EMV®
Payment Account Reference (PAR)

EMVCo White Paper on Payment Account Reference (PAR)

Version 2.1.1

February 2022

Legal Notice

This document is subject to change by EMVCo at any time. This document does not create any binding obligations upon EMVCo or any third party regarding the subject matter of this document, which obligations will exist, if at all, only to the extent set forth in separate written agreements executed by EMVCo or such third parties. In the absence of such a written agreement, no product provider, test laboratory or any other third party should rely on this document, and EMVCo shall not be liable for any such reliance.

No product provider, test laboratory or other third party may refer to a product, service or facility as EMVCo approved, in form or in substance, nor otherwise state or imply that EMVCo (or any agent of EMVCo) has in whole or part approved a product provider, test laboratory or other third party or its products, services, or facilities, except to the extent and subject to the terms, conditions and restrictions expressly set forth in a written agreement with EMVCo, or in an approval letter, compliance certificate or similar document issued by EMVCo. All other references to EMVCo approval are strictly prohibited by EMVCo.

Under no circumstances should EMVCo approvals, when granted, be construed to imply any endorsement or warranty regarding the security, functionality, quality, or performance of any particular product or service, and no party shall state or imply anything to the contrary. EMVCo specifically disclaims any and all representations and warranties with respect to products that have received evaluations or approvals, and to the evaluation process generally, including, without limitation, any implied warranties of merchantability, fitness for purpose or non-infringement. All warranties, rights and remedies relating to products and services that have undergone evaluation by EMVCo are provided solely by the parties selling or otherwise providing such products or services, and not by EMVCo, and EMVCo will have no liability whatsoever in connection with such products and services.

This document is provided "AS IS" without warranties of any kind, and EMVCo neither assumes nor accepts any liability for any errors or omissions contained in this document. EMVCO DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AS TO THIS DOCUMENT.

EMVCo makes no representations or warranties with respect to intellectual property rights of any third parties in or in relation to this document. EMVCo undertakes no responsibility to determine whether any implementation of this document may violate, infringe, or otherwise exercise the patent, copyright, trademark, trade secret, know-how, or other intellectual property rights of third parties, and thus any person who implements any part of this document should consult an intellectual property attorney before any such implementation.

Without limiting the foregoing, this document may provide for the use of public key encryption and other technology, which may be the subject matter of patents in several countries. Any party seeking to implement this document is solely responsible for determining whether its activities require a license to any such technology, including for patents on public key encryption technology. EMVCo shall not be liable under any theory for any party's infringement of any intellectual property rights in connection with this document.

Revision Log – Version 2.1.1

The following changes have been made to the document since the publication of version 2.1:

- Definitions in the Glossary have been updated to Version 2.3 of EMV® Payment Tokenisation Specification – Technical Framework
- Language in the text in various sections have been updated to match the updated definitions

Contents

Figures

Tables

Glossary

Abbreviations and Acronyms

Abbreviation	Definition
AML	Anti-Money Laundering
BIN	Bank Identification Number (term for IIN as defined in ISO/IEC 7812)
IEC	International Electrotechnical Commission
IIN	Issuer Identification Number
ISO	International Organization for Standardization
PAN	Primary Account Number
PAR	Payment Account Reference
PCI	Payment Card Industry
PCI SSC	Payment Card Industry Security Standards Council

EMVCo References (available on www.emvco.com)

Publication Date	Version	Document Title
October 2021	Version 2.3	EMV® Payment Tokenisation Specification – Technical Framework
August 2021	Version 2.1	EMV® Payment Tokenisation – A Guide to Use Cases

Normative References

Reference	Document Title
ISO/IEC 7812	Identification cards — Identification of issuers

Reference	Document Title
ISO 20022 ATICA	Acquirer to Issuer Card Messages - Version 2 Message Definition Report - Part 2
ISO 8583	Financial transaction card originated messages — Interchange message specifications (1987, 1993, 2003 and others variants where appropriate)
PCI Standards	Payment Card Industry Data Security Standard and Payment Card Industry Token Service Providers – Additional Security Requirements and Assessment Procedures for Token Service Provider (EMV Payment Tokens)

Definitions

Term	Definition
Bank Identification Number (BIN)	BINs are assigned to ISO IIN Blockholders and ISO IIN Card Issuers. BIN is a term for an IIN that is consistent with ISO/IEC 7812.
BIN Controller	Determines the rules for use of the IINs under their control. See EMV Payment Tokenisation Specification – Technical Framework for further details.
BIN Controller Identifier	A unique identifier consisting of four uppercase Alphanumeric Roman characters assigned by EMVCo to Registered BIN Controllers, as defined in the EMV Payment Tokenisation Specification – Technical Framework.
Cardholder	Any individual where a Card Issuer provides a Payment Account that is represented by one or more PANs, with each PAN typically provisioned to a card.
Card Issuer	A financial institution or its Third Party Service Provider that provides Cardholder with a Payment Account represented by one or more PANs.

Term	Definition
Consumer Device	Any Consumer-operated device such as a smartphone, laptop, personal computer or tablet that the Consumer uses to conduct payment activities.
De-Tokenisation	The process of converting a Payment Token and Token Expiry Date to its underlying PAN and PAN Expiry Date based on the Payment Token / Token Expiry Date affiliation with the underlying PAN / PAN Expiry Date stored in the Token Vault.
EMV Based Application	An application that uses EMV contact or contactless technology and techniques as a foundation of transaction processing.
Non-EMV Based application	An application that uses a different technology than EMV contact or contactless technology and techniques as a foundation of transaction processing.
ISO IIN Blockholder	A “card scheme blockholder” as defined in ISO/IEC 7812-2:2017. Card scheme blockholders represent a group of card issuers. These blockholders are assigned a block of IINs (BINs), for assignment to members of the card scheme for the purpose of issuing Primary Account Numbers (PANs). If a card issuer relinquishes membership of that scheme, the IIN reverts back to the card scheme blockholder.
ISO IIN Card Issuer	A “card issuer” as defined in ISO/IEC 7812-1:2017. A card issuer which will be the issuer of the cards and has applied for and been assigned by the ISO Registration Authority one or more IINs (BINs) for the purpose of issuing Primary Account Numbers (PANs).
Payment Account	A representation of the unique financial relationship between account holders and a financial institution for a specific financial funding source represented by one or more PANs assigned to Cardholders.

Term	Definition
Payment Account Reference (PAR)	A non-financial reference assigned to each unique PAN and used to link a Payment Account represented by that PAN to affiliated Payment Tokens. The use of the term “PAR” in this document refers to the overall concept, rather than any specific component (for example, PAR Data, PAR Field).
PAR Data	Refers to a specific Payment Account Reference value generated in the format specified in the EMV Payment Tokenisation Specification – Technical Framework.
PAR Enquiry Function	A function that supports the enquiry and distribution of PAR Data using a real-time or batch process.
PAR Field	A message field that contains PAR Data.
Payment Network	A role within the Payment Tokenisation ecosystem that operates an electronic system for payment transaction processing, including operating a network switch for purposes of completing authorisation, clearing, and settlement for one or more Payment Systems.
Payment Processor	An existing entity in the payment ecosystem that provides payment processing services for Acquirers and / or Card Issuers. A Payment Processor may, in addition to processing, provide operational, reporting and other services for the Acquirer or Card Issuer.
Payment System	A role within the Payment Tokenisation ecosystem that maintains a consumer-facing brand and provides branding guidelines, inclusive of branding requirements for issuers and merchant acceptance environments, may distribute IINs/BINs, defines rules and guidelines for payment ecosystem participants, and develops products and respective product requirements for payment system participants that are derived from a variety of technologies.

Term	Definition
Payment Token	A surrogate value for a PAN that is a variable length, ISO/IEC 7812-compliant numeric issued from a designated Token BIN or Token BIN Range and flagged accordingly in all appropriate BIN tables. A Payment Token must pass basic validation rules of a PAN, including the Luhn check digit. Payment Tokens must not collide or conflict with a PAN.
Payment Tokenisation	A specific form of tokenisation whereby Payment Tokens are requested, generated, issued, provisioned, and processed as a surrogate for PANs as described by the processes defined in the EMV Payment Tokenisation Specification – Technical Framework.
Primary Account Number (PAN)	A variable length, ISO/IEC 7812-compliant account number that is generated within account ranges associated with a BIN by a Card Issuer.
Registered BIN Controller	A BIN Controller that has successfully registered with EMVCo and is in receipt of an assigned BIN Controller Identifier.
Third Party Service Provider	An authorised entity that provides a service, capability or function, to or on behalf of, a stakeholder in the payment ecosystem.
Token BIN	A specific BIN that has been designated only for the purpose of issuing Payment Tokens and is flagged accordingly in BIN tables.
Token BIN Range	A specific BIN Range that has been designated only for the purpose of issuing Payment Tokens and is flagged accordingly in BIN tables.
Token Cryptogram	A cryptogram, containing a transaction-unique value, typically generated using the Payment Token, Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.
Token Domain	The usage environment of a Payment Token.

Term	Definition
Token Domain Restriction Controls	A set of parameters that are applied during Token Processing to constrain a Payment Token to the permitted usage scenarios.
Token Expiry Date	The expiration date of the Payment Token that is generated by and maintained in the Token Vault and is passed in the PAN Expiry Date field during Token Processing to ensure interoperability and minimise the impact of Payment Tokenisation. The Token Expiry Date is a 4-digit numeric value that is consistent with the ISO 8583 format.
Token Issuance	The process whereby a Payment Token and related data is issued in preparation for Token Provisioning.
Token Location	The mode of storage for a Payment Token and related data.
Token Processing	The process whereby a Payment Token and related data is used to enable payments with PAN. Token Processing may span payment processes that include authorisation, capture, clearing, and exception processing. Token Processing is comprised of the elements: • Token Payment Request / Response • Token Authorisation • Application of Token Domain Restriction Controls • De-Tokenise / Tokenise • PAN Authorisation
Token Programme	A Token Programme is comprised of the policies, processes and registration programmes associated with the oversight of Token Service Providers and Token Requestors within a Payment System.
Token Provisioning	The process whereby a Payment Token and related data is delivered to the Token Location.

Term	**Definition**
Token Request	The process in which a Token Requestor requests a Payment Token from the Token Service Provider.
Token Requestor	A role within the Payment Tokenisation ecosystem that initiates Token Requests. Each Token Requestor will be registered and identified uniquely in accordance with the policies and processes of the Token Programme.
Token Service Provider	A role within the Payment Tokenisation ecosystem that is authorised by a Token Programme to provide Payment Tokens to registered Token Requestors.
Token Vault	A repository that maintains the established Payment Token / Token Expiry Date affiliation with the underlying PAN / PAN Expiry Date and includes Payment Token related data. The Token Vault may also maintain other attributes of the Token Requestor that are determined at the time of registration and that may be used to apply Token Domain Restriction Controls.
Tokenisation	The process within Payment Tokenisation by which the Primary Account Number (PAN) and the PAN Expiry Date are replaced with surrogate values called Payment Token and Token Expiry Date. During Token Processing, a Payment Token / Token Expiry Date may be de-tokenised to the underlying PAN / PAN Expiry Date and subsequently tokenised from the underlying PAN / PAN Expiry Date back to that affiliated Payment Token / Token Expiry Date.

1 Executive Summary

The concept of EMV Payment Tokenisation was introduced to the payment ecosystem with the publication by EMVCo of the EMV Payment Tokenisation Specification – Technical Framework version 1.0 in March 2014. Since its introduction as a Specification, the payment ecosystem has experienced the introduction of digital payments secured through Payment Tokenisation in various digital payment solutions.

Payment Tokenisation enhances the underlying security of digital payments by potentially limiting the risks typically associated with the compromise, or the unauthorised or fraudulent use, of Primary Account Numbers (PANs). Payment Tokenisation achieves this by replacing PANs with Payment Tokens that differ significantly in terms of the ability to control or restrict usage. Payment Tokens offer improvements in security due to the Token Domain Restriction Controls that constrain the usage of Payment Tokens issued to a Token Requestor for use in a particular transaction environment, device, or other Token Domain.

The introduction of Payment Tokenisation provides opportunities to enhance the security of digital payments for Merchants, Acquirers, Payment Processors and other stakeholders in the broader acceptance community. The acceptance community has identified challenges with maintaining the same level of capability for PAN-based services in pre-authorisation or post-authorisation applications. These challenges are most clear when the transaction mix changes from PAN-only based transactions to a transaction mix that includes both PAN and Payment Token transactions.

Value added services such as fraud screening, AML monitoring and some PAN-based loyalty systems have been identified as business services impacted by the changing transaction mix. These value added services often leverage historical transactional data to derive velocity counters or measurements based on the PAN and a changing transaction mix results in Payment Tokens not being linked to the velocity measurements tied to transactions that are based on the underlying PAN.

The value proposition that underlies increased security through Payment Tokenisation offers great promise for protecting transactions from current and emerging security threats. While the use of Payment Tokens improves the security of the payment ecosystem, existing PAN-dependent services no longer have a full historical transaction view which impacts the continuity and integrity of such services.

A long-term solution to the challenges introduced by Payment Tokenisation is necessary in order to transition the acceptance community away from the dependence on Full PAN for historical analysis of transactions which include either the underlying PAN or affiliated Payment Token(s). This solution is referred to as Payment Account Reference (PAR) and was introduced by EMVCo through EMV Specification Bulletin No. 167, which was a Specification Bulletin update to the EMV Payment Tokenisation Specification – Technical Framework version 1.0.

EMV Specification Bulletin No. 167 was fully incorporated into the EMV Payment Tokenisation Specification – Technical Framework with the publication of version 2.0 in September 2017. This White Paper is consistent with the current EMV Payment Tokenisation Specification – Technical Framework.

2 Payment Account Reference Overview

Payment Tokenisation introduces several security benefits to the payments industry as an alternative to PANs in various existing and emerging usage scenarios. It is recognised, however, that complexity is introduced when the transaction mix moves from PAN-only transactions to transactions which include a mixture of the underlying PAN and affiliated Payment Token(s).

The term PAR is a general reference that encompasses the governance, by the Registered BIN Controller, of all the following components:

- PAR Field
- PAR Data
- PAR Data generation method
- PAR delivery mechanisms
- PAR Enquiry Function

The term PAR Data refers to a specific Payment Account Reference or References generated in the format specified in the EMV Payment Tokenisation Specification – Technical Framework.

The term PAR Field refers to a field designated to carry PAR Data between the various entities within the payment ecosystem.

The term PAR Enquiry Function refers to an implementation-specific method for the enquiry and distribution of PAR Data.

Implementation of PAR is outside of the scope of EMVCo: it is the responsibility of each Registered BIN Controller to specify how PAR will be used within its payment ecosystem. The PAR Field and PAR Data may also be included in PAN-based transactions in which Payment Token(s) have been previously generated for the PAN. Feedback from multiple stakeholders where PAR has been deployed suggests there is also inherent value in propagating PAR Data for PANs in situations where Payment Tokens have not yet been generated for such PANs.

Making PAR Data available in advance of the generation of any Payment Tokens allows for the payment ecosystem to more rapidly adapt to business and technical processes and solutions around the use of PAR Data as it becomes more widely available. This enables the support of multiple use cases in advance of the implementation of Payment Tokenisation and avoids the need to develop redundant/non-interoperable solutions to address the same problem. If Payment Tokens for such PANs are subsequently generated, then the linkage between a PAN and its affiliated Payment Token(s) is readily supported since PAR has been fully enabled due to wide scale availability of PAR Data. Wide availability and adoption of PAR and PAR Data will provide an impetus to break the dependencies on Full PAN availability throughout the payment ecosystem.

The following sections provide an overview of the types of challenges introduced by Payment Tokenisation and the value that PAR provides as a mechanism to link historical transactional data to new transactions which involve the underlying PAN and affiliated Payment Token(s).

2.1 History

The EMV Payment Tokenisation Specification – Technical Framework version 1.0 was published in 2014 to provide a detailed technical specification for interoperable Payment Tokenisation solutions that will benefit Acquirers, Merchants, Card Issuers, and Cardholders. The EMV Payment Tokenisation Specification – Technical Framework version 2.0, was published in September 2017 to further define Payment Tokenisation and fully incorporate PAR into the specification, superseding the prior publications. This White Paper is consistent with the current EMV Payment Tokenisation Specification – Technical Framework.

With Payment Tokenisation, a Cardholder's PAN is substituted with a Payment Token that looks and functions like a PAN but is differentiated from a PAN by the underlying security of Token Domain Restriction Controls. These Token Domain Restriction Controls may include dynamic Token Cryptograms, POS Entry Mode and other parameters managed by the Registered Token Service Provider. With usage constrained to applicable Token Domains, Payment Tokens cannot be readily subject to the level of unauthorised or fraudulent use commonly associated with PANs. Payment Token usage scenarios continue to expand as a variety of entities begin to gain experience with Payment Tokenisation and take advantage of the security proposition offered by tokenised transactions.

As Payment Tokenisation adoption growth continues, all entities in the payment ecosystem may benefit from the security protections attributed to Payment Tokens as an alternative to PAN in transactions. Cardholders will have multiple Payment Tokens affiliated with an underlying PAN due to payment enablement of multiple devices and expanding usage scenarios.

The impact of Payment Account transactions that have a mix which include both the underlying PAN and its affiliated Payment Token(s) has implications to a variety of entities including Merchants and others in the acceptance community. The implications of this transaction mix include challenges in establishing a mechanism to link historical transactional data to current or future transactions which include the underlying PAN and affiliated Payment Token(s).

In the acceptance community, use of PAN occurs in various pre-authorisation or post-authorisation value-added service applications to identify the Payment Account across transactions which is readily known when the same PAN is present. After the introduction of Payment Tokenisation, a transaction will be initiated using either an underlying PAN or by initiating a Token Payment Request using its affiliated Payment Token(s). This limits the ability of payment ecosystem participants to link transaction history data to both current and future transactions for the same Payment Account.

A goal of Payment Tokenisation is to devalue the data in order to reduce the risk associated with data compromise by removing the PAN from digital payments and other usage scenarios. Therefore, risk exposure will be limited as a result of:

- PAN availability decreasing.
- The number of entities that have access to both underlying PAN and affiliated Payment Token(s) reducing.
- The number of entities that have access to only Payment Tokens increasing.

PAR is linked to the underlying PAN and associated with all affiliated Payment Tokens. Linkage of transaction history data to current and future transactions which include underlying PAN and affiliated Payment Token(s) can be accomplished by using PAR as the linkage mechanism. It is important to note that Cardholders do not need to be aware of

PAR and it may not be visible or known to the Cardholder, since it is intended to be used by Merchants, Acquirers and other entities for non-payment operations.

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). Enabling PAR more broadly on PANs prior to the generation of Payment Tokens mainstreams PAR Data availability. This ensures that PAR Data availability is not viewed as being limited to Payment Token use cases but rather a business as usual construct to break the reliance on the availability of Full PAN within the payment ecosystem.

2.2 Usage of PAR

PAR alone is not sufficient to initiate a payment transaction including authorisation, capture, clearing or exception messages, although PAR Data may be present as an accompanying data field (the PAR Field) within the transaction. For EMV-based transactions Tag 9F24 has been specifically designated for this purpose.

For PAR to be most effective, PAR Data needs to be available in as many places as possible within the payment ecosystem. Therefore PAR Data should be present in all transactions which include underlying PAN and affiliated Payment Token(s). The presence of PAR Data provides a mechanism to link transaction history to current and future transactions which include underlying PAN and affiliated Payment Token(s). The presence and wide-scale adoption of PAR provides the rationale to reduce the exposure of Full PAN and an affiliated Payment Token together in the same transactional message.

PAR Data may also be included in PAN-initiated transactions not linked to any affiliated Payment Tokens, to provide consistency and promote widespread adoption. Including PAR Data in transactions that are initiated with PANs for which Payment Tokens have not yet been generated will enable a transactional history to be established. As awareness of PAR and insights regarding the underlying value proposition has matured within the payments industry, increasingly stakeholders have expressed strong interest in propagating PAR for PANs in advance of the generation of any Payment Tokens. For PAR to be fully effective and implemented across a wide variety of payment uses cases, strategies to drive broad assignment and distribution of PAR Data need to evolve to mainstream PAR availability in the payment ecosystem.

2.3 Principles of PAR

BIN Controllers control the issuance and allocation of ISO/IEC 7812 BINs used to issue PANs and the affiliated Payment Tokens. BIN Controllers are registered as either ISO IIN Blockholders or ISO IIN Card Issuers. BIN assignees or sub-licensees are not considered BIN Controllers and are expected to work under the principles for PAR governance that are determined by the ISO IIN Blockholder.

BIN Controllers that choose to implement PAR must register with EMVCo to be assigned a BIN Controller Identifier for purposes of PAR governance and in accordance with the defined structure of PAR Data. The BIN Controller Identifier will ensure the uniqueness of PAR Data across different Registered BIN Controllers.

Registered BIN Controllers determine the governance of PAR and the process for ensuring PAR uniqueness covering the IINs (BINs) under their direct control. Registered BIN Controllers will need to ensure that:

- PAR Data is generated using a method that cannot be reverse engineered to determine the underlying PAN or Payment Token and will prevent unintended disclosure of the underlying PAN
- PAR Data is unique in its assignment to a given underlying PAN and, in light of applicable privacy considerations, is not intended to be a consumer identifier
- PAR Data assigned to each underlying PAN must be unique across all PAR Data governed by any one Registered BIN Controller to ensure no collision or conflict
- PAR Data alone cannot be used to initiate a financial transaction or authorisation message
- Assigned PAR Data will be the same value when assigned to an underlying PAN shared by multiple Cardholders since PAR Data is individually associated with the underlying PAN and not the Cardholder
- PAR Data assigned to an underlying PAN will be also associated with all affiliated Payment Tokens to enable the linkage of transactions
- PAR Data meets the data format defined by EMVCo for format consistency in the payment ecosystem

There is no expectation that PAR Data generation methods should be consistent between Registered BIN Controllers. However, an implementation will need to comply with the PAR criteria defined in the EMV Payment Tokenisation Specification – Technical Framework.

2.4 PAR Management & Lifecycle

PAR Data is intended to be generated and associated with a current PAN for a given Payment Account with a Card Issuer. PAR represents the Payment Account at the same level that PAN represents the Payment Account. The assignment practices of PAN by a Card Issuer within a Payment Account will determine PAR Data assignment for that Payment Account. Assignment of PAR Data for PANs where the underlying PAN is not yet ready for, or prioritised for, Payment Tokenisation, is a viable strategy and impetus for priming the payment ecosystem with broad availability of PAR Data. Broad availability will help drive changes to business processes and technologies to adapt to PAR and establish linkage mechanisms that will be fully established regardless of the adoption of Payment Tokenisation. When Payment Token(s) are generated for a PAN, the PAR Data will then be associated with all affiliated Payment Tokens. It does not represent the individual consumer or the overall relationship between the Payment Account and the Card Issuer.

There are a variety of business conditions and lifecycle events that may result in an original underlying PAN being replaced by a Card Issuer with a new underlying PAN for the same Payment Account. Conditions include a reissuance due to expiration of the original underlying PAN as well as a forced reissuance due to lost/stolen cards, account data compromise, and other fraud-related events. The reissuance of a new underlying PAN does not require that new PAR Data be generated.

It is understandable that Card Issuers will prefer to remap the PAR Data to the new PAN when the Payment Account itself remains in place. This allows for all existing Payment Tokens that were previously affiliated with the original underlying PAN to be affiliated to the new underlying PAN and maintain the current associated PAR Data. This may simplify an implementation approach by ensuring that provisioned PAR Data does not have to be re-provisioned. This is due to the PAR Data associated with the Payment Token persisting even though the underlying PAN has changed.

In the event a Payment Account with a Card Issuer has multiple authorised users with the same underlying PAN issued to primary and additional Cardholders, the PAR Data will be the same since there is only one underlying PAN.

Payment Accounts that have multiple PANs issued will need to ensure that unique PAR Data is generated for each underlying PAN. The appropriate PAR Data is then associated to affiliated Payment Tokens.

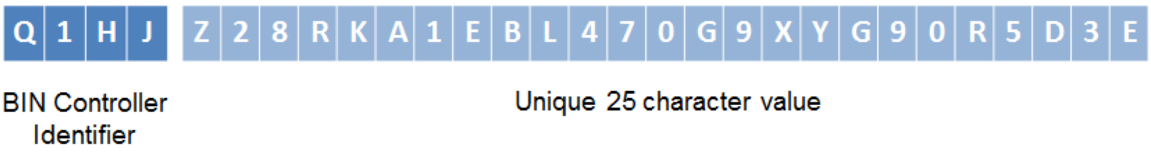
2.5 PAR Data Structure and Format

PAR Data will be generated in accordance with the following format defined in the EMV Payment Tokenisation Specification – Technical Framework:

- Fixed field length of 29 characters (uppercase Alphanumeric Roman)
- PAR Data is comprised of a 4 character BIN Controller Identifier assigned by EMVCo to Registered BIN Controllers followed by a unique 25 character value

The structure of the PAR Data is:

Figure 1 – PAR Data Structure and Format


Q 1 H J
Z 2 8 R K A 1 E B L 4 7 0 G 9 X Y G 9 0 R 5 D 3 E
BIN Controller Identifier
Unique 25 character value

Note: PAR Data cannot be used to initiate a financial transaction and therefore PAR Data does not have an associated expiry date.

PAR Data may be optionally provided in the authorisation, capture, clearing and exception messages. In addition, the PAR Field may be provided in Token Processing response messages.

2.6 Availability of PAR

EMV Payment Tokenisation Specification – Technical Framework defines a number of ways that the PAR Field and PAR Data may be introduced into transaction processing.

Depending on the need, PAR Data is available before, during or after the authorisation.

Table 1 – Availability of PAR

PAR Availability Method	Source of PAR Data
From an EMV Based Application	EMV Tag '9F24'
From a non-EMV Based Application	Implementation specific field
From the authorisation	Returned in the authorisation response message in an ISO 8583 data field which is version and implementation specific
PAR Enquiry – Payment Token or underlying PAN	PAR Enquiry Function – implementation specific interface

PAR Data may enter into transaction processing from an EMV-Based Application within a card or Consumer Device, or from a non-EMV Based Application such as in the Card-On-File E-Commerce or In-Application Using a Consumer Device use cases, that has received PAR Data during Token Provisioning. When PAR Data has been assigned and linked to the Payment Token, PAR Data availability may flow through Token Processing. When PAR Data is present in an EMV Based Application, PAR Data will be identified through the use of EMV Tag '9F24'. EMV Tag '9F24' is available for use with both PAN-based transactions and Payment Token based transactions. Its use is not dependent upon Payment Tokens having been generated for a PAN.

The PAR Field may be included in the authorisation response messages to provide PAR Data availability to Merchants and the broader acceptance community. ISO has assigned ISO-specific Payment Token fields for the purposes of carrying PAR Data in authorisation response messages. The assigned fields include, but are not limited to, Field 56 for ISO 8583 (1987), Field 112 for ISO 8583 (1993), and Field 51 for ISO 8583 (2003). The inclusion of PAR in these ISO 8583 messages is also available for use with both PAN-based transactions and Payment Token based transactions. Its use is not dependent upon Payment Tokens having been generated for a PAN.

Note: PAR Data may be available in Field 55 of the above ISO 8583 referenced message formats.

PAR Data may be available through a PAR Enquiry Function as an implementation-specific interface that is designed to return PAR Data in response to a request initiated with a Payment Token or underlying PAN. The definition of the PAR Enquiry Function will be implementation specific and is outside of EMVCo scope.

2.7 Token Provisioning and PAR

The Registered BIN Controller will define how a Registered Token Service Provider will facilitate PAR provisioning as part of the interaction and interface with the Token Requestor and the Card Issuer. The Registered Token Service Provider may need to source PAR Data from the Card Issuer and provide the provisioning response to the Token Requestor. The response to a Token Request will contain all of the related data inclusive of PAR.

2.8 Token Processing and PAR

Transactions that are initiated by a Token Payment Request may also include PAR Data in the transaction message. The availability of PAR Data in transaction messages will be determined by the Registered BIN Controller. The Payment Network shall make an ISO-defined field (the PAR Field) for PAR Data available in their transaction message specifications. If the PAR Data is unavailable in the transaction message, Merchants, Acquirers or Payment Processors may optionally use the PAR Enquiry Function.

Adoption of PAR with Token Processing involves the support of multiple entities including Merchants, Acquirers and Payment Processors, Payment Networks, and Card Issuers.

Based on the direction provided by BIN Controller governance programs, PAR Field and PAR Data support will be defined in the various message specifications associated with Token Processing including those defined by Payment Networks, Acquirers and Payment Processors, and Card Issuers. Other options for supporting PAR Data availability outside of traditional payment processing include the development of PAR Enquiry Functions based on proprietary implementation specific interfaces.

2.9 PAR Data Security Considerations

PAR Data is not a substitute for PAN or Payment Tokens. Its sole purpose is to provide a linkage mechanism between underlying PAN and affiliated Payment Token(s). However, there is nothing to prevent PAR Data being created for a PAN regardless of any future Payment Token generation.

One of the fundamental principles of proper PAR implementation is that PAR Data cannot be reverse engineered to determine the underlying PAN or affiliated Payment Tokens. The PCI SSC has published an FAQ on its website, www.pcisecuritystandards.org, in order to formally acknowledge PAR Data is not associated with PCI Account Data as defined in PCI Standards. PAR Data should be used and protected in accordance with international, regional, national or local laws and regulations.

2.10 PAR Data Privacy Considerations

PAR's sole purpose is to provide a linkage mechanism between transactions performed on the underlying PAN and those performed on affiliated Payment Token(s). However, there is nothing to prevent PAR Data being created for a PAN regardless of any future Payment Token generation.

PAR Data is assigned directly to an underlying PAN and is not intended to be a consumer identifier. It does not represent the individual consumer or the overall relationship between the Payment Account and the Card Issuer.

Nonetheless, the implementation of PAR 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.

3 PAR Stakeholder Considerations

There are a number of potential roles and considerations associated with the ongoing governance of PAR implementations within the payment ecosystem. These are introduced in this section.

3.1 BIN Controller

BIN Controllers must register with EMVCo in order to be assigned a BIN Controller Identifier which will serve as the initial 4 characters of PAR Data generated and assigned to PANs from BINs under its control. Details regarding BIN Controller registration can be found at www.emvco.com.

Registered BIN Controllers are responsible for the governance of PAR for the IINs (BINs) that are under their direct control, including determining the approach to PAR Data generation and ensuring that the unique component of PAR Data is generated to ensure there is no conflict in PAR Data assigned to PANs from BINs within its control.

3.2 Token Service Providers

Token Service Providers play an important role associated with the provisioning of PAR Data. This includes implementing support of PAR Fields and PAR Data within the provisioning interfaces so that PAR Data can be included along with the Payment Token at the time of provisioning in accordance with the governance guidelines established by the Registered BIN Controller and in conjunction with the Card Issuer.

PAR Data may be provisioned along with Payment Tokens in support of a variety of usage scenarios. These include provisioning of an EMV Based Application in the Proximity at Point of Sale use case or to a non-EMV Based Application when the application does not initiate EMV-based transactions such as the In-Application using a Consumer Device and Card-On-File E-Commerce use cases.

When provisioning to an EMV Based Application, PAR Data is uniquely identified using EMV Tag '9F24'. This EMV Tag is only to be used when provisioning to EMV Based Applications. When provisioning to Non-EMV Based Applications, EMV Tags should not be used to identify PAR Data. Instead an implementation-specific PAR Field should be used.

Token Service Providers also integrate PAR Field and PAR Data into various Payment Tokenisation functions. These include providing PAR Data in De-Tokenisation requests as well as passing PAR Data in response to successful Token Requests.

3.3 Card Issuers

Card Issuers need to support PAR as designated by the Registered BIN Controller that is associated with the Token BIN or Token BIN Range used to support Payment Tokenisation. Card Issuers need to understand the applicability and governance of PAR Field and PAR Data as defined by the Registered BIN Controller. Card Issuers may also help drive PAR Data availability by supporting efforts to deploy PAR for PANs that are not yet ready for, or prioritised for, Payment Tokenisation.

Card Issuers may be required to support the PAR Field and PAR Data for Payment Networks that are not also BIN Controllers.

3.4 Acquirers

PAR Field may be implemented in the Acquirer financial and authorisation messages in accordance with the PAR Data requirements defined by the Payment Networks that the Acquirer supports.

3.5 Merchants

Merchants may elect to support PAR Field and PAR Data. Considerations include:

- Authorisation, capture, clearing, and exception messages
- PAR Enquiry Function for PAR Data retrieval
- Reading of PAR Data from EMV terminals
- Interactions with Token Requestors to receive PAR Data for non-EMV based transactions

Merchants should consult with their Acquirers and Payment Processors in relation to details associated with PAR Field and PAR Data implementation.

3.6 Payment Systems

Payment Systems that are Registered BIN Controllers define the governance of the PAR Field and PAR Data within Payment Networks, including supporting the PAR Field and PAR Data. Governance options may include strategies to assign PAR Data for PANs prior to the generation of any Payment Tokens in an effort to ensure wide scale availability of PAR Data and facilitate its broad adoption by stakeholders across the payment ecosystem.

3.7 Payment Networks

Payment Networks support and implement PAR Field and PAR Data within the payment ecosystem. Based upon the PAR governance requirements defined by Registered BIN Controllers, Payment Networks should define the fundamental requirements for support of PAR within their specific Payment Network including support for an ISO-defined PAR Field in their message specifications.

This includes authorisation, capture, clearing and exception messages which are available to Acquirers and Payment Processors. This includes passing of PAR Data in transaction messages, including the ability to return PAR Data in the authorisation response message resulting from any transactions whether these are PAN-initiated or initiated using a Token Payment Request.

Payment Networks that are not BIN Controllers should support the implementation of PAR in their transaction messages based upon the requirements for PAR defined by the relevant Registered BIN Controller(s).

Payment Networks should support multiple methods for delivering PAR Data. This may include the financial transactions as well as the PAR Enquiry Function.

PAR is used to link underlying PAN and affiliated Payment Token(s). PAR can also be used for PAN-initiated transactions where Payment Tokens have not yet been generated. Specifically, PAR Data cannot be used as a mechanism for transaction routing and financial transactions cannot be initiated using PAR Data on its own. Payment Networks should take these restrictions into account when implementing PAR.

3.8 Token Requestors

Token Requestors are responsible for awareness of PAR Data affiliated to Payment Tokens and ensuring PAR Data availability to Merchants.

There are subtle nuances associated with different transaction environments that may result in some cases in the Token Requestor not being explicitly aware that it is passing PAR Data in a transactional message. This is particularly true when the transaction is initiated from an EMV Based Application in which PAR Data was identified with EMV Tag '9F24' and the resulting transaction includes the PAR Data as part of the payload of data which accompanies the EMV transaction.

Transactions initiated using a Token Payment Request through a non-EMV Based Application such as the In-Application using a Consumer Device or Card-On-File E-Commerce use cases will result in the Token Requestor having a full understanding as to whether PAR Data is passed in the transactional message. In these use case examples, Token Requestors are expected to pass PAR Data to the Merchant whenever PAR Data has been included in Token Provisioning.

Token Requestors should refer to their respective Token Service Providers for details of PAR Data handling.