

TOKENISATION ANNEX

© European Cards Stakeholders Group AISBL.
Any and all rights are the exclusive property of
EUROPEAN CARDS STAKEHOLDERS GROUP AISBL.

Abstract	This document contains the ECSG work on SEPA tokenisation to date
Document Reference	ECSG001-18
Issue	Tokenisation Annex v9.0
Date of Version	15 January 2020
Reason for Issue	Publication
Reviewed by	ECSG Board 26 September 2019
Produced by	ECSG Tokenisation Task-Force
Owned by	ECSG
Circulation	Public

THIS DOCUMENT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS DOCUMENT SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER EUROPEAN CARDS STAKEHOLDERS GROUP AISBL ("ECSG"), NOR ANY OF ITS MEMBERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS DOCUMENT, NOR SHALL ECSG OR ANY OF ITS MEMBERS HAVE ANY RESPONSIBILITY FOR IDENTIFYING ANY INTELLECTUAL PROPERTY RIGHTS

Change History of Tokenisation Annex		
8.50	17 December 2018	First Draft version for consultation alongside Volume version 8.5
8.5.3	29 July 2019	Working Version to V9
9.0	15 January 2020	ECSG Published Version – Volume 9.0

Table of Contents

1. GENERAL	5
1.1. Tokenisation Annex - Executive summary	5
1.2. Content overview	6
2. TOKENISATION STANDARDS, GUIDELINES AND MODELS	7
2.1. Taxonomy	10
2.2. ANSI X9	12
2.3. EMV® Payment Tokenisation Specification – Technical Framework	12
2.3.1. EMV® Payment Tokenisation Model Description	12
2.3.2. Description of EMV® Payment Tokenisation Specification – Technical Framework v2.0	13
2.3.3. Token Request and Token Processing Diagrams	13
2.3.4. EMV® Payment Tokenisation Use Cases	16
2.3.5. EMV® Payment Account Reference (PAR)	17
2.4. PCI SSC Token Service Provider	19
2.4.1. PCI SSC Tokenisation Guidelines	20
2.4.2. PCI SSC Tokenisation Domains	20
2.4.3. Relation between PCI and EMVCo's PAR	21
2.5. Non-standardised Issuer-Led Payment Tokens	21
2.6. Merchant led non-payment tokenisation	23
2.6.1. Model description	23
2.6.2. Merchant tokenisation use cases	24
3. BUSINESS PRINCIPLES	26
3.1. Business principle related to the EMV tokens	26
3.1.1. Option 1	26
3.1.2. Option 2	27
3.1.3. Token Issuance diagram	28

4. RETAILERS PERSPECTIVE AND NEEDS IN RELATION TO IDENTIFYING THE PAN 'BEHIND' THE PAYMENT TOKEN	30
5. PAR (PAYMENT ACCOUNT REFERENCE) MANAGEMENT AND CO-BADGED CARDS	32
5.1. PAR in a co-badge environment with separate PANs	32
5.2. PAR in a co-badge environment with same PAN	34
6. GDPR CONSIDERATIONS	36
6.1. PAN, Token and PAR under the GDPR	36
6.1.1. PAN, Token, and PAR are Personal Data	36
6.1.2. Anonymous and pseudonymous data	37
6.2. Key GDPR aspects relevant for Pseudonymisation	37
6.3. Responsibilities of the relevant stakeholders when using pseudonymous data	38
7. ECSG REQUIREMENTS	39
8. DEFINITIONS	41
8.1. Definitions not considered for this document	41
8.2. Book 1 definitions amended with Tokenisation definitions	41
8.3. New definitions in the Volume	42
9. FIGURES AND TABLES	50

1. GENERAL

1.1. Tokenisation Annex - Executive summary

Background and context

The success of card payments continues to spread well beyond the traditional plastic card that effects a contact transaction at a merchant face-to-face terminal.

The card industry has been actively leveraging technological innovations such as e-&m-commerce, proximity NFC-based contactless, mobile phone wallets, watches and other wearables, etc.

In that context, it becomes crucial for the whole 'card' ecosystem to continue to ensure the maximum levels of security possible for all parties involved, while preserving at the same time a convenient user-experience.

Indeed, as the physical, face to face point of interaction has increased its security, among other factors by adopting the EMV specifications, fraud has migrated towards remote transactions.

The Primary Account Number (PAN) of a credit or debit based card is one of the prime data elements sought by criminals as it is essential to enable many of the crimes to be undertaken (Card not present fraud, Card cloning etc.) As a result the compromise of the PAN such as, in broad terms, the stealing of valid card numbers from mostly within the acceptance domain, results in a significant cost for the card payments industry both in terms of the actual fraud as well as in terms of reputation.

All forms of tokenisation relate to replacing the PAN with a surrogate.

Replacing the PAN by a surrogate, such as a 'token', minimises the risk by removing the key data element and as a consequence, reduces the risk of fraud and the accompanying costs of data compromise.

A specific form of 'Tokenisation' used in the ecosystem is EMV Payment Tokenisation and can be adopted in a number of different use cases for card-based Face to Face and e-commerce payment scenarios. It supports payment innovation and evolution while managing cross-channel and intra-channel risks including allowing separate management usage control(s) (e.g., blocking of transactions outside of a specific channel or domain) of the PAN and/or EMV Payment Token.

'Tokenisation' of the PAN ("Primary Account Number") has been playing a critical role in this common task of ensuring security for a number of years. Standards, guidelines and solutions have been defined, developed and implemented in the last few years.

As a logical consequence of all the above, the ECSG Board of 3 May 2017 acknowledged the importance of tokenisation and hence the need to have it included in the ECSG SEPA Cards Standardisation Volume Book of Requirements (the "Volume").

The following document details the requirements or recommendations for the adoption and implementation of Tokenisation in the SEPA region and includes references to Global

standards where available.

1.2. Content overview

Tokenisation is not only a wide area involving a rich eco-system of players but also one that is evolving rapidly on the wings of innovation and competition.

When considering comments to this document, the reader is invited to keep in mind the remit of the ECSG. Commercial models and implementation aspects are outside of the scope of what the ECSG organisation can standardise. Security and interoperability at the point where 'Payer' and 'Payee' interact is the main area of focus of the ECSG as an organisation.

As a consequence of the above, the present document should not be regarded as an all-encompassing 'encyclopaedia' or reference document on Tokenisation, but addresses the topic from a few particular angles that have been deemed of interest from the ECSG members at this point in time:

- A holistic approach that covers different tokenisation models (issuer, acquirer, merchant)
- A view on both payment and non-payment tokens
- Adoption of global standards and guidelines from EMVCo and PCI SSC amongst others
- Openness towards other existing payment token solutions such as 'alternate PAN' or 'dynamic' virtual numbers.
- Considerations about the Token Service Provider (resulting in the adoption of a Business Principle)
- Retailer needs following the introduction of tokenisation, and in particular, considerations around the EMVCo Payment Account Reference (PAR) data element
- Clarifying the flexibility needed around PAR generation and:
 - Exploring the links between co-badging and tokenisation
 - European regulatory considerations especially GDPR

2. TOKENISATION STANDARDS, GUIDELINES AND MODELS

In its simplest form, a 'Token' can be described as a surrogate of an original value – in this document, we limit our scope to consider **surrogates of a card**.

At a high level, if the resulting token has the attributes of a PAN, as per ISO 7812 Part 1 (e.g., length and structure) it can be used for payment. However, other types of tokens exist, for example in cases where the purpose of the token is not to effect payments, and therefore it is not needed that the resulting token has the 'appearance' of a PAN.

Depending on what the purpose of the token is and who the entity requesting the token (directly or indirectly) is, we can picture three 'token models'; one led by the *issuer*, one by the *acquirer* and one by the *merchant*.

Existing global bodies such as EMVCo and PCI SSC have addressed the needs by way of the publication of the pertinent frameworks, specifications and guidelines.

Therefore, the three models mentioned above are supported by the global standards, frameworks and guidelines, although alternatives to these may also exist.

The following table tries to depict in a highly summarised form how models and standards/guidelines relate to each other.

'Model' ¹	Primary Use of the token ²	Applicable <u>Global</u> Framework or Guidelines ³
Issuer-led model	Payment, used to initiate a payment at a merchant location whether face to face or Card Not Present	EMV® Payment Tokenisation Specification – Technical Framework
Acquirer-led model	<p>May be used within the payment transaction lifecycle, but not used to initiate a payment.</p> <p>Security of the information either stored, processed or transmitted.</p> <p>This purpose or objective can be achieved through various mechanisms.</p> <p>Can also support other use-cases</p>	PCI Data Security Standards Tokenization Guidelines
Merchant-led model	<p>May be used within the payment transaction lifecycle, but not used to initiate a payment.</p> <p>Security of the information either stored, processed or transmitted.</p> <p>This purpose or objective can be achieved through various mechanisms.</p> <p>Can also support other use-cases</p>	PCI Data Security Standards Tokenisation Guidelines

¹ Depends on the party that is the ultimate requestor (directly or indirectly) or approver of the token request

² The primary purposes mentioned here are for illustrative purposes and are not meant to be considered as exhaustive

³ Other regional, local or proprietary standards may apply but are out of scope of this document and out of scope of the ECSG

TABLE 1: SUMMARY OF HOW TOKENISATION MODELS AND STANDARDS/GUIDELINES RELATE TO EACH OTHER

The preceding table introduces us to two of the global standards (PCI SSC and EMVCo) that currently exist in the tokenisation area.

For the sake of completeness, we make reference in this report to one additional available tokenisation standard from another standards organisation, namely the “ANSI X9” standard.

2.1. Taxonomy

The following two diagrams illustrate at a high-level of detail how the different frameworks and models span across the different domains of the overall card payment ecosystem.

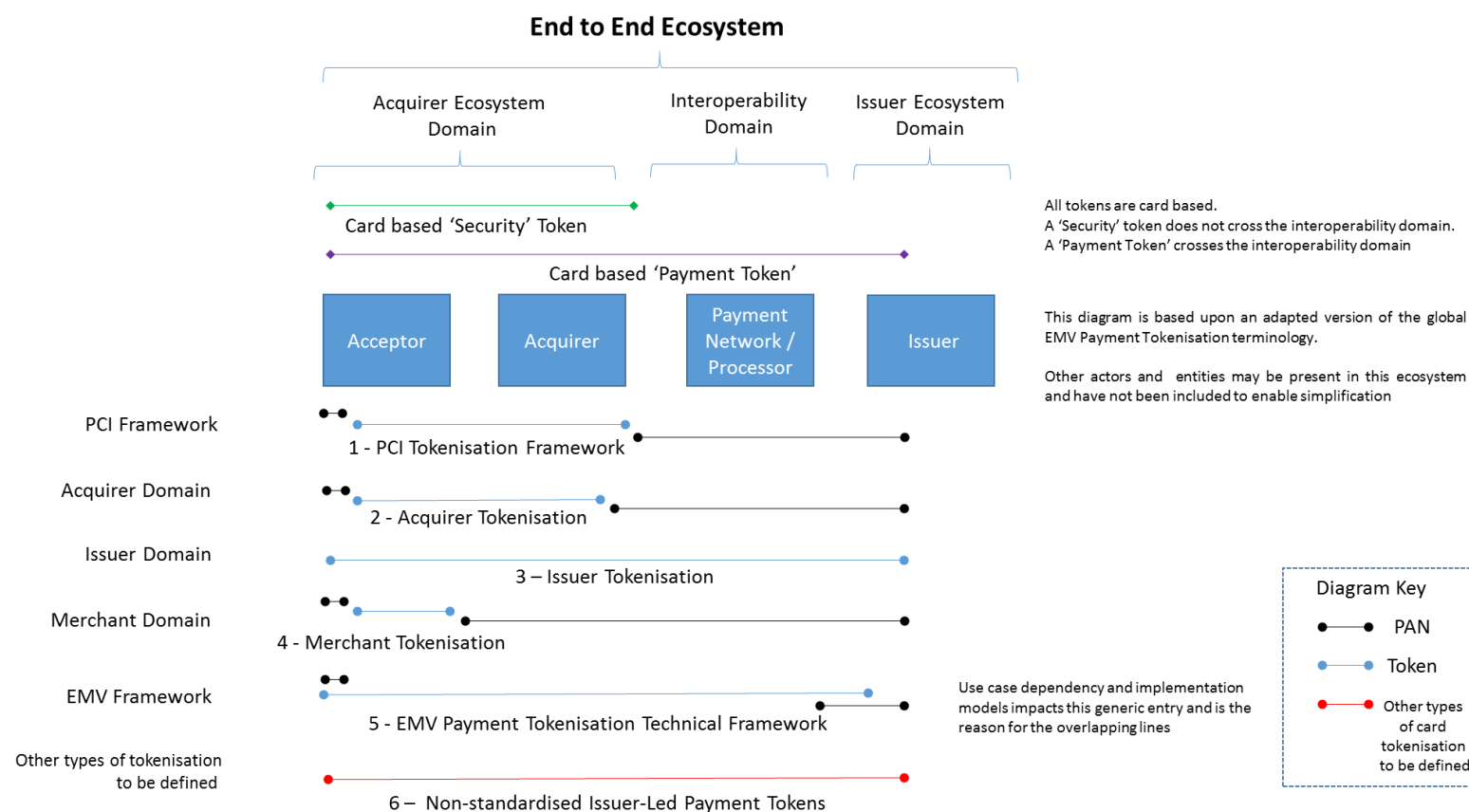


Figure 2: Card Tokenisation: Analysis of environment

Card Tokenisation Ecosystem Protecting the PAN

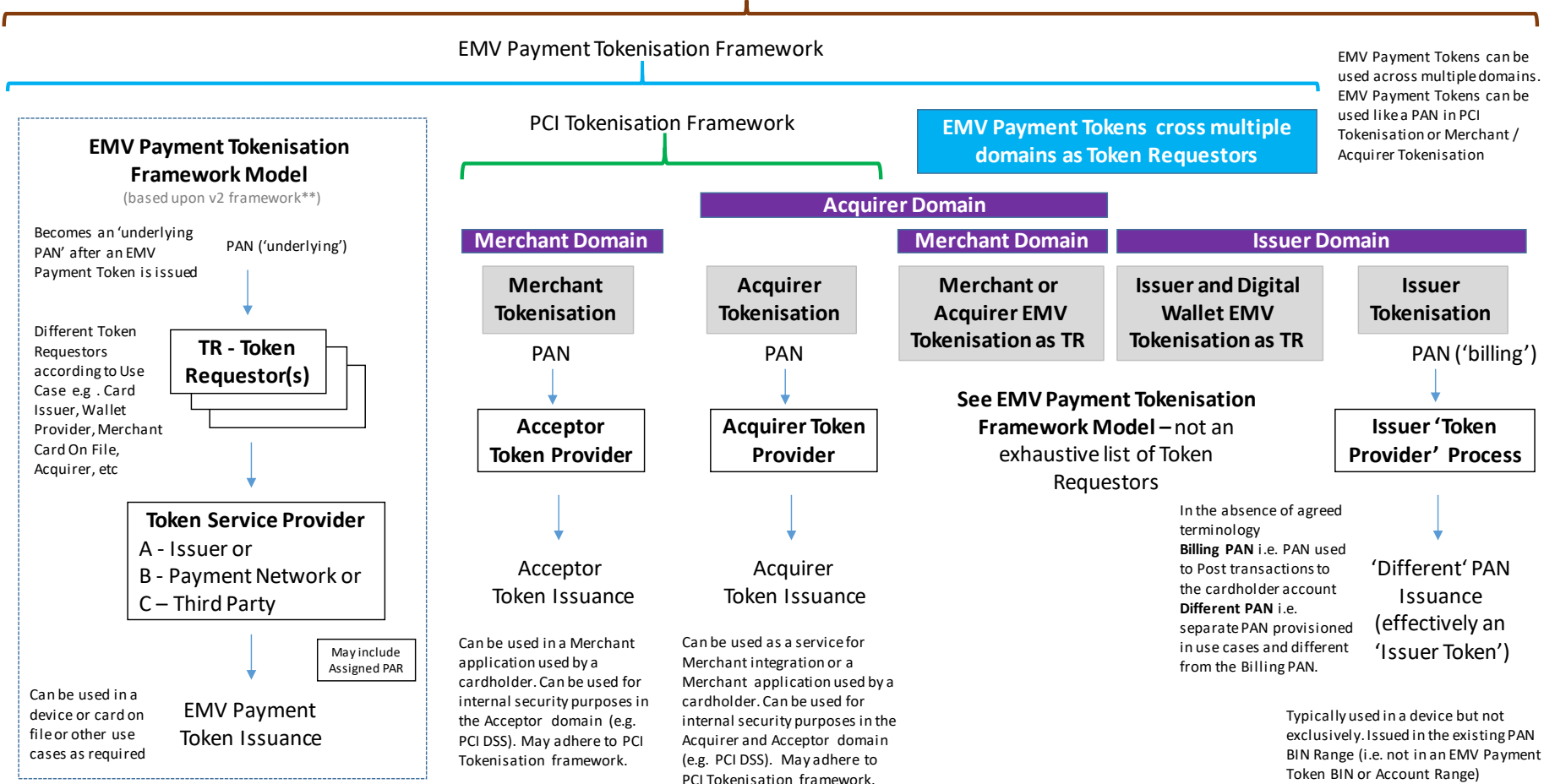


Figure 3: Card Tokenisation Ecosystem Protecting the PAN

2.2. ANSI X9

The Accredited Standards Committee X9 Inc. is a non-profit organisation accredited by the American National Standards Institute (ANSI) to develop both domestic and international standards for the financial services industry.

According to its website:

- The X9 organisation has over 100 member companies and over 400 company representatives that work to develop and maintain approximately 100 domestic standards and 58 international standards.
ASC X9 published in October 2017 a document
 - ANSI X9.119-2-2017: Retail Financial Services - Requirements for Protection of Sensitive Payment Card Data - Part 2: Implementing Post-Authorization Tokenisation Systems
- This new ANSI X9 standard defines the minimum-security requirements for implementing Tokenisation in systems that operate after a payment has been approved, to protect sensitive payment card data from data breaches.

From the ECSG perspective, this standard therefore is one of the options available – other may exist - to retailers and their processors to implement solutions against data breaches.

2.3. EMV® Payment Tokenisation Specification – Technical Framework

2.3.1. EMV® Payment Tokenisation Model Description

EMVCo does not dictate specific implementations or usage of its specifications or define any set of required use cases. Any implementation of the EMV® Payment Tokenisation Specification – Technical Framework v2.0 (“technical framework”) should account for the unique business rules, practices and stakeholder needs of the specific payment ecosystem(s) in which it will be deployed.

The following summary is not a complete representation of Payment Tokenisation or any single component. The EMV® Payment Tokenisation Specification – Technical Framework takes precedence over anything in this summary.

The implementation of Payment Token solutions as outlined in this paper, and in a manner consistent with the technical framework itself, involves a number of roles within the Payment Tokenisation ecosystem. Some are existing roles within the traditional payment ecosystem, and others are Payment Tokenisation specific roles defined by the technical framework. Payment Tokenisation specific roles may be fulfilled by existing entities within the payment ecosystem or by newly-emerging entities.

The technical framework is intended solely as an interoperable technical overview of the possibilities afforded through EMV Payment Tokenisation but must also be considered in its entirety. No single aspect or function of EMV Payment Tokenisation should be considered in isolation; instead, implementers should consider all aspects holistically with due consideration of all potential impacts on the relevant payment ecosystem(s) when designing their solutions.

2.3.2. Description of EMV® Payment Tokenisation Specification – Technical Framework v2.0

The technical framework defines a basis for EMV Payment Tokenisation by providing a level of commonality across the payment ecosystem to support adoption, while enabling levels of differentiation that promotes innovation. It aims to bring benefit to ecosystem stakeholders by describing a global Payment Tokenisation ecosystem that overlays and interoperates with existing payment ecosystems to support digital commerce and new methods of payment.

The technical framework is intended to create a common baseline set of functions for EMV Payment Tokenisation that can be adopted to meet the unique payment ecosystem requirements of international, regional, national or local implementations.

The payment ecosystem is evolving to support payment form factors that provide increased protection against counterfeit, account misuse, and other forms of fraud. While EMV chip cards can provide substantial protection for card-present transactions, a similar need exists to minimise the risk of unauthorised use of Primary Account Number (PAN) and to reduce cross channel and intra-channel fraud for card-not-present and emerging transaction environments that combine elements of card-present and card-not-present transactions.

An EMV Payment Token provides improved protection when its use is limited to a specific domain(s), such as a Merchant, Card / Form Factor (including mobile devices, wearables, etc.) or channel such as proximity payments. The application of these underlying usage controls, known as the Token Domain Restriction Controls, is a primary component and benefit of EMV Payment Tokens. The Token Domain Restriction Controls can be used to limit the use of an EMV Payment Token to its intended use. Examples include prevention of the successful use of an EMV Payment Token outside of a specific channel, limiting the use of an EMV Payment Token to a single Cardholder-Initiated Transaction and subsequent Merchant-Initiated Transactions or allowing an EMV Payment Token to be used by multiple Token Users.

2.3.3. Token Request and Token Processing Diagrams

Additional diagrams from the technical framework cover Token Request and Token Processing.

2.3.3.1. EMV Payment Tokens – Token Request example

There are many different implementations for the various processes and the diagram below is not intended to be definitive.

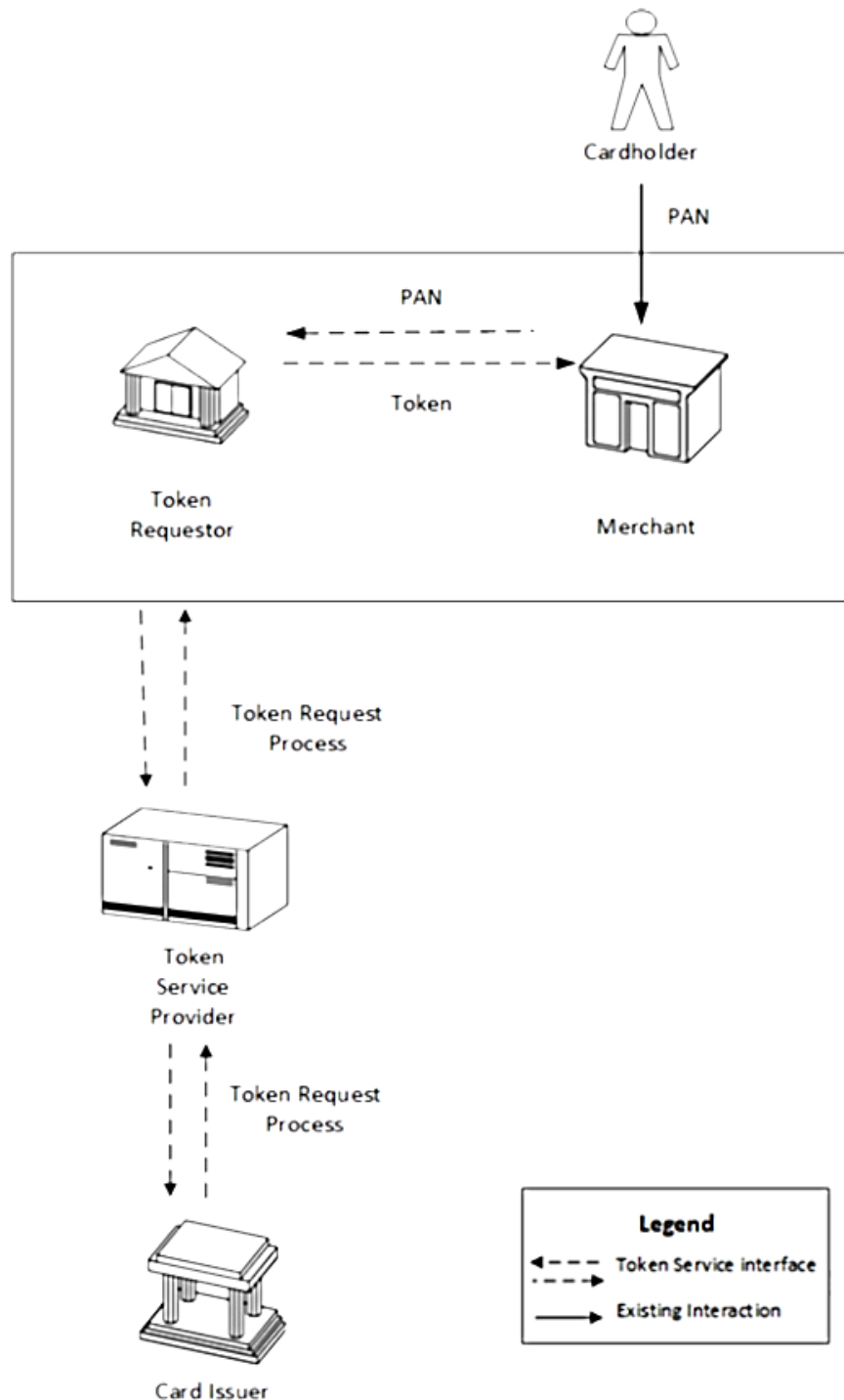


FIGURE 4: EMV PAYMENT TOKENS – TOKEN REQUEST EXAMPLE

2.3.3.2. EMV Payment Tokens – Token Processing

The figure below gives an example of how a Payment Token Transaction might occur, starting from the point where the Cardholder presents a token to the Merchant.

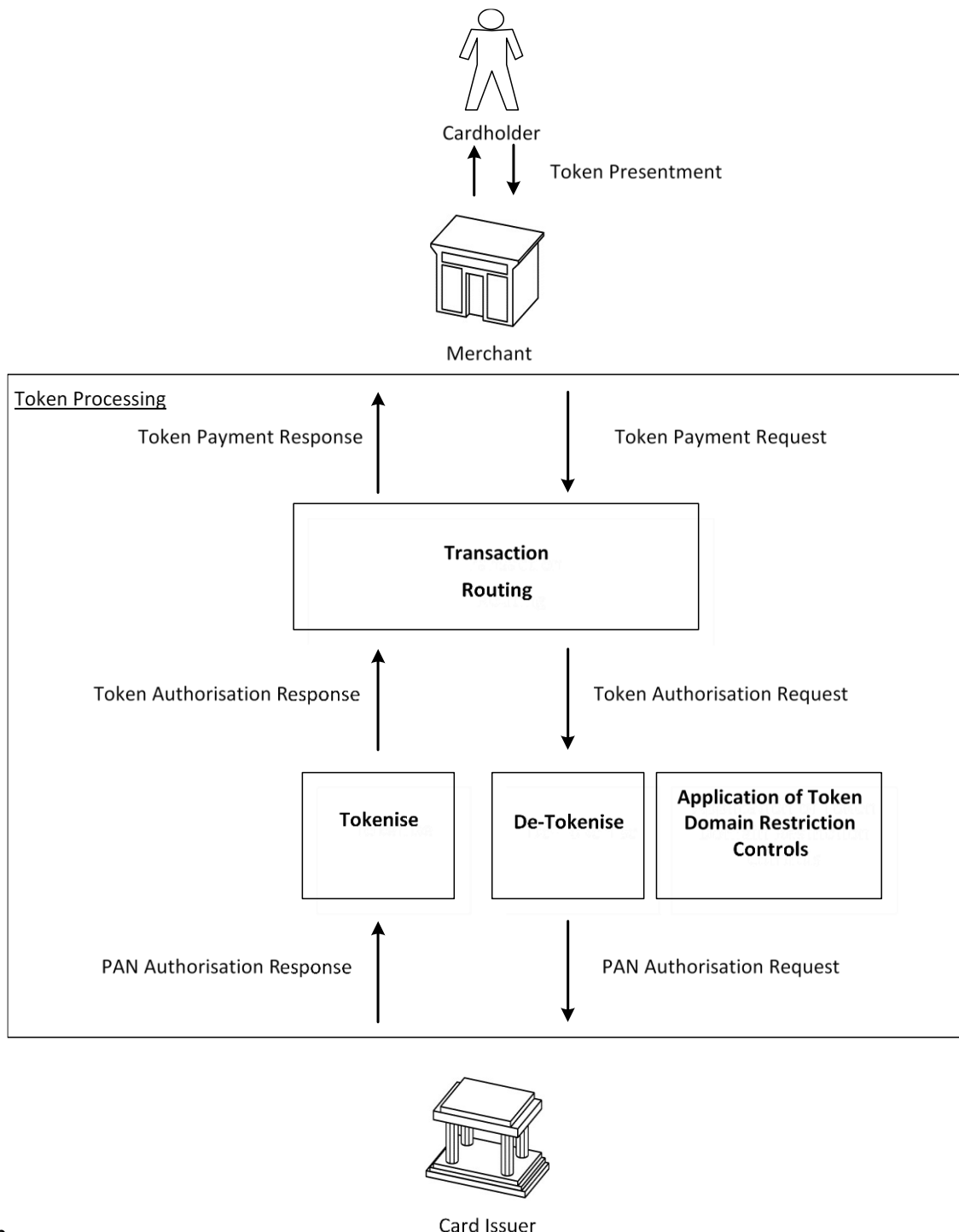


FIGURE 5: EMV PAYMENT TOKENS – BASIC AUTHORISATION FLOW

Token Processing follows Token Presentment and is divided into the following functions

Token Payment Request: includes the request that originates from the point of interaction with the

Merchant (such a Terminal, website or application) and the response that provides the results of the authorisation decision

Token Authorisation: includes the request and corresponding response between the Payment Network and the Acquirer up to but not including De-Tokenisation and the application of Token Domain Restriction Controls

Application of Token Domain Restriction Controls: is optionally performed and involves validating the Payment Token against the established Token Domain Restriction Controls. Processing may be performed independently of the De-Tokenisation function

De-Tokenisation: includes the request and corresponding response processing converting a Payment Token and Token Expiry Date to an underlying PAN and PAN Expiry Date. De-Tokenisation may or may not include the application of Token Domain Restriction Controls

PAN Authorisation: includes the request and corresponding response to/from the Card Issuer that contains the data necessary, including Token Processing related data, to determine the Card Issuer authorisation decision. The response contains the Card Issuer notification of the approve or decline decision

Note that during response processing, the PAN and PAN Expiry Date are tokenised back to the affiliated EMV Payment Token and Token Expiry Date before the Token Authorisation Response. In this context tokenised means the value of the PAN field in the Token Authorisation response is restored to the EMV Payment Token contained in the incoming Token Authorisation request.

2.3.4. EMV® Payment Tokenisation Use Cases

Here follows some use cases provided by EMVCo which may evolve over time. Please note that these are to be considered as examples only.

2.3.4.1. Use case 1: NFC mobile

This use case example outlines using an NFC-enabled mobile device at a contactless-enabled Terminal and communication is made using NFC. Cardholder experience may differ based on mobile device type.

In this use case, an EMV Payment Token is stored within an NFC-enabled mobile device or alternatively in a remote server and delivered to the mobile device prior to commencing a transaction.

2.3.4.2. Use case 2: E-commerce using a mobile digital wallet

This use case example outlines using an e-commerce site or application with a mobile / digital wallet to transfer payment and other order information. In this use case, an EMV Payment Token is stored by the Token Requestor so as to no longer need to store the PAN in the wallet platform for security or other business rationales. Cardholders have a wallet-branded checkout experience (sign in / sign up) unique to each wallet.

2.3.4.3. Use Case 3: Card on File

This use case example outlines an e-commerce Merchant that has EMV Payment Token and related data stored in a Merchant platform. For each Cardholder, a Merchant-specific EMV Payment Token is stored in the Merchant platform. Cardholders have a Merchant-branded checkout experience (sign in / sign up) unique to each Merchant.

2.3.4.4. Use Case 4: new Shared Payment Token

This use case example outlines a Token Requestor sharing an EMV Payment Token between multiple Merchants (Token Users). An EMV Payment Token or Token Reference ID is stored by the Token Requestor and made available to a Token User. The Token Requestor enables controls over which Merchants (Token Users) that it supports, will have access to the Shared Payment Token.

EMVCo is not able to provide a diagram showing these use cases since it goes beyond EMV® Payment Tokenisation Specification – Technical Framework v2.0 content.

2.3.5. **EMV® Payment Account Reference (PAR)**

2.3.5.1. Background

The introduction of Payment Tokenisation provides opportunity 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.

PAR Data is a newly-defined data field that is linked to the underlying PAN and will be associated with all affiliated Payment Tokens. Linkage of transaction history data to current and future transactions initiated on the underlying PAN and any affiliated Payment Tokens can be accomplished by using PAR as the linkage mechanism.

2.3.5.2. Overview of PAR

PAR is a non-financial reference assigned to each unique PAN and used to link a Payment Account represented by that PAN to affiliated Payment Tokens.

EMVCo Registered BIN Controllers (who can be either an ISO IIN Blockholder with allocated BINs or an ISO IIN Card Issuer with an allocated BIN(s)) determine the governance of the PAR Field and

PAR Data for the BINs under their jurisdiction.

BIN Controllers are responsible for the implementation of PAR and for specifying and communicating how PAR will be used within a given Payment System.

BIN Controllers must ensure that PAR Data is generated using their EMVCo-assigned BIN Controller Identifier to guarantee uniqueness across BIN Controllers and ensure the global uniqueness of PAR Data assignment to PANs generated from BINs under its control to ensure no collision or conflict.

They also define the generation method of the last 25 characters of the PAR Data.

PAR must be directly associated with the Payment Account as represented by the PAN and must have the same value for a PAN and all of its affiliated Payment Tokens without respect to the Payment Network that processes that PAN or any of its affiliated Payment Tokens.

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 non-tokenised PANs will enable a transactional history to be established.

PAR Data is unique in its assignment to a given PAN and is not intended to be a PAN replacement or a consumer identifier. Where there are two separate PANs within a 'Payment Account', each PAN will have a separate PAR value.

PAR Data alone is not sufficient to initiate a payment transaction including authorisation, capture, clearing or chargeback. Payment transactions can only be initiated on a Payment Token or underlying PAN, although PAR Data may be present as an accompanying data field within the transaction. BIN Controllers determine the specific usage for PAR Data for Payment Tokens and underlying PANs.

PAR Data shall not be capable of being used to derive underlying PAN attributes that identify product type.

PAR Data shall not be used as a consumer identifier (it is unique to a PAN not to the cardholder).

PAR Data shall not be used to route transactions

PAR Data shall be generated using a method that cannot be reverse engineered to determine underlying PAN or Payment Token information. Cardholders will generally be unaware of PAR Data. This will not adversely impact the ability of Cardholders to transact.

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. 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 mapped to the original underlying PAN to be remapped to the new underlying PAN and maintain the current associated PAR Data.

BIN Controllers are responsible to identify the entities that are permitted to participate in PAR Data generation and assignment for BINs under their control.

The PAR Data is a composite field consisting of 29 uppercase Alphanumeric Roman characters with two components:

- a 4-character BIN Controller Identifier assigned by EMVCo
- a 25-character unique value assigned to each underlying PAN

Implementation of PAR is outside of the scope of the EMV® Payment Tokenisation Specification – Technical Framework and EMVCo: it is the responsibility of each Registered BIN Controller to communicate and specify how PAR will be used within its payment ecosystem. Multiple PAR governance approaches are possible covering, PAR generation, PAR participants, etc

PAR Data provisioned to an EMV Based Application (e.g. Mobile NFC at Point of Sale) SHALL utilise EMV Tag '9F24' to identify PAR Data.

When provisioned in an EMV Based Application, PAR Data may be made available to the Merchant, both online and off-line, according to the EMV® Payment Tokenisation Specification Technical Framework. This could be done through the following means:

- PAR Data is identified at the point of sale through EMV Tag '9F24'
- Through a PAR Enquiry Function
- In the authorisation response from the Acquirer or Payment Processor

When provisioned in a non-EMV Based Application (e.g. Card on File), PAR Data may be made available by the Token Requestor with the Payment Token in the related data.

ISO fields for PAR have been agreed - Field 56 for ISO 8583 (1987), Field 112 for ISO 8583 (1998), Field 51 for ISO 8583 (2003).

2.4. PCI SSC Token Service Provider

The purpose of the Payment Card Industry (PCI) Token Service Providers Additional Security Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens) Version 1.0 is to define physical and logical security requirements and assessment procedures for Token Service Providers that generate and issue EMV Payment Tokens, as defined under the EMV® Payment Tokenisation Specification - Technical Framework.

The EMV® Payment Tokenisation Specification - Technical Framework defines Token Service Providers as an entity "that is responsible for a number of discrete functions which may include, but are not limited to: Maintenance and operation of a Token Vault, token generation, application of security and related controls, token issuance and token provisioning, including the facilitation of PAR filed and PAR data in provisioning request, Token Requestor registry function, detokenisation and tokenisation, application of Token Domain restriction controls".

In their capacity as the authorized party for issuance of Payment Tokens, Token Service Providers, (TSP) are responsible for a number of discrete functions, which are defined in the EMV® Payment Tokenisation Specification - Technical Framework. For a detailed description of the Payment Token ecosystem, terminology definitions, key responsibilities, and controls specific to each entity within the ecosystem, refer to the EMV® Payment Tokenisation Specification - Technical Framework.

The Payment Card Industry (PCI) Token Service Providers Additional Security Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens) Version 1.0 does not address how a Token Service Provider would meet the requirements in the EMV® Payment Tokenisation Specification - Technical Framework. Rather, it defines the security controls needed to protect environments where the tokenization services occur. Entities designated as a Token

Service Provider under the EMV® Payment Tokenisation Specification - Technical Framework may be subject to these requirements. To determine if an entity is required to meet these requirements, confirm with the Global Card brand for which services are provided. These requirements cover EMV Payment Tokens, not acquiring tokens or other types of tokens. While organizations may choose to use the Payment Card Industry (PCI) Additional Security Requirements for Token Service Providers (EMV Payment Tokens) to assess other token deployments, it is not required that these requirements be applied to those implementations.

2.4.1. PCI SSC Tokenisation Guidelines

With a rising demand for tokenization products, the PCI Security Standards Council (PCI SSC) believes it is imperative to build, test, and deploy products that provide strong support for compliance with the PCI Data Security Standard (PCI DSS). With this aim, the Council has produced the PCI SSC technical guidelines for evaluating tokenization products that replace the primary account number (PAN) with a surrogate value called a 'token'. The security and robustness of a tokenization system relies on many factors, including the configuration of different components, the overall implementation, and the availability and functionality of specific security features for each product. A tokenization product can be a hardware device, such as an appliance, a software application, and/or a service offering.

PCI SSC's 'Tokenization Product Security Guidelines', provides best practices for 'acquiring tokens', which are defined as Tokens created by the acquirer, merchant, or a merchant's service provider. This token is created after the cardholder presents their payment credentials. Acquiring tokens may be used as part of the authorization process, including card-on-file transactions.

The General Guidelines/Best Practices statements provided within the PCI SSC Tokenization product Security guidelines are intended for all types of token-generation methods, and there are also specific Guidelines/Best Practices for irreversible and reversible tokens. This document also describes different classifications of tokens (i.e., tokenization taxonomy), including their general use cases. This document is neutral to which approach is used by product developers and builders.

One issue that will remain is regardless of when the PAN is turned into a token, the initial point of contact by the PAN into the merchant will need to conform to PCI DSS guidelines (Data Security Standards)

2.4.2. PCI SSC Tokenisation Domains

The PCI Tokenization guideline is broken into 5 sections:

- General guidelines and best practices applicable to all token types
- "Domain 1": Token Generation: For each tokenisation class, this so called 'domain' defines considerations for securely generating tokens
- "Domain 2": Token Mapping. Only applicable to reversible tokenisation implementations. Addresses the mapping of tokens to their original PAN. Includes access controls and logging needs for tokenisation and de-tokenisation requests.
- "Domain 3": Card Data Vault. Only applicable to reversible tokenisation implementations. This domain covers the encryption of the PAN and the access controls used to access the vault.

- “Domain 4”: Defines the proper Cryptographic key management practices for all the operations performed by the tokenisation product.

Further description of each domain and specific examples as well as associated requirements can be found in the PCI SSC Tokenization Guidelines document.

2.4.3. Relation between PCI and EMVCo’s PAR

Provided the PAR is generated following the EMVCo guidelines, it cannot be used to initiate a payment transaction and cannot be reverse engineered to obtain a PAN or other PCI Account Data. Therefore, **it is not considered Account Data and not in scope for PCI DSS.**

For reference please see FAQ #1374

(https://pcissc.secure.force.com/faq/articles/Frequently_Asked_Question/Is-Payment-Account-Reference-PAR-as-defined-by-EMVCo-considered-PCI-Account-Data)

2.5. Non-standardised Issuer-Led Payment Tokens

Within the Issuer-Led model, several forms of tokens exist outside the referenced global standards. Actually, such forms of Tokens – which are still operational in some markets for some use cases - were thought of and implemented before the emergence of EMV Payment Tokens. One can think of them as somehow the historical forms of Payment Tokens.

Before continuing, it has to be noted that non-standardised Tokens may also exist within the realm of the merchant-led or acquirer-led models. These may be the result of applying proprietary solutions or domestic or regional standards.

Coming back to the issuer-led model. In order to refer to those Tokens, terms like ‘Alternate PAN’, ‘Virtual Card Number’ or ‘Dynamic Card’ are often used, sometimes interchangeably.

Although no common, standard definition exists, one attempt to clarify the differences among the three ‘flavours’ is offered here:

- Alternate PAN is static (i.e. it does not change at every transaction) and a typical use case would be a bank-issued, HCE (Host Card Emulation) mobile wallet
- Virtual PAN is also static (i.e. it does not change at every transaction) and a typical use case would be a PAN communicated by the issuer to the cardholder without a physical secured support (chip card, mobile phone secure element). Its intended use could be for e-commerce, aiming at internet use only, isolating the use of the primary, underlying PAN to Face-To-Face environments only.
- Dynamic PAN: It is by definition dynamic, will change at every transaction, and could also be thought of as a ‘single-use’ PAN. This kind of Token by definition can’t reside on a plastic chip card or be issued on any kind of static support.

In all of the above three cases, the resulting PAN used for the transaction is – needless to say – interoperable.

Equally, in all three cases, the BIN's under which these PAN numbers will be issued will have been assigned or delegated to the issuer, under the applicable governance in place so as to guarantee the uniqueness needed for interoperability, security and the seamless overlay of the tokenized PAN over all the existing card transaction processes. As an example, it will continue to be necessary to properly register the new BIN under the right product id (credit, debit, commercial, prepaid).

In order to provide some 'firewall-like' protection between them, the Token BIN will typically be different from that of the primary or underlying PAN.

As has been previously stated, the Token PAN (Alternate, Virtual, Dynamic) will be such that it ensured a seamless overlay into existing infrastructure and processes, as illustrated in the following diagram.

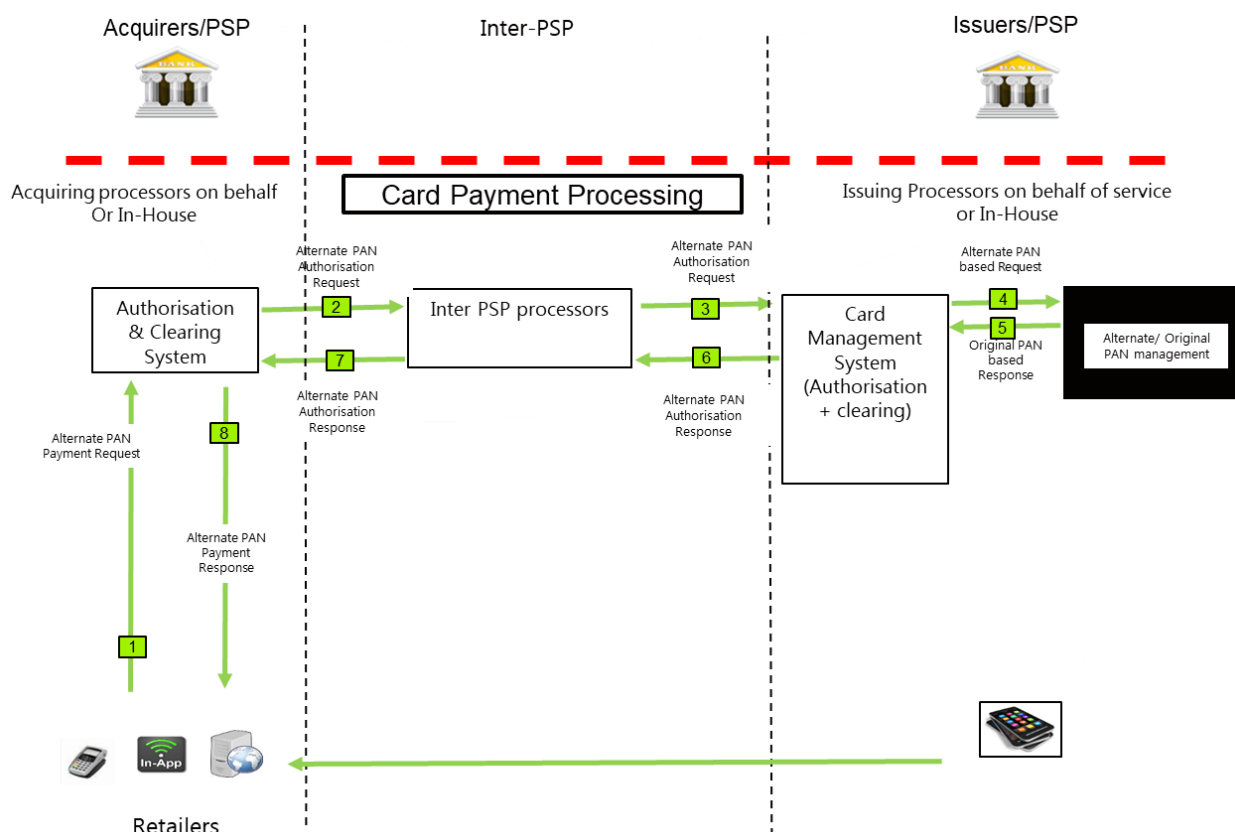


FIGURE 6: ISSUER LED /ALTERNATE PAN DIAGRAM (ALSO VALID FOR OTHER FORMS OF TOKENS SUCH AS 'VIRTUAL' OR 'DYNAMIC' PANs)

The actual methods used for the generation and mapping (and subsequent de-mapping) of such card numbers will generally reside in the issuer domain and are not subject to any defined global standard, therefore they are an issuer implementation option that remains at issuer discretion within the boundaries set by the applicable scheme rules.

Differences when compared to EMVCo Tokens and ECSG recommendation

The use of such Payment Tokens ('alternate PAN's', 'virtual card numbers') is different to the EMV Payment Tokens in that they do not necessarily possess all the security attributes, e.g. Token Domain Restriction Control, that conform to 'EMVCo token', as has been explained in the relevant

earlier section of this document. The ECSG has adopted⁴ the use of “EMV® Payment Tokenisation Specification - Technical Framework” V2 (as well as of the “PCI Tokenisation Guidelines”) as the reference for tokenisation in the SEPA Cards Standardisation Volume going forward.

This support is understood primarily as a baseline support, i.e., meaning that the adequate references will be made from the Volume to these applicable standards, re-using their terminology, concepts, roles, processes and functions wherever needed.

Because the EMV® Payment Tokenisation Specification - Technical Framework is a global, secure, interoperable standard, and because it defines a certain number of useful features such as e.g. ‘Token Domain Restriction Controls’, ‘Token Assurance Methods’, ‘PAR’ (Payment Account Reference) and others, the ECSG recommends – but does not require - the use of EMV Payment Tokens.

Conversely, the use of Alternate/Virtual/Dynamic PANs, i.e. more generally the use of non EMV Payment Tokens, is not preferred by the ECSG but it is not forbidden.

Note that PAR is further developed in subsequent sections of this document. By linking an EMV Payment Token to an underlying PAN, the PAR enables the transparency needed to support some retailer needs, while preserving security.

2.6. Merchant led non-payment tokenisation

Merchant led tokens are another model of tokens which unlike the EMV Payment Tokens cannot be used to request a payment transaction.

2.6.1. Model description

Merchants deploying non-payment tokenisation solutions usually seek to implement some use cases and value-added services while avoiding entering into possession or processing sensitive payment information such as PANs. This enables them to increase the level of security of their payment solution and to facilitate their compliance with PCI rules.

In order to do so, merchants retailers actually ‘outsource’ the storage and processing of PAN information to another actor in the value chain (typically a payment processor or an acquirer), who has to implement PCI compliant platforms for its own activities.

Such tokens are used in closed loop environments between a subset of ecosystem participants for specified purpose and do not traverse the interoperability domain. They are used where transaction data are stored, but the Card PAN and other sensitive information have substitute values (tokens). Typical use cases include Fraud management, Merchant analytics, omni channel use cases, ...

Such tokens can either have the same format as a standard Card PAN or can ‘look’ completely

⁴ ECSG Board decision of November 28th 2017: “The ECSG board approves the proposal for ETs guidance regarding the inclusion in the Volume of EMVCo framework and PCI security requirements as well as PAR implementation recommendations”.

different. In any case, they cannot be used for initiating payment transactions.

Merchant tokens are to be seen as a process reducing the amount of cardholder data stored in merchant environments and potentially lowering merchant's efforts with PCI DSS requirements compliance rather than as a competing alternative to EMV Payment Tokens.

2.6.2. Merchant tokenisation use cases

Note: these are non-exhaustive examples.

2.6.2.1. Merchant Stored Card Data / Card on File

In this use case, the Merchant securely stores a Token provided by its token provider in the Cardholder profile instead of the PAN.

The Cardholder buying experience is simplified in forthcoming transactions, as he doesn't need to provide its card details once more. The Cardholder will be proposed to reuse one of the cards previously registered. The merchant will send the transaction with the Token information to its token provider, and the token provider will replace the Token by the actual Card PAN before forwarding the transaction to the Acquirer.

2.6.2.2. Refund by web

In this use case, the token solution provider keeps the actual PAN used for each payment transaction and generates a token to the merchant.

The merchant then has the possibility to initiate a total or partial refund of the transaction through an online back office interface. The merchant will send the refund request with a reference to the initial transaction or with the provided token to the token solution provider (typically a PSP gateway or the acquirer) who will replace by the actual PAN before forwarding the refund request to the acquirer.

2.6.2.3. Click and Collect

In this use case, a consumer will make an online purchase and will choose to pick up the goods at some merchant location. The token solution provider keeps track of the card used for the purchase and provides a token to the merchant.

Upon pick up of the goods, the consumer will present the card used for the online purchase to the merchant, the token solution provider will be able to match this with the order and give a feedback to the merchant to deliver the goods. The actual payment can either take place at the time of order or at the time of pick up.

2.6.2.4. Payment by instalment

In this use case, the token solution provider generates a token to the merchant upon the 1st

transaction.

The merchant keeps this token and then has the possibility to initiate following instalment transactions containing the token. The token solution provider will replace the token by the actual PAN before forwarding the transactions to the acquirer.

2.6.2.5. Fraud Management

In this use case, the token solution provider generates a token for each different PAN the merchant will receive.

The merchant will then be able to process the token data and implement fraud detection mechanisms without any concern about PCI DSS constraints.

2.6.2.6. Merchant analytics management

In this use case, the token solution provider generates a token for each different Card PAN the merchant will receive.

The merchant will then be able to process the token data and implement analytics tools for reporting, marketing, and business improvement purposed without any concern about PCI DSS Constraints.

2.6.2.7. Loyalty

In this use case, the token solution provider generates a token for each different PAN the merchant will receive.

The merchant will then be able to identify consumers (subject to their prior consent) based on this token, and provide their benefits, customised offers, etc...

3. BUSINESS PRINCIPLES

3.1. Business principle related to the EMV tokens

In the context of the preceding sections, where the conceptual basis and global standard foundations have been established, it may be the case that card issuers want to be a Token Service Provider (TSP). Alternatively, it may also happen that card issuers want to use third party providers to perform tokenisation services.

While recognizing those cases, it is equally important to ensure the integrity of the overall ecosystem in general and of any given Token Programme in particular.

In order to bridge these two needs, flexibility of choice for the important function of the TSP and preserving the integrity of the system, the following business principle:

“The issuer is free to select one or more approved supplier(s) for the role of Token Service Provider within any single Token Programme. The approval will be performed by a Payment System who has defined the Token Programme and will include a number of Security, Functional and Operational requirements.

These requirements must be based on the principles of:

- Competition
- Transparency
- Non-Discrimination
- Efficiency
- Security

In conformance with this business principle and with the Book 7 of the Volume, the TSP (Token Service Provider) is in the Issuing domain.

Two options of functional architecture are illustrated below:

- Option 1: the TSP is connected behind the CMS (Card Management System) of the Issuer which is in direct relation with the inter-PSP processor
- Option 2: the TSP is directly connected to an Inter-PSP processor (switching)

3.1.1. Option 1

Note: This is a logical diagram and does not represent the physical location of a TSP

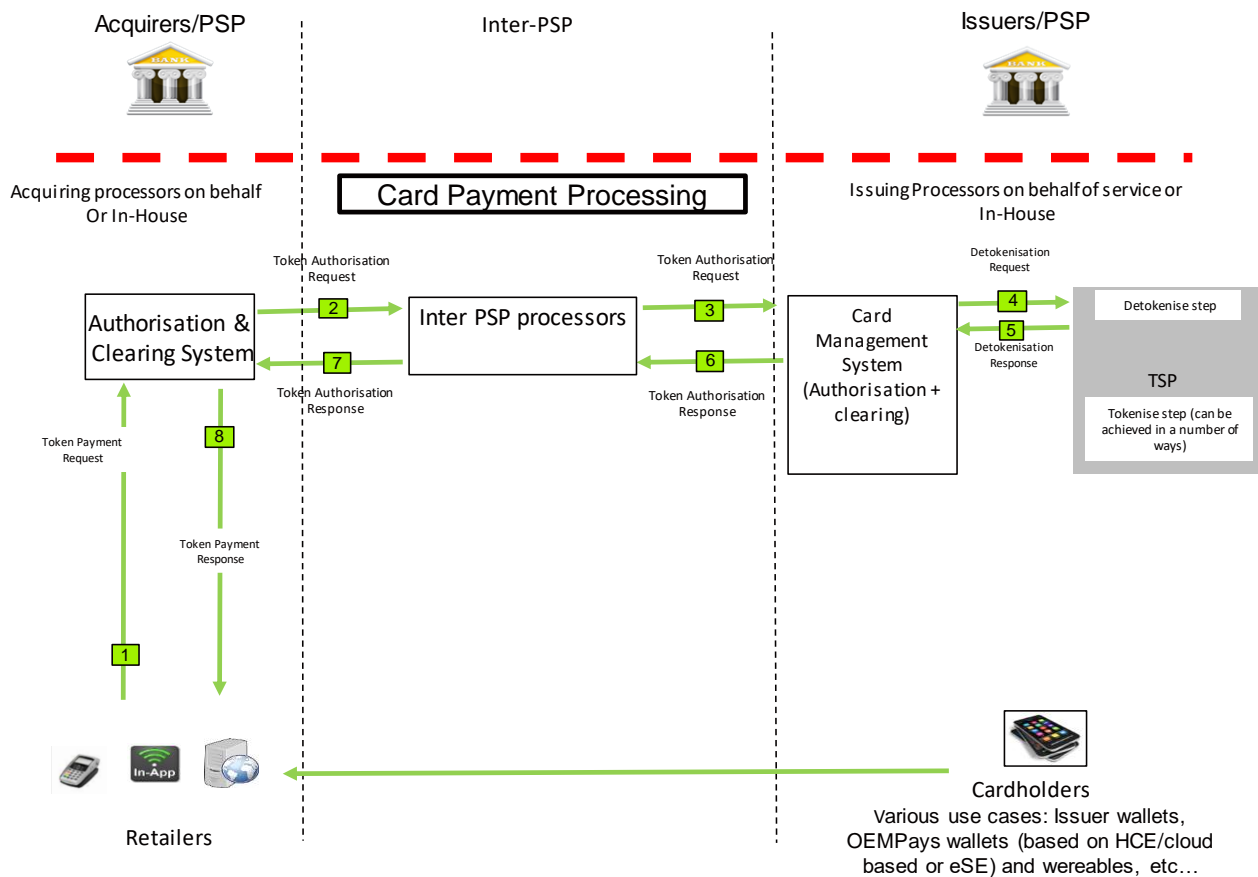


FIGURE 7: OPTION 1: TSP IN THE ISSUING DOMAIN BEHIND THE CMS

The CMS of the Issuer, linked to the Inter-PSP processor for the authorisation and clearing flows, sends a detokenisation request to the TSP in order to retrieve the PAN.

Only the EMV Payment Token (not the PAN) is transmitted to the acquirer in the token authorisation response.

3.1.2. Option 2

Note: This is a logical diagram and does not represent the physical location of a TSP

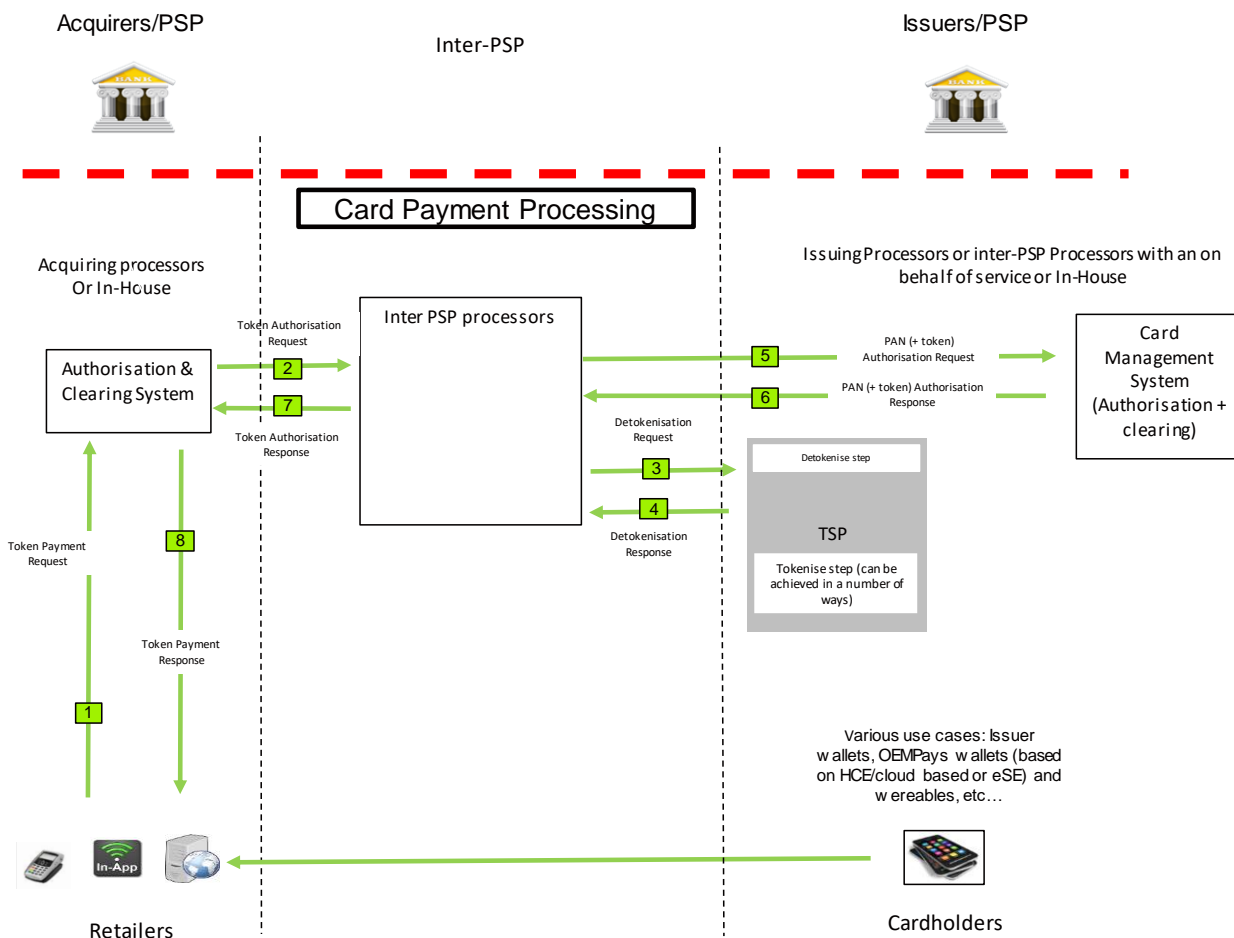


FIGURE 8: OPTION 2: TSP IN THE ISSUING DOMAIN IN FRONT OF THE CMS

In this option, the inter-PSP processor send:

1. To the TSP (always in the issuing domain) a detokenisation request to retrieve the PAN
2. And in a second step to the CSM an authorisation request with the PAN and the token

Only the token is transmitted by the Inter-PSP processor to the acquirer in the token authorisation response.

3.1.3. Token Issuance diagram

The previous diagrams only represent the interoperability of EMV Payment Tokens-based payment flows that is the functional scope of the Volume. However, as additional information, here below a diagram of the token issuance for any token issuance models. This diagram works for the both options above.

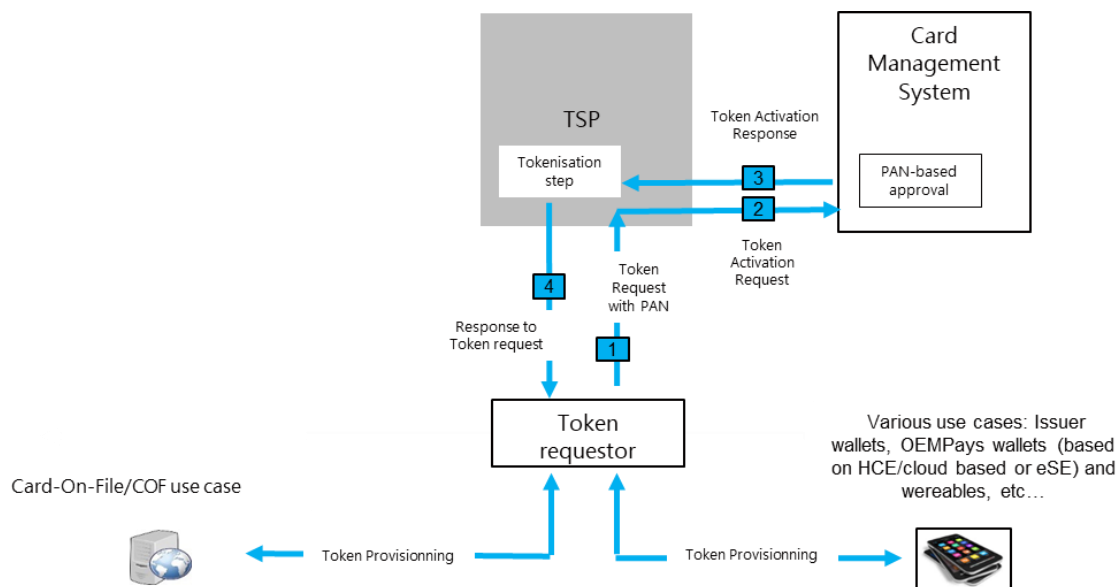


FIGURE 9: DIAGRAM FOR ANY TOKEN PAYMENT MODELS

The token provisioning is intended both the use cases (i.e. wallets) on the cardholder's side, and the use cases (i.e. Card-On-File) on the merchant side.

4. RETAILERS PERSPECTIVE AND NEEDS IN RELATION TO IDENTIFYING THE PAN 'BEHIND' THE PAYMENT TOKEN

The EMVCo Payment Tokenisation Specification - Technical Framework enables retailers to secure a card's Primary Account Number (PAN) credential by tokenising the card PAN in underlying Payment Tokens during the entire transaction flow. Retailers have a requirement to link the use of different Payment Tokens to the same underlying card PAN in order to support:

- current merchant loyalty programs, loyalty points or reward schemes
- fraud management and fraud related enquiries
- anti money-laundering monitoring

EMVCo has addressed these issues by introducing a new data element called Payment Account Reference (PAR). PAR Data is linked to the underlying PAN and will be associated with all affiliated Payment Tokens. Building a transaction history of current and future transactions initiated on the underlying PAN and any affiliated Payment Tokens can be accomplished by using PAR as the linkage mechanism.

The PAR links the EMV Payment Tokens to their unique, 'underlying' PAN and it is important to point out that the PAR does not link either a PAN or an EMV Payment Token to an individual customer. Indeed, a customer may hold multiple cards (i.e. multiple PAN's) with one or more issuing institutions. Each one of these unique PAN's would have its own PAR in order to establish the link to any affiliated EMV Payment Tokens that may have been generated for that PAN.

In summary, for transactions done with an EMV Payment Token and where a PAR is available, the PAR can be used to link the affiliated and different EMV Payment Tokens to the respective single underlying PAN. Users of PAR need to take this into account when implementing solutions based on this data element.

The EMV® Payment Tokenisation Specification - Technical Framework specifies that "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 PAR is made available to the retailer in different ways, for example

- as part of the authorization response message
- through a separate enquiry message⁵
- In defined data fields of the application (see section 2.3.5.2 of this document)

Note that according to the EMV® Payment Tokenisation Specification - Technical Framework:

⁵ This is outside the EMV® Payment Tokenisation Specification - Technical Framework as it is implementation dependent under the boundaries of the governance defined by the BIN controller

- PAR governance is established by the BIN controller. A definition of 'BIN Controller' can be found in section 7.3 of this document. The allocation of BIN's to issuers and the use of BIN's by issuers is done as per current practices and falls outside of the scope of the EMV® Payment Tokenisation Specification - Technical Framework.
- EMV Payment Tokens governance is part of a Token Programme in which the issuers of the underlying PAN participate. A definition of 'Token Programme' can be found in Section 8.3 of this document.

Retailers have a need to access the PAR information early in the transaction process, for example before the authorization request, to apply or redeem some targeted offers if they wish, or later in the transaction as part of the authorization response, to apply some loyalty points or rewards.

Making the PAR field available to retailers requires a number of technical adaptations along the value chain (terminals, acquirers, networks, issuers) and functional rules agreed and implemented until all the technical requirements are delivered.

Widespread implementation of these changes may require several years to complete and needs to be coordinated by the card industry in order to minimise any detrimental impact and contain costs.

In conclusion, the use of EMV Payment Tokens has the capability of supporting retailer's needs, as long as the associated PAR is made available to them. This is not necessarily the case for other types of tokens or 'pseudo-tokens' such as 'alternate PANs' or 'Virtual Card Numbers' - unless a similar PAR solution could also be used for them.

5. PAR (PAYMENT ACCOUNT REFERENCE) MANAGEMENT AND CO-BADGED CARDS

The concept of PAR (Payment Account reference) was introduced by EMVCo through EMV Specification Bulletin N°167 which has been fully incorporated into the Version 2 of the EMV® Payment Tokenisation Specification – Technical framework (September 2017).

In June 2018, EMVCo has also released a White Paper on Payment Account Reference (PAR), a dedicated document on the management of this new data.

The PAR is a non-financial reference assigned to each unique PAN and used to link a Payment Account represented by that PAN to affiliated Payment Tokens. In other words, the PAR makes the connection between the physical world (the PAN of the plastic card) and the digital world (the various Payment Tokens of the underlying PAN). The PAR is linked to the BIN of the PAN and not to the BIN of the Tokens.

The goal of this section is not to describe the EMVCo specifications of the PAR but to illustrate the management of this data in two co-badged cards models existing in the SEPA market for example between an ICS (International Card Scheme) and a LCS (Local Card Scheme).

It is only to remind that the PAR management is under the governance of the BIN owner (the BIN Controller) of the BIN used for the underlying PAN.

5.1. PAR in a co-badge environment with separate PANs

The first model associates on the same plastic card two BIN owners:

- The ISO IIN Blockholder: an ISO/IEC 7812 registered IIN Blockholder is an assigned owner of several IINs (BINs) for the purposes of issuing, sub licensing or otherwise assigning BINs for use by Card Issuers. It can be the ICS
- The ISO IIN Card Issuer: an ISO/IEC 7812 registered IIN card Issuer is an assigned owner of an IIN (BIN) for the purposes of issuing Primary Account Numbers (PANs)

There are two PANs on the plastic card (one PAN for each BIN owner and BIN controller) and two AIDs in the chip (one AID for each PAN). This approach varies by markets in terms of front (i.e. the embossed data) of card PAN and other PAN on card and/or use of AIDs for each PAN in the EMV based Payment Application (i.e. the data in the chip). *NB: the Italian Central Bank assigns an IIN for the purpose of identifying PSPs for several banking functions (Cards, direct debit, credit transfer, etc...)*

The initial (i.e.: in the physical world of the card) diagram of this co-badge model is as following:

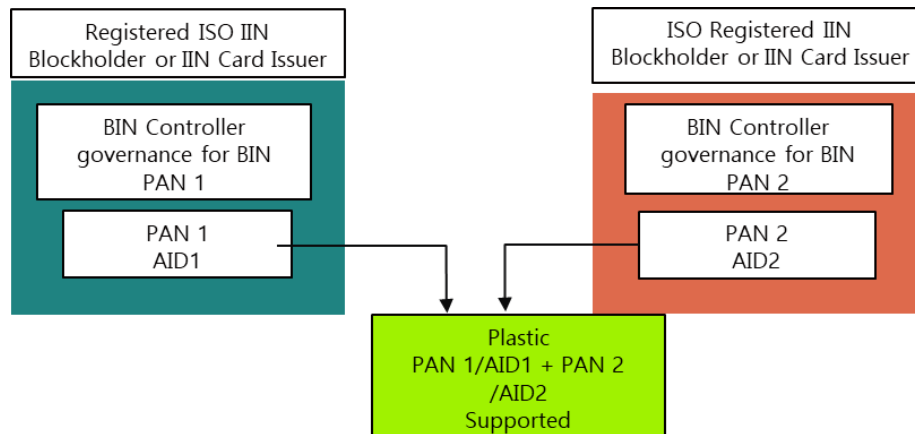


FIGURE 10: CO-BADGE APPROACH 1

The tokens (of the digital world) and the PAR extend the diagram, as following considering that the personalisation of the PAR in the chip card is optional.

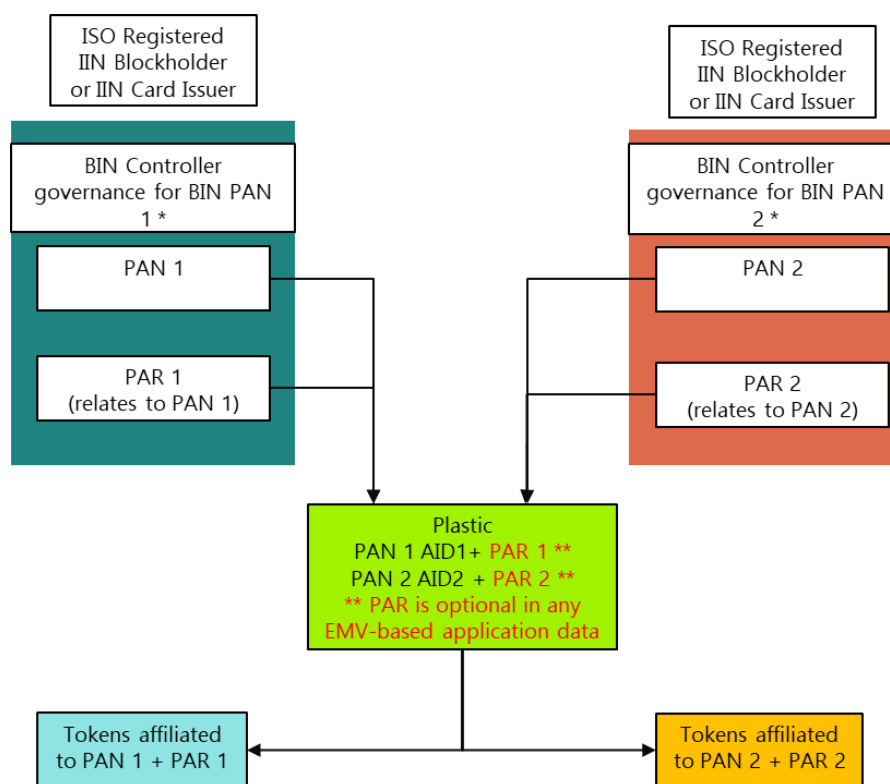


FIGURE 11: CO-BADGE APPROACH 1: PAR in a CO-BADGE ENVIRONMENT WITH SEPARATE PANs

In this model, there are two PARs, one PAR linked to each underlying PAN and to each BIN owner or BIN controller.

It is the responsibility of each EMVCo registered BIN Controller to specify how PAR will be used/generated within its payment ecosystem. The generation of the PAR can be either centralised on an unique entity or distributed through Authorised Entities like payment system, card issuer, etc...

PAR should be available to the various entities issuing Payment Tokens (i.e. TSP/Token Service Provider) irrespective of the Token BIN being used.

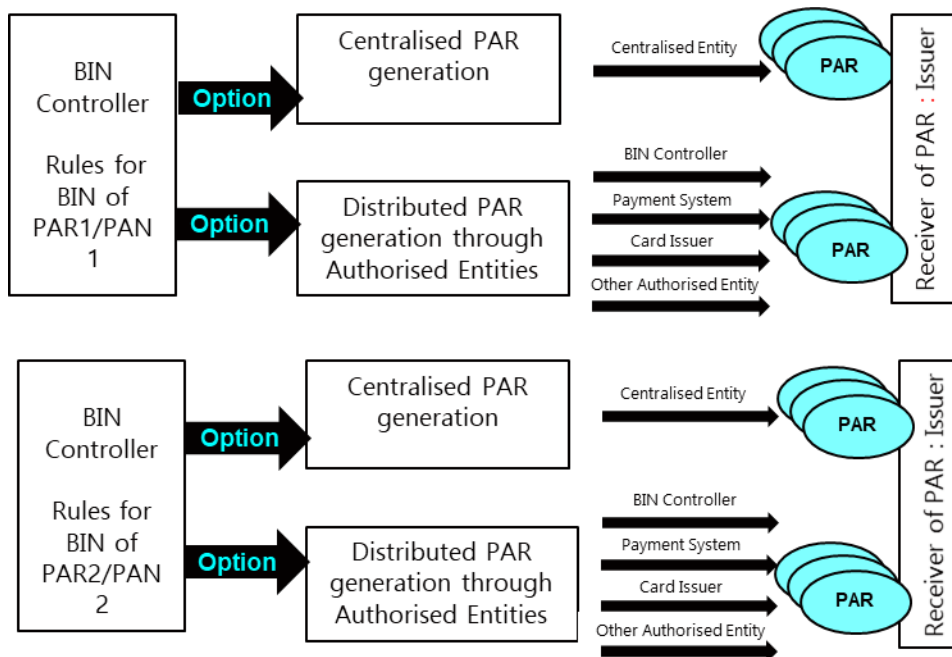


FIGURE 12: PAR GOVERNANCE: ILLUSTRATION OF EXAMPLE MODEL - CO-BADGE APPROACH 1

5.2. PAR in a co-badge environment with same PAN

The second model hosts on the same plastic card an only one BIN owner (an ISO Registered IIN Blockholder or IIN Card Issuer) with a co-badging entity, which is not a BIN owner.

There is an only one PAN on the plastic card, from the BIN owner but two AIDs in the chip card: one AID per co-badge entity. This approach is used in several markets with a single PAN and use of this PAN with different AIDs in the EMV based Payment Application.

The initial (i.e.: in the physical world of the card) diagram of this co-badge model is as following:

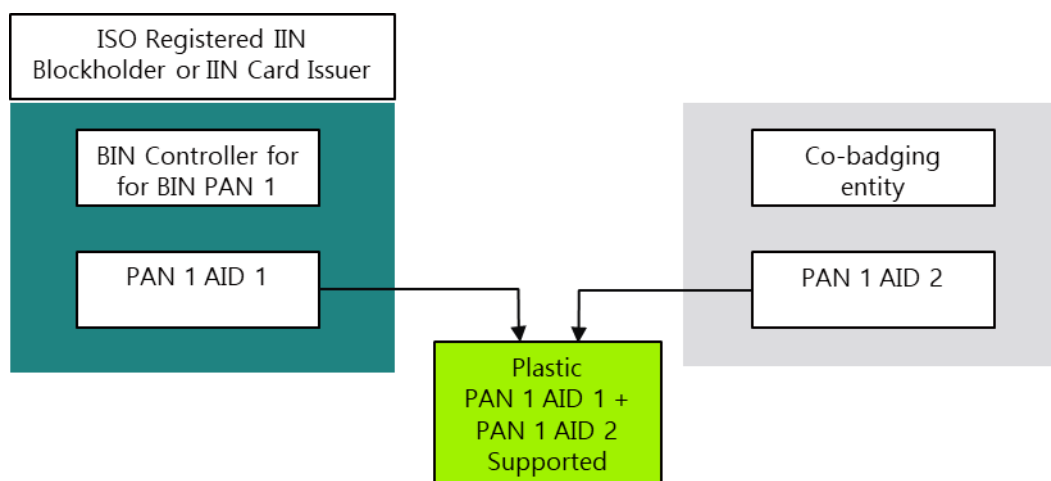


FIGURE 13: CO-BADGE APPROACH 2: PAR IN A CO-BADGE ENVIRONMENT WITH THE SAME PAN

The Payment Tokens (of the digital world) and the PAR extend the diagram, as following

considering that the personalisation of the PAR in the chip card is optional.

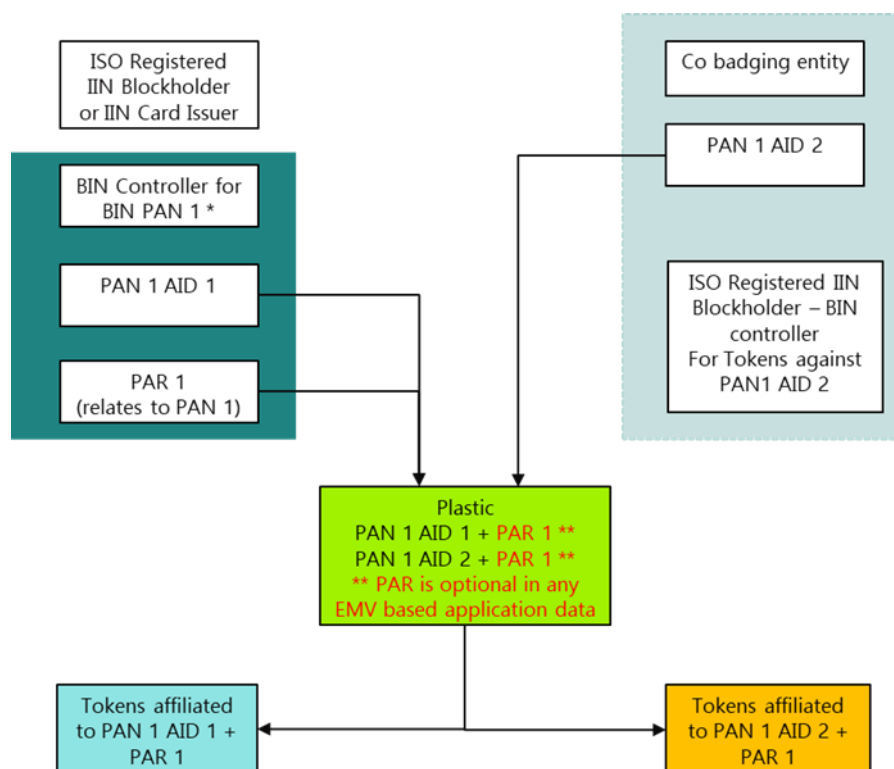


FIGURE 14: CO-BADGE APPROACH 2: PAR IN A CO-BADGE ENVIRONMENT WITH ONLY ONE PAR LINKED TO THE ONLY ONE UNDERLYING PAN

In this model there is an only one PAR linked to the only one underlying PAN

It is the responsibility of each registered BIN Controller to specify how PAR will be used/generated within its payment ecosystem. The generation of the PAR can be either centralised on a unique entity or distributed through Authorised Entities like payment system, card issuer, etc...

PAR should be available to the various entities issuing tokens (i.e. TSP/Token Service Provider) irrespective of the Token BIN being used.

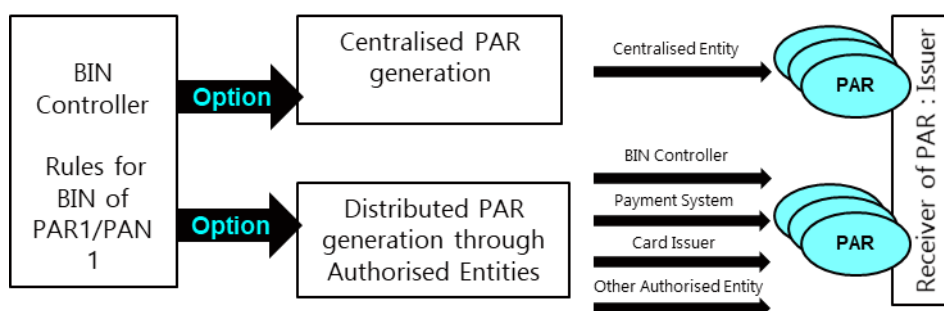


FIGURE 15: PAR GOVERNANCE: ILLUSTRATION OF EXAMPLE MODEL - CO-BADGE APPROACH 2

In this use case, the co-badging entity can issue tokens with its own BIN (different from a BIN token of the BIN owner of the PAN) but the PAR will be linked to the BIN of the PAN of the physical card.

6. GDPR CONSIDERATIONS

The ECSG acknowledges the importance of ensuring compliance with the mandatory provisions of applicable rules and regulations related to data protection and privacy in the context of tokenisation, notably the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, “GDPR”).

GDPR requires **privacy by design** which encourages Pseudonymisation as a measure to ensure that appropriate technical measures and safeguards are in place for the protection of personal data. This can help organisations meet a number of the key GDPR principles, such as data minimization, data integrity and confidentiality.

Tokenisation is one of the techniques of data Pseudonymisation defined in the GDPR (Article 4). Pseudonymisation can reduce the risks to the data subjects concerned and help controllers and processors to meet their data protection obligations.

In particular Tokenisation helps organisations ensure GDPR compliance by implementing **data security** (GDPR, Article 32.1(a)) and limiting the risk of harm to the rights and freedoms of individuals (Cardholders) in case of Personal Data Breach which could result in unauthorised use of Personal Data for fraudulent purposes.

6.1. PAN, Token and PAR under the GDPR

6.1.1. PAN, Token, and PAR are Personal Data

GDPR provides for a broad definition of Personal Data, which covers any information relating to an identified or identifiable natural person.

PAN (as defined in Book1), Token and PAR relate to an identified or identifiable individual (i.e. a Cardholder) and are therefore personal data. PAN, Token and PAR, are therefore subject to all relevant requirements applicable to the processing of Personal Data under the GDPR.

PAN, Token and PAR as such are not considered Special Categories of Personal Data (also known as sensitive personal data) under the GDPR.

Please note that other legislations such as PSD2 may contain separate definitions for data that is considered sensitive.

6.1.2. Anonymous and pseudonymous data

Personal Data which has undergone Pseudonymisation techniques, such as Tokenisation, continues to relate to an identified or identifiable individual, therefore it continues to be Personal Data, even though the connection between the pseudonymised data and such individual is not possible without certain additional information.

By contrast, **anonymous data** is information which does not relate to an identified or identifiable individual or data rendered anonymous in such a manner that an individual is not or no longer identifiable (GDPR, Recital 26).

The reader is invited to refer to available regulatory guidelines for further information.⁶

6.2. Key GDPR aspects relevant for Pseudonymisation

The purpose of this Chapter is to highlight some GDPR aspects relevant to Pseudonymisation, and therefore to Tokenisation. The purpose is not to provide comprehensive clarifications or explanations of all possible aspects of Pseudonymisation and the Tokenisation technique. It remains the responsibility of each stakeholder to ensure that its activities related to Card services, including Tokenisation, are fully compliant to those regulations.

GDPR imposes stringent compliance obligations on stakeholders (data controllers and data processors) when they process Personal Data. At the same time, GDPR offers incentives to stakeholders to use Pseudonymisation:

- **Data security.** Pseudonymisation is deemed to be a technical security measure under the GDPR (Article 32.1 (a) of the GDPR).
- **Data breach notification.** The requirement for data controllers to notify individuals of personal data breaches may not apply if the affected Personal data has been rendered unintelligible following Pseudonymisation (GDPR, Article 34.1 and 34.3.a).
- **Individual rights.** Under some circumstances, a data controller may not be required to (i) maintain or process additional information in order to identify an individual where the relevant Personal Data is pseudonymised and the data controller is not in a position to identify the individual, and (ii) comply with requests concerning certain individual rights (rights of access, rectification, erasure, restriction of processing and data portability),

⁶ https://edpb.europa.eu/guidelines-relevant-controllers-and-processors_en

except where the individual provides additional information enabling his or her identification (GDPR, Article 11).

6.3. Responsibilities of the relevant stakeholders when using pseudonymous data

Each stakeholder is responsible for identifying its role under the GDPR, understanding which Personal Data it processes, and analysing the relevant obligations applicable to them under the GDPR including whether it processes Pseudonymised data and which legal bases should be relied upon.

7. ECSG REQUIREMENTS

The ECSG SEPA Cards Standardisation Volume, includes high-level requirements, notably in the Functional and Security aspects, that are necessary to realise the SEPA vision in the cards payments arena.

In the area of Tokenisation, the ECSG has evaluated the need to add new requirements and has found that the adherence to existing global standards and frameworks such as EMVCo and PCI provides sufficient detail to guarantee interoperability and security, preventing fragmentation while at the same time allowing for different implementations to compete and offer innovative solutions in the marketplace.

The ECSG recommends the use of the EMV® Payment Tokenisation Specification - Technical Framework for Payment Tokens, as well as the business principles defined in chapter 3 and the options defined in chapter 5.

Regarding payment interoperability, the nature of the EMVCo Tokenisation is such that by definition it overlays the existing eco-system in a way that is transparent and de-facto guarantees the interoperability. The adherence to the EMVCo framework referenced by the ECSG guarantees the integrity and global interoperability, given how the relationship between the different elements has been defined (BIN's and BIN Controllers, PAN's and PAR's etc.).

In particular, PAR (Payment Account Reference) has been the subject of great interest for the industry in general and the retailer sector in particular. The ECSG has however agreed that the EMVCo framework provides the necessary flexibility in terms of generation and availability:

PAR Generation: Flexibility as to who can generate the PAR is included in the EMVCo framework, where the BIN controller may delegate this generation to a third party, such as e.g. an issuer.

PAR Availability: Regardless of who generates the PAR, the EMVCo framework also includes provisions stating that the PAR has to be made available to any party in the transaction value-chain that may need it.

Above and beyond the flexibility of PAR generation and its availability, one has to bear in mind that the EMV Tokenisation Framework defines PAR as an optional element.

Therefore, and in order to cater for the needs expressed by the retailer community, the ECSG has agreed the following requirement:

If EMV tokens are being generated for a PAN, then it is recommended to support EMV PAR.

If PAR is used, several systems and protocols will need to be adapted:

- Personalisation systems
- Terminal specifications
- Messaging protocols between merchants and acquirers as well as between acquirers and issuers, and this for e-commerce as well as for face-to-face transactions.

8. DEFINITIONS

This section contains definitions that are related to the scope of the ECSG work on Tokenisation.

At present, all the definitions are taken from the EMV® Payment Tokenisation Specification – Technical Framework. It shall be completed with definitions from other sources (e.g. from the PCI guidelines or from the Issuer, Acquirer and Merchant models).

Subsection 8.2 lists terms that are already present in Book 1 of the Volume, which are completed with the addition of a specific Tokenisation-related definition.

Subsection 8.3 lists terms that are not present in Book 1 for which a definition related to Tokenisation exists.

The origin of the definition is indicated under square brackets. For example, [EMVCo-FW v2] stands for a definition present in v2 of the EMVCo Framework.

8.1. Definitions not considered for this document

Some definitions present in the EMVCo Framework which are also present in Book 1 have not been considered for update because they refer to general concepts where tokenisation aspects would add very little value. These are namely:

- 3D-Secure
- BIN
- Card
- Cardholder
- Card Issuer
- Card Verification Number
- EMV Based Application / Non-EMV Based Application
- ISO IIN Blockholder
- ISO IIN Card Issuer
- Payment Account
- Payment Processor
- Primary Account Number (PAN)
- Third Party Service Provider

8.2. Book 1 definitions amended with Tokenisation definitions

Term	Amended definition
Consumer	(3) 'consumer' means a natural person who, in payment service contracts covered by this Regulation, is acting for purposes other

Term	Amended definition
	than the trade, business or profession of that person; [EMVCo-FW v2] In the EMVCo Tokenisation Framework, any individual that enters a relationship with an entity where validated account credentials are used to access services.
Payment System	A funds transfer system with formal and standardised arrangements and common rules for the processing, clearing and/or settlement of payment transactions. [EMVCo-FW v2] In the EMVCo Tokenisation Framework, a role within the Payment Tokenisation ecosystem that provides branding guidelines, assigns IINs/BINs, defines rules and guidelines for payment ecosystem participants, and develops products and respective product requirements that are derived from a variety of technologies.

8.3. New definitions in the Volume

Note: the definition of the terms 'Payment Token' and 'Payment Tokenisation' will presumably be extended to also cover non-EMV tokens.

Term	Proposed new or updated definition
BIN Controller	[EMVCo-FW v2.0] In the EMVCo Tokenisation Framework determines the rules for use of the IINs under their control.
BIN Controller Identifier	[EMVCo-FW v2.0] In the EMVCo Tokenisation Framework, identifier assigned by EMVCo to Registered BIN Controllers.
Cardholder-Initiated Transaction	[EMVCo-FW v2.0] Any transaction where the Cardholder is present and provides their payment credential. This can be through a Terminal in store or online through a checkout experience. A Cardholder-Initiated Transaction contains verification that a Cardholder was involved in the transaction.
De-Tokenisation	[EMVCo-FW v2.0] In the EMVCo Tokenisation Framework, 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 mapping to the underlying PAN / PAN Expiry Date stored in the Token Vault.
ID&V Actor	[EMVCo-FW v2.0] In the EMVCo Tokenisation Framework, the entity performing the ID&V Method(s) as part of ID&V.

Term	Proposed new or updated definition
ID&V Method	[EMVCo-FW v2.0] In the EMVCo Tokenisation Framework, an individual action through which an ID&V Actor may verify a previously established identity as part of ID&V.
Identification and Verification (ID&V)	[EMVCo-FW v2.0] In the EMVCo Tokenisation Framework, the process to ensure that the legitimate Cardholder that was issued the PAN by the Card Issuer is interacting with the Token Requestor during the request of a Payment Token. This involves the verification of the previously-established identity of the Cardholder.
Limited Use Payment Token	[EMVCo-FW v2.0] In the EMVCo Tokenisation Framework, a Payment Token that is issued for use in a single Cardholder-Initiated Transaction and subsequent Merchant-Initiated Transactions.
Merchant-Initiated Transaction	[EMVCo-FW v2.0] An authorisation request that relates to a previous Cardholder-Initiated Transaction but conducted without the Cardholder present, and without any Cardholder validation performed.
Non-EMV Based Application	[EMVCo-FW v2] An application that uses a different technology than EMV contact or contactless technology and techniques as a foundation of transaction processing.
PAN Authorisation	[EMVCo-FW v2] The process following De-Tokenisation whereby the underlying PAN is made available to the Card Issuer for authorisation. The authorisation request message may include the Payment Token and other related data.
PAR Data	[EMVCo-FW v2] In the EMVCo Tokenisation Framework, refers to a specific Payment Account Reference value generated in the format specified in Table 9.1 in the EMV® Payment Tokenisation Specification – Technical Framework document.
PAR Enquiry Function	[EMVCo-FW v2] In the EMVCo Tokenisation Framework, a function that supports the enquiry and distribution of PAR Data using a real-time or batch process.
PAR Field	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, a message field that contains PAR Data.
Payment Account Reference (PAR)	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, a non-financial reference assigned to each unique PAN and used to link a Payment Account represented by

Term	Proposed new or updated definition
	that PAN to affiliated Payment Tokens. The use of the term “PAR” in this technical framework refers to the overall concept, rather than any specific component (for example, PAR Data, PAR Field).
Payment Network	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, a role within the Payment Tokenisation ecosystem that operates an electronic system used to accept, transmit, or process transactions made by payment cards for money, goods, or services, and to transfer information and funds among Card Issuers, Acquirers, Payment Processors, Merchants, and Cardholders for one or more Payment Systems.
Payment Token	A Payment Token can be an EMV Payment Token as defined by EMV® Payment Tokenisation Specification – Technical Framework or a surrogate value for a PAN.
Payment Token - EMV® Payment Tokenisation	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework a EMV® Payment Token is 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.
Registered BIN Controller	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, a BIN Controller that has successfully registered with EMVCo and is in receipt of an assigned BIN Controller Identifier.
Registered Token Service Provider	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, a Token Service Provider that has successfully registered with EMVCo and is in receipt of an assigned Token Service Provider Code.
Shared Payment Token	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, a Payment Token is considered a Shared Payment Token when used by one or more Token Users in relevant application based commerce and e-commerce scenarios. There is a direct relationship between the Token Users and the Token Requestor. The use of a Shared Payment Token is limited by its Token Domain Restriction Controls.
Token Assurance	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, the performance of ID&V within Payment Tokenisation.

Term	Proposed new or updated definition
Token Assurance Data	In the EMV® Payment Tokenisation Specification – Technical Framework, supporting information for the Token Assurance Method.
Token Assurance Method	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, a value that allows the Token Service Provider to indicate the ID&V performed representing the binding of the Payment Token to underlying PAN and Cardholder. It is determined as a result of the ID&V Method(s) performed and the ID&V Actor involved performing them. The Token Assurance Method is assigned as part of the Token Issuance process and may be updated if additional ID&V is performed.
Token Assurance Method Category	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, a group of ID&V Method(s) with similar characteristics enabling a consistent categorisation by Token Service Providers as part of setting the Token Assurance Method.
Token Authorisation	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, the process within Token Processing whereby a Payment Token and related data are used to facilitate a subsequent PAN Authorisation.
Token BIN	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, 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	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, a specific BIN Range that has been designated only for the purpose of issuing Payment Tokens and is flagged accordingly in BIN tables.
Token Control Fields	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, fields containing data that may be used to restrict Payment Token use to the appropriate Token Domains using Token Domain Restriction Controls.
Token Cryptogram	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, 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.

Term	Proposed new or updated definition
Token Domain	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, the types of transactions for which a Payment Token may be used. Token Domains may be channel-specific, Merchant-specific, digital wallet-specific, transaction-specific, or a combination of any of the above.
Token Domain Restriction Controls	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, a set of parameters established as part of Token Issuance that will allow for enforcing appropriate usage of the Payment Token during Token Processing.
Token Expiry Date	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, 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 Generation	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, the process whereby a Payment Token is generated and is assigned a value associated with a Token BIN or Token BIN Range
Token Issuance	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, the process whereby a Payment Token and related data is issued in preparation for Token Provisioning.
Token Location	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, the mode of storage for a Payment Token and related data.
Token Payment Request / Response	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, the process within Token Processing whereby a Payment Token and related data is used to facilitate a subsequent Token Authorisation. The Token Payment Response will include results of the Token Authorisation.
Token Presentment	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, the interaction of the Cardholder and Merchant where the Card / Form Factor is presented for payment.

Term	Proposed new or updated definition
Token Presentment Mode	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, the mode through which a Payment Token is presented to the Merchant during Token Presentment. This information resolves to an existing field called Point of Sale (POS) Entry Mode as defined in ISO 8583 messages. Each Payment Network will define and publish any new POS Entry Mode values as part of its existing message specifications and customer notification procedures.
Token Processing	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, 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: <ul style="list-style-type: none"> • Token Payment Request/Response • Token Authorisation • Application of Token Domain Restriction Controls • De-Tokenise/Tokenise • PAN Authorisation
Token Programme	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, 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	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, the process whereby a Payment Token and related data is delivered to the Token Location.
Token Reference ID	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, a substitute for the Payment Token that does not expose information about the Payment Token or the underlying PAN.
Token Request	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, the process whereby a Token Requestor requests a Payment Token from the Token Service Provider.
Token Request Indicator	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, a value used to indicate that an authentication / verification message is related to a Token Request. It is optionally passed to the Card Issuer as part of the Identification and Verification (ID&V) process to inform the Card

Term	Proposed new or updated definition
	Issuer of the reason that the account status check is being performed.
Token Requestor	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, 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 Requestor ID	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, an 11-digit numeric value that identifies each unique combination of Token Requestor and Token Domain(s) for a given Token Service Provider.
Token Requestor Type	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, identifies the type of entity that is serving as the Token Requestor.
Token Service Provider	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, a role within the Payment Tokenisation ecosystem that is authorised by a Token Programme to provide Payment Tokens to registered Token Requestors.
Token Service Provider Code	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, a unique three-digit value, assigned by EMVCo, to a Registered Token Service Provider.
Token User	<p>[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, a role within the Payment Tokenisation ecosystem performed by a Merchant or an entity acting on the Merchant's behalf that initiates a Token Payment Request using a Shared Payment Token.</p> <p>[ECSG Note: in the Volume, Merchant is also referred as Acceptor as per definition in Book 1.]</p>
Token Vault	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, a repository that maintains the established Payment Token / Token Expiry Date mapping to 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.

Term	Proposed new or updated definition
Tokenisation	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework, 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.

9. FIGURES AND TABLES

Table 1: Summary of how Tokenisation models and standards/guidelines relate to each other	9
Figure 2: Card Tokenisation: Analysis of environment	10
Figure 3: Card Tokenisation Ecosystem Protecting the PAN	11
Figure 4: EMV Payment Tokens – Token Request example	14
Figure 5: EMV Payment Tokens – Basic Authorisation Flow	15
Figure 6: Alternate PAN diagram (also valid for other forms of TOKENS such as ‘Virtual’ or ‘Dynamic’ PANs)	22
Figure 7: Option 1: TSP in the issuing domain behind the CMS	27
Figure 8: Option 2: TSP in the issuing domain in front of the CMS	28
Figure 9: Diagram for any token payment models	29
Figure 10: Co-Badge Approach 1	33
Figure 11: Co-badge approach 1: PAR in a co-badge environment with separate PANs	33
Figure 12: PAR Governance: Illustration of example model - Co-badge approach 1	34
Figure 13: Co-badge approach 2: PAR in a co-badge environment with the same PAN	34
Figure 14: Co-badge approach 2: PAR in a co-badge environment with only one PAR linked to the only one underlying PAN	35
Figure 15: PAR Governance: Illustration of example model - Co-badge approach 2	35