EMV® 3-D Secure Data Elements

February 12, 2019
U.S. Payments Forum Mission

• ... the cross-industry body focused on supporting the introduction and implementation of EMV and other new and emerging technologies that protect the security of, and enhance opportunities for payment transactions within the U.S.

Current EMV-related Topics and Issues
• Petro, Transit and Hospitality merchants EMV-enablement issues
• EMV contactless/mobile acceptance testing & certification
• Issuer considerations for contactless EMV (dual interface, offline data authentication)

Beyond EMV – Advanced Payments Topics and Issues
• Mobile payment and tokenization
• Authentication: biometrics, future of CVM, new signature requirements
• EMV 3-D Secure 2.0, Secure Remote Commerce and other CNP fraud tools
Forum Activities & Resources

- Collaboration on projects to develop resources to assist with U.S. EMV migration and implementation of other new and emerging payments technologies
  - White papers, educational resources
  - Best practices and technical recommendations

- Education programs for members and the industry
  - Webinars, workshops, Forum member meeting tutorials, published resources

- Communications
  - Market outreach with recommended best practices and industry positions

- Networking
  - Forum for industry stakeholders to interact with all payments industry stakeholders

Information and resources available at www.uspaymentsforum.org
Today’s Speakers

- Randy Vanderhoof, U.S. Payments Forum
- Kristy Cook, Target, U.S. Payments Forum Steering Committee Chair
- Michael Horne, American Express
- Ian Poole, CardinalCommerce
US Payments Forum: EMV 3DS Data Project

Goals
• Foster open discussion amongst merchants and issuers of new data elements in EMV 3DS
• Identify and share best practices to reduce gross fraud

Merchant & Issuer Prep Sessions

Merchant Focus: EMV 3DS data elements that have historically have indicated risk

Issuer Focus: generate questions for in-person discussion about the data elements and EMV 3DS

Guest attendance available for merchants and issuers interested in the discussion (email cmedich@uspaymentsforum.org)

Feb 12 Educational Webinar

Mar 11 In-Person Meeting
Phoenix, USPF
EMV® 3-D Secure Overview

Michael Horne, Sr. Product Manager, American Express
Remote commerce or e-commerce continues to grow worldwide. Payment transactions are occurring on various devices (e.g. mobile phones, tablets, PCs) where a high degree of e-commerce fraud can exist.

**EMV® 3-D Secure (3DS)**

Promotes an improved consumer experience when making e-commerce purchases by enabling intelligent risk-based decisioning.

- Allows for a rich data set to be exchanged between cardholder, merchant, and issuer
- Provides a secure communication channel between the cardholder, merchant, and issuer
- Enables issuers to authenticate their cardholder before transaction authorization
How It Works

3DS Authentication

Merchant

Is this the Cardholder?

The cardholder’s identity is verified by the issuer before the transaction is authorized

3DS enables the merchant and issuer to work together through the exchange of data to authenticate the cardholder’s identity before authorization occurs

Authorization

Issuer

The 3DS authentication improves the issuer’s confidence to authorize the transaction
What’s New

More Data Than Before
Additional data helps reduce friction during the authentication process.

Additional Device Channels
Smart devices including mobile phones, tablets, televisions, and wearables can now be enabled with 3DS. Merchant-initiated transactions are also supported.

Non-Payment Authentications
Identity verifications for card or token provisioning as well as account confirmations.

New Authentication Methods
Out-of-band and decoupled authentication methods to support more payment scenarios and checkout preferences.
Key Benefits

**Merchants**
- Enables merchants to integrate authentication into their checkout process for both app- and browser-based implementations
- Minimizes checkout abandonment during authentication
- Ability to perform merchant-initiated authentications
- Helps reduce potential for fraud-related chargebacks
- Improved authorization rates

**Consumers**
- Most authentications will be invisible to consumers
- Enhances online security
- Improved and consistent user experience

**Issuers**
- Reduces risk of fraud
- Richer data exchange enables less friction during authentications
- Supports new devices and channels
- Flexibility to support a variety of authentication methods
- Encourages cardholders to make purchases using their preferred medium

**More Data Than Before**
- Additional Device Channels
- Non-Payment Authentications
- New Authentication Methods
Additional data is provided by the merchant for inclusion in the Authentication Request message.

Issuer receives additional data and evaluates risk of the transaction. If the issuer determines the transaction to be low-risk and believes the transaction is legitimate, authentication may occur without cardholder interaction. Proof of authentication will be provided in the Authentication Response message.
Challenge Flow

1. Merchant w/ 3DS Server
2. Authentication Request
3. Authentication Response
4. Challenge Request/Response
5. Results Request/Response
6. Additional data is provided by the merchant for inclusion in the Authentication Request message.

Issuer receives additional data and evaluates risk of the transaction and determines a cardholder challenge is necessary.

Merchant, through its 3DS Server, proceeds with cardholder challenge and issuer authenticates cardholder.
EMV® 3-D Secure Data Elements

Ian Poole, Sr. Director, Global Product, CardinalCommerce
EMV® 3-D Secure Authentication Strategy
Moving towards dynamic, risk-based authentication

• Reduce false-declines while minimizing fraud loss

• Optimize the consumer experience
  – Mostly friction-free, introduction of biometrics, universal device usage

• Enable global interoperability
  – Regulatory smart for regional/country compliance

• Greater Data Exchange
  – Including non-payment, 3RI
More Data Shared between Stakeholders

<table>
<thead>
<tr>
<th>3DS 1.0 DATA</th>
<th>EMV 3DS DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquirer Merchant ID</td>
<td>3DS Requestor Name, Non-Payment Indicator, Prior transaction Authentication Information</td>
</tr>
<tr>
<td>DS URL</td>
<td>Cardholder Account Information (account age, password change, number of transactions per day/year, shipping name indicator, suspicious activity, payment account age, etc)</td>
</tr>
<tr>
<td>Message, Extension, Version</td>
<td>Merchant Risk Indicator (Delivery Timeframe, Re-Order, Pre-Order, Gift Card)</td>
</tr>
<tr>
<td>Browser User-Agent</td>
<td>Browser User-Agent</td>
</tr>
<tr>
<td>Acquirer BIN</td>
<td>Message Category, Extension, Type, Version</td>
</tr>
<tr>
<td>Cardholder Account Number</td>
<td>Purchase Date &amp; Time</td>
</tr>
<tr>
<td>DV URL</td>
<td>Cardholder Account Identifier</td>
</tr>
<tr>
<td>Acquirer BIN</td>
<td>Acquirer BIN</td>
</tr>
<tr>
<td>Cardholder Email Address</td>
<td>3DS Requestor URL</td>
</tr>
<tr>
<td>Home Phone Number</td>
<td>EMV Payment Token Indicator</td>
</tr>
<tr>
<td>Mobile Phone Number</td>
<td>SDK Reference Number, SDK Transaction ID</td>
</tr>
<tr>
<td>Work Phone Number</td>
<td>Installment Payment Data</td>
</tr>
<tr>
<td>Recurring Expiry, Frequency</td>
<td>Purchase Amount, Currency, Date &amp; Time</td>
</tr>
<tr>
<td>Merchant Category Code</td>
<td></td>
</tr>
<tr>
<td>Cardholder Shipping Address</td>
<td></td>
</tr>
<tr>
<td>Billing Address</td>
<td></td>
</tr>
<tr>
<td>Merchant Category Code</td>
<td></td>
</tr>
<tr>
<td>Merchant Risk Indicator</td>
<td></td>
</tr>
<tr>
<td>Address Match Indicator</td>
<td></td>
</tr>
<tr>
<td>Transaction Type</td>
<td></td>
</tr>
<tr>
<td>Device Channel, Device</td>
<td></td>
</tr>
<tr>
<td>Information, Rendering</td>
<td></td>
</tr>
<tr>
<td>Options Supported</td>
<td></td>
</tr>
<tr>
<td>Merchant Risk Indicator</td>
<td></td>
</tr>
<tr>
<td>Transaction Type</td>
<td></td>
</tr>
<tr>
<td>3DS Server Reference Number</td>
<td></td>
</tr>
<tr>
<td>Operator ID, Transaction ID,</td>
<td></td>
</tr>
<tr>
<td>URL</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td></td>
</tr>
<tr>
<td>Merchant Name</td>
<td></td>
</tr>
<tr>
<td>Browser Time Zone</td>
<td></td>
</tr>
<tr>
<td>Cardholder Name</td>
<td></td>
</tr>
<tr>
<td>3DS Requestor Authentication Information (Methods, Challenge Indicator, ID, Initiated Indicator)</td>
<td></td>
</tr>
</tbody>
</table>
4 Types of Data

1. Transaction & Consumer Data
2. Authentication Data
3. Merchant Data
4. Device Data
<table>
<thead>
<tr>
<th>Data Type</th>
<th>Data Description</th>
<th>Data Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction &amp; Checkout Page Data</td>
<td>• Contains required or conditional information gathered from the cardholder’s checkout process with the merchant and transaction elements</td>
<td>Required / Conditional</td>
</tr>
<tr>
<td>Authentication Data</td>
<td>Authentication Data</td>
<td>Optional</td>
</tr>
<tr>
<td>Merchant Authentication</td>
<td>• Pertains to the use of non-3DS authentication which may be used in order for the cardholder to gain access to the merchant website, account or card on file details</td>
<td></td>
</tr>
<tr>
<td>Prior Authentication:</td>
<td>• Is data elements gathered to present on a new transaction, from an existing transaction with the same cardholder and PAN where EMV 3DS was applied</td>
<td></td>
</tr>
<tr>
<td>Merchant Data</td>
<td>Merchant Data</td>
<td>Optional</td>
</tr>
<tr>
<td>Merchant Risk Info:</td>
<td>• Data that only the merchant would be able to verify based on the current order details and utilized for risk analysis</td>
<td></td>
</tr>
<tr>
<td>Cardholder Account Info:</td>
<td>• Merchant specific account information on the cardholder related to the history or details of their account</td>
<td></td>
</tr>
<tr>
<td>Device Data</td>
<td>• Specific device information per channel like Native App iOS vs Native App Android, vs Browser</td>
<td>Required / Conditional</td>
</tr>
</tbody>
</table>
Transaction & Checkout Page Information

*Action: Required*

**Cardholder Info**
- Account Number & Expiration Date
- Billing: Address, City, Postal Code, State, Email, Mobile Phone, Cardholder Name
- Shipping: Address, City, Country, Postal Code, State

**Merchant Info**
- Merchant Name, URL, Country, MCC, Acquiring BIN/MID, 3DS Network Identifier

**Transaction Info**
- Amount, Currency Code Transaction Type

**Device Info**
- **Device Channel** (App, BRW, 3RI), **Browser**: Header, IP Address, Java Enabled, Language, Color Depth, Screen Height, Screen Width, Time Zone, User Agent, **App**: SDK Encrypted Data
Merchant Authentication:
Merchants can convey to the issuer whether the cardholder logged in successfully or not to the merchant site, to help the issuer with their risk decision.

- No authentication occurred – Guest Checkout
- Login using Merchant system credentials
- Login using Federated ID
- Login using FIDO authenticator

Date & Time when the authentication occurred on the merchant’s site

Any data to document specifics of the authentication process that previously occurred
Authentication Data (cont’d)

Prior Authentication:
Passing previous EMV 3DS authentication that occurred on a cardholder transaction

Authentication Method

- Frictionless authentication occurred
- Cardholder challenge occurred by ACS

Authentication Date

- Date & Time when the prior EMV 3DS authentication occurred on the merchant’s site

Authentication Data

- Any data to document specifics of the authentication process that previously occurred
- ACS Transaction ID to link the prior authentication
Merchant Data

Merchants can provide their own risk identifiers that can improve the scoring of a transaction with an issuer. Sharing this data frequently can build or validate consumer buying patterns leading to more frictionless authentication opportunities.

**Shipping & Delivery**
- Ship Method Indicator
  - Ship to billing address, ship to another verified address on file, Ship to address different from Billing, Ship to store
- Delivery Email
- Delivery Timeframe
  - Electronic Delivery, Same day shipping, Overnight shipping, Two or more day shipping
- Amount, Currency, Count

**Pre-Order/Re-Order**
- Merchandise available, Future availability
- First time order, Reordered product

**Gift Card**
- Action: Optional
Merchant Data (cont’d)

Cardholder Account Info:
Merchants have the unique ability to collect data based on their historical relationship with the cardholder and their account at the merchant.

Account Standing

- Account Age Indicator
- Account Creation Date
- Account Change Indicator, Change Date
- Account Password Change, Indicator, Date
- Ship Name Indicator
- Payment Account Indicator and Age

Shipping Usage

- Shipping Address usage & date
  - When address was first used

Transaction Counts

- Number of transactions within the last 48hrs
- Amount, Currency Code, Count

Fraud Activity

- Suspicious activity on account
- Account purchases and Add-Card attempts
Device Data

**Browser-based**

Device Channel (App, BRW, 3RI), Browser: Header, IP Address, Java Enabled, Language, Color Depth, Screen Height, Screen Width, Time Zone, User Agent, App: SDK Encrypted Data

**Native App-based**

**Common:** Platform, Device Model, OS Name, OS Version, Locale, Time zone, Advertising Id, Screen Resolution, Device Name, IP Address, Latitude, Longitude

- **iOS:** 10+ fields like Family Names, System Font, Label Font Size, System Locale, Preferred Languages
- **Android:** 100+ fields like Subscriber Id, IMEI, Device Id, Network Country Code

Note: All brand names and logos are the property of their respective owners, are used for identification purposes only, and do not imply product endorsement or affiliation with Visa.
## Data Category Recap

<table>
<thead>
<tr>
<th>DATA TYPE</th>
<th>DATA REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction &amp; Checkout Page</td>
<td>Required / Conditional</td>
</tr>
<tr>
<td>Information</td>
<td></td>
</tr>
<tr>
<td>Authentication Data</td>
<td>Optional</td>
</tr>
<tr>
<td>Merchant Data</td>
<td>Optional</td>
</tr>
<tr>
<td>Device Data</td>
<td>Required / Conditional</td>
</tr>
</tbody>
</table>
Imagine how powerful ...

... if these data were shared
Q&A
• **U.S. Payments Forum EMV 3DS Data Elements Project**
  – If you’d like to participate in the project, contact Cathy Medich, cmedich@uspaymentsforum.org

• **March U.S. Payments Forum Member Meeting and 2019 Payments Summit**, Mar. 11-14, Phoenix, AZ
  – Mar. 11-13 – **Forum Member Meeting**: roundtables, SIGs, working committee and birds-of-a-feather sessions
  – Mar. 12-14 – **2019 Payments Summit**: multiple tracks covering all things payments, including FinTech, EMV chip technology, mobile wallets, NFC, contactless, open transit systems and more

• Other resources available at: [www.uspaymentsforum.org](http://www.uspaymentsforum.org)
Randy Vanderhoof, rvanderhoof@uspaymentsforum.org
Kristy Cook, kristy.cook@target.com
Michael Horne, michael.horne@aexp.com
Ian Poole, ipoole@cardinalcommerce.com
Cathy Medich, cmedich@uspaymentsforum.org

www.uspaymentsforum.org