varies based on the use case, and may be limited to a few or even no data elements.

Beyond the challenges of collecting device and other transaction-related data, the payments ecosystem has challenges with sharing that data. Merchants, processors, acquirers, networks, and issuers all collect data, that while useful to the entity collecting the data, would have a much greater impact on detecting and deterring fraudulent activities if the data could be shared among all of the stakeholders.

[1] Device ID does not have one unique definition.

Contents

1. Introduction

Authenticating the true customer identity for card-not-present (CNP) transactions is more important than ever for stakeholders in the payment industry. Fraudsters are finding new ways to conduct online transactions through various phishing techniques. The reliable identification of a consumer's device and its association with the actual cardholder are two cornerstones of a more robust and secure card-not-present interaction. However, the industry currently lacks standard device information that can be shared across the payment ecosystem.

This white paper provides an overview of the device identification data that can be captured and used in today's market and frameworks for CNP transaction flows. Acquirers, processors, and payment networks will learn the device identification data fields that are generally available for both browser and in-app payment use cases. The paper also discusses the merchant and issuer challenges with gathering and exchanging device data and potential solutions to overcome those challenges.

2. Payment-Related Use Cases

Two of the methods currently used by the payments industry for device identification and consumer authentication are 3-D Secure and network tokenization. This section provides an overview of both methods, the data collected, and the process flows.

2.1 EMV 3-D Secure (3DS) Authentication

3-D Secure was originally introduced in 1999 as a method to authenticate CNP transactions in a growing digital world. Using a three-domain model (merchant/acquirer, issuer, interoperability), the exchange of transactional data elements and the ability to perform strong consumer authentication through a cardholder challenge strengthen CNP transaction security. In 2015, EMV 3DS was announced as the next generation of 3-D Secure. The EMV 3DS specification is a product of EMVCo through the efforts of its members and business and technical associates. In the years following the introduction of EMV 3DS, revisions have been introduced, addressing new use cases and device channels, additional authentication methods, and refined device parameters (see Section 5 below regarding device parameters).

As of 2023, the original 3-D Secure protocol has been sunset by all payment networks in favor of the EMV 3DS specification and its rich data set. A vital aspect of the EMV 3DS specification is the exchange of transactional data elements and the emphasis on device identification. Several message types and functions (including the initial authentication request and functions such as the 3DS Method) create a viable method for data exchange between the merchant/acquirer domain and the issuer domain, including the ability to profile a consumer's device.

2.1.1 Processing Flow

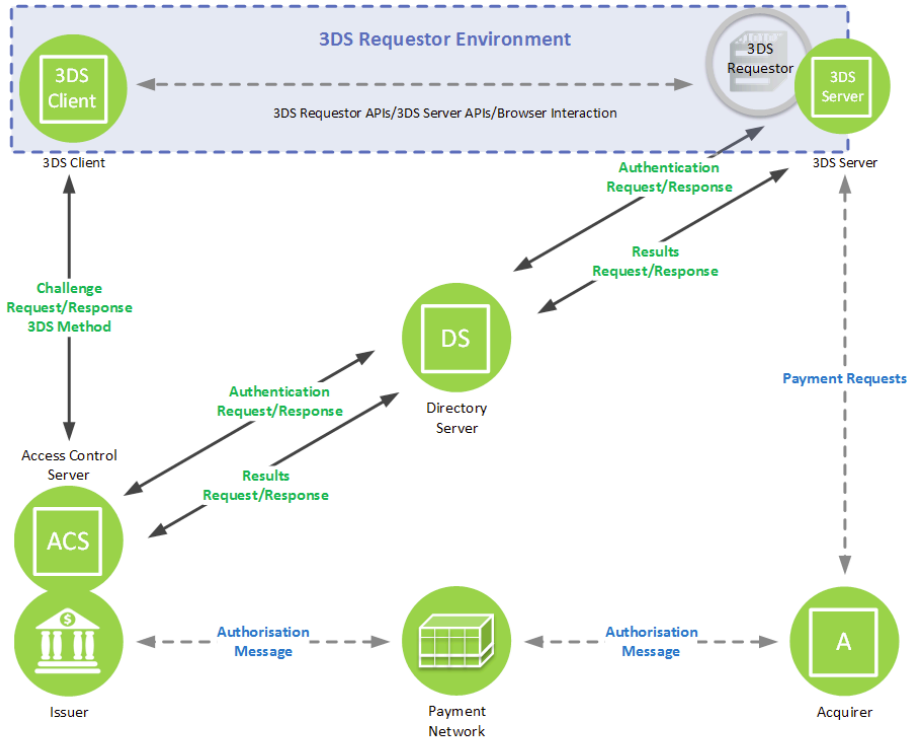
An EMV 3DS authentication is facilitated via multiple messages sent and received among the 3DS Server used by the merchant/acquirer, the directory server (DS) used by the payment network to provide interoperability, and the access control server (ACS) used by the issuer. Along with the messages being exchanged, several key integration points and data exchanges take place.

Table 1 describes EMV 3DS messages and Figure 1 illustrates the EMV 3DS message and process flow.

Table 1. EMV 3DS Messages

Message	Description	Parties
Preparation Request (PReq) and Preparation Response (PRes) messages	The 3DS Server requests card range information and the DS provides information on the supported card ranges for authentication and the applicable use cases.	3DS Server DS
Authentication Request (AReq) and Authentication Response (ARes) messages	The 3DS Server and 3DS software development kit (SDK) that collects and sends transactional data, device information and other data elements to the issuer via an ACS provider for risk assessment. The issuer ACS provider responds with authentication results or indicates that the cardholder must provide an additional proof of identity (i.e., step-up authentication)	3DS Server DS ACS

Message	Description	Parties
Challenge Request (CReq) and Challenge Response (CRes) messages	These messages provide the ability to prompt the cardholder for additional information for strong consumer authentication and to verify their identity through credentials on file.	3DS Server ACS
Results Request (RReq) and Results Response (RRes) messages	The ACS delivers the results of the authentication request to the merchant/acquirer domain. The 3DS Server responds by acknowledging receipt of the authentication results.	ACS DS 3DS Server



Note: Dashed arrows and 3DS Requestor are not part of 3DS specification and are shown for clarity only

Figure 1. EMV 3DS Domains, Components and Messages[2]

Prior to the authentication request, an initial device profiling step is executed. This profiling step will either be executed via the 3DS Method – an ACS/issuer-provided URL to be loaded within the browser – or via a mobile software development kit (SDK) embedded within the merchant's iOS™ or Android™ application. The device profiling will complement the authentication request and enable the issuer to accurately assess the risk of the request when authenticating the transaction.

For browser-based transactions, the 3DS Method URL implementation is defined by the EMVCo specification; however, the issuer's ACS provider defines the specific device data collection mechanism.

[2] EMVCo®, *Figure 1. EMV 3DS Domains, Components, and Messages*

The use of third-party device profiling scripts is likely, and the collected data is stored in the issuer environment.

The cardholder's issuing bank will determine the result of an EMV 3DS authentication. Using a risk model, the issuer will assess the cardholder's behavior against the current transaction and the device information. If prior shopping behavior and the current transaction appear low risk, the issuer will likely approve the authentication request, resulting in a frictionless shopping experience. The authentication request does not impact the cardholder, and the merchant can confidently continue processing the authorization.

If a transaction is deemed a moderate risk, the issuer may request a cardholder challenge (also referred to as step-up authentication). In this scenario, the cardholder will be presented with additional user interface prompts instructing them to complete the entry of a one-time passcode, biometric, or another form of authentication that the issuer has on file for that cardholder. This challenge will deter potential fraud and prevent merchants from accepting risky orders. If the risk is considered high, an issuer may fail the authentication result, indicating to the merchant to prompt for another form of payment or abandon the order altogether.

Figure 2 illustrates an approved transaction with EMV 3DS with a frictionless experience for the customers. Figure 3 shows a step-up authentication where the customer receives a one-time password challenge on their mobile phone.

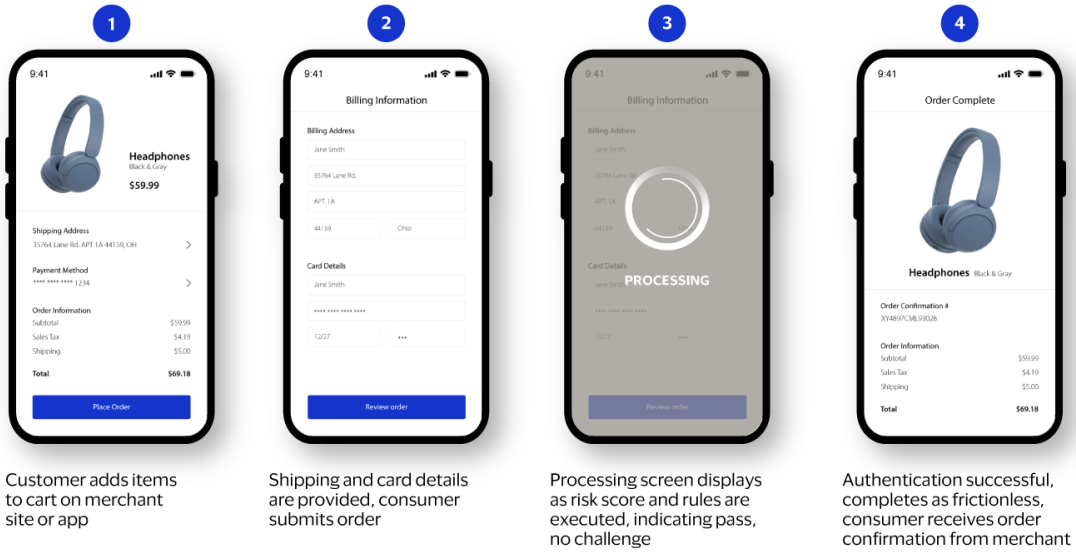


Figure 2. Frictionless Approved Transaction with EMV 3DS

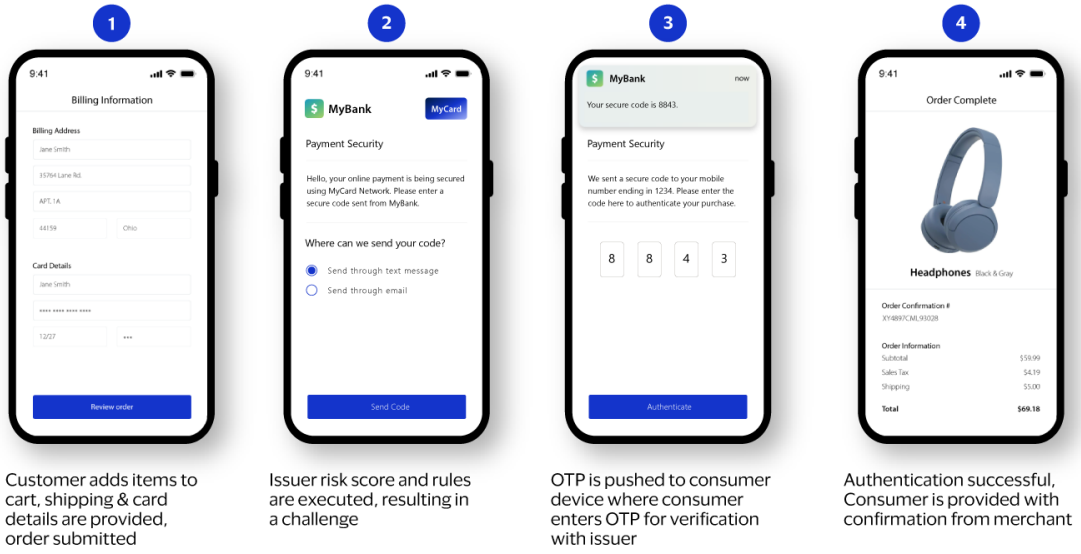


Figure 3. One-Time Passcode Challenge on Mobile Phone

2.1.2 Device Profiling Elements

In either the web (browser) or native app channel, a Device ID will be identified as part of the device profiling step. This Device ID is the primary element used to identify the consumer device; however, additional data elements are collected to inform the issuer risk decisioning.

In a web (browser) authentication, both required and conditional data elements may be collected.

- **Required (R) data elements**. Per EMVCo® 3DS Core Spec v.2.3.1.1, sender shall include the data element in the identified Message Type, Device Channel, and Message Category; recipient shall check for data element presence and validate data element contents.[3]
- **Conditional (C) data elements**. Per EMVCo® 3DS Core Spec v.2.3.1.1, sender shall include the data element in the identified Message Type if the conditional inclusion requirements are met; recipient shall check for data element presence and validate data element contents. When no data is to be sent for an optional data element (including a conditional data element that is not required based on the contents of the message), the data element should be absent.[4]

The primary device data elements collected are the following:

- Browser Accept Headers (R)
- Browser JavaScript Enabled (R)
- Browser User-Agent (R)

[3] EMVCo® 3DS Core Spec v.2.3.1.1

[4] EMVCo® 3DS Core Spec v.2.3.1.1

- Browser IP Address (C)
- Browser Java Enabled (C)
- Browser Language (C)
- Browser Screen Color Depth (C)
- Browser Screen Height (C)
- Browser Screen Width (C)
- Browser Time Zone (C)
- Browser User Device ID[5] (C)
- Browser User ID (C)

An important consideration is that Device IDs may not be consistent across all channels. A single merchant may use a vendor to generate and send a unique Device ID for a particular customer. The same device used at another merchant with a different vendor may generate a different Device ID. The entity performing risk-based analysis of transactions for these two merchants may perceive the two IDs differently, even though they represent the same device. The lack of consistency in Device IDs limits the ability of risk managers to identify, track, and manage device-specific fraud activity across the ecosystem.

In a native app authentication, EMVCo has defined over 150 datapoints that can be collected based on device and app permissions. The data points collected will vary by operating system (OS) and are only collected when the user (cardholder) has provided consent (when required). For the full list of data elements, refer to EMV® 3-D Secure SDK – Device Information.[6]

Note: Several versions of this specification are available; therefore, the collected device data points may vary.

2.1.2.1 Metrics

The rate at which the device data is successfully collected for a browser-based transaction will be dependent upon the successful completion of the 3DS Method. Per the EMVCo specification, this process should be granted up to ten seconds to complete as part of the consumer checkout. If there is any disruption to this process, device data may be only partially collected or fail to collect entirely. Even with the occasional connectivity service disruptions and the uniqueness of the user journey, collection of the Device ID and IP address has close to a 100 percent collection rate in scenarios where the 3DS Method completes.

In app-based transactions, with the 3DS SDK responsible for collecting the device data natively in-session, are reliable.

2.1.2.2 Privacy

The following types of permissions are required for collecting device identification parameters:

1. **No permissions required** – indicates that the 3DS SDK can directly collect the device parameters without user approval or system permissions.
2. **Installation-time permissions** – indicates that the collection of device parameters requires system permissions to be granted to the app during installation.

---

[5] The Device ID captured for a browser-based transaction will differ from a native mobile app-based transaction, even though the same device may be used. For example, a transaction completed via the mobile Safari® browser will register a different Device ID than a transaction from the merchant's native application on the same device.

[6] "EMV® 3-D Secure SDK – Device Information," Data Version 1.6, May 2023, EMVCo, https://www.emvco.com/specifications/emv-3-d-secure-sdk-device-information-5/.

3. **Run-time permissions** – indicates that the device parameters can be collected by the 3DS SDK only if the required permissions have already been granted to the app through user approval at run-time.

If permissions are not available for a given parameter, the 3DS SDK sends one of the following EMV Device Parameter Unavailability reason codes within the Device Not Available (DPNA) tag.

Table 2. ***Device Parameter Unavailability Reasons and Reason Codes***[7]

	Device Parameter Unavailability Reasons
Reason Code	**Description**
RE01	Market, regional or privacy restriction on the parameter.
RE02	Platform version does not support the parameter, or the parameter has been deprecated.
RE03	Parameter collection is not possible without prompting the user for permission.
RE04	Parameter value returned is null or blank.

2.1.2.3 Impacts

Authentication strategies will vary based on the issuer, accounting for regional regulations and mandates. If partial or incomplete device data is collected with an authentication request, it is more likely that an issuer will request a step-up challenge to verify the cardholder's identity, or the issuer may choose to fail authentication in extreme circumstances (e.g., regions where step-up is mandated). While device data plays a large role in the risk assessment of the request, other factors, such as the cardholder and transaction details, will also be used by the issuer to decide on the experience to provide to the consumer. For example, a high-ticket purchase with no device data may indicate a likely fraud scenario.

2.1.3 Conclusion

In summary, device-related data capture is not happening consistently, if at all, across all 3DS authentication requests. The lack of consistency is primarily due to a difference in the mechanisms used to collect device data today (e.g., browser- vs. application-based instances of 3DS, mobile OS-specific security policies). As a result, while Device ID can be a useful input for recognizing and authenticating a user for a specific instance (e.g., a specific browser within an OS), it cannot be used as a source of truth across different instances.

2.2 Network Tokenization

Tokenization substitutes a non-sensitive value that represents a card number, called a payment token, for the primary account number (PAN) in a financial transaction. The tokenization service is offered by a token service provider (TSP), typically a payment network, an acquirer, a third-party service provider, or an issuer.[8]

[7] Device Parameter Unavailability Reasons and Reason Codes, Cardinal

[8] "EMV Payment Tokenization Primer & Lessons Learned," U.S. Payments Forum, June 2019, https://www.uspaymentsforum.org/emv-payment-tokenization-primer-and-lessons-learned/.

Tokenization protects payment data using a combination of techniques, ensuring that an unauthorized party cannot mathematically reverse engineer the token value to obtain the original PAN or use a compromised token in an unauthorized environment. Techniques used to secure tokens are the following:

- **Domain Restriction**. A token's use is restricted to a single token requestor (identified by their Token Requestor ID or TRID.) The token service provider will reject an attempt to use the token in another domain.
- **Cryptogram Validation.** A dynamic security code specific to a particular transaction is generated and passed to the network to be decrypted and validated. The use of an invalid or expired cryptogram will be rejected by the token service provider or, in some instances, be passed on to the issuer with notice of the validation failure. (Note: Cryptogram validation only occurs on customer-initiated transactions. Recurring and subscription payments initiated by the token requestor do not carry a cryptogram.)

2.2.1 Token Verification

In addition to the standard security features offered by tokens, token ownership can also be verified to provide additional security – i.e., ensure that they are created and/or used by the right cardholder.

The verification of the token is performed by the issuer, with different use cases where the token service provider may request the issuer to verify that the token belongs to the legitimate owner of the account. Examples of when this may happen are the following:

1. At the time when a token is requested so that the token can be bound to the consumer device and/or can be activated for payments.
2. After a token was created, to establish a binding between the token and the consumer device.

In both use cases, the token service provider may share data and/or recommendations with the issuer. The issuer can then decide if the request can be approved without additional cardholder authentication or if a challenge is needed (e.g., one-time passcode, biometric, or another form of authentication) to confirm the identity of the cardholder.

The data shared during that interaction typically includes:

- Device binding data that can be used by the network and/or the issuer to associate the payment card to one or multiple consumer devices; and
- Consumer and device data collected from the merchant or the digital wallet, which allows the issuer to identify the cardholder and the cardholder's device.

2.2.1.1 Device Binding Data

Device binding data can be created from a "device-bound key" that is generated and stored within the secure environment of the consumer device, or from alternate mechanisms such as a browser cookie.

Examples of device-bound keys include the use of symmetric keys or a public key pair (where the private key does not leave the device). Device-bound keys are often used by native (merchant or wallet) applications and may be attested by the operating system. For web applications, the creation and use of device-bound keys are standardized with the FIDO Alliance Fast Identity Online (FIDO) industry specifications.[9] However, operating systems currently synchronize the FIDO keys (passkeys) across

[9] FIDO Alliance web site, https://fidoalliance.org/

devices and do not support an additional set of keys that do not leave the consumer device. It is anticipated that some operating systems may update their platforms in the near future to provide access to device-bound keys.

Networks may require merchant or wallet applications that are using device-binding data to go through a security evaluation process, for example through EMVCo,[10] before the binding data can be considered secure.

After a device-bound key is registered by the network and/or the issuer during the validation of the cardholder's identity, the key may then be used in each transaction to encrypt or sign a transaction counter or a random challenge. This process allows the network and/or the issuer to validate that the device used by the cardholder is the same device that was bound during the initial request.

2.2.1.2 Consumer/Device Data

Consumer and device data may be shared by the token requestor as part of individual network programs. The data is not standardized but may include a cardholder name, an email address, a device name, and/or a device IP address.

2.2.2 Transaction Approval

During the transaction, the possession of the device may be confirmed through network or issuer validation of device-bound data – for example, the validation of a signature generated by the device using a device-bound key during checkout. This validation can be used as a possession authentication factor. Another authentication factor such as biometric authentication can be performed in addition to the device possession validation in some use cases and/or some markets.

Individual network programs may also facilitate sharing consumer and device data to help the issuer with their risk decisioning.

A cardholder may be unaware of the existence of the token, and the use of the token in payments is mainly transparent.

[10] "Multi-Factor Authentication Solutions for Payments Security Requirements," Version 1.0, June 2023, EMVCo, https://www.emvco.com/resources/multi-factor-authentication-solutions-for-payments-security-requirements/

Table 3 summarizes the use cases currently supported by network tokenization.

Table 3. Network Tokenization Use Cases

Token Use Case	Example	Description	Device Information Capture
Device	Apple Pay® (secure element) Google Pay™, Samsung Pay™ (host card emulation)	Token stored on a device to make payments at the point of sale, or with a buy-button in-app and online.	Yes – Device Name/ID
Merchant Card-on-File	Netflix™	A token issued directly to a merchant from a token service provider.	May receive device name and IP address through participation in network authentication programs.
eCommerce/Payment Facilitator (PayFac)	Stripe™, Adyen™	A payment facilitator requests a token on behalf of a merchant from a token service provider.	May receive device name and IP address through participation in network authentication programs.
Browser	Safari®, Chrome OS™	A token used to replace card credentials stored within an internet browser application.	Yes – Device ID could still be unique for each individual merchant.
Cloud	Apple® MPAN	A subscription is initiated with a device token. The device token is then used to request a new token that the merchant uses to process subsequent transactions.	No

3. Device Identification and Payments: Challenges and Opportunities

Payments-related fraud is still prevalent in the e-commerce environment. Device ID-related data can be a useful tool to discern trusted activity from non-trusted payments activity, given the reliable association of a consumer's device(s) with a particular consumer.

However, there are two key challenges to leveraging Device ID-related information at scale within payments:

1. Consistent capture and/or validation of Device ID data elements
2. The sharing of Device ID-related data elements across the payments ecosystem

We do not believe that there is cross platform integration across the different operating systems or browsers to consistently solve for this first challenge. There is an opportunity for technology providers to set forth a solution for device identity to gain consistency.

To address the second challenge, data-sharing protocols across payments ecosystem players need to be adopted at scale. Networks can be uniquely situated to support this type of solution as they connect the information within a payment flow and have visibility to both the issuer and merchant side of the transaction. That information, if aggregated and anonymized, could be used to generate signals whenever use of a compromised device is suspected. When combined with better communication among stakeholders, this type of collaboration could lead to deeper engagement and greater innovation in the process.

4. Glossary: EMV 3-D Secure Terms

For Consumer Device Identification, as defined in EMV 3-D Secure SDK-Device Information Data Version 1.6, Section 2, EMV 3DS collects and provides to the 3DS Server either:

- **The Common Device Identification parameters available in all mobile platforms**
  - Please refer to Table 2.2 in section 2.5 of the specification to view the Common Device Parameters available on Android and iOS platforms.
- **Android-specific device parameters**
  - Please refer to Table 2.3 in section 2.6 of the specification to view the Android-specific device parameters that shall be collected by the 3DS SDK from the Android mobile platform for risk analysis by the ACS.
- **iOS-specific device parameters**
  - Please refer to Table 2.4 in section 2.7 of the specification to view the iOS-specific device parameters that shall be collected by the 3DS SDK from the iOS mobile platform for risk analysis by the ACS.
- **Platform provider-specific device parameters**
  - Please refer to Table 2.5 in section 2.8 of the specification to view the platform-specific device parameters that shall be collected by the 3DS SDK from the platform provider mobile platform for risk analysis by the ACS.

Note: The specification mentions that the availability of a higher number of device identification parameters improves the effectiveness of risk-based decision-making by the ACS. This, in turn, increases the probability of applying a frictionless flow.

5. Acknowledgements

Participants
Greg Aurre – FIS Global
Christopher Bohatka – Visa
Olha Bohun – FIME
Willis Clow – Bank of America
Steve Cole – Merchant Advisory Group
Scott Green – SHAZAM
Jonathan Grossar – Mastercard
Monica Gullickson – Best Buy
Michael Horne – American Express
Sue Koomen – American Express
Tim Mansfield – Truist
Edward Perez – Verifone
Suyash Somani – Visa
Jerrin Thomas – FIME
Henk van Dam – FIME
Hui Zhu – Visa

6. Legal Notice

The Identity & Access Forum endeavors to ensure, but cannot guarantee, that the information described in this document is accurate as of the publication date. This document is intended solely for the convenience of its readers, does not constitute legal advice, and should not be relied on for any purpose, whether legal, statutory, regulatory, contractual, or otherwise. All warranties of any kind are disclaimed, including but not limited to warranties regarding the accuracy, completeness, or adequacy of information herein. Merchants, issuers, and others considering Device Identification & Authentication technologies are strongly encouraged to consult with the relevant identity & access networks, vendors, and other stakeholders prior to implementation.