EMV® 3-D Secure

Version 1.0

Publication Date: March 2020

U.S. Payments Forum
191 Clarksville Road
Princeton Junction, NJ 08550

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum is a cross-industry body focused on supporting the introduction and implementation of EMV chip and other new and emerging technologies that protect the security of, and enhance opportunities for payment transactions within the United States. The Forum is the only non-profit organization whose membership includes the entire payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on, and have a voice in the future of the U.S. payments industry. Additional information can be found at http://www.uspaymentsforum.org.

EMV® is a registered trademark of EMVCo, LLC in the United States and other countries around the world.

Comments or recommendations for edits or additions to this document should be submitted to: info@uspaymentsforum.org.

Table of Contents

1. Introduction

Over the past three years, the buzz in the card-not-present (CNP) payments industry has been about the new EMV® 3-D Secure (3DS) protocols. However, the market may not be fully aware of exactly what EMV 3DS is and how it can help reduce fraud in the payments ecosystem. This U.S. Payments Forum white paper describes the differences between EMV 3DS and previous 3DS versions, discusses the new EMV 3DS features, and provides an overview of the data and transaction process.[1]

1.1 3DS Protocol Timeline

The original protocol was developed and owned by Visa Inc. and licensed to other major payment networks including American Express (SafeKey), Discover and Diners Club (ProtectBuy), JCB (J/Secure) and Mastercard (SecureCode). Each network created 3DS programs with the same goals: to reduce fraud within the ecosystem, and to let the issuer validate the cardholder during web-based transactions. 3-D Secure 1.0.2 has been used in the payments industry for nearly 20 years and widely adopted internationally for regulated markets which require two-factor authentication.[2]

In the early 2000s, technology was limited; the online payments industry was new, high-speed Internet service was not widely available, and smart phones did not exist yet. While the capabilities of the original version of 3DS were limited to browser-based transactions with a minimal data set, it was instrumental in helping to blaze the trail and define a far more integrated solution that can be implemented with the new EMV 3-D Secure protocol.

EMV 3DS is a work product of EMVCo, and was first announced in 2015. Over the years, EMVCo has been instrumental in creating specifications supporting interoperability, flexibility and payment acceptance across the globe for many of the solutions used today, including chip cards, contactless payments, tokenization, QR codes, Secure Remote Commerce (for digital wallet providers), as well as 3DS. EMVCo's solutions are influenced and steered by the global payment networks including American Express, Discover, JCB, Mastercard, UnionPay and Visa, with input from business and technical associates. Additional information is available on the EMVCo web site.[3]

The latest version of EMV 3DS that is currently in production is 2.1.0. The specification for this version was released in November 2017, and since then, EMVCo released version 2.2.0 in December 2018. Figure 1 illustrates the typical cycle and steps for releasing a new specification version into production. The timeline for this cycle can vary and may be different based on the solution provider the issuer or merchant used for 3DS, or even the payment network and the management of version support for their program.

Although EMVCo can include new functionality and feature support in a specification, the payment network decides when and how long a version will be supported in their 3DS program, along with any compliance announcements. Solution providers control when their documentation and support are available, which may be released before or after version certification with EMVCo as well as network

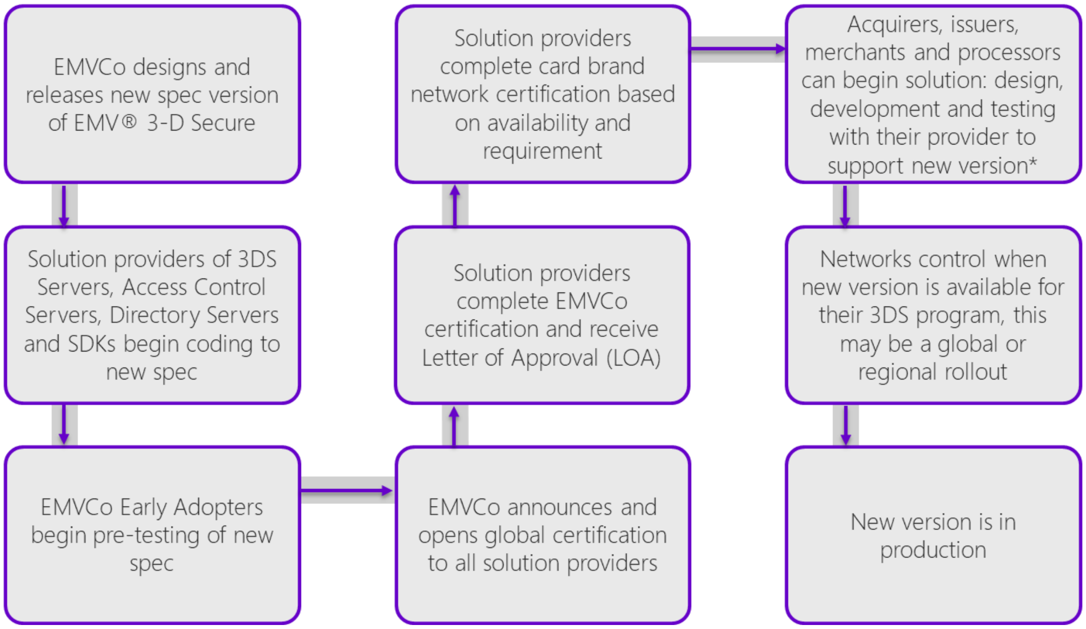
[1] Additional information can also be found U.S. Payments Forum webinar recording, "EMV 3-D Secure Data Elements," available at https://www.uspaymentsforum.org/emv-3-d-secure-data-elements-webinar/.

[2] For the purposes of this white paper, regulated markets are those that have a law by a governing body/entity, or the payment networks have specifically required "3DS," Strong Customer Authentication (SCA, PSD2), or 2 Factor Authentication (2FA), to process authorizations for approval. The EU is a regulated market by this definition; the U.S. is a non-regulated market.

[3] http://www.emvco.com

certification. Specific cycles of version availability by network should be discussed with the chosen 3DS solution provider to help merchants and issuers analyze the development and support impact to their business.

Figure 1. Typical Cycle for Releasing a New Version of EMV 3DS[4]


EMVCo designs and releases new spec version of EMV® 3-D Secure
Solution providers of 3DS Servers, Access Control Servers, Directory Servers and SDKs begin coding to new spec
EMVCo Early Adopters begin pre-testing of new spec
EMVCo announces and opens global certification to all solution providers
Solution providers complete EMVCo certification and receive Letter of Approval (LOA)
Solution providers complete card brand network certification based on availability and requirement
Acquirers, issuers, merchants and processors can begin solution: design, development and testing with their provider to support new version*
Networks control when new version is available for their 3DS program, this may be a global or regional rollout
New version is in production

1.2 EMV 3-D Secure Network Programs

Six payment networks already support 3DS 1.0.2: American Express, Discover, Diners Club, JCB, Mastercard and Visa. With EMV 3DS, new networks implementing 3DS programs for their credit and debit cards include: Cartes Bancaires in France, for support of PSD2 initiatives and local processing (Fast'R); ELO (ELO 3DS 2.0) in Brazil, who currently has point-of-sale acceptance and is adding CNP support; and Union Pay International (UnionPay 3DS), which is expanding services.

1.2.1 EMV 3DS Programs and Payments Ecosystem Benefits

While EMVCo protocol specifications set requirements for interoperability, payment networks create program rules that inform acquirers, issuers, merchants and processors on how to operate the EMV 3DS protocol for their specific network, when new versions are available, and what benefits EMV 3DS brings to the payments ecosystem.

Networks offer an added program benefit for merchants implementing EMV 3DS – a liability shift on fraudulently reported chargebacks. When EMV 3DS authentication is applied to a CNP transaction and that transaction results in a chargeback reason code related to fraud, the liability is shifted from the merchant (where it resides today) to the card issuer. Each network has its own program operating rules and procedures; actual use case scenarios relating to liability shift vary. Merchants and issuers are advised to contact their acquirers, processors or payment networks for additional information.

By securing remote commerce with EMV 3DS authentication, higher authorization approvals may also result, since the issuer is able to see the transaction before it comes for authorization. Each network

[4] Source: CardinalCommerce

may have different statistics on authorization approvals, and they can vary by region, country, or even merchant category code or vertical. However, improving card approval rates and avoiding false declines for remote commerce are goals that benefit everyone, including the consumer.

In the U.S., payment networks anticipate that over 90 percent of authentication requests may result in a frictionless experience for the consumer and can be attributed to risk-based authentication application by the Access Control Server. Payment networks anticipate a challenge and issuer engagement with the cardholder to be less than 10 percent of the time.[5]

As EMV 3DS expands and is adopted in the United States and across the globe, additional statistics will surface as issuers gain valuable insight into the transactions, based upon the 135-plus data elements that are used with EMV 3DS. Through network support, issuers are provided with dynamic linking capabilities to match authentication and authorization requests together, which can help an issuer determine what happened in authentication and then use this information to improve authorizations.

As of the publication of this white paper, all networks are supporting transactions for EMV 3DS. Additional information on EMVCo-approved/evaluated EMV 3DS products can be found on the EMVCo website.[6]

1.2.2 Other EMV 3DS Benefits

While the past 20 years of 3DS history solely focused on payment transactions for CNP, EMV 3DS will continue to provide new use cases. With EMVCo owning and delivering new versions regularly, merchants and issuers are encouraged to regularly review updates and new capabilities.

Providing the ability for a merchant or issuer to engage in active authentication with the cardholder during a non-payment transaction request will widen the scope of transactions where validating the consumer is just as important as when they are attempting to purchase. A common use case where non-payment requests are initiated is for account verification, card-add, and stored card scenarios. This type of request to an issuer will result in active authentication or challenge to the consumer before the action is completed.

Later, this paper discusses the expanded data that the protocol supports; these fields have values which help issuers identify transaction details on a granular level. Another use case that improves merchant-to-issuer transaction visibility occurs during recurring, installment, or split-shipment transactions. These added capabilities notify an issuer that the cardholder is present to initiate the transaction, but may not be present for subsequent transactions.

To obtain details of specific use cases and how the new EMVCo fields and values are used within EMV 3DS programs, please refer to the network program guides or contact the network or acquirer.

[5] "Mastercard Identity Check Program Guide," November 2019.

[6] https://www.emvco.com/approved-registered/approved-products/

2. EMV 3-D Secure

EMV 3DS is a messaging protocol that enables consumers to authenticate themselves with their issuer when making CNP purchases.

This section discusses the following topics:

- EMV 3DS terminology and its differences from 3DS 1.0.2
- Major EMV 3DS improvement themes
- The EMV 3DS transaction flow

2.1 Terminology

EMV 3DS terminology is different from that used with 3DS 1.0.2. **Table 1**, **Table 2**, and **Table 3** list definitions of important EMV 3DS terms used in this white paper.

Table 1. Naming Conventions of Technology

EMV 3-D Secure (EMV 3DS)	The new protocol owned by EMVCo which will be version-controlled as technology advancements occur. Versions 2.1.0 and 2.2.0 have been implemented in production today by all major payment networks.
Access Control Server (ACS)	Technology solution provider which allows issuers and processors to deploy a 3DS program for their cardholders. This service may be on premise or hosted, and receives authentication messages, prompting an action and response. Before being used in production, the ACS could be certified by EMVCo, PCI, and every network it supports for each version of EMV 3DS.
3DS Server (3DSS)	Formerly known as the merchant plug-in (MPI), this technology solution provider supports acquirer and merchant implementation of 3DS programs from payment networks. Before being used in production, the 3DSS could be certified by EMVCo, PCI, and every network it supports for each version of EMV 3DS.
3DS SDK (Software Development Kits)	Technology solution provider or platform which provides merchants with the ability to deploy authentication within a native mobile application environment. Before being used in production, the 3DS SDK could be certified by EMVCo, PCI, and every network it supports for each version of EMV 3DS.
Directory Server (DS)	Server that controls the routing of an authentication request to the proper ACS. The DS may also "stand-in" for authentication when an ACS has downtime or if issuers are not yet enabled with EMV 3DS. The DS also supports the PReq/PRes messages, informing the 3DSS of issuer BIN enablement.

Table 2. Request and Response Messages

Preparation Message (PReq/PRes)	A preparation message is typically performed daily between the 3DSS and the network DS. The response from the DS provides the 3DSS with a list of participating issuer BINs that are enabled in a specific EMV 3DS version of the protocol. This also includes coordinating the 3DS Method URL that the issuer uses for device fingerprinting and risk assessment. In later versions (v2.2+) of this message, additional data elements will be included, providing insight into issuer program offerings such as whitelisting and version management.
Authentication Message (AReq/Ares)	This is the first message between a merchant and their 3DSS or 3DS SDK, and subsequently sent to the DS and ACS, requesting that an authentication message be

	performed. It includes all optional, conditionally required, and required data fields, along with indicators for the issuer to acknowledge. The response message returns from the ACS and lets the merchant know if a frictionless experience or a challenge experience will be rendered with the consumer. If frictionless, the ECI and CAVV data elements will be included in this message response from the ACS.
Challenge Message (CReq/Cres)	If a challenge and issuer engagement with the cardholder needs to occur, then a series of these messages will occur.
Results Message (RReq/RRes)	The results message will provide the ECI and CAVV results back when a challenge occurs and CReq/Cres messages complete. This will end the challenge sequence.

Table 3. Other Notable Components

Electronic Commerce Indicator (ECI) or Security Level Indicator (SLI) value	A two-digit value that is sent back to the merchant, acknowledging that the transaction completed, was attempted, or failed/rejected authentication. Although the networks may call it an ECI or an SLI (Mastercard, three digits) value in authorization, the value is the same. The ECI also helps to determine if the merchant qualifies for liability shift.
Cardholder Authentication Verification Value* (CAVV)	A cryptogram attached to the authentication response, which is partly or wholly produced by the issuer and/or their ACS provider. The CAVV includes data pertaining to the authentication that occurred and is decrypted in authorization. *This data element can also be referred to as: Accountholder Authentication Value (AAV), or Authentication Value (AV).
3DS Method URL	Formerly used as an ACS URL with a redirect, the 3DS Method URL is attached to an enabled issuer's BIN or BIN range and allows the issuer to gather device fingerprint data before the authentication request is initiated by a merchant. This URL comes back to a 3DSS on the PRes message and is commonly loaded onto the merchant's page using JavaScript.[7] The 3DS Method URL helps achieve frictionless authentications more frequently as issuers are given additional data points that can be consumed in their risk decisioning.

2.2 EMV 3-D Secure Improvement Themes

EMV 3DS focuses on four major areas of improvement and feature attributes that are essential to advancing its ability to leverage today's technology.

- **Improving the 3DS consumer experience** – by limiting friction or engagement during the consumer checkout, supporting new authentication methods, applying risk-based authentication, and streamlining implementation for merchants.
- **Providing universal device support** – with optimization for all types of devices, customizable screens for issuers and merchants, expanded support for native apps, digital wallets and non-payment authentication.
- **Allowing greater data sharing** – 10-fold expansion of the data shared between issuers and merchants to aid in risk-based authentication and provide the capability to dynamically link to authorization.

[7] The manner in which the message is consumed and presented on the merchant page can vary by solution.

- **Being regulatory smart** – providing added elements to meet the growing application of strong customer authentication (aka challenges) for remote transactions, as well as SCA exemption requests to reduce fraud from CNP transactions.

Each of these themes speaks to how consumers are buying today, where they are buying, and how an issuer can improve their risk-decision processes during authentication and authorization to minimize the consumer impact. The following sections review these improvements in more detail.

2.2.1 3DS Consumer Experience Improvement

Maintaining a simple, secure, seamless and fast consumer experience is at the top of the priority list for every merchant and issuer, whether applying 3DS in a regulated market, or using it as an additional layer of security to reduce fraud in a non-regulated market like the United States. Making sure that consumers can shop, merchants can sell, and issuers can have confidence in approving transactions were the fundamental priorities driving the definition and roll-out of the new EMV 3DS protocol.

The payment networks actively addressed some challenges experienced with the 3DS 1.0.2 programs by eliminating both static passwords as a primary authentication method, as well as "activation during shopping," where consumers were asked to enroll their card into the program while trying to make a purchase. Static passwords are widely known as providing weak authentication and introducing a security risk; the payments industry responded by increasingly using dynamic authentication of consumers.

As issuers and merchants migrate to support EMV 3DS, and with regulations gradually being enforced internationally, strong customer authentication (SCA) will likely continue to proliferate. SCA uses two of three factors to authenticate a cardholder during checkout: something the consumer has, something the consumer knows and something the consumer is. To support SCA, more issuers are switching to support one-time-passcodes via text messages (SMS) and biometric confirmation using fingerprint, facial and voice recognition. When a challenge during the authentication process must occur, these solutions are already widely trusted by consumers, as they are used daily to access their smart phones and use mobile banking, merchant, and digital wallet apps.

When 3DS 1.0.2 was first implemented, challenges regularly occurred which caused high friction in the authentication process. Risk-based authentication (RBA) was introduced by ACS providers and has gained wide traction with issuers in the past few years. By using RBA with EMV 3DS, issuers can quickly and dynamically assess the risk of a transaction, apply rules based on data modeling, and determine if they have confidence to authenticate their cardholder passively in the background, or if they need to engage the cardholder for further validation. The more data that a merchant can share through EMV 3DS, the better the issuer's decisioning on the transactions will become over time, resulting in less friction for the customer.

EMV 3DS was designed to be used for all transactions sent by the merchant to an issuer – regardless of the transaction risk being high, medium or low. A merchant's normal payment processing can use the EMV 3DS authentication as a decision layer in the merchant's fraud stack. The more transactions and data that merchants can provide through EMV 3DS, the higher the authorization approvals may become, because of increased issuer confidence in the transactions.

Reducing fraud and false declines, recognizing legitimate orders, and increasing approvals are critical goals for everyone in the payments ecosystem. For the past two decades, issuers approved CNP transactions with limited visibility of consumer identity. Merchants accepted CNP transactions and implemented their own fraud systems to deal with increasing amount of fraud. Legacy authorization systems had been designed for the face-to-face point-of-sale (POS) environment, where a consumer stands in front of a cashier at POS terminal, which may be a short distance from the consumer's home, and transactions take place during the open hours of the retail location. Those legacy authorization systems were challenged to support purchases from the Internet, a gaming device, a TV, or an AI device running in a household.

Times have changed; purchases are now made wherever and whenever the consumer wants. EMV 3DS is a way to start evolving the authentication process through sharing device, transaction, prior authentication and merchant data with issuers.

2.2.2 Universal Device Support

3DS 1.0.2, as implemented in the early 2000s, was intended to support browser-based transactions initiated from a personal computer or laptop. EMV 3DS addresses the ability for authentication requests and responses to be supported in a universal design and takes advantage of device technology advances. At the forefront of these advances are mobile browsers and applications.

Purchases made on mobile devices are growing at a rapid pace in the U.S.; mobile retail commerce was over $156 billion in 2017, rising to $207 billion in 2018.[8] By 2020, mobile commerce (mCommerce) revenue is expected to reach more than $339 billion.[9] According to the Aite Group, CNP sales in the U.S. are expected to reach $443 billion (USD) by 2021.[11] Authentication and authorization solutions are critically needed to support both mCommerce and eCommerce transactions.

EMV 3DS offers a 3DS SDK (software development kit) component as part of the technology solution stack supported by the protocol. The SDK performs 3DS functions on behalf of the 3DS Server. When a 3DS solution provider offers an SDK for merchants, the SDK is installed and configured within the merchant's mobile and native application. Features supported include:

- **Main components –** Initialization and rendering of an EMV 3DS transaction, device data collection, encryption management, challenge flow management, network user interface (UI) guidelines and compliance, controlling UI type (native and HTML screens), EMV 3DS identifier version management, and support of various authentication methods
- **Encryption management –** Directory server and payment network public key management, device data encryption algorithms based on payment network, signature verification of ACS signed content, SDK challenge encryption of all Challenge Request/Response messages
- **Security features –** Jailbreaking, rooting maintenance, SDK integrity checks, emulators, debugger attachments, operating system (OS) version support/status checks, protection from reverse engineering, disablement of screenshots, run-time data integrity and data protection checks, encryption of stored data, Universal Unique IDentifier (UUID) generations

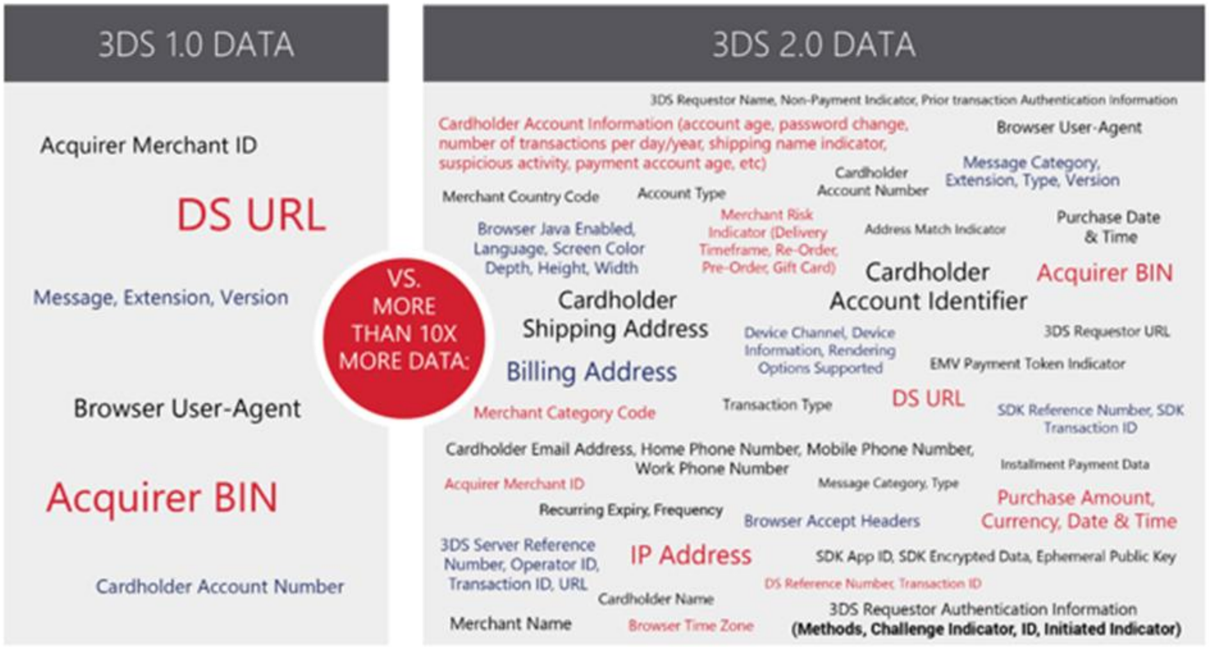
2.2.3 Greater Data Sharing

The greater data sharing –10 times more data – delivers significant value. The original 3DS only collected a handful of data elements during an authentication request. More specifically, these included the card primary account number (PAN), expiry date, transaction amount, date/time and some merchant and vendor identifiers.

[8] https://www.statista.com/statistics/249855/mobile-retail-commerce-revenue-in-the-united-states/

[9] Ibid.

Figure 2. Differences between 3DS 1.0.2 Data and EMV 3DS Data Collected by the Merchant and 3DS Server[10]


3DS 1.0 DATA
Acquirer Merchant ID
DS URL
Message, Extension, Version
Browser User-Agent
Acquirer BIN
Cardholder Account Number
VS. MORE THAN 10X MORE DATA:
3DS 2.0 DATA
3DS Requestor Name, Non-Payment Indicator, Prior transaction Authentication Information
Cardholder Account Information (account age, password change, number of transactions per day/year, shipping name indicator, suspicious activity, payment account age, etc)
Browser User-Agent
Cardholder Account Number
Message Category, Extension, Type, Version
Merchant Country Code
Account Type
Browser Java Enabled, Language, Screen Color Depth, Height, Width
Merchant Risk Indicator (Delivery Timeframe, Re-Order, Pre-Order, Gift Card)
Address Match Indicator
Purchase Date & Time
Cardholder Account Identifier
Acquirer BIN
Cardholder Shipping Address
Device Channel, Device Information, Rendering Options Supported
3DS Requestor URL
Billing Address
EMV Payment Token Indicator
Merchant Category Code
Transaction Type
DS URL
SDK Reference Number, SDK Transaction ID
Cardholder Email Address, Home Phone Number, Mobile Phone Number, Work Phone Number
Installment Payment Data
Acquirer Merchant ID
Message Category, Type
Recurring Expiry, Frequency
Browser Accept Headers
Purchase Amount, Currency, Date & Time
3DS Server Reference Number, Operator ID, Transaction ID, URL
IP Address
SDK App ID, SDK Encrypted Data, Ephemeral Public Key
DS Reference Number, Transaction ID
Cardholder Name
3DS Requestor Authentication Information (Methods, Challenge Indicator, ID, Initiated Indicator)
Merchant Name
Browser Time Zone

© Visa Inc. 2019

As previously discussed, legacy payment authorization systems were built for face-to-face transactions, where consumers were present. The merchant POS payment terminals and EMV chip cards provide many data elements for issuers to make an authorization decision and approve or decline a transaction. In a study conducted by Aite Group LLC, CNP sales in the US are expected to reach $443 billion (USD) by 2021.[11] While authorization rates of card-present transactions are in the 97% percent range, CNP transaction authorization rates are in the 80-85% range,[12] highlighting a large disparity and a need to improve CNP authorization rates and attack the false declines that are occurring. A layered fraud management approach can not only prevent fraud but also address false declines.

EMV 3DS has increased the number of data points to more than 135 different elements. Sending these data points with every transaction will help create a healthy and data-rich CNP ecosystem and may result in improvements to both authentication and authorization. The EMV 3DS data elements can be categorized into four major categories:

- **Device Data** – includes specific device information per channel, such as native app iOS versus native app Android versus browser details. These fields are conditionally required based on where the payment originates.
- **Transaction and Checkout Page Data** – contains required (and sometimes conditionally required) information gathered from the consumer's checkout process with the merchant and transaction elements.
- **Authentication Data** – is composed of two categories of optional data elements, both related to authentication, that a merchant can provide to an issuer for added insight.

[10] "EMV 3-D Secure Data Elements" webinar, Ian Poole, U.S. Payments Forum webinar, February 12, 2019, https://www.uspaymentsforum.org/emv-3-d-secure-data-elements-webinar/

[11] Aite Group LLC, "The E-Commerce Conundrum: Balancing False Declines and Fraud Prevention," July 2019

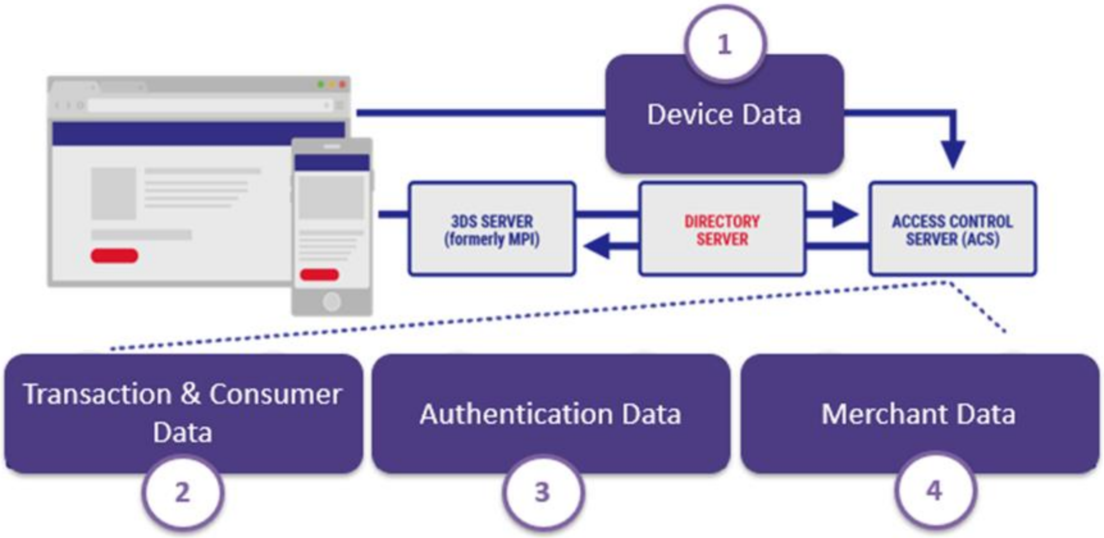
[12] Ibid.

- *Merchant authentication* includes data about the any non-3DS authentication which may be used by the consumer to gain access to the merchant website, account or card-on-file details.
- *Prior authentication* includes data elements gathered from a previous transaction with the same consumer and PAN where EMV 3DS was applied and presented with a new transaction.

- **Merchant Data** – is composed of two categories of optional data elements, related to consumer risk and account information, that a merchant can provide to an issuer for added insight.
  - *Merchant risk Information* includes data that only the merchant would be able to verify based on the current order details and that is used for merchant-level risk analysis.
  - *Cardholder account information* includes data specific to the consumer's account on the merchant website or app; it is related to the history or details of their account.

Additional details of data categories and the elements included are included in Appendix A.

Figure 3. High-level Flow Diagram of Data Element Categories[13]


1
Device Data
3DS SERVER (formerly MPI)
DIRECTORY SERVER
ACCESS CONTROL SERVER (ACS)
Transaction & Consumer Data
2
Authentication Data
3
Merchant Data
4

© CardinalCommerce 2019

2.2.3.1 Device, Transaction and Consumer Data Elements

These first two categories of data elements are required or conditionally required to be sent for an EMV 3DS authentication request (AReq) message by the merchant, to their 3DSS and/or 3DS SDK. These data fields are specific to the device that the consumer is using for their purchase, plus the transaction and consumer details, and identify the consumer and their purchase request to their card issuer. These data elements go beyond the card being used, and include billing/shipping details, mobile phone number, cardholder name, merchant category code (MCC) and more. Most of these elements are data that the merchant is currently collecting or has on file for the consumer, either from guest checkout or existing account information. This data provides visibility into transaction details and will help issuers validate that their cardholder is making the transaction.

[13] EMV 3-D Secure Data Elements Webinar, op. cit.

2.2.3.2 Authentication Data and Merchant-Specific Data

With EMV 3DS, merchants also have the capability to provide the issuer with optional information based on the merchant's information about consumer authentication and account data. This data could assist issuers with identifying transaction risk. Regularly receiving this information can increase an issuer's confidence in transaction authentication and enable a frictionless experience (vs. requiring a challenge). Issuers also have access to the cardholder's buying patterns by PAN/account and to a variety of data that a merchant does not see. This data can include:

- Other merchants where the cardholder transacts
- Cardholder purchase channels and patterns
- Interaction with the mobile banking app, including authentication access
- Cardholder's average spend
- Any reported fraud
- Velocity of transactions
- Activity on other cards in the issuer's portfolio
- Geolocation information

Merchants have the unique capability to see the consumer's activity directly with them, which can be beneficial for authentication. This data can include:

- Stored cards on a consumer's merchant account, regardless of issuer
- Authentication within the merchant's website/application
- Password and account history
- Email address used
- Consumer's order frequency with the merchant
- Shipping method and delivery timing
- Consumer interaction with their website/application
- Gift card amount and count within order
- Any fraud activity

By receiving merchant-specific data and any prior authentication data (non-3DS or EMV 3DS), issuers can see an in-depth view of the cardholder's activity that they've never seen before. This additional data can help the issuer accept a transaction with confidence, since the merchant has additional visibility of that consumer and trusts that the transaction is valid.

These different data categories provide merchants with a powerful tool. By implementing EMV 3DS, merchants can influence risk modeling by sharing these data elements, which can lead to frictionless transactions, fraud liability shift when applying authentication, and healthy issuer authorization decisions.

2.2.4 Regulatory Smart

Since 3DS 1.0.2 has been widely used within the standard payment processing flow in international markets for over two decades, it meets compliance regulations for two-factor authentication (2FA) in countries such as India, Singapore, Japan, Brazil, South Africa and others. Regulations can come into a market a few different ways, but the most common is a mandate for authentication directly from a payment network or from local governing bodies. When fraud increased on CNP transactions, 3DS has often been the solution to address the challenge. With the introduction of EMV chip cards and the resulting reduction in card-present fraud, fraudsters shifted their attacks to the CNP environment.

The U.S. does not have regulations requiring 2FA, as in India, or SCA, as recently adopted in Europe under the second Payment Services Directive (PSD2). EMV 3DS version 2.1 has supporting features that can help manage the application of authentication in regulated markets. Merchants can communicate with the issuer and influence the issuer's decision through a field known as 3DS Challenge Indicator. This field allows a merchant to request no challenge, challenge, or challenge due to mandate, in addition to the default request indicating no preference.[14] While acknowledgement of this field needs to be identified by the issuer and their EMV 3DS solution, it provides an opportunity that never existed with 3DS 1.0.2.

While this white paper provides an introduction to EMV 3DS version 2.1, it is important to note that many more features for regulatory applications are supported in the upcoming version 2.2, which will help to meet regulatory requirements (e.g., PSD2).

The U.S. Payments Forum plans to share information on EMV 3DS version 2.2 as it nears its production date.

2.3 EMV 3DS Transaction Flow[15]

EMV 3DS has an improved transaction flow versus 3DS 1.0.2 and helps speed the processing time for the overall authentication request. The flow includes the application of risk-based authentication by the issuer, collection of device fingerprint data, and focus on driving an enhanced consumer experience by only increasing friction via challenge when necessary. As shown in Table 4 and Table 5, EMV 3DS enables single message support for merchants, streamlining the processes into multiple steps handled mainly by solution providers.

Table 4. Message Requests Made by Merchants (Response Received)

3DS 1.0.2	EMV 3DS
Verify Enrollment	Authenticate Message
Payer Authentication	

Table 5. Message Requests Made by 3DS Servers on Behalf of Merchants (Response Received)

3DS 1.0.2	EMV 3DS
Verify Enrollment	Preparation Message
Payer Authenticate	Authenticate Message
	Challenge Message
	Result Message

Another area that has been improved and will contribute to faster processing speeds is the elimination of the redirect to the issuer's ACS URL. In 3DS 1.0.2, the ACS URL redirect was key to facilitating a challenge between the cardholder and card issuer, creating a secure connection and rendering a 400x400 pixel iframe. The ACS URL, for advanced 3DS 1.0.2 issuers, was also a way to run device fingerprinting and gather the necessary data to apply risk-based authentication, even if a challenge was not required. This redirection to the ACS URL sometimes caused problems, such as added latency, incorrect handling of the redirection by the merchant, full-page redirects from the merchant site, and the consumer experiencing an error with rendering the page.

[14] Merchants and issuers are advised to contact their acquirers, processors or payment networks for additional information on liability implications.

[15] Source for Figures 4, 5, 6 and 7: CardinalCommerce CCA Demo for Merchants; https://demos.cardinalcommerce.com

2.3.1 Frictionless Flow

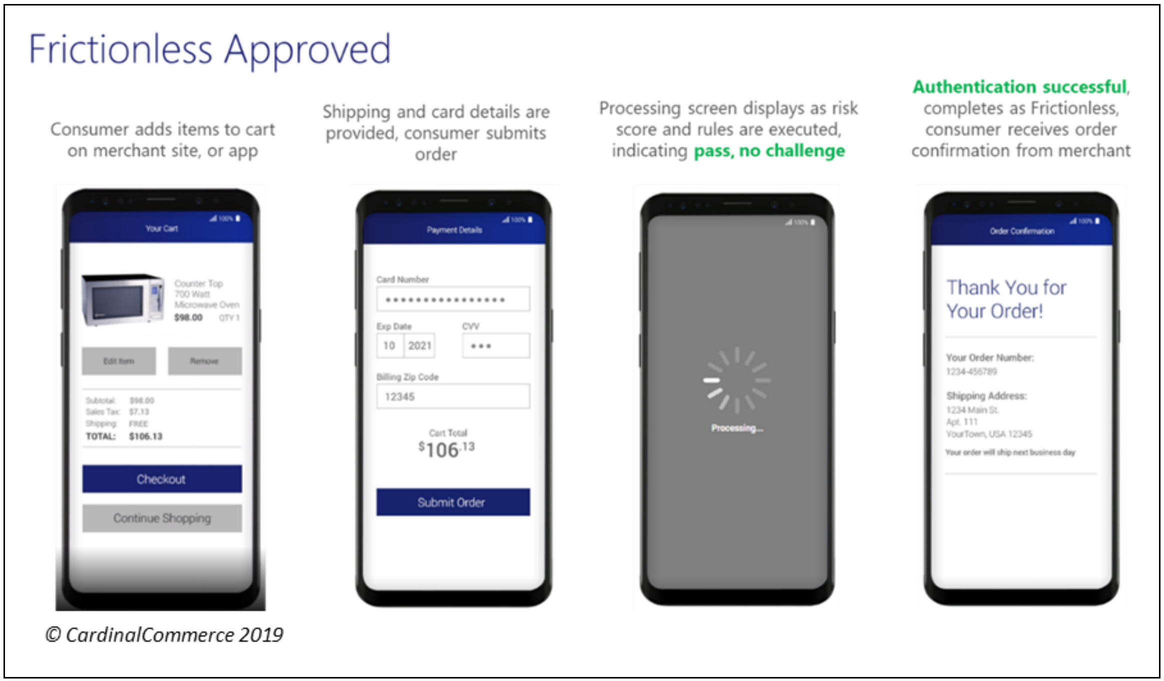
EMV 3DS streamlines and simplifies the technology that a merchant needs to launch an authentication through a 3DS Server provider. Not all implementations will be the same. Different providers will have unique capabilities, but the EMV 3DS protocol itself delivers interoperability, improvement to the protocols, and less implementation work for the merchant.

The issuer's ACS URL has been replaced with the 3DS Method URL. As mentioned earlier, the Method URL has the same ability to run device fingerprint collection that helps the issuer's RBA application. One important difference is that the Method URL is gathered by the 3DS Server using the Preparation Message. This allows the 3DS Method URL to be identified based on the card's bank identification number (BIN) used in the transaction and placed onto the merchant's web page earlier in the process. By eliminating the need for a redirect later in the process and allowing the Method URL to run before the buyer commits to the order, transaction processing time for the authentication request becomes faster than with the previous protocol.

If everything passes and no anomalies or high-risk factors are detected, the transaction can be authenticated passively by the issuer, and an authentication response message provided. Again, with improvements to implementation, gathering device details earlier, and use of RBA, payment networks expect that over 90 percent of transactions[16] (in non-regulated markets) would complete without a challenge or interaction from the cardholder.

Figure **4** illustrates an example of the user experience for frictionless transaction.

Figure 4. Frictionless Approved Transaction Flow with EMV 3DS



Frictionless Approved

Consumer adds items to cart on merchant site, or app

Shipping and card details are provided, consumer submits order

Processing screen displays as risk score and rules are executed, indicating **pass, no challenge**

Authentication successful, completes as Frictionless, consumer receives order confirmation from merchant

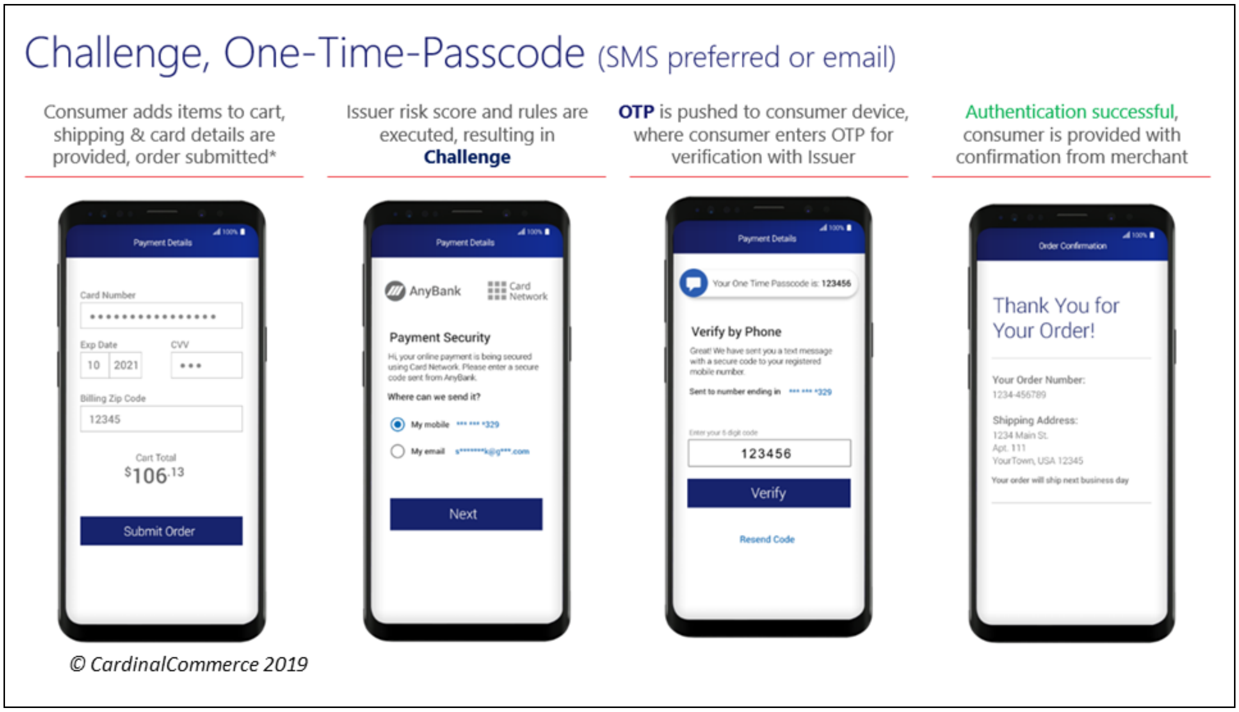
© CardinalCommerce 2019

[16] "Mastercard Identity Check Program Guide," November 2019

2.3.2 Challenge Flow

For a challenge flow, the Challenge Request/Response message is applied. These message formats provide information that a challenge is needed, the type of challenge that will be delivered, and the supporting information for screen rendering. Challenges will use new authentication methods that are allowed by the payment networks. Authentication methods can include the use of one-time-passcodes delivered via SMS, and out-of-band methods such as biometric fingerprint and facial recognition – authentication methods that are used today by consumers when accessing merchant sites, merchant apps, mobile banking apps and other similar systems. Figure 5 and Figure 6 illustrate an EMV 3DS challenge flow using a one-time-passcode with a mobile phone and browser. Figure 7 illustrates how a future implementation with an EMV 3DS challenge flow with a biometric fingerprint would render through a merchant mobile application.

Figure 5. Challenge One-Time-Passcode on Mobile Phone



Challenge, One-Time-Passcode (SMS preferred or email)

Consumer adds items to cart, shipping & card details are provided, order submitted*

Payment Details

Card Number: ••••••••••••••••

Exp Date: 10 2021

CVV: •••

Billing Zip Code: 12345

Cart Total $106.13

Submit Order

Issuer risk score and rules are executed, resulting in **Challenge**

Payment Details

AnyBank | Card Network

Payment Security

Hi, your online payment is being secured using Card Network. Please enter a secure code sent from AnyBank.

Where can we send it?

● My mobile *** *** *329

○ My email s*******k@g***.com

Next

OTP is pushed to consumer device, where consumer enters OTP for verification with Issuer

Payment Details

Your One Time Passcode is: **123456**

Verify by Phone

Great! We have sent you a text message with a secure code to your registered mobile number.

Sent to number ending in *** *** *329

Enter your 6 digit code: 123456

Verify

Resend Code

Authentication successful, consumer is provided with confirmation from merchant

Order Confirmation

Thank You for Your Order!

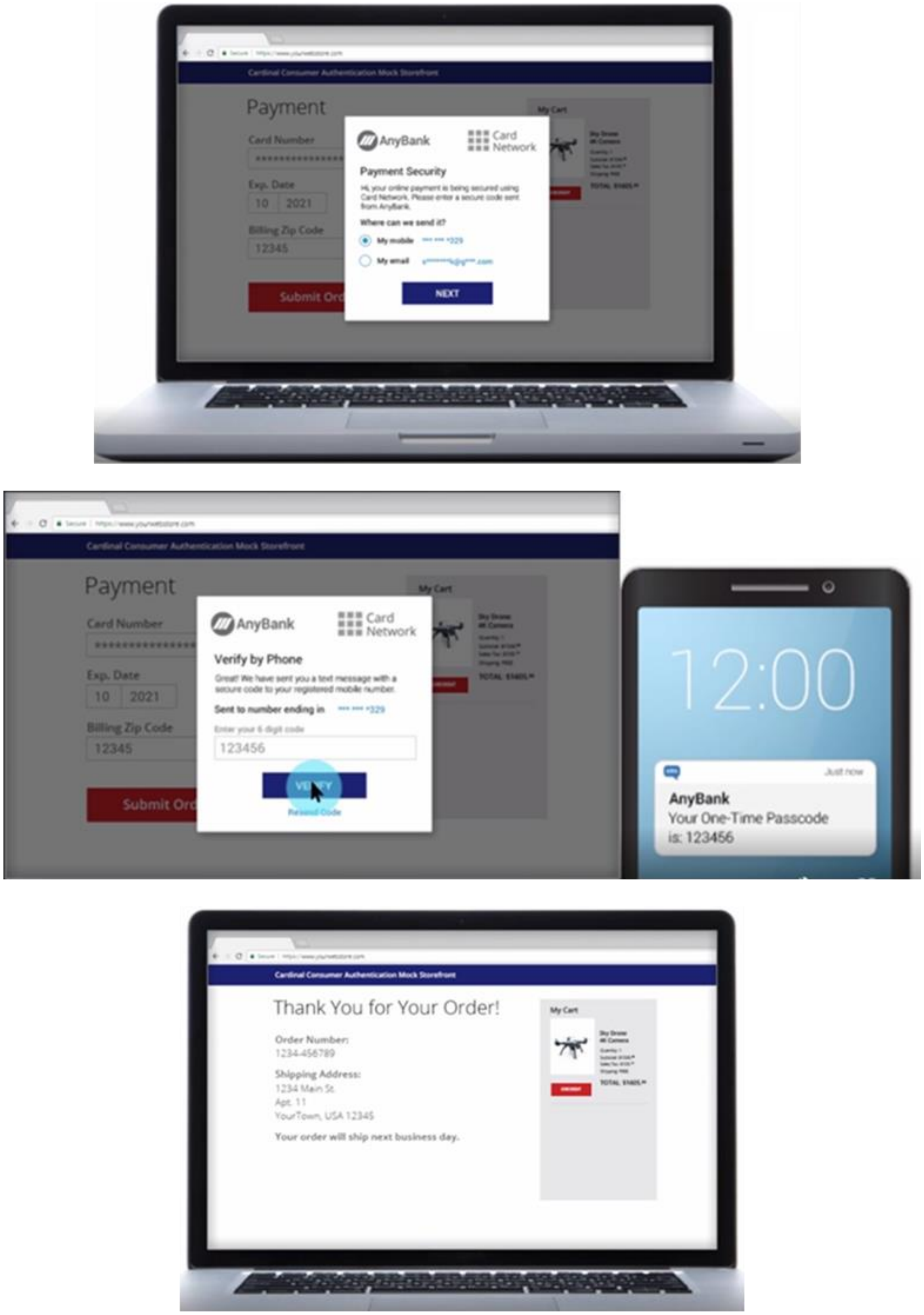
Your Order Number: 1234-456789

Shipping Address:
1234 Main St.
Apt. 111
YourTown, USA 12345

Your order will ship next business day

© CardinalCommerce 2019

Figure 6. Challenge One-Time-Passcode with Browser



Cardinal Consumer Authentication Mock Storefront

Payment

Card Number: ***************

Exp. Date: 10 2021

Billing Zip Code: 12345

Payment Security

Hi, your online payment is being secured using Card Network. Please enter a secure code sent from AnyBank.

Where can we send it?

● My mobile *** *** *329

○ My email s*******s@g***.com

Verify by Phone

Great! We have sent you a text message with a secure code to your registered mobile number.

Sent to number ending in *** *** *329

Enter your 6 digit code: 123456

AnyBank
Your One-Time Passcode is: 123456

Thank You for Your Order!

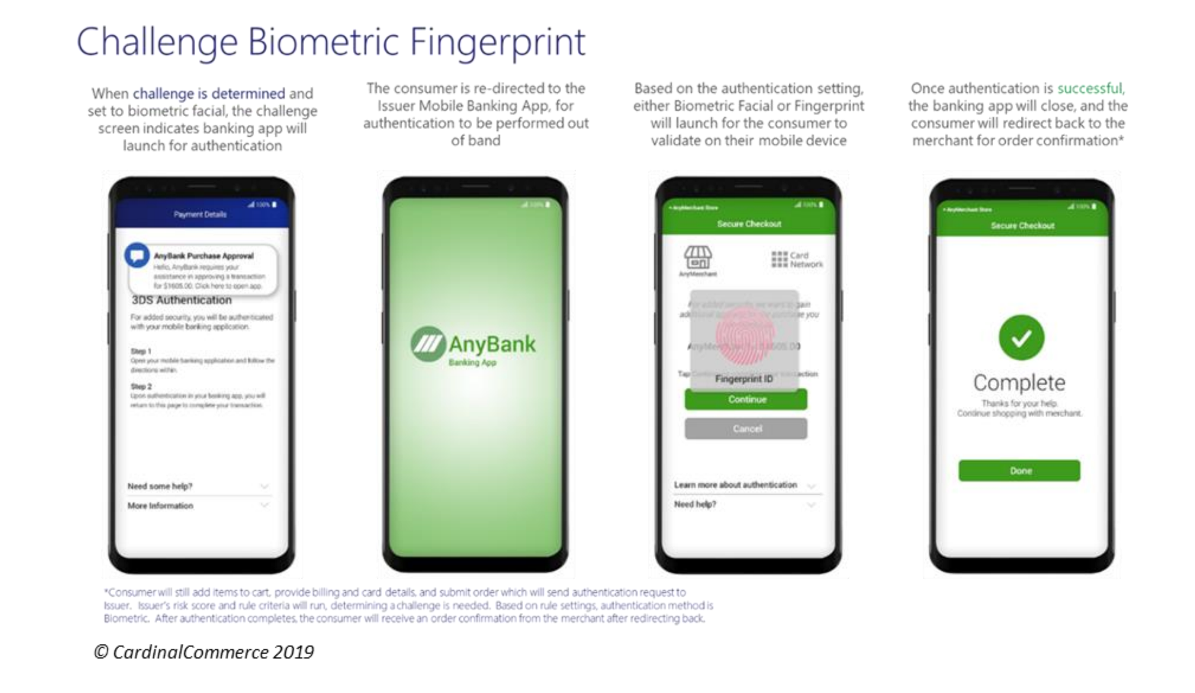
Order Number:
1234-456789

Shipping Address:
1234 Main St.
Apt. 11
YourTown, USA 12345

Your order will ship next business day.

© CardinalCommerce 2019

Figure 7. Challenge Biometric Fingerprint Transaction Flow with EMV 3DS



Challenge Biometric Fingerprint

When challenge is determined and set to biometric facial, the challenge screen indicates banking app will launch for authentication

AnyBank Purchase Approval
Hello, AnyBank requires your assistance in approving a transaction for $1605.00. Click here to open app.

3DS Authentication

For added security, you will be authenticated with your mobile banking application.

Step 1
Open your mobile banking application and follow the directions within.

Step 2
Upon authentication in your banking app, you will return to this page to complete your transaction.

The consumer is re-directed to the Issuer Mobile Banking App, for authentication to be performed out of band

Based on the authentication setting, either Biometric Facial or Fingerprint will launch for the consumer to validate on their mobile device

Once authentication is successful, the banking app will close, and the consumer will redirect back to the merchant for order confirmation*

Complete

Thanks for your help.
Continue shopping with merchant.

*Consumer will still add items to cart, provide billing and card details, and submit order which will send authentication request to Issuer. Issuer's risk score and rule criteria will run, determining a challenge is needed. Based on rule settings, authentication method is Biometric. After authentication completes, the consumer will receive an order confirmation from the merchant after redirecting back.

© CardinalCommerce 2019

3. Conclusions

This white paper provides an overview of EMV 3-D Secure and covers the current version, EMV 3DS 2.1, which is available for use in market today. As mentioned, EMVCo intends to update the specifications on a regular basis to address changes in the marketplace and regulations throughout the world. The next version, version 2.2, which was discussed briefly, is available in production from certified vendors and addresses, among other things, exemption handling for merchants and issuers impacted by PSD2's SCA requirement.

4. Legal Notice

This document is provided solely as a convenience to its readers. While great effort has been made to ensure that the information provided in this document is accurate and current, this document does not constitute legal or technical advice, should not be relied upon for any legal or technical purpose, and all warranties of any kind, whether express or implied, relating to this document, the information or materials set forth or otherwise referenced herein, or the use thereof are expressly disclaimed, including but not limited to all warranties as to the accuracy, completeness or adequacy of such information or materials, all implied warranties of merchantability and fitness for a particular purpose, and all warranties regarding title or non-infringement. All third party materials referenced herein are the property of their respective owners, the U.S. Payments Forum is not responsible or liable for the content or use thereof, and all references to or summaries of such third party materials are qualified by the actual third party materials, as made available by such third parties. Stakeholders interested in EMV 3DS are strongly encouraged to consult with their respective payment networks, acquirer processors, and appropriate professional and legal advisors regarding all aspects of implementation, prior to implementation.

5. Appendix A: Data Categories, Sub-categories and Details

The table below provides a high-level description of EMV 3DS data.[17] Refer to the EMVCo EMV 3DS specification for additional detail.[18]

Transaction and Checkout Page Information - REQUIRED	Cardholder Information	Account Number and Expiration Date, Billing (Address, City, Postal Code, State), Email, Mobile Phone, Cardholder Name, Shipping (Address, City, Country, Postal Code, State), Network Payment Token Indicator (conditional)
	Merchant Information	Merchant Name, URL, Country, MCC, Acquiring BIN/MID, 3DS Network Identifier
	Transaction Information	Amount, Currency Code, Transaction Type
Device Data	Device Information	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)
	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
Authentication Data	Merchant Authentication (performed outside of 3DS)	Authentication method (no authentication occurred [guest checkout], login using merchant system credentials or federated ID, FIDO authenticator), authentication date/time, any data that documents specifics of the authentication process that previously occurred
	Prior Authentication (passing previous EMV 3DS authentication data)	Authentication method (frictionless or challenge), authentication date and time of prior EMV 3DS on merchant site, any data that documents specifics of the authentication that occurred, ACS Transaction ID, to link the prior authentication

[17] "EMV 3-D Secure Data Elements" webinar, U.S. Payments Forum, February 2019, https://www.uspaymentsforum.org/emv-3-d-secure-data-elements-webinar/

[18] Click to link to: EMVCo Specification Search

Merchant Data	Shipping Information	Ship to billing address, ship to another verified address on file, ship to address different from billing, ship to store, delivery email
	Delivery Timing	Delivery timeframe (electronic, same day, overnight, two or more days)
	Pre-Order/Re-Order	Merchandise available, future availability, first time order, reorder of product
	Gift Card	Amount, currency, count
	Account Standing	Account age indicator, account creation date, account change indicator, change date, account password change (indicator and date), ship name indicator, payment account indicator and age
	Shipping Usage	Shipping address usage and date (when address was first used)
	Transaction Counts	Number of transactions within last 48 hours, amount, currency, count
	Fraud Activity	Suspicious activity on account, account purchases and add-card attempts