



**In this Document:**

- [EMV Payment Tokenisation – General FAQ](#)
- [EMV Payment Tokenisation – Payment Account Reference \(PAR\) FAQ](#)
- [EMV Payment Tokenisation – Technical FAQ](#)

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

**Status of EMVCo's Payment Tokenisation Activity**

**1. What is an EMVCo compliant payment token?**

A payment token based upon EMVCo Specifications is a reversible token generated at the payment issuer level. This means that the reversible token can be securely mapped back to its original card account number by the provider of the payment token and authorised entities only. 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.

The tokenisation process happens in the background in a manner that is typically invisible to the consumer. Such tokens could be used by merchants or digital wallet operators, and can be stored in EMV chip cards and NFC devices. The payment tokens are restricted to specific domains. For example, a token may be usable only within the e-commerce acceptance channel at a specific merchant. An additional payment token capability is the ability to unlink the token from the original card account number in case that token is either no longer needed, or a mobile device or card has been lost or stolen. Payment tokens will be of particular value in card-not-present transactions, as well as in mobile devices and other form factors.

**2. What is the first work item to be progressed by EMVCo?**

EMVCo has released the EMV Payment Tokenisation Specification – Technical Framework v1.0. Available to download from the EMVCo website without charge, the technical document provides the payments community with the framework to facilitate consistent, secure and globally interoperable digital payments when using a mobile handset, tablet, personal computer or other smart device.

**3. What will I learn from reading the EMV Payment Tokenisation Specification – Technical Framework v1.0?**

The document provides readers with a clear insight into EMVCo's work and remit to standardise payment tokenisation and encourage global interoperability. It describes



the payment tokenisation landscape, the key entities necessary to support payment tokenisation, the data fields that can be implemented to support a tokenisation service and the benefits of adopting a unified approach, as well as delineating several payment token use cases.

From a technical perspective, the document explains the role of the specification in facilitating broad-based acceptance of a payment token as a replacement for a traditional card account number. This includes data message formats to ensure the interoperability of payment tokens and the consistent approach that should be used to route and authenticate a payment token. The framework also explains how security can be improved by limiting payment tokens for use in a specific environment, and how an existing ecosystem can advance to become globally interoperable.

In addition, Section 1 of the EMV Payment Tokenisation Specification – Technical Framework v1.0 provides defined terms and other useful information relevant to parties new to payment tokenisation.

#### **4. What is the difference between a specification and framework?**

EMVCo calls this release a framework since it is the foundation of the tokenisation specification. It serves as a specification in that it is implementable for defined use cases and is available to download and use by the industry. EMVCo actively solicits EMVCo Associate, Subscriber and public feedback to support enhancements and inclusion of additional use cases and further ecosystem requirements. Over time, the specification will evolve with industry input to broaden its applicability to diverse marketplace needs.

#### **5. Will the specification be available to all parties without charge?**

Yes. All EMV Specifications, including the EMV Payment Tokenisation Specification – Technical Framework v1.0, are available to all payment participants in the industry, royalty-free. EMVCo has an established framework for delivering payment specifications through open and transparent processes in consultation with industry stakeholders.

#### **6. What are the benefits of using a payment token based on EMVCo Specifications?**

As the payment token generation process happens at the payment issuer level, it will bring many benefits to:

- Issuers. Consistency in risk management processes and implementation of cardholder data for current and emerging mobile and digital solutions.



- Acquirers. Enabling their merchants to securely participate in the payments system, using payment tokens that work with the existing services they provide today. Additionally they have the ability to provide new payment token services to their merchants.
- Merchants. By utilising the current payments infrastructure, merchants may not have to build their own proprietary systems to secure payment data. Once they have put in place the capability to convert their account numbers into payment tokens, they can capitalise on existing integration processes within the larger payments community. Such payment tokens are also compatible with the existing acceptance infrastructure, so merchants can accept transactions initiated with payment tokens without needing to make substantial costly changes to their acceptance environments.

### **Implementation of EMVCo's Payment Tokenisation Work**

#### **7. How will the specification be adopted by the payment systems and other payments stakeholders?**

EMVCo recognises that what is being progressed today is comparable to how the industry came together to develop and implement the required infrastructure for magnetic stripe, chip-based and NFC payments on a global scale. While EMVCo provides a 'tool box' of specifications, these are adaptable to meet regional variations and the unique needs of different industry stakeholders. It is ultimately up to the stakeholders to determine how the EMVCo Specifications will be adopted.

#### **8. Will the specification work for all brands, card products, networks and payment types such as credit, debit, prepaid, etc.?**

Yes, the specification is designed to be inclusive of all product types and adaptable to implementer requirements.

#### **9. Can EMVCo's Specification be used for non-payments?**

The aim of the specification is to create a set of requirements where payment tokens can interoperate and be used in a secure manner. These same requirements, while not designed for non-payment use, can be applied as best practices for non-payment tokens where applicable, for example, with merchant closed loop loyalty cards.

#### **10. Will EMVCo's Specification support multiple payment environments, for example e-commerce, m-commerce as well as in-store transactions or online purchases?**



EMV Payment Tokenisation Specification – Technical Framework v1.0 is form factor agnostic and is designed to support end-to-end tokenisation for the above use cases.

At this early stage, EMVCo is aware that additional work may need to be undertaken to include and address new use cases and operational considerations. EMVCo is working with multiple standards organisations to discuss its tokenisation specification, as well as engaging with industry participants directly through the EMVCo Associates Programme. For further details see below – EMVCo Tokenisation Activity and the Wider Payments Community.

It is worth noting that since payment tokens based on EMVCo Specifications must be domain-limited, there are some use cases for which an EMVCo token would not be suitable, for example, a token for a magnetic stripe card. Such a token would have to be usable at any location where magnetic stripe cards are used, and this would be too broad a domain for a token as defined by EMVCo to add value.

**11. Are the EMVCo Specifications available to all parties who wish to participate in the payment tokenisation space?**

Yes, EMVCo provides a 'tool box' of royalty-free specifications which are available to be adapted to meet regional variations and the unique needs of different industry stakeholders.

Those wishing to build EMVCo specification-compliant products or services can use the specification to meet EMVCo's global requirements.

**12. Can industry participants develop proprietary frameworks that will operate in adherence to the specification?**

While EMVCo Specifications are designed for global interoperability, there is ample opportunity within these specifications 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 the EMVCo Specifications and continues to be a key priority for its tokenisation work.

**EMVCo Payment Tokenisation Activity and the Wider Payments Community**

**13. To create a technology neutral specification requires broad industry participation in its development. Will other industry stakeholders be able to provide input into EMVCo's payment tokenisation activity?**

The EMV® Payment Tokenisation Specification - Technical Framework v1.0 was published in March 2014 on EMVCo's website. It can be downloaded without charge



and implemented royalty-free. EMVCo's 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 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 framework that allows stakeholders to play an active role in providing input to the technical and operational issues connected to all the EMV Specifications – including tokenisation – and related processes.

**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 specifications and ensure a harmonised set of industry documents related to payment and non-payment tokenisation. Clarity and consistent use of terminology will allow specifications and their offering to be clearly communicated to the marketplace.

**15. Is EMVCo's work complementary to that being developed by other bodies?**

EMVCo has developed a technical specification which will enable the creation of a globally interoperable, implementable tokenisation framework used for payment initiation. The specification from EMVCo maintains compatibility with the current payment infrastructure and is intended to complement the existing EMV Chip Specifications to ensure consistency across all payment environments.

By adopting consistent terminology and remaining engaged with the various national and international standards groups, the goal is to allow market stakeholders to easily understand its offering and how it interconnects with other standards and specifications as and when they are brought to market.

At this stage, EMVCo is not aware of any conflicts between its specification and other tokenisation standards which are scheduled for market release.

**EMVCo Credentials**

**16. What experience does EMVCo have to manage and maintain a payment tokenisation specification?**



EMVCo has the strategic breadth, industry knowledge and technical depth to develop a holistic specification that will support digital payments. Its member-owners – American Express, Discover, JCB, MasterCard, UnionPay and Visa – have committed resources to this initiative to ensure the specifications are brought to market successfully and effectively.

In addition to EMVCo's expertise, the global technical body has a legal framework that enables collaboration within the payments community, and a well-established track record of technical specification delivery. EMVCo is committed to developing pro-competitive, objective specifications as the risk landscape continues to evolve.

The global adoption of EMV Chip Specifications and the international payment framework that has been implemented will also assist in the acceptance of this new framework at an international level. This reach and coverage is important to support the digital payments community in achieving its potential.



## **EMV Payment Tokenisation Frequently Asked Questions (FAQ) – Payment Account Reference**

### **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](http://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.