In this Document:

EMV Payment Tokenisation – General FAQ

1. What is an EMV® Payment Token?

An EMV Payment Token is a surrogate value that replaces a primary account number (PAN) in the payment ecosystem. It is used as part of the payment chain and, when submitted in a transaction to the payment system, would cause a payment to occur. One PAN may have multiple EMV Payment Tokens associated with it depending on the usage scenario.

Payment tokens are restricted to specific domains. For example, a payment token may be usable only within the e-commerce acceptance channel at a specific merchant. They can be updated for a variety of reasons, such as in the event of a lost or stolen device or other lifecycle events.

2. What is the role of EMVCo within this area?

EMVCo defines the technical framework to generate, deploy and manage payment tokens in a reliable and interoperable manner globally. This technical framework must maintain compatibility with the existing payment infrastructure while delivering consistency and achieving a common level of robust security.

3. What are the benefits of using a payment token based on EMVCo's framework?

Payment tokenisation enhances the underlying security of digital payments by potentially limiting the risk typically associated with compromised, unauthorised or fraudulent use of PANs. Payment tokenisation achieves this by replacing PANs with payment tokens that differ significantly in terms of the ability to control or restrict usage to a particular transaction environment, device or other domain.

The implementation of payment tokenisation solutions aligned with EMV Payment Tokenisation Specification – Technical Framework v2.0 provides opportunities to enhance the security of digital payments for issuers, merchants, acquirers, payment processors and stakeholders in the broader acceptance community.

4. What are the outputs of EMVCo in relation to payment tokenisation?

- EMV Payment Tokenisation Specification – Technical Framework v2.0. The document describes the payment tokenisation landscape, key entities and the data fields to be implemented to support a payment tokenisation service. From a technical perspective, the framework explains the acceptance of payment tokens as a replacement to PANs and how security can be improved by limiting their use to a specific environment.

- EMVCo's registration service for token service providers. EMVCo has established a Token Service Provider Code (TSP Code), a three-digit code assigned to a TSP and maintained by EMVCo. The TSP Code is included in the 'token requester ID', which uniquely identifies the pairing of a 'token requester' with the TSP. This helps achieve transparency of the entity that provided the payment token.

- EMV Payment Account Reference (PAR). This newly defined data element enables merchants, acquirers and payment processors to link together a cardholder's EMV Payment Token with their PAN transactions without needing to use their underlying card account number. This enables all payment transactions – regardless of how they are initiated - to be processed in a consistent manner providing the payment acceptance community with the mechanism to support its consumers' transactional history for security and regulatory reasons. Examples include risk analysis and anti-money laundering, as well as to value-added services such as loyalty and couponing.

- EMVCo's registration process for Banking Identification Number (BIN) Controllers**.** A BIN Controller is responsible for the governance of PAR for the BINs that are under its direct control, including determining the approach to PAR data generation meeting the industry aligned PAR data format defined by EMVCo. BIN Controllers must register with EMVCo to be assigned a BIN Controller Identifier which is the unique first four characters of a PAR value.

5. What are the main changes in version 2.0 of the payment tokenisation technical framework?

The latest document addresses the adoption of payment token use cases in e-commerce beyond card-on-file, and offers enhancements to how payment tokens can be controlled within a single payment channel. It also builds on the ecosystem established in version 1.0 by refining the EMV payment tokenisation roles of token service provider and token requestor, introducing the roles of token programme merchant and token user, and detailing their interrelationships within the global payments environment.

Key updates within version 2.0 include the:

- Recognition that the entity introducing payment tokenisation to a payment ecosystem is responsible for establishing a **payment token programme.** This programme will define the business policies and processes for the generation, issuance and full lifecycle management of payment tokens to ensure their effective delivery.
- Additional detail on **payment token processing** which clarifies the use of a payment token in the authorisation process.
- Introduction of new concepts around shared and limited use payment token to support the expansion of **e-commerce use cases.**
    - *Limited use payment token is used for a single cardholder-initiated transaction and subsequent merchant-initiated transactions.*
    - *Shared payment token is used by one or more merchants or token users in scenarios where token requestors are not the merchant or token user.*
- Introduction of the **payment token assurance method** (replacing token assurance level) to enable a token requestor, such as an issuer, digital wallet provider or merchant, to have information available related to the identification and verification processes associated with the issuance of a payment token.
- Expansion of the **payment token issuance processes** to enable the request of a payment token with a value other than a PAN.
- Integration of the PAR Specification Bulletin-167.

6. Will the EMV Payment Tokenisation Specification – Technical Framework v2.0 be available to all parties without charge?

Yes. The EMV Payment Tokenisation Specification – Technical Framework v2.0 is available on a royalty-free basis to all industry participants.

7. How can the EMV Payment Tokenisation Specification – Technical Framework v2.0 be adopted by the payment systems and other payments stakeholders?

EMVCo provides a ‘tool box’ of technical documents and guidelines that facilitate the worldwide interoperability and acceptance of secure payment transactions. These materials are designed to be flexible and can be adapted regionally to meet national payment requirements and accommodate local regulations.

Any industry participant wanting to build an EMV payment token solution can use the technical framework.

EMVCo does not mandate the use of its specifications and industry participants are free to choose from any or all of the related EMV technical documents to address their customer and market needs.

To learn more about the role EMVCo plays within the payments ecosystem, read its Operating Principles.

8. Will EMVCo be offering a supportive testing and certification infrastructure for payment tokenisation?

There can be no certification from EMVCo in its traditional sense due to the framework nature of payment tokenisation and the diverse environment of the ecosystem and related infrastructure.

EMVCo has established and will manage the EMV TSP Code and BIN Controller Identifiers Registration Programmes to facilitate unique identification of the entities within this space.

9. Will the technical framework work for all payment systems, card products, networks and payment types such as credit, debit, commercial or prepaid for example?

The technical framework is designed to be inclusive of all product types and adaptable to implementer requirements.

10. Can industry participants develop proprietary solutions that will operate in adherence to the EMV technical framework?

While all EMVCo technical documents are designed for global interoperability, there is ample opportunity for implementers to create their own business solutions and proprietary add-ons, alongside additional services.

This level of implementation flexibility and support for a range of business models and use cases has been core to EMVCo’s work and continues to be a key priority for its payment tokenisation activity.

13. Will other industry stakeholders be able to provide input into EMVCo's payment tokenisation activity?

Yes. The EMV Payment Tokenisation Specification - Technical Framework v2.0 can be downloaded without charge and implemented on a royalty-free basis. EMVCo's aim in publicly sharing this specification technical framework is to promote transparency, maximise industry engagement, and encourage marketplace comments so that the document can continue to evolve in line with commercial and technical industry needs.

EMVCo has already witnessed significant industry interest in the specifications and calls on other parties to engage in its work through the EMVCo Associates Programme, a forum that allows stakeholders to play an active role in providing input to the technical and operational issues connected to all the EMV Specifications – including payment tokenisation – and related processes.

Industry participants can also stay informed of this activity through the EMVCo Subscriber Service.

14. In addition to engagement with industry participants through the EMVCo Associates Programme, how is EMVCo engaging with other standardisation bodies?

EMVCo does not work in isolation. It engages with other industry bodies, including many merchant groups globally, to understand and support individual sector requirements. EMVCo has started engagement with ANSI ASC X9, ISO TC68/SC2/WG13, PCI SSC and other industry partners to advance the various tokenisation standards and specifications to help ensure a harmonised set of industry documents related to payment and non-payment tokenisation. Clarity and consistent use of terminology will allow such standards and specifications to be clearly communicated to the marketplace.

1. **What is the objective of Payment Account Reference (PAR)?**

   PAR re-introduces a relationship that already exists in the payment ecosystem today for Primary Account Number (PAN) post EMVCo Payment Tokenisation. PAR may be used to link transactions initiated on Payment Tokens with transactions initiated on the underlying PAN to support the needs of a variety of payment processing and value added services that rely on PAN prior to the introduction of Payment Tokenisation.

2. **Why did EMVCo introduce PAR?**

   PAR was introduced to resolve the challenges faced in the broader acceptance community including Merchants, Acquirers and Payment Processors, in regards to linking Payment Token transactions with each other or transactions initiated on the underlying PAN. This supports a variety of payment processes and value added services.

3. **Can PAR Data be used to initiate a financial transaction or authorisation request?**

   PAR Data alone cannot be used to initiate a financial transaction, authorisation request or any other message such as capture, clearing or chargeback.

4. **Is PAR Data unique to a PAN or a Payment Account?**

   A Payment Account is the unique financial relationship between account holder(s) and a financial institution for a specific financial funding source (e.g. credit, debit, commercial, prepaid) represented by one or more PANs. The PAR Data is unique to a single PAN. A Payment Account that has multiple different PANs issued will need to ensure that unique PAR Data is generated for each unique PAN.

5. **Is PAR considered PCI data?**

   Please refer to the PCI Security Standards Council website. PAR Data should be used and protected in accordance with national, regional and local laws and regulations, including privacy laws.

6. **Is PAR a consumer identifier?**

PAR is not intended to be a consumer identifier in a similar way that an EMVCo Payment Token or a PAN is not intended to be a consumer identifier.

7. **Is PAR considered Personally Identifiable Information (PII) or Personal Data in accordance with privacy laws or regulations?**

   PAR is explicitly not intended to be used to identify cardholders and therefore it aims to minimise being categorised as PII (Personal Identifiable Information) / Personal Data. However, privacy laws vary by jurisdiction, and the categorisation of PAR may also depend on the manner of implementation. Since PAR is linked to the PAN, PAR might be governed under laws and BIN Controller requirements similar to those applicable to PAN.

8. **Can PAR Data be encoded in a magnetic stripe of a payment card?**

   Within Track 1 and Track 2 of a magnetic stripe there is insufficient space for PAR Data alongside other existing track data.

9. **How does PAR impact recurring payments?**

   PAR has no impact on recurring payments as PAR data alone cannot be used to initiate a financial transaction.

10. **Will PAR Data be sent in an authorisation response?**

    PAR Data may be made available in the authorisation response message according to BIN Controller governance and Payment Network support of PAR Data in messages. The assigned PAR Field is Field 56 for ISO 8583 (1987), Field 112 for ISO 8583 (1993), and Field 51 for ISO 8583 (2003).

11. **Who can generate PAR Data?**

    The BIN Controller is the entity that governs the generation of PAR Data and ensures PAR Data uniqueness.

12. **Will PAR Data be generated and issued by a Token Service Provider (TSP)?**

    PAR governance, including the designation of entities eligible to generate PAR Data, is the responsibility of the BIN Controller. TSP may be aware of PAR in support of business processes such as Token Provisioning and involvement in PAR Data generation.

13. **Does the PAR Data apply to both EMVCo Payment Tokens and their underlying PANs?**

    PAR Data is assigned to a single PAN and will be attributed to all Payment Tokens affiliated to that underlying PAN.

14. **Will PAR Data be unique?**

    PAR Data is intended to be unique within the PAR ecosystem governed by the BIN Controller as delineated by the EMVCo-assigned BIN Controller Identifier. The BIN Controller is responsible for ensuring the uniqueness for PAR Data associated with its BIN Controller Identifier.

15. **Who assigns the BIN Controller Identifier?**

    EMVCo assigns and maintains a list of BIN Controller Identifiers. Entities may register for a BIN Controller Identifier using EMVCo's registration form and process.

16. **How many characters is the PAR Data and who decides its unique values?**

    The PAR Data is made up of 29 characters and is comprised of a 4 character value that EMVCo assigns as the BIN Controller Identifier and a 25 character unique value that is generated and assigned in accordance with the governance of the BIN Controller.

17. **Is there any way of determining or predicting a Payment Token or a PAN from its PAR Data?**

    PAR Data should be generated in such a way as to ensure that PAR Data cannot be reverse engineered to determine or predict a PAN or any Payment Token.

18. **How can terminals recognise PAR Data as part of an EMV transaction?**

    EMVCo has assigned EMV Tag '9F24' for the PAR Data. Terminals should be able to pass the PAR Data along with other EMV data to the Merchant's Payment Processor or Acquirer within Field 55.

19. **Who governs a particular PAR implementation?**

    The governance of a PAR implementation is under the control of the BIN Controller.

20. **Who provides the PAR Enquiry Mechanism and when is it needed?**

The PAR Enquiry Mechanism is supported by the entity that defines PAR in accordance with the BIN Controller's governance of PAR. Merchants, Acquirers, Payment Processors, Token Service Providers and others can use the PAR Enquiry Mechanism to obtain the PAR Data in addition to or instead of the PAR Data's inclusion in transaction processing.

21. What are the permissible uses of PAR Data?

PAR Data usage is limited to the following functions:

- Completing the reversal of transactions with PAR Data and either a PAN or Payment Token (e.g. returns and chargebacks)
- Complying with regulatory requirements (e.g. Anti-Money Laundering (AML))
- Performing Risk Analysis (e.g. fraud detection and control services)
- Performing other non-payment operational needs as defined by the registered BIN Controller (e.g. supporting a loyalty program for consumers that have opted in to the service, as permitted by law)

All PAR implementations MUST NOT conflict with any national, regional or local laws or regulations, including those concerning privacy. Registered BIN Controllers MUST define appropriate rules governing the use of PAR Data for all implementations within the payment ecosystem.

22. Will a cardholder ever see the PAR Data?

Cardholders will be generally unaware of PAR Data even if provisioned. The lack of cardholder awareness of PAR Data should in no way impact the cardholder's ability to transact. The length and format of PAR Data is not considered to be consumer friendly.

23. Can the same PAR Data continue to be used when there is a change in the PAN?

For payment account lifecycle events such as lost/stolen cards or card replacements, the same PAR Data should be used to represent the successor PAN for the same payment account. In these scenarios, the continued use of the same PAR Data is at the discretion of the BIN Controller.

24. Does PAR only relate to payment cards with EMV Payment Tokenisation?

PAR is intended to allow the linkage of Payment Token transactions to transactions associated with PANs that have been tokenised. While PAR can also have broader industry use such as being assigned to PANs prior to any payment tokenisation, the underlying details for such are at the discretion on the BIN Controller and are implementation-specific and outside of EMVCo scope.

25. **Does the PAR Data need to be included in signed data?**

    This is under the discretion of the BIN Controller and is implementation-specific and outside of EMVCo scope.

26. **After closure of a consumer account should PAR Data be reused and, if so, how long after closure does the retention period last?**

    This is under the discretion of the BIN Controller and is implementation-specific and outside of EMVCo scope.

27. **Can PAR Data alone be used to initiate chargebacks, returns or reversals?**

    PAR Data alone cannot be used to initiate financial transactions. Transactions are initiated with a Payment Token or a PAN.

EMV Payment Tokenisation
Frequently Asked Questions (FAQ) – Technical

General Payment Tokenisation Questions

1. **How does Payment Tokenisation compare with strong encryption as another way of securing cardholder data?**

   Payment Tokens can help card-on-file merchants and digital wallet providers to greatly reduce the threat and consequences of a potential data breach. While encryption provides this as well, encrypted data cannot be processed without being first decrypted, thereby not fully alleviating the risks of a potential security breach. Brick and mortar merchants, however, may wish to use encryption to protect their transaction data since they cannot ensure that they will only process tokenised card/mobile transactions.

2. **Are Payment Tokens the same length as its associated PAN?**

   The Payment Token is a 13 to 19 digit numeric value that passes basic validation rules of an account number, including the Luhn check digit. Generally Payment Tokens are the same length as the PAN they replace, though this is not a requirement. Payment Tokens are generated within a BIN range that has been designated as a Token BIN Range and flagged accordingly in all appropriate BIN tables. Payment Tokens must not have the same value as or conflict with a real PAN.

3. **Can a single PAN be bound to multiple Payment Tokens?**

   Yes, one PAN may have multiple Payment Tokens associated with it depending on the use case and the payment domain assigned to the Token Requestor.

4. **Could the Payment Token linked to a PAN be updated, if necessary?**

   Payment Tokens may be updated for a variety of reasons, such as in the event of a lost or stolen device.

Use Case Implementation Related Payment Tokenisation Questions

5. **In the Mobile QR code (QRC) use case, QRC may be easily copied and stored. Are there plans to create one-time use QRC Payment Tokens or have a short validity period to enhance its security? Will the QRC contain only the Payment Token or will it include other dynamic components issued by the QRC service provider?**

The Mobile QR code use case is an example of how tokenisation could be used in an emerging acceptance environment. Currently EMVCo does not specify QR code solutions. However, the example use case illustrates how a QR code could include a token cryptogram to protect against reuse.

6. **In the specification, a payment enabler such as Original Equipment Manufacturer (OEM) device manufacturers could act as a Token Requestor. Does this mean that a handset provider's OEM could also request Payment Tokens? Can a telecommunications service provider also be the Token Requestor?**

   Yes, a handset provider's OEM or a telecommunications service provider could be a Token Requestor if approved by the Token Service Provider.

Merchant Related Payment Tokenisation Questions

7. **Can the Merchant/Acquirer match a Payment Token to the partial PAN (last 4 digits), in order to handle exception cases and chargeback flows?**

   Yes, where a Token Service Provider has enabled this capability, the last 4 digits of the PAN would be transferred back to the Merchant/Acquirer for business use.

8. **In the card-on-file merchant use case, if Merchant X is approved by a Token Service Provider to be a Token Requestor, could it then provide Token Request services for Merchant Y as well?**

   Yes, if Merchant X has contractual agreements to provide payment acceptance services to Merchant Y, then Merchant X's Payment Tokens could be used at Merchant Y, so long as the Token Service Provider can perform all necessary Token Domain Restriction Controls needed to ensure that the Payment Tokens cannot be used at non-participating merchants.

9. **The Assigned Token Assurance Level is one of the key outputs of a Token Request. How would this be used in a Payment Token-based transaction?**

   The Assigned Token Assurance Level indicates the level of Identification and Verification performed at the time the Payment Token was issued (or at subsequent times post-issuance). It may be used to drive proprietary business rules as defined by each Payment Network that could make specific rules pertaining to Token Assurance levels depending on supported use cases.

Token Service Provider/Card Issuer Related Payment Tokenisation Questions

10. **In the specification, the Token Service Provider already plays a role as an authorised party, managing issuance, security control and other functions related to the Payment Token. Could the Token Service Provider play other roles, such as a Payment Processor?**

    The Token Service Provider may be a wholly independent party from the Payment Network or Payment Processor or alternatively a Token Service Provider could be integrated with a Payment Network or Payment Processor.

11. **In the specification Figure 2, the Payment Network initiates the de-tokenisation function. Does this mean that only the Payment Network could be a Token Service Provider?**

    No, Figure 2 is an example implementation where the Payment Network is the Token Service Provider. Other organisations, such as Card Issuers or third party service providers could act as a Token Service Provider.

12. **Who can perform TSP services for a given BIN Range that allows token issuance?**

    The authorised user of the BIN.

13. **Should Token Service Providers apply to ISO/IEC JTC1 SC17/WG5 for new IINs (BINs) since the Token Service Provider will manage the Token BIN and Token BIN Range?**

    The specification does not necessarily require new IINs beyond those already licensed from ISO. In general Token Service Providers will need to use existing IINs for Token Issuance so that the Payment Tokens can pass through the payment network without coding changes being required by each entity in the processing chain.

14. **Why is Identification and Verification performed by the Card Issuer or Token Service Provider?**

    Identification and Verification is a method through which either the Token Service Provider or Card Issuer may validate the Cardholder and the Cardholder's account to establish the Token Assurance Level for the Payment Token. Since the Card Issuer is responsible for managing the Cardholder's account information, the Card Issuer will be able to evaluate this Token Assurance Level when a transaction occurs. The Token Service Provider can alternatively, or in conjunction with the Card Issuer, perform risk analysis with the information collected to help establish the Token Assurance Level.

15. **In the specification Figure 1, the Token Service Provider connects to the Card Issuer for Token Assurance Identification and Verification. Does this mean that the connection is physical (i.e. directly to the Card Issuer) or logical (i.e. the Token Service Provider connects to the Payment Network first and then transfers the data through the Payment Network to the Card Issuer)?**

    In the specification Figure 1, the data flow connection between the Token Service Provider and Card Issuer could be physical or logical. There is no requirement or restriction and entities may determine what business and technical objectives work best for them, respectively.

16. **In the specification, section 6 provides several examples of different Identification and Verification methods. This is a process within each use case combining risk mechanisms, account verification and Cardholder authentication together and may require cooperation by Card Issuers and Token Requestors. Does EMVCo have plans to further define Identification and Verification methods in more detail within the Payment Token Specification?**

    EMVCo will continue to assess industry need and where appropriate further define aspects of the EMV Payment Token Specification – Technical Framework v1.0.

17. **Is there any plan for EMVCo to validate implementations according to the Payment Token Specification?**

    EMVCo will continue to assess industry need as regarding potential testing and evaluation programmes it might put in place for the EMV Payment Tokenisation Specification – Technical Framework v1.0.

18. **I have ideas, concerns and questions to make sure this specification is implementable in my specific market, where can I download the specification and participate further?**

    As a global technical body, EMVCo ensures that its ISO-based specifications are open for use across different markets and in different environments, and can support a truly interoperable global payments framework. We encourage all industry stakeholders to engage in our work and contribute to the development of the EMV Specifications to enable smarter and more secure payments. The EMV® Payment Tokenisation Specification - Technical Framework v1.0 was published in March 2014 on our website www.emvco.com and can be downloaded by anyone without charge and implemented royalty-free. Our aim in publically sharing this specification framework is to promote transparency, maximise industry engagement and encourage market comments so that the document can evolve in line with commercial and technical market requirements. We have already witnessed significant interest and call on other parties to get involved through the EMVCo Associates Programme, a framework that allows stakeholders to play an active role in providing input to the technical and operational issues connected to the EMV Specifications and related processes. In addition to this, EMVCo also engages with other industry bodies, including many merchant groups globally, to understand and support individual sector requirements.