In this Document:

EMV® Payment Tokenisation –

General FAQ

Payment Account Reference (PAR) FAQ

Technical FAQ

Note that throughout these FAQs, the term "Technical Framework" refers to the EMV® Payment Tokenisation Specification – Technical Framework and the term "A Guide to Use Cases" refers to the EMV® Payment Tokenisation – A Guide to Use Cases. Unless otherwise specified, all references to the Technical Framework or A Guide to Use Cases refer to the current version.

EMV® Payment Tokenisation Frequently Asked Questions (FAQ) – General

1. What is an EMV Payment Token?

A Payment Token is a surrogate value that replaces the primary account number (PAN) in the payment ecosystem. Payment Tokens are designed to provide transparency to payment ecosystem stakeholders when accepting and processing Payment Tokens.

Payment Tokens are restricted in use through the application of Token Domain Restriction Controls. For example, a Payment Token may be usable only within the e-commerce acceptance channel at a specific Merchant.

2. Is the security of Payment Tokens delivered from just replacing the PAN?

No. While the replacement of PAN is one security benefit, the presence and application of Token Domain Restriction Controls (TDRC) is unique to Payment Tokens compared to PANs and critical to transaction integrity and fraud prevention.

Two examples are provided below. Both are use cases defined in A Guide to Use Cases

Example 1. Proximity at Point of Sale

The following layers of security can be implemented:

- PAN replaced to protect from any terminal skimming or in-transmission data attack
- Payment Token is within a Mobile Payment Application (MPA) that requires authentication to open and use the Payment Token (e.g. biometric or control for separate access authentication) providing authorised user information and validation
- Token Domain Restriction Controls that, as potential options, link the Payment Token to the specific device where the MPA is installed. Device information can be included with the transaction data as part of Token Processing
- Contactless transaction security, including cryptographic data, is used

Example 2: Card-on-File E-Commerce

The following layers of security can be implemented:

- PAN replaced to protect credential storage while in a Card-On-File Database and during the transmission of data to initiate Token Processing
- Cardholder identity verification via EMV® 3DS or other relevant Identity and Verification solution
- Transaction integrity using a Token Cryptogram that is obtained and then verified during Token Processing, ensuring transaction integrity

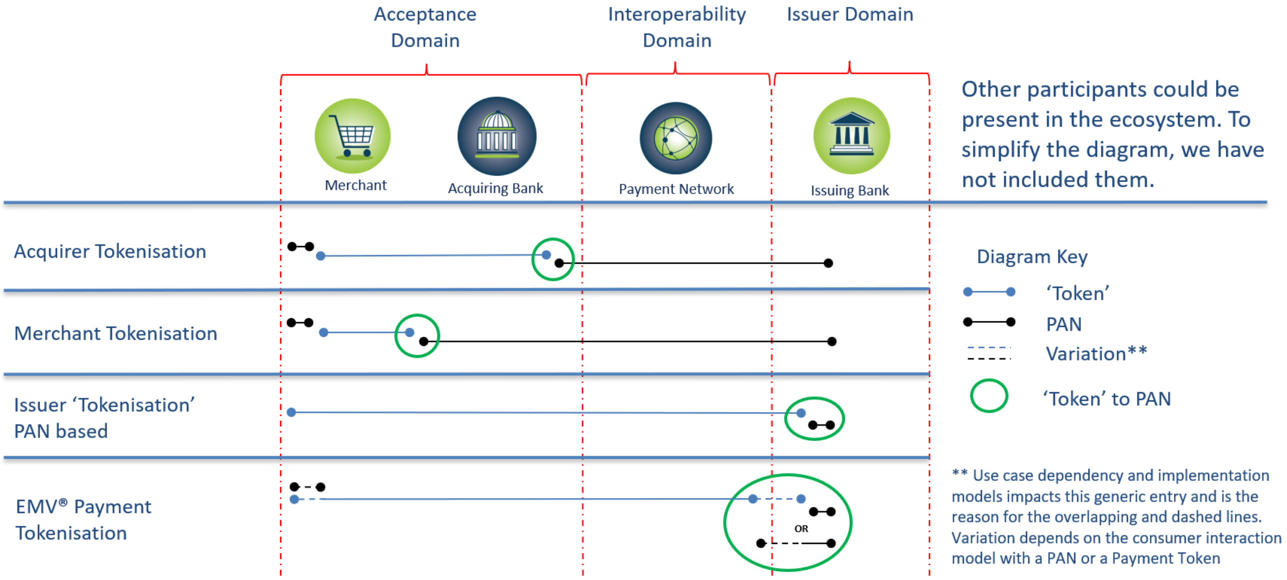
3. Are EMV Payment Tokens different from Acquirer or Issuer Tokens?

Yes, and EMVCo is aware of these tokenisation solutions. Other token solutions are often referred to within the payments ecosystem as “Acquirer Tokens” and “Issuer Tokens”. The use of EMV Payment Tokenisation is not intended to exclude other solutions and they may co-exist based on implementation decisions.

Acquirer Tokens typically will be a replacement value for a PAN but are used exclusively within the acceptance domain (of Merchants and Acquirers).

Issuer Tokens are typically created by Issuers as replacements for the PAN and are generally known as one-time use account numbers or virtual cards. Issuer Tokens do cross the interoperability domain.

The following diagram is intended to show characteristics of these various types of tokens and the point at which the token is replaced with the PAN for transaction processing purposes.


Acceptance Domain
Interoperability Domain
Issuer Domain
Merchant
Acquiring Bank
Payment Network
Issuing Bank
Other participants could be present in the ecosystem. To simplify the diagram, we have not included them.
Acquirer Tokenisation
Merchant Tokenisation
Issuer 'Tokenisation' PAN based
EMV® Payment Tokenisation
OR
Diagram Key
'Token'
PAN
Variation**
'Token' to PAN
** Use case dependency and implementation models impacts this generic entry and is the reason for the overlapping and dashed lines. Variation depends on the consumer interaction model with a PAN or a Payment Token

For additional information on non-EMV payment tokens, please reference these external materials below:

- Secure Payments Technologies Demystified – Payments Security Taskforce
- U.S. Payments Security Evolution and Strategic Road Map – Payments Security Taskforce
- EMV Payment Tokenization Primer and Lessons Learned – US Payments Forum
- What is the difference between "acquiring tokens", "issuer tokens", and "Payment Tokens"? – PCI Security Standards Council

4. What is the role of EMVCo within Payment Tokenisation?

EMVCo defines the Technical Framework to generate, deploy and manage Payment Tokens in a reliable and interoperable manner globally at the point of acceptance. The aim is to provide a level of commonality across the payment ecosystem to support adoption while enabling levels of differentiation that promote innovation. This is achieved while maintaining compatibility with the existing payment infrastructure and providing the potential for increased security by limiting the risk typically associated with compromised, unauthorised or fraudulent use of PANs.

5. **What are the benefits of using a Payment Token based on EMVCo's Technical 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 its intended use, e.g. a device or other domain.

   The implementation of Payment Tokenisation solutions aligned with the Technical Framework provides opportunities to enhance the security of digital payments for Issuers, Merchants, Acquirers, payment processors and stakeholders in the broader acceptance community.

6. **What are the outputs of EMVCo in relation to Payment Tokenisation?**

- EMV® Payment Tokenisation Specification – Technical Framework. The Technical Framework describes the Payment Tokenisation ecosystem, key roles and the fields to support Payment Tokenisation. From a technical perspective, the Technical Framework explains the acceptance of Payment Tokens as a surrogate value that replace the PAN. Payment Tokens limit usage to a specific domain. This reduces the risk typically associated with compromised, unauthorised or fraudulent use of PANs.

- EMV® Payment Tokenisation – A Guide to Use Cases. A Guide to Use Cases describes a limited number of Payment Tokenisation use case examples, some of which are based on established EMV defined-technology. These examples exist to show the extent and flexibility of the Technical Framework. They are not intended to be exhaustive or representative of all possible usage scenarios supported by the Technical Framework.

- EMVCo's registration service for Token Service Providers Codes. EMVCo has established a Token Service Provider Code (TSP Code), which is 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.

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

For the purpose of clarity, Card Issuers who have been assigned BIN(s) by an ISO IIN Blockholder are not BIN Controllers for the BINs assigned by an ISO IIN Blockholder.

7. **Why have the registration processes for TSP Code and BIN Controller ID been updated?**

   A review of both registration services revealed a number of opportunities to enhance and refine current processes.

   However, applicants continue to have access to a clearly defined step-by-step process. The processes continue to leverage DocuSign® for time saving online form submission and online signatures.

8. **Is there any impact from the registration process changes to existing TSP Code or BIN Controller ID registrants?**

   No – zero impact from the process enhancements for existing entities that have a TSP Code and/or BIN Controller ID from EMVCo.

9. **How can the status of an EMVCo TSP Code or BIN Controller ID be checked?**

   EMVCo maintains listings of Registered IDs, including the TSP Code and BIN Controller IDs on its website at www.emvco.com. If the TSP Code or BIN Controller ID is listed on the EMVCo website, then the agreement between EMVCo and the registered entity is active. The TSP or BIN Controller can choose to supply a copy of their EMVCo Letter of Registration to any party or entity that may request it as further verification that they are registered with EMVCo.

10. **Can all merchants process EMV Payment Tokens?**

    An EMV Payment Token is interoperable and any PAN in an authorisation message may be replaced by a Payment Token. While Payment Tokens are interoperable, a merchant may have additional implementation specific requirements which are subject to the specifics of the use case(s) being deployed by the merchant.

    For example, a Merchant that already supports EMV® Contactless transactions could accept Payment Tokens as described in the use case Proximity at POS from A Guide to Use Cases. Other use cases may have additional implementation requirements necessary to support use of Payment Tokens.

11. What are the reserved TSP Codes of 000, 998 and 999 used for?

There are 3 special or reserved TSP codes that are retained for specific purposes:

- 000 can be used for testing purposes by any TSP or by a TSP in test environments that is waiting for their own TSP Code registration to progress. This must never be used in a live production environment.
- 998 is available for a Card Issuer who acts as a TSP for their own portfolio and has a Card Issuer IIN assigned by ISO. The implementation usage may include “not on us” (separate Acquirer) and “on us” (they are the Acquirer and Card Issuer).
- 999 has some similarities to the 998 option, the Card Issuer and Acquirer may be different entities but the cards are so-called “Private Label” such as a store card or other closed loop card.

The 998 and 999 values are NOT tracked by EMVCo, they are reserved values that may only be used for the stated purposes.

A Token Service Provider, that already has an assigned TSP Code from EMVCo, that is also supporting activities described as eligible to use the 998 or 999 reserved codes should continue to use their assigned TSP code for all TSP activities. It is not required to use the reserved TSP codes.

12. What are the changes in version 2.3 of the Technical Framework?

The latest Technical Framework has minor revisions and clarifications in the following areas:

- Replacement of the term “channel” with “POS Entry Mode” and / or “Usage Scenario” to more accurately reflect the situation
- Replacement of the term “mapping to” with “affiliation with” to describe the relationship between a Payment Token / Token Expiry Date and the underlying PAN / PAN Expiry Date
- Removal of Token Requestor Type. Different types of Token Requestors are addressed by variations in the application of Token Domain Restriction Controls
- Removal of the defined terms Limited Use Payment Token and Shared Payment Token to reflect the emphasis on the use of all Payment Tokens being constrained by their Token Domain Restriction Controls
- Editorial changes regarding Payment Tokenisation lifecycle management to provide consistency with A Guide to Use Cases

- Addition of the ISO 20022 ATICA Messages to Technical Framework Section 9 - Payment Token Fields Used in ISO 8583 and 20022 ATICA Messages
- Clarification on the use of Token Cryptograms in Merchant-Initiated Transactions in Technical Framework Section 10 - Token Processing

13. Why have the definitions for Shared Payment Token and Limited Use Payment Token been removed?

These definitions were introduced to support some new concepts. One of these is Token Users, who do not have Payment Tokens for their own unique use. A second example is Payment Tokens that are constrained to a very specific situation, such as an e-Commerce Guest checkout. By making the two definitions, the unintended consequence was that there were “Types” of Payment Tokens.

A Payment Token’s Token Domain Restriction Controls define and constrain its use as intended by the Token Service Provider based on Token Programme policies and processes. The removal of the defined terms removes the unintentional suggestion that there are “Types” of Payment Tokens.

Whether the Payment Token is used by multiple Tokens Users (previously known as “Shared”) or is intended for a single Guest Checkout (previously known as “Limited Use”), or assigned for use by a single Token Requestor is simply a factor of the Payment Token’s Token Domain Restriction Controls.

14. What are the considerations for Token Issuance for a Token Requestor supporting Token Users?

One of the key aspects of the Technical Framework is to allow flexibility and innovation. This means that there are multiple usage scenarios and possibilities of how a function may be implemented or a role fulfilled. A Token Requestor can request Payment Tokens for themselves and/or for any Token User(s) that they support. If a Token Requestor does support Token Users, the Payment Tokens may be used by multiple Token Users and constrained by appropriate Token Domain Restriction Controls. The Token Requestor may also use Payment Tokens for their own direct transactional needs. Each of the above scenarios are implementation decisions that are subject to the policies and processes for each individual Token Programme.

15. Why is a role category of Payment Tokenisation Aggregator included?

Within the broader Payments Industry ecosystem, it is already common for Service Providers, sometimes referenced as Third Party Service Providers, to support roles and functions on behalf of an entity, such as a Card Issuer or an Acquirer. Similarly, there are service providers within the Payment Tokenisation ecosystem. This new role category has been defined to enable support within the Technical Framework of service providers in a Payment Tokenisation role(s).

16. What is a Token Requestor Aggregator?

This is a role within Payment Tokenisation where a service provider is providing services to support a Token Requestor interacting with a Token Service Provider. A Token Requestor may have a Token Requestor Aggregator provide services to support the necessary processes for Token Requests, but the Token Requestor Aggregator will use the Token Requestor ID of the Token Requestor for whom the Token Requestor Aggregator is providing the “on behalf of” service.

17. Can an Entity be both a Token Requestor and a Token Requestor Aggregator?

Yes. An entity may perform multiple roles. If an entity is performing the role of Token Requestor, but also provides Token Requestor Aggregator services, it must use the correct Token Requestor ID based on the role performed.

- As a Token Requestor Aggregator, the Token Requestor ID used will always be that of the Token Requestor for whom the Token Request is being made. The Token Requestor Aggregator role does not have a Token Requestor ID.
- As a Token Requestor, the Token Requestor ID used will be assigned by the Token Service Provider.

18. What is a Card Issuer Aggregator?

This is a role within Payment Tokenisation where a service provider is providing services to support a Card Issuer interacting with a Token Service Provider. In the traditional Payments Industry, a Card Issuer may have service providers to support the cardholder management system, manage transaction processing etc.

A Card Issuer may have a Card Issuer Aggregator provide services on its behalf to support some of the processes for Payment Tokenisation.

19. How does the “A Guide to Use Cases” further elaborate on the Lifecycle Management requirements introduced in the Technical Framework?

The Technical Framework covers the lifecycle management (LCM) aspects, primarily from the interfaces aspect (Section 8.6) to ensure that there are common interfaces to support both PAN lifecycle management events as well as Payment Token lifecycle management events within a Token Programme. It is important to note that lifecycle management is a concept that has existed for PANs prior to the introduction of Payment Tokenisation into the payment ecosystem. The introduction of Payment Tokens into the ecosystem requires that PAN LCM interfaces are supported to ensure Payment Tokens remain affiliated with the correct PAN and that Payment Token LCM interfaces are in place to ensure the ongoing lifecycle management of Payment Tokens.

With A Guide for Use Cases, the use cases provide practical examples of LCM situations that will be managed within a Token Programme. The following helps identify the interface(s) defined in the Technical Framework that might be used within a Use Case example.

Use Case Example	Technical Framework LCM Interface(s) Used
Merchant Deletion of Payment Credential	Unlink Payment Token
Lost / Stolen Consumer Device	Initially Suspend Payment Token followed by Unlink Payment Token
PAN Replacement	Initially Update PAN Attributes followed by Update Payment Token Attributes

20. Will the EMV® Payment Tokenisation Specification – Technical Framework be available to all parties without charge?

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

21. **How can the EMV® Payment Tokenisation Specification – Technical Framework be adopted by payment 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.

22. **Will EMVCo be offering a supportive testing and certification infrastructure for Payment Tokenisation?**

    There can be no certification level programme requirements defined in EMVCo for EMV Payment Tokenisation as the specification is defined at a higher Technical Framework level. Other parties in the ecosystem such as Payment Systems may have certification level requirements for implementations and this is beyond the scope of EMVCo.

    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.

23. **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.

24. **Can industry participants develop proprietary solutions that will operate in adherence to the 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.

25. **Will other industry stakeholders be able to provide input into EMVCo's Payment Tokenisation activity?**

    Yes. The Technical Framework can be downloaded without charge and implemented on a royalty-free basis. EMVCo's aim in publicly sharing this 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.

26. **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.

EMV® Payment Tokenisation
Frequently Asked Questions (FAQ) – Payment Account Reference (PAR)

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

   PAR establishes the relationship between affiliated Payment Tokens and the underlying PAN, which had been previously achieved solely by PAN, before Payment Tokenisation was introduced. PAR may be used to link transactions initiated on Payment Tokens with transactions initiated on the underlying PAN. The payment ecosystem can also benefit by adopting practices of assigning PAR Data to PANs prior to any issuance of Payment Tokens so that PAR Data becomes widely available and further justifies enhancements to business practices and technologies to leverage PAR Data as the linkage mechanism between PANs and Payment Token(s).

   For further information, please refer to the EMV® White Paper on Payment Account Reference.

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 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 unique PAR Data 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. TSPs may be aware of PAR in support of business processes such as Token Provisioning. Any involvement in PAR Data generation is under the governance of the BIN Controller.

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

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 affiliated with multiple Payment Tokens?**

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

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 Technical Framework, 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.

6. **Does the Technical Framework support reversible Payment Tokens?**

   The methods of Token Generation are implementation specific and are defined in the policies and processes established in a Token Programme.

   De-Tokenisation is the process of converting a Payment Token to its underlying PAN. The description of “reversible” is not something used within the Technical Framework.

7. **Does the Technical Framework support cryptographic Payment Tokens?**

   The methods of Token Generation are implementation specific and are defined in the policies and processes established in a Token Programme. Considerations for the structure of Payment Tokens can be found in section 4.1 Numeric Management, of the Technical Framework.

8. **Can a single entity perform one or more Payment Tokenisation role?**

   Yes, an entity can perform multiple Payment Tokenisation roles.

   The Technical Framework is not intended to define who can perform certain roles as these will be implementation specific decisions and managed by the policies and processes of any given Token Programme.

9. **Where can I learn more about the status of a Payment Token which is used in the field “Token Status Indicator” in the 3DS Token Message Extension?**

   Payment Token related data is stored in the Token Vault (section 4.3 and section 5.6 of the Technical Framework). This includes the Token Expiry Date, Token Domain Restriction Controls and the status of the Payment Token. The status of the Payment Token may change during its ongoing use. Examples include, but are not limited to, whether it is active or suspended. The status values may be defined in the Token Programme. Changes to the status of the Payment Token are managed via the interfaces described in section 8.6 of the Technical Framework.

10. **What is the purpose of the "Token Additional Data" field which is defined in the 3DS Token Message Extension?**

    The Token Additional Data is a field that is defined in the optional 3DS Token Message Extension. This field allows the Token Service Provider, subject to the polices and processes of the relevant Token Programme(s), to provide any necessary data from the Token Vault and make it available to the Directory Server (DS) and/or Access Control Server (ACS). The aim is to give as much relevant data as possible to the DS and/or ACS to facilitate authentication for 3DS requests that involve a Payment Token. The contents and any requirements for the use of this field are Token Programme specific.

Merchant Related Payment Tokenisation Questions

11. **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.

12. **The Assigned Token Assurance Method 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 Method 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 by ecosystem participants for proprietary business needs.

13. **Is the Use of a Token Cryptogram Allowed with a Merchant-Initiated Transaction?**

    There are no restrictions on a Token Programme defining support for the use of a Payment Token Cryptogram to be used with a Merchant-Initiated Transaction. For this reason, Table 10.6 lists Token Cryptogram as "optional" for Merchant-Initiated Transactions.

14. **Can a Token Cryptogram from a Cardholder-Initiated Transaction be re-used in a subsequent Merchant-Initiated Transaction(s)?**

    A Token Cryptogram from a Cardholder-Initiated Transaction may be re-used in subsequent Merchant-Initiated Transactions for reasons which are outside the scope of the Technical Framework. However, any re-use of Token Cryptograms should follow rules as defined by each Token Programme.

Token Service Provider/Card Issuer Related Payment Tokenisation Questions

15. **In the Technical Framework, 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.

16. **Who can perform TSP services for a given BIN Range that allows Token Issuance?**

    The Token Service Provider is a role within the Payment Tokenisation ecosystem that is carried out by entities authorised to provide Payment Tokens to registered Token Requestors within a Token Programme.

17. **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 Technical Framework does not necessarily require new IINs beyond those already licensed from ISO. In general, Token Programmes will need to use existing IINs for Token Issuance so that the Payment Tokens can pass through the payment ecosystem with minimal impact.

18. **Is there any plan for EMVCo to validate implementations according to the Technical Framework?**

    Technical frameworks do not have sufficient detail to support an EMVCo testing infrastructure to confirm product/service compliance.

19. **I have ideas, concerns and questions to make sure this Technical Framework is implementable in my specific market, where can I download the Technical Framework 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 is published on our website www.emvco.com and can be downloaded by anyone without charge and implemented royalty-free. Our aim in publicly 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.