A US PAYMENTS FORUM WHITE PAPER

Exploring Data Elements in Mobile Payment Transactions

Version 1.0

October 2024

U.S. Payments Forum
544 Hillside Road
Redwood City, CA 94062

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum is a cross-industry body that brings stakeholders together on neutral ground to enable efficient, timely and effective implementation of emerging and existing payment technologies. This is achieved through education, guidance and alternative paths to adoption. The Forum is the only non-profit organization whose membership includes the whole 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. The organization operates within the Secure Technology Alliance, an association that encompasses all aspects of secure digital technologies.

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

Table of Contents

Executive Summary

The U.S. Payments Forum white paper, "Exploring Data Elements in Mobile Payment Transactions," reviews the increasingly complex landscape of mobile and online payments. The main focus is to provide detail on the expanded range of data elements that are available in digital transactions as compared to legacy systems, and to illustrate how these can be used for enhanced security, fraud prevention, and optimal user experiences. Key white paper insights include:

- **Expanded data elements**. Mobile transactions access data elements that are not available in traditional payments, including data relating to EMV 3-D Secure (3DS), geolocation, digital wallet behavior, and tokenization. The expanded data offers opportunities for a multifaceted approach to transaction security and user experience.
- **Authentication and fraud prevention**. The paper underscores the significance of additional data elements, like device fingerprinting and location data, for improving authentication methods and detecting fraudulent activities. Enhanced authentication using 3DS elements and biometrics is highlighted for its potential in strengthening transaction security.
- **Data handling best practices**. With the increase in available data, the paper describes best practices for handling personally identifiable information (PII), stressing the importance of compliance with Fair Information Practices Principles and relevant legal frameworks.
- **Stakeholder implications**. The implications for various stakeholders (issuers, mobile providers, payment networks, processors, and merchants) are considered. Emphasis is placed on the need for sophisticated data analysis tools and adherence to privacy and security standards.
- **Future research and trends**. The paper suggests opportunities for exploring additional data fields and payment technologies (e.g., EMVCo Secure Remote Commerce (SRC)) and the potential benefits of industry-wide cooperation in data sharing and management.

The white paper concludes that the expanded use of diverse data elements in mobile transactions offers significant opportunities for the payments industry. However, the use also brings challenges in terms of data privacy, regulatory compliance, and the balance of security with user convenience. The white paper highlights the transformative potential of mobile payment technologies and urges stakeholders to navigate this evolving landscape with a commitment to security, ethical data practices, and a forward-looking approach.

1. Introduction

Mobile, online, and in-app payment transactions can access more data elements than were available with legacy transactions, which were limited to the fields in the current financial messages. Use of these additional data elements in authorization and provisioning can reduce fraud in online and mobile payments and provide other potential benefits.

The objectives of this white paper are to:

- Explore the additional data elements that are available for mobile and online transactions
- Identify how these additional data elements could be used for fraud prevention, provisioning, or other benefits
- Explore trends and potential best practices
- Outline considerations for stakeholders in the payments industry, including issuers, mobile providers, payment networks, processors, and merchants

The scope of this white paper includes:

- Existing data elements from existing standards that may not be used today during authorization
- EMV 3-D Secure (3DS) data elements
- IP address and other data from a mobile device

This white paper does not, and should not be construed to create new standards or data elements.

2. Overview of Authentication Request Data Elements

In the rapidly evolving payments landscape, mobile and online transactions are increasingly using a broader array of data elements as compared to legacy transaction systems. These enhanced data elements play a critical role in authorization and provisioning, offering significant potential for reducing fraud and optimizing payment processing. This section reviews the additional data elements available for mobile and online transactions and the implications for stakeholders in the payment ecosystem.

2.1 Expanded Data Elements

Data elements that can provide enhanced opportunities for authentication in payment transactions include the following:

- **3DS and Click to Pay data elements**. EMV 3DS technology, a cornerstone of online transaction security, provides layers of authentication data that were previously unavailable. Click to Pay, which leverages EMVCo's Secure Remote Commerce (SRC) specifications, further enhances authentication by simplifying checkout processes and adding security layers.
- **Data sharing solutions**. Innovations like 'Data Only' 3DS authentication, APIs such as Capital One's Enhanced Decisioning Data,[1] and other proprietary solutions offer a wealth of transaction-related information. These solutions facilitate better decision-making by leveraging additional data points during the authorization process.
- **Wallet provisioning and model scores**. Digital wallet services provide unique data elements related to device use and customer behavior. Model scores, derived from customer interaction with digital wallets, offer predictive insights for fraud detection and customer experience enhancement.
- **Geolocation data**. GPS and other geolocation technologies offer precise information about the physical location of devices used for transactions, adding another layer of verification that can be used for fraud prevention. However, the use of virtual private networks (VPNs) and other methods that hide IP addresses introduces complexities in accurately determining the transaction origin and requires advanced fraud detection strategies.
- **Tokenization**. Card-on-file token data, where sensitive card details are replaced with unique tokens, greatly reduces the risk of data breaches and fraud in online transactions and can include transaction-specific cryptographic data that can, in some cases, be validated by the token service provider.
- **Mobile driver's license indicator**. This emerging data element can verify the identity of the cardholder in mobile transactions, enhancing security as a result. The U.S. Payments Forum recently published white paper, "The Role of Mobile IDs in Payments," offers insights into the use of digital identities (e.g., mobile driver's licenses (mDLs)) as data elements in payment processing. These technologies can enhance transaction security, improve identity verification, and potentially streamline e-commerce experiences. The white paper highlights the future direction of digital transactions and their impact on the payments ecosystem.

[1] See explanation of "Enhanced Decisioning Data" at Capital One's Developer Exchange, https://developer.capitalone.com/documentation/enhanced-decisioning-data?id=23343-1.

2.2 Data Element Categories in Authentication Requests

Section 9, Appendix B, Table 1, includes detailed information on authentication request message data elements. The following are the categories of data elements that can be included in authentication requests.

- **Channel (browser/app)**. Identifies the medium through which the transaction is initiated, providing insights into the user interface and potential security features.
- **Transaction data**. Includes critical details of the transaction such as type, amount, currency, and timestamp, forming the core of the authentication request.
- **Cardholder data**. Includes the personal and contact information of the cardholder, crucial for verifying user and transaction legitimacy.
- **Device data**. Encompasses specifics about the device used, including its type, browser or app details, and software development kit (SDK) information for app-based transactions.
- **3DS requestor data**. Contains information about the merchant or entity initiating the transaction, such as their identification, website URL, and risk assessment metrics.
- **Directory server data**. Relates to the network directory server managing the request, including reference numbers and URLs, which are vital for tracking and security purposes.
- **Additional data**. Comprises various other data elements like message extensions, notification URLs, and specific transaction types that can further aid in the authentication and authorization process.

3. Potential for Augmenting Payment Transactions with Mobile Data

Data is powerful, and additional data offers new opportunities to improve processes. As noted in Section 2, mobile transactions include a significant amount of incremental data. How can that incremental data be used to improve payment transactions? This section outlines examples of how these additional data elements could be used.

3.1 Potential Uses Associated with Payment Transactions

Mobile transaction incremental data may be used to augment payment transactions to achieve the following:

- **Improved authentication**. 3DS data elements (such as cardholder account number, device information, and browser IP address) enable stronger authentication mechanisms, such as biometric authentication or one-time passcodes sent to the user's mobile device. Their use enhances security by adding an extra layer of verification beyond traditional cardholder information.
- **Fraud prevention**. Additional data elements, such as device fingerprinting or location data, can help in detecting potentially fraudulent transactions. Analyzing these data points allows payment processors to identify suspicious activities and prevent unauthorized transactions more effectively.
- **Improved authorization rates**. By leveraging additional data points from mobile transactions, issuers can make more informed decisions during the authorization process. This can lead to fewer false declines and increased approval rates for legitimate transactions, improving the overall user experience.
- **Personalization of the payment experience.** Mobile payment transactions can provide data about user preferences, purchasing behavior, and location. This information can be used to personalize the payment experience, offering targeted promotions, loyalty rewards, or tailored recommendations to users based on their transaction history and preferences.
- **Seamless user experience**: Mobile payment transactions can streamline the checkout process, allowing users to complete transactions more quickly and conveniently. By integrating additional data elements, such as “Requestor Decoupled Max Time” and “Browser User-Agent,” users can enjoy an improved frictionless payment experience without the need to input sensitive card details repeatedly.
- **Insights from data analytics**. The wealth of data generated by mobile payment transactions, including 3DS data elements, can be analyzed to gain valuable insights into consumer behavior, market trends, and spending patterns. This data can help businesses make informed decisions, optimize their marketing strategies, and identify opportunities for growth.

Industry-wide benefits can also be derived from the incremental data. Realizing these benefits would require cooperation among numerous industry stakeholders, as opposed to those that can be realized by stakeholders individually.

4. Future Trends and Considerations in Mobile Payment Data

Even as the adoption of newer payments technologies such as 3DS and SRC increases, future technology is under development that will continue to push the boundaries of digital payment experiences for all stakeholders. The impact of adopting existing payments technologies should be carefully considered, as well as how future technology may change the use of existing technologies.

4.1 Proposed Data Handling Best Practices

The current trend of increasing data availability is expected to continue, with more data collected, processed, and stored than ever before. While comprehensive data and privacy practices are far beyond the scope of this paper, some core tenets should be kept in mind when using any personally identifiable information (PII). At a high level, these best practices are loosely described as Fair Information Practices Principles (FIPPS)[2]. The practices have been codified into various laws on a state-by-state basis, as well as at national and regional levels, such as the European Union General Data Protection Regulation (GDPR) for European citizens. Any potential handling of PII should be discussed with relevant legal counsel and senior leadership to thoroughly understand the implications of collecting, processing, storing, and managing the lifecycle of PII prior to implementation.

Some high-level general considerations when handling PII include the following:

- **Rights of individuals**. Definition and consensus regarding cardholders' (i.e., "individuals") rights with respect to their personal information. For example, companies handling PII may be required to "allow individuals to determine what records pertaining to them are collected, maintained, used, or disseminated by an agency; require agencies to procure consent before records pertaining to an individual collected for one purpose could be used for other incompatible purposes; afford individuals a right of access to records pertaining to them and to have them corrected if inaccurate; and require agencies to collect such records only for lawful and authorized purposes and safeguard them appropriately."[3]
- **Information controls**. Technical, physical, and administrative controls to manage and protect cardholder PII.
- **Information lifecycle**. Policies and implementation for managing the entire data lifecycle of cardholder PII; for example, the collection, processing, use, retention, disclosure, and erasure of cardholder PII.
- **Management and administration**. Policies and processes for defining, documenting, communicating, monitoring, and enforcing PII policy adherence.

Mishandling of PII can lead to serious risks and consequences, including: legal (e.g., regulatory non-compliance and lawsuits); reputational (e.g., loss of consumer confidence); operational (e.g., business efficiency vs. compliance); and investment (e.g., return on investment from PII-processing activities vs. opportunity cost).

[2] U.S. Department of Justice, "Overview of the Privacy Act of 1974," 2020 Edition, page 1, https://www.justice.gov/Overview_2020/dl?inline.

[3] Ibid.

Careful consideration of the impact of PII collection and processing on the business prior to implementation is strongly encouraged. Depending on the jurisdiction, avoiding the collection of PII altogether or utilizing an anonymization function on collected PII may be prudent. Generally speaking, data can be considered anonymized only if the process is irreversible (e.g., it is not possible to reconstruct the original PII from the anonymized output).

Examples of data that might be good candidates for anonymization include (but are not limited to):

- Email addresses containing first and last names
- Email addresses containing an identifiable domain address (e.g., john@johndoe.com)
- Cookie IDs
- IP addresses
- Identification numbers (e.g., driver's license or passport number)

No "one-size fits all" approach applies to data handling best practices given the wide variety of possible data elements and uses. Careful planning and research are critical when considering the use of personally identifiable data elements, regardless of the data source. Seek legal counsel and support of senior management in determining whether the use of mobile data elements is prudent to furthering the organization's goals.

5. Stakeholder Implications

For payments industry stakeholders (including issuers, mobile providers, payment networks, processors, and merchants), understanding and using the expanded data elements are crucial. The data offers enhanced fraud prevention capabilities, improved accuracy in authorization and provisioning, and opportunities for optimizing the user experience. However, their use also requires the adoption of sophisticated data analysis tools and strategies to effectively leverage this data while ensuring compliance with privacy and security standards.

The following general observations can be made for specific stakeholder groups:

- **Merchants**. With an expanded mobile data set, merchants can potentially better manage and challenge chargebacks. An expanded data set has the potential to uncover additional fraud patterns and give merchants more compelling evidence to fight spurious chargebacks. Merchants can also use this data to create more compelling user experiences such as location-based offers.
- **Merchant acquirers**. With richer data available for each transaction, merchant acquirers can make more informed authorization decisions. Using the data can improve the ability to assess the legitimacy of transactions, leading to a reduction in fraudulent transactions and saving costs associated with chargebacks and fraud management. In addition, achieving higher authorization rates may be possible, increasing sales for merchants and reducing false declines.
- **Issuers**. Issuers may also notice additional patterns with the use of expanded data elements. For example, issuers may see certain transaction types being disputed more or less often on certain networks, allowing disputes to be resolved more quickly. If the issuer already has the data elements that merchants would provide for dispute resolution, the amount of back and forth required between merchant and issuer could be reduced, decreasing resolution time.
- **Issuer processors**. Issuer processors can leverage expanded data elements, such as model scores and geolocation information, for enhanced risk management and more accurate fraud detection. Additional data points from technologies like 'Data Only' 3DS authentication may aid in making informed decisions during authorization, improving risk assessments and customer experience. However, understanding the interplay between heightened security measures and user experience is crucial, as increased security protocols may cause transaction friction and affect customer satisfaction.

The expanded use of data elements in mobile and online transactions offers a multifaceted approach to improving transaction security, enhancing customer experience, and reducing fraud. As the payments landscape continues to evolve, stakeholders must consider how best to adapt to these changes and harness the potential of these new data elements.

6. Potential Areas of Future Research

While the bulk of this paper addresses the use of standard EMV 3DS data elements in mobile payment transactions, other optional fields and additional payments technologies in the ecosystem are potentially worth considering. In addition, topics related to acceptable use of collected data and systems design should be explored.

First, optional fields (as outlined in Section 9, Appendix B: Detailed Analysis of Key EMV 3DS Data Elements and Uses) are technically feasible in the existing 3DS specification; however, these fields often are not used. One of the greatest challenges in improving data utilization is that certain data is generally not shared among the various 3DS stakeholders, either for legal, business, or other reasons. Cooperation in sharing data presumably could be fostered through either: 1) required adoption (via some third party such as legislation or industry bodies); or 2) voluntary adoption. A future proposed research topic is cross-party data sharing, and methods for how payments-related data can be effectively shared, transmitted, utilized, stored, and managed, without negatively impacting consumers or causing legal/compliance/ethical issues.

Second, payments technologies such as EMVCo Secure Remote Commerce contain even more data elements than 3DS. While SRC adoption is arguably still in its early stages, it continues to gain traction. As SRC can be leveraged for non-payment purposes as well, the amount of data that is potentially present in an SRC transaction can be relatively large. A proposed future research topic includes developing a similar white paper on SRC and the possibilities for sharing constituent data elements.

In addition, generally accepted standards for permissible data usage vary by jurisdiction and stakeholder, and technical and industry nuances need to be considered. For example, what might be permissible use by a merchant may be very different from that of an issuer. A future proposed research topic is to provide an overview of the various accepted standards at the stakeholder and industry level.

It should be noted that any proposed changes to existing specifications[4] or their use will likely cause a ripple effect. The length of time required for networks, standards organizations, and regulators to change specifications and/or to be implemented by the various stakeholders may make such changes unrealistic. Generally, the regulatory landscape requires more lead time to adapt to changes than technology providers do, creating a potential delay in innovation if changes to compliance are proposed or required. This level of impact on the various stakeholders should be considered and is a proposed topic for future research.

Although the data elements discussed in this white paper originate from payments transactions, the data could potentially be leveraged for other purposes, such as onboarding and provisioning cardholders (both digitally and in-person). The applicability of this data beyond the scope of payment authorization is a rapidly unfolding topic and has been identified as an area of future research. Many topics are considerations in cross-functional use of data elements, including, but not limited to:

- Data custody and onward transfers
- Data security and acceptable use
- Legal implications, including terms and conditions of data collection, usage, and consent
- Cross-border data transfers (e.g., state-to-state, or international)
- Data residency requirements

[4] See data flow diagram in **Figure 1**

Lastly, any research in mobile data elements should have security and privacy by design from the very outset. Generally speaking, security best practices espouse “white box” security. That is, the security system’s design functions and processes are publicly exposed and accessible to anyone, while the specifics of an implementation (such as keys, secrets, key values) are obscured and unique to the implementing organization. For example, public key infrastructure (PKI) underpins virtually all modern secure electronic communications among parties without a prior relationship (such as a consumer using an EMV chip card at a physical point of sale).

Any proposed research in mobile data elements should generally follow this paradigm, where the data elements and their use are publicly available, but the unique properties of an implementation are not. The data payloads themselves and any associated secrets are the security mechanism for the implementing organization. This approach can prevent bad actors from gaining a scalable advantage. That is, the bad actor cannot apply their knowledge of how a control works widely to all implementations of a technology, but rather the actor must concentrate on a specific implementation for their attack to be successful. (There are, of course, exceptions to this generalization.)

7. Conclusion

As the mobile payments landscape continues to evolve rapidly, the significance of using expanded data elements in transactions is becoming increasingly evident. This white paper has provided a comprehensive examination of the data elements involved in mobile payment transactions, highlighting their potential in revolutionizing the industry. It has also delved into the implications of these advances for various stakeholders in the payment ecosystem, from issuers to merchants.

Foremost, the significance of EMV 3DS data in constructing a robust framework for secure mobile transactions cannot be overstated. This security protocol exemplifies how specific data elements can be leveraged to bolster transaction integrity, significantly reducing the likelihood of fraudulent activities. However, understanding the balance between security measures and user experience is crucial, as heightened security may also the convenience, user trust and widespread adoption associated with mobile payments.

The key takeaways underscore the immense benefits of using mobile device data, which not only augments transaction security but also paves the way for innovative solutions in fraud prevention. While these technological advancements offer remarkable opportunities, they also introduce challenges regarding data privacy, regulatory compliance, and the balance between security and user convenience. Additionally, the paper emphasizes the need for ongoing innovation and adaptation in the face of ever-changing consumer behaviors and technological advances.

Looking ahead, the continuous evolution of standards and technologies in mobile payments will remain vital in addressing emerging security challenges. The paper has highlighted the importance of responsible data governance and ethical considerations in handling sensitive information. As mobile payment technologies evolve, so too should the industry approach to data management, prioritizing consumer privacy and regulatory compliance. Stakeholders must remain vigilant and proactive, embracing these changes while upholding ethical data governance practices. By doing so, they can leverage the full potential of mobile payment data elements, ensuring secure, efficient, and user-friendly payment experiences in an increasingly digital world.

In terms of implementation, the white paper has outlined key considerations, drawing attention to the need for agility and foresight in integrating these data elements into existing systems. This aspect is particularly critical, considering the dynamic nature of technology and consumer preferences.

The continuous evolution in standards and technologies will play a pivotal role in addressing emerging security challenges. By remaining engaged and proactive in developing new standards, stakeholders can help ensure that the mobile payments ecosystem is not only secure but also innovative and responsive to future demands.

In conclusion, the white paper's exploration of the data elements in mobile payment transactions reveals a landscape rich with opportunities and challenges. Stakeholders across the board, from service providers to end users, must navigate this terrain with a commitment to security, ethical data practices, and a forward-looking approach, ready to embrace the transformative potential of mobile payment technologies.

8. Legal Notice

This document is provided solely as a convenience to its readers, as a high-level overview of the additional data elements available in payment transactions originating from mobile, online and in-app, how these data elements could be used for fraud prevention, provisioning or other benefits, and associated considerations for stakeholders. 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 and should not be relied upon for any legal or technical purpose; accordingly, all warranties of any kind, whether express or implied, relating to this document, the information herein, or the use thereof are expressly disclaimed, including but not limited to warranties as to the accuracy, completeness or adequacy of such information, all implied warranties of merchantability and fitness for a particular purpose, and all warranties regarding title or non-infringement. Any person that uses or otherwise relies on the information set forth herein does so at his or her sole risk. Without limiting the foregoing, note that this document provides only a high-level description of the subject matter, and is not exhaustive; for example, there may be other potential uses for the aforementioned data elements, and notwithstanding anything in this paper, there may be limits (legal, contractual, or otherwise) that prevent the use and/or sharing of particular data elements for one or any purposes. Accordingly, readers interested in exploring the use of such data elements are strongly encouraged to consult with their respective subject matter experts and professional and legal advisors, as well as relevant payments industry stakeholders, such as payment networks, issuers, acquirers, and others, prior to any implementation decisions.

Appendix A: EMV 3DS Flow

Figure 1 illustrates the data flow in an EMV 3DS transaction.

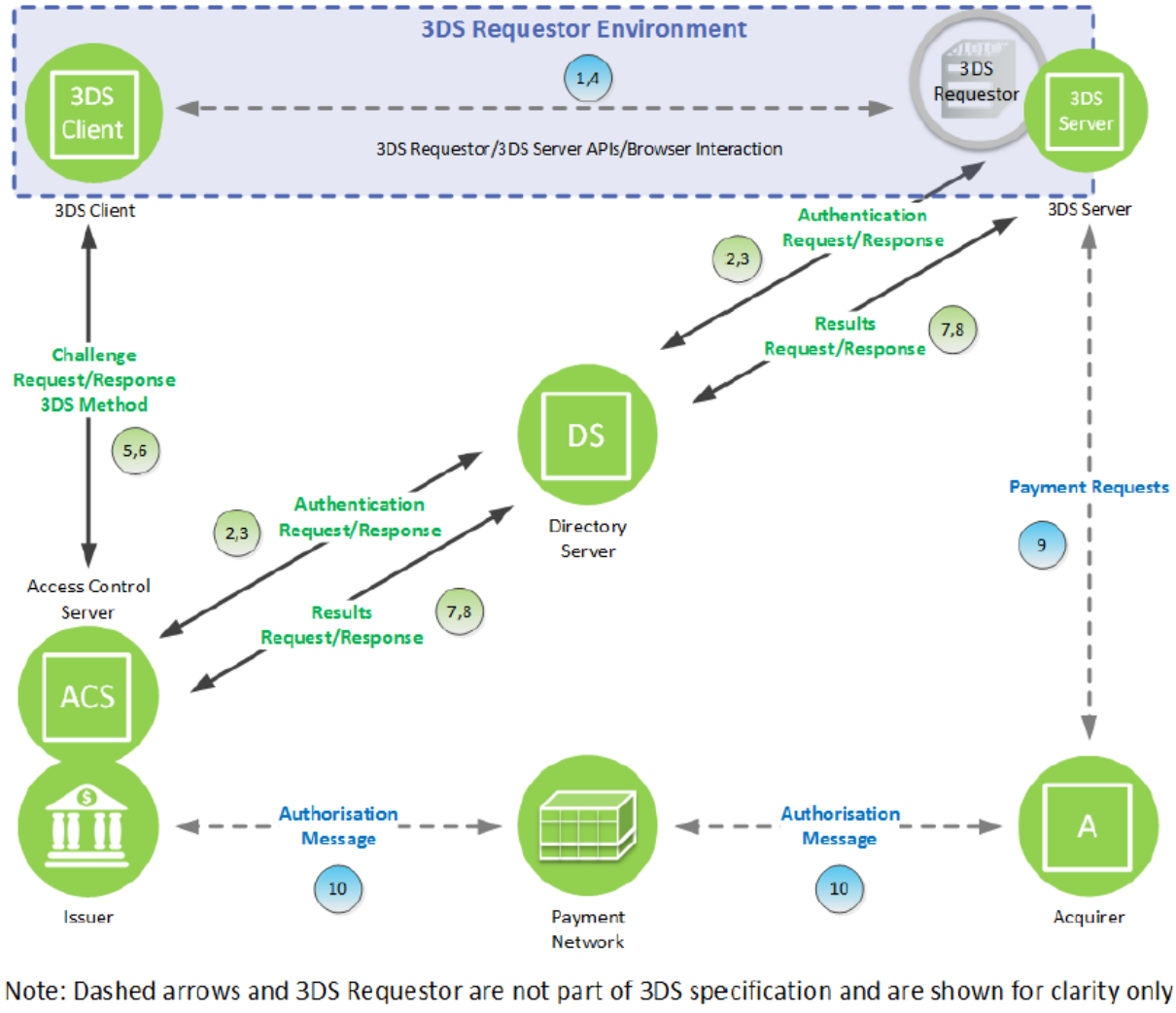

Figure 1. EMV 3DS Data Flow[5]

The cardholder starts the flow by initiating a transaction on a consumer device. The cardholder provides the information necessary for the authentication. (See the numbers in Figure 1 to follow the flow described below.)

1. **3DS Requestor Environment**. Within the 3DS Requestor Environment, the necessary 3DS information is gathered and provided to the 3DS Server for inclusion in the AReq message.

[5] EMVCo, "EMV@ 3-D Secure Protocol and Core Functions Specification Version 2.3.0.0," September 2021, https://www.emvco.com/specifications/emv-3-d-secure-protocol-and-core-functions-specification/

2. **3DS Server through Directory Server (DS) to Access Control Server (ACS)**. Using the information provided by the cardholder and data gathered within the 3DS Requestor Environment, the 3DS Server creates and sends an AReq message to the DS, which then forwards the message to the appropriate ACS.
3. **ACS through DS to 3DS Server**. In response to the AReq message, the ACS returns an ARes message to the DS, which then forwards the message to the initiating 3DS Server.

   Before returning the response, the ACS evaluates the data provided in the AReq message.

   - In a frictionless flow, the ACS determines that further cardholder interaction is not required to complete the authentication.
   - In the challenge flow, the ARes message indicates that further cardholder interaction is required to complete the authentication.

4. **3DS Server to 3DS Requestor Environment**. The 3DS Server communicates the result of the ARes message to the 3DS Requestor Environment which then informs the cardholder.
5. **3DS Client to ACS**. The 3DS Client initiates a CReq message based on information received in the ARes message. The manner in which this is done depends on the model: app-based or browser-based.
6. **ACS to 3DS Client**. The ACS receives the CReq message and interfaces with the 3DS Client to facilitate cardholder interaction. The manner in which this is done depends on the model: app-based or browser-based.
7. **ACS through DS to 3DS Server**. The ACS sends an RReq message that can include the Authentication Value (AV) to the DS, which then routes the message to the appropriate 3DS Server.
8. **3DS Server through DS to ACS**. The 3DS Server receives an RReq message and in response, returns an RRes message to the DS, which then routes the message to the ACS.
9. **Payment request** messages are outside the scope of the 3DS specification.
10. **Authentication request** messages are outside the scope of the 3DS specification.

Appendix B: Detailed Analysis of Key EMV 3DS Data Elements and Uses

This table outlines the default validation requirements for the Authentication Request (AReq) message. A specific Directory Server (DS) may specify other DS validations or actions to meet requirements specific for that DS.[6]

The source for Table 1 information on data elements, requirements and definitions was the EMVCo document, "EMV 3-D Secure Protocol and Core Functions Specifications Version 2.3.0.0."

Table 1: "Authentication Request" Message Data Elements

Data Element	Requirement	Definition	Potential Use	Notes	Channel (Browser (BRW)/ App)
3DS Method Completion Indicator	**Required**	Indicates whether the 3DSMethod successfully completed. Values accepted: • Y = Successfully completed • N = Did not run or did not successfully complete • U = Unavailable – 3DSMethod URL was not present in the Pres message data for the card range associated with the Cardholder AccountNumber.	Sent by 3DS Server in AReq		BRW
3DS Requestor Authentication Indicator	**Required**	Indicates the type of Authentication request. This data element provides additional information to the ACS to determine the best approach for handling an authentication request Values accepted: • 01 = Payment transaction • 02 = Recurring transaction • 03 = Installment transaction • 04 = Add card • 05 = Maintain card • 06 = Cardholder verification as part of EMV token ID&V • 07 = Billing agreement • 08 = Split shipment • 09 = Delayed shipment • 10 = Split payment	Risk assessment or customer validation if it was a $0 transaction		BRW/APP

[6] EMVCo, "EMV@ 3-D Secure Protocol and Core Functions Specification Version 2.3.0.0," September 2021, https://www.emvco.com/specifications/emv-3-d-secure-protocol-and-core-functions-specification/

Data Element	Requirement	Definition	Potential Use	Notes	Channel (Browser (BRW)/ App)
		• 11–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo) • 80–99 = Reserved for DS use			
3DS Requestor Authentication Information	Optional (recom-mended)	Information about how the 3DS Requestor authenticated the cardholder before or during the transaction.	Reduces need for step-up authentication		BRW/APP
3DS Requestor Authentication Method Verification Indicator	Conditional (based on DS rules)			Part of #3	BRW/APP
3DS Requestor Challenge Indicator	Optional	Indicates whether a challenge is requested for this transaction. Example: For 01-PA, a 3DS Requestor may have concerns about the transaction and request a challenge. For 02-NPA, a challenge may be necessary when adding a new card to a wallet. Note: When providing two preferences, the 3DSRequestor ensures that they are in preference order and are not conflicting. For example, 02 = No challenge requested and 04 = Challenge requested (Mandate). Values accepted: • 01 = No preference • 02 = No challenge requested • 03 = Challenge requested (3DS Request or preference) • 04 = Challenge requested (mandate) • 05 = No challenge requested (transactional risk analysis is already performed) • 06 = No challenge requested (data share only) • 07 = No challenge requested (strong consumer authentication is already performed) • 08 = No challenge requested (use Trust List exemption if no challenge required) • 09 = Challenge requested (Trust List prompt requested if challenge required) • 10 = No challenge requested (use low value exemption) • 11 = No challenge requested (secure corporate payment exemption)	Indicates whether step-up authentication is needed		BRW/APP

Data Element	Requirement	Definition	Potential Use	Notes	Channel (Browser (BRW)/ App)
3DS Requestor Decoupled Max Time	Optional	Indicates the maximum amount of time that the 3DS Requestor will wait for an ACS to provide the results of a Decoupled Authentication transaction (in minutes).	Not applicable	Very limited use case	BRW/APP
3DS Requestor Decoupled Request Indicator	Optional	Indicates whether the 3DS Requestor requests the ACS to use Decoupled Authentication and agrees to use Decoupled Authentication if the ACS confirms its use. Note: if the element is not provided, the expected action is for the ACS to interpret as N (do not use Decoupled Authentication). Values accepted: • Y = Decoupled Authentication is supported and is preferred as a primary challenge method if a challenge is necessary. (Transaction Status = D in ARes) • N = Do not use Decoupled Authentication. • F = Decoupled Authentication is supported and is to be used only as a fallback challenge method if a challenge is necessary. (Transaction Status = D in RReq) • B = Decoupled Authentication is supported and is to be used only as a primary or fallback challenge method if a challenge is necessary. (Transaction Status = D in either ARes or RReq)	Not applicable	Very limited use case	BRW/APP
3DS Requestor ID	**Required**	DS-defined 3DS Requestor identifier		See merchant name for similar applicability	BRW/APP
3DS Requestor Name	**Required**	DS-defined 3DS Requestor Name	Sent by 3DS Server in AReq	See merchant name for similar applicability	BRW/APP
3DS Requestor Prior Transaction Authentication Information	Optional (recom-mended)	Information about how the 3DS Requestor authenticated the cardholder as part of a previous 3DS transaction. Required for 3RI in the case of Decoupled Authentication Fallback or for SRC.	Not applicable	Very limited use case	BRW/APP
3DS Requestor URL	**Required**	The Fully Qualified URL of the 3DS Requestor website or customer care site. This data element provides additional information to the receiving 3DS system if a problem arises and contact information should be provided.	Risk-based authentication		BRW/APP
3DS Server Reference Number	**Required**	Unique identifier assigned by the EMVCo Secretariat upon testing and approval.	Incorrectly populated results in transaction failure		BRW/APP

Data Element	Requirement	Definition	Potential Use	Notes	Channel (Browser (BRW)/ App)
3DS Server Operator ID	Conditional (based on DS rules)	DS-assigned 3DS Server identifier. Each DS can provide a unique ID to each 3DS Server on an individual basis.	Incorrectly populated results in transaction failure		BRW/APP
3DS Server Transaction ID	**Required**	Universally unique transaction identifier assigned by the 3DS Server to identify a single transaction.	Not applicable		BRW/APP
3DS Server URL	**Required**	Fully Qualified URL of the 3DS Server to which the DS will send the RReq message after the challenge has completed. Incorrect formatting will result in a failure to deliver the transaction results via the RReq message.	Incorrectly populated results in transaction failure		BRW/APP
Account Type	Conditional Required if 3DS Requestor is asking cardholder which Account Type they are using before making the purchase. Required in some markets (for example, for merchants in Brazil). Otherwise, Optional.	Indicates the type of account. Values accepted: • 01 = N/A • 02 = Credit • 03 = Debit • 04–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo) • 80–99 = DS or payment system-specific	Helps payment systems route the transaction for faster authorization and more accurate risk assessment, which impacts fraud & dispute management Allows merchants to follow local card network rules & settlement practices, which can differ depending on whether a credit or debit card is used Ability to present cardholder tailored options for installment payments, rewards, or offers which might depend on whether they are using a credit or debit card		BRW/APP
Acquirer BIN	**Required**	Acquiring institution identification code as assigned by the DS receiving the AReq message.		settlement	BRW/APP
Acquirer Merchant ID	**Required**	Acquirer-assigned merchant identifier. This may be the same value that is used in Authentication requests sent on behalf of the 3DS Requestor and is represented in ISO 8583 formatting requirements. Value accepted: Individual Directory Servers may impose specific format and character requirements on the contents of this field.	See Merchant Name	Identifies merchant	BRW/APP

Data Element	Requirement	Definition	Potential Use	Notes	Channel (Browser (BRW)/ App)
Address Match Indicator	Optional	Indicates whether the Cardholder Shipping Address and Cardholder Billing Address are the same. Values accepted: • Y = Shipping Address matches Billing Address • N = Shipping Address does not match Billing Address	Strong indicator it is the account holder	Worth tracking	BRW/APP
Broadcast Information	Conditional (DS specific)	Structured variable information to be sent between parties involved in a 3DS authentication (3DS Server, DS, ACS). Can be used to send any information (maximum 4000 characters) between parties.	Merchant can inform issuer of prior risk assessment Merchant can inform issuer of loyalty program information Merchant can inform issuer of additional device data	Data sent needs to be understood by both the party sending and receiving. Would require coordination across the ecosystem. Likely best suited for network program definition.	BRW/APP
Browser Accept Headers	**Required**	Exact content of the HTTP except headers as sent to the 3DS Requestor from the cardholder's browser.	Strong Identifier – browser fingerprinting – uniqueness		BRW
Browser IP Address	Conditional	IP address of the browser as returned by the HTTP headers to the 3DS Requestor.	Useful - geographic region	Issue: Header IP address can be spoofed	BRW
Browser Java Enabled	**Conditional** Required when Browser JavaScript Enabled = true; otherwise, Optional.	Boolean that represents the ability of the cardholder browser to execute Java.	Improves transaction security by flagging environments where Java is enabled, which may indicate higher risk or potential vulnerabilities	Uncommon as it may allow access to altering data.	BRW
Browser Java Script Enabled	**Required**	Boolean that represents the ability of the cardholder browser to execute JavaScript.	Ensures secure & smooth transactions through improved user experience by enabling dynamic interactions during payment, device & behavior tracking for fraud detection, seamless authentication	It is very common to have Java Script enabled.	BRW

Data Element	Requirement	Definition	Potential Use	Notes	Channel (Browser (BRW)/ App)
Browser Language	**Required**	Value representing the browser language as defined in IETF BCP47. Returned from navigator.language property.	Browser fingerprinting – uniqueness		BRW
Browser Screen Color Depth	Conditional Required when Browser JavaScript Enabled = true; otherwise, Optional.	Value representing the bit depth of the color palette for displaying images, in bits per pixel. Obtained from cardholder browser using the screen.colorDepth property. Values accepted: • 1 = 1 bit • 4 = 4 bits • 8 = 8 bits • 15 = 15 bits • 16 = 16 bits • 24 = 24 bits • 32 = 32 bits • 48 = 48 bits	Browser fingerprinting – uniqueness		BRW
Browser Screen Height	Conditional Required when Browser JavaScript Enabled = true; otherwise, Optional.	Total height of the Cardholder's screen in pixels. Value is returned from the screen.height property.	Browser fingerprinting – uniqueness		BRW
Browser Screen Width	Conditional Required when Browser JavaScript Enabled = true; otherwise, Optional.	Total width of the cardholder's screen in pixels. Value is returned from the screen.width property.	Browser fingerprinting – uniqueness		BRW
Browser Time Zone	Conditional - Required when Browser JavaScript Enabled = true;	Time-zone offset in minutes between UTC and the cardholder browser local time. Note that the offset is positive if the local time zone is behind UTC and negative if it is ahead. Value is returned from the getTimezoneOffset() method. Example time zone offset values in minutes: If UTC -5 hours:	Browser fingerprinting – uniqueness		BRW

Data Element	Requirement	Definition	Potential Use	Notes	Channel (Browser (BRW)/ App)
	otherwise, Optional.	• 300 • +300 If UTC +5 hours: • -300			
Browser User-Agent	**Required**	Exact content of the HTTP user-agent header. Length: Variable, maximum 2048 characters JSON Data Type: String	Browser fingerprinting – uniqueness		BRW
Card/Token Expiry Date	Conditional	As described by element name.	Fraud mitigation		BRW/APP
Cardholder Account Information	Optional (strongly recommended)	Additional information about the cardholder's account provided by the 3DS Requestor.	Potential fraud mitigation	Refer to table A-10 in EMVCo document for list of elements; most elements have to do with the date the account was registered with 3DS.	BRW/APP
Cardholder Account Number	**Required**	As described by element name; could be a primary account number (PAN) or payment token.	Fraud mitigation Marketing	If payment token, additional uses may be limited	BRW/APP
Cardholder Account Identifier	Optional	Additional information about the account optionally provided by the 3DS Requestor.	Potential use will depend on what that additional information is	Not described in tables	BRW/APP
Cardholder Billing Address City	Conditional	As described by element name.	Fraud mitigation Marketing		BRW/APP
Cardholder Billing Address Country	Conditional	As described by element name.	Fraud mitigation Marketing		BRW/APP
Cardholder Billing Address Line 1	Conditional	As described by element name.	Fraud mitigation Marketing		BRW/APP
Cardholder Billing Address Line 2	Conditional	As described by element name.	Fraud mitigation Marketing		BRW/APP
Cardholder Billing Address Line 3	Conditional	As described by element name.	Fraud mitigation Marketing		BRW/APP

Data Element	Requirement	Definition	Potential Use	Notes	Channel (Browser (BRW)/ App)
Cardholder Billing Address Postal Code	Conditional	As described by element name.	Fraud mitigation Marketing		BRW/APP
Cardholder Billing Address State	Conditional	As described by element name.	Fraud mitigation Marketing		BRW/APP
Cardholder Email Address	Conditional	As described by element name.	Fraud mitigation Marketing		BRW/APP
Cardholder Home Phone Number	Conditional	As described by element name.	Fraud mitigation Marketing		BRW/APP
Cardholder Mobile Phone Number	Conditional	As described by element name.	Fraud mitigation Marketing		BRW/APP
Cardholder Name	Conditional	As described by element name.	Fraud mitigation Marketing		BRW/APP
Cardholder Shipping Address City	Conditional	As described by element name.	Fraud mitigation Marketing		BRW/APP
Cardholder Shipping Address Country	Conditional	As described by element name.	Fraud mitigation Marketing		BRW/APP
Cardholder Shipping Address Line 1	Conditional	As described by element name.	Fraud mitigation Marketing		BRW/APP
Cardholder Shipping Address Line 2	Conditional	As described by element name.	Fraud mitigation Marketing		BRW/APP
Cardholder Shipping Address Line 3	Conditional	As described by element name.	Fraud mitigation Marketing		BRW/APP
Cardholder Shipping Address Postal Code	Conditional	As described by element name.	Fraud mitigation Marketing		BRW/APP

Data Element	Requirement	Definition	Potential Use	Notes	Channel (Browser (BRW)/ App)
Cardholder Shipping Address State	Conditional	As described by element name.	Fraud mitigation Marketing		BRW/APP
Cardholder Work Phone Number	Conditional	As described by element name.	Fraud mitigation Marketing		BRW/APP
Device Channel	**Required**	Indicates the type of channel interface being used to initiate the transaction.	Useful for determining available data gathering methods (e.g., browser vs. app SDK).	Could be used for cross-channel or cross-device risk aggregation. Fraud uses for number of utilized devices/velocity checks.	BRW/APP
Device Information	Conditional (From DS to ACS)	Device information gathered by the 3DS SDK from a Consumer Device. This is JSON name/value pairs that as a whole Base64 URL encoded. This will be populated by the DS as unencrypted data to the ACS obtained from SDK Encrypted Data.	For example, device profiling: looking for device fingerprint drift or differences in payloads returned over time.	See payload: https://www.emvco.com/specifications/emv-3-d-secure-sdk-device-information-5/	APP
Device Rendering Options Supported	**Required**	Defines the SDK UI types that the device supports for displaying specific challenge user interfaces within the SDK.	Device rendering capabilities should not materially change from session to session. If it does, this might be an indication of spoofing or tampering.	Promising field, need to explore exceptions such as OS updates.	APP
DS Reference Number	Conditional (From DS to ACS)	Identifies the network directory server used to process the authentication request.	Not applicable	Only potential use would be to identify the DS to either a) prevent tampering, or b) collate information for reporting.	BRW/APP
DS Transaction ID	Conditional (From DS to ACS)	Uniquely identifies the authentication request at the network directory server.	Not applicable		BRW/APP
DS URL	Conditional (From DS to ACS)	Presents the URL to be redirected to from the 3DS Server for authentication processing.	Not applicable		BRW/APP
EMV Payment Token Indicator	Conditional	Indicates whether the account number was detokenized prior to sending the authentication request to the downstream party.	Inform other ecosystem parties on whether de-		BRW/APP

Data Element	Requirement	Definition	Potential Use	Notes	Channel (Browser (BRW)/ App)
			tokenization has already occurred. If it has, they can bypass that step, potentially improving the performance of the authentication request.		
EMV Payment Token Source	Conditional	Indicates where the detokenization occurred (either the 3DS Server or DS).	Not applicable		BRW/APP
Instalment Payment Data	Conditional (Required if merchant and cardholder have agreed to installment payments)	Indicates the maximum number of authorizations permitted for installment payments.	Indicator of credit worthiness. Could be used to market preference for installment payments or tailor payment options.	"EMV® 3-D Secure Protocol and Core Functions Specification v2.2.0–2.3.1.1," August 2023, combines installment and recurring: indicator, frequency, and date	BRW/APP
Merchant Category Code	Optional but strongly recommended to include if the merchant is also the 3DS Requestor	Specific code describing the merchant's type of business, product, or service.	Flag unusual transaction outside customer's typical MCC pattern. Provide relevant offers based on spending habits.		BRW/APP
Merchant Country Code	Optional but strongly recommended to include if the merchant is also the 3DS Requestor	Country Code of the merchant. This value correlates to the Merchant Country Code as defined by each payment system or DS.	Monitor transactions from high-risk countries. Offer dynamic currency conversion or targeted exchange rate offers. Help customers comply with international trade and financial regulations.		BRW/APP
Merchant Name	**Required**	Merchant name assigned by the acquirer or payment system. Same name used in the authorization message as defined in ISO 8583-1.	Tailor offers and recommendations toward frequently visited merchants.		BRW/APP

Data Element	Requirement	Definition	Potential Use	Notes	Channel (Browser (BRW)/ App)
		(Acquirer Merchant ID. This may be the same value that is used in authorization requests sent on behalf of the 3DS Requestor and is represented in ISO 8583-1 formatting requirements.)	Integrate with merchant loyalty programs. Provide clear merchant names on statements to improve transaction clarity, reducing confusion (reducing chargebacks).		
Merchant Risk Indicator	Optional (strongly recommended)	Merchant's assessment of the level of fraud risk for the specific authentication for both the cardholder and the authentication being conducted. Includes Shipping Indicator: • 08 = Pick-up and go delivery • 09 = Locker delivery (or other automated pick-up), or Transaction Characteristics: • 01 = Cryptocurrency transaction, or • 02 = NFT transaction or Gift Card Amount/Currency in ISO 4217	Analyze merchant risk profiles based on cryptocurrency or gift card acceptance. Could indicate potentially fraudulent mule and anti-money-laundering (AML) activity. Step-up authentication using biometrics.		BRW/APP
Message Category	**Required**	Identifies if the authentication request is for a Payment Authentication or Non-Payment (i.e., Card Add) transaction. Can also be used to identify additional use cases, such as 'Data Only.'	Indicate the type of transaction to align authentication request requirements and issuer risk assessment.		BRW/APP
Message Extension	Conditional (DS specific)	Represents a custom extension element exchanged between 3DS parties	Not applicable	Used to support network-specific programs (i.e., Visa Digital Authentication Framework)	BRW/APP
Message Type	**Required**	Identifies the EMV 3DS message (e.g., AReq, CReq, RReq)	Not applicable		BRW/APP
Message Version Number	**Required**	Protocol Version Identifier	Not applicable	Immediate use is for reporting on EMV 3DS performance across versions	BRW/APP
Notification URL	**Required**	Fully qualified URL of the system that receives the CRes message or Error Message. The CRes message is posted by the ACS through the cardholder browser at the end of the challenge and receipt of the RRes message.	More reliable for location than using an IP address.		BRW

Data Element	Requirement	Definition	Potential Use	Notes	Channel (Browser (BRW)/ App)
Purchase Amount	**Required**	Purchase amount in minor units of currency with all punctuation removed. (When used in conjunction with the Purchase Currency Exponent field, proper punctuation can be calculated.)	Flag unusually low or high amounts for alerts. Segment customers and tailor offers based on average transaction sizes. Consistently high purchase amounts may indicate higher or lower credit risk.		BRW/APP
Purchase Currency	**Required**	Currency in which purchase amount is expressed.	Foreign currency may be higher risk. Understand customer geographic preferences for targeted marketing. Offer customers ability to pay in home currency to improve customer experience.		BRW/APP
Purchase Currency Exponent	**Required**	Minor units of currency as specified in the ISO 4217 currency exponent. Example: USD = 2, Yen = 0.	Not applicable		BRW/APP
Purchase Date & Time	**Required**	Date and time of the authentication converted into UTC.	Target marketing campaigns to peak shopping times/dates. Flag transactions at unusual hours. Time marketing communication to when customers are most likely to purchase.		BRW/APP
Recurring Expiry	Conditional (Required if there is an end date)	Date after which no further authorizations are performed.	Help businesses manage subscriptions efficiently and predict revenue. Identify when subscriptions are due to trigger renewal offers.		BRW/APP

Data Element	Requirement	Definition	Potential Use	Notes	Channel (Browser (BRW)/ App)
Recurring Frequency	Conditional (Required if Recurring Indicator/ Frequency Indicator = 01)	Indicates the minimum number of days between authorizations for a recurring or installment transaction.	Help businesses manage subscriptions efficiently and predict revenue. Identify when subscriptions are due to trigger renewal offers.		BRW/APP
SDK App ID	**Required**	Universally unique ID created upon all installations of the 3DS Requestor App on a Consumer Device. This will be newly generated and stored by the 3DS SDK for each installation.	Use to correlate fraud and risk across devices *and* applications (e.g., multiple apps have real estate on a single device). Candidate for primary key for tracking purposes.		APP
SDK Encrypted Data	Conditional (Only from 3DS Server to DS)	JWE Object (represented as a string) as defined in Section 6.2.2.1 containing data encrypted by the SDK for the DS to decrypt.	Part of the normal process; not sure how this would be utilized for bolstering security. Ciphers used for encryption might become weak over type, but beyond the scope of this project.	Not applicable	APP
SDK Ephemeral Public Key	**Required**	Public key component of the ephemeral key pair generated by the 3DS SDK and used to establish session keys between the 3DS SDK and ACS.	Part of the normal process, not sure how this would be utilized for bolstering security. Ciphers used for encryption might become weak over type, but beyond the scope of this project.	Not applicable	APP
SDK Maximum Timeout	**Required**	Indicates maximum amount of time (in minutes) for all exchanges.	N/A		APP
SDK Reference Number	**Required**	Identifies the vendor and version for the 3DS SDK that is integrated in a 3DS Requestor App, assigned by EMVCo when the 3DS SDK is approved.	Utilize in conjunction with SDK App ID to put context around which vendor has deployed a particular SDK instance.		APP
SDK Transaction ID	Conditional (Required if deviceChannel is “01”)	Universally unique transaction identifier assigned by the 3DS SDK to identify a single transaction.	Could use this to bind transactions to an identity and look for fraud signals in the aggregate data set.		APP

Data Element	Requirement	Definition	Potential Use	Notes	Channel (Browser (BRW)/ App)
Transaction Type	Conditional	Identifies the type of transaction being authenticated. Values accepted: • 01 = Goods/service purchase • 03 = Check acceptance • 10 = Account funding • 11 = Quasi-cash transaction • 28 = Prepaid activation and load	Customize risk management to transaction type. Guide development of new products or services. Ensure regulatory compliance especially for quasi-cash and prepaid.	Values derived from the ISO 8583-1 Standard	BRW/APP
Trust List Status	Optional	Communication of trust list status between ACS, DS and 3DS Requestor. Example: "Would you like to add this Merchant to your Trust List?" Values accepted: • Y = 3DS Requestor is trust listed by cardholder • N = 3DS Requestor is not trust listed by cardholder • E = Not eligible as determined by issuer • P = Pending confirmation by cardholder • R = Cardholder rejected • U = Trust List status unknown, unavailable, or does not apply	Step-down authentication for trusted merchants. Integrated with loyalty programs to provide seamless rewards. More rigorous fraud screening for non-trusted merchants.	Valid values in the AReq message are Y or N	BRW/APP