EMV®
Payment Tokenisation Specification

Technical Framework

Version 2.3
October 2021

Legal Notice

The EMV® Specifications are provided “AS IS” without warranties of any kind, and EMVCo neither assumes nor accepts any liability for any errors or omissions contained in these Specifications. 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 THESE SPECIFICATIONS.

EMVCo makes no representations or warranties with respect to intellectual property rights of any third parties in or in relation to the Specifications. EMVCo undertakes no responsibility to determine whether any implementation of the EMV® Specifications 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 the EMV® Specifications should consult an intellectual property attorney before any such implementation.

Without limiting the foregoing, the Specifications 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 these Specifications 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 the EMV® Specifications.

Revision Log – Version 2.3

The following changes have been made to the document since the publication of version 2.2:

- Replacement of the term “channel” with “POS Entry Mode” and / or “Usage Scenario” to more accurately reflect the situation
- Replacement of the term “mapping to” with “affiliation with” to describe the relationship between a Payment Token / Token Expiry Date and the underlying PAN / PAN Expiry Date
- Removal of Token Requestor Type. Different types of Token Requestors are addressed by variations in the application of Token Domain Restriction Controls
- Removal of the defined terms Limited Use Payment Token and Shared Payment Token to reflect the emphasis on the use of all Payment Tokens being constrained by their Token Domain Restriction Controls
- Editorial changes regarding Payment Tokenisation lifecycle management to provide consistency with A Guide to Use Cases
- Addition of the ISO 20022 ATICA Messages to Section 9 Payment Token Fields Used in ISO 8583 and 20022 ATICA Messages
- Clarification on the use of Token Cryptograms in Merchant-Initiated Transactions (See Section 10 Token Processing)

Some of the numbering and cross references in this version have been updated to reflect changes due to the introduction of new concepts.

Contents

Figures

Tables

1 Introduction

The purpose of this technical framework is to define a basis for Payment Tokenisation by providing a level of commonality across the payment ecosystem to support adoption, while enabling levels of differentiation that promotes innovation. This technical framework 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.

This technical framework:

- Describes the Payment Tokenisation ecosystem
- Describes existing payment ecosystem entities that maintain their roles in support of Payment Tokenisation and identifies potential impacts
- Describes specific functions that can be used to enable Payment Tokenisation
- Describes a level of common definition, concepts, controls and flexibility, supporting Payment Tokenisation in differing ecosystem models
- Specifies the required, conditional and optional fields associated with Token Requests, Token Generation, Token Issuance, Token Provisioning and Token Processing
- Identifies the necessary and common interfaces that support the Payment Tokenisation ecosystem

Note that the terminology and definitions used in this technical framework are intended to support a global understanding of the payment ecosystem or Payment Tokenisation ecosystem functions within it. Local market differences in terminology and definitions may exist and are not reflected in this technical framework.

1.1 Scope

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

The technical framework is not designed to mandate, incentivise, or define commercial rules, requirements or policies for the implementation of Payment Tokenisation solutions by international, regional, national or local Payment Systems.

Payment Tokenisation works alongside, or falls within, standards and specifications applicable to the payment ecosystem. Entities that choose to implement this technical framework should ensure that they adhere to applicable international, regional, national or local laws and regulations.

EMVCo operates registration processes for Token Service Providers and BIN Controllers, and maintains a list of assigned Token Service Provider Codes and BIN Controller Identifiers to aid global interoperability of Payment Tokenisation. EMVCo does not develop, operate, maintain, service, test, evaluate, approve or otherwise endorse Token Programmes, Token Service Providers or BIN Controllers.

1.2 Overview

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. Payment Tokenisation systems hold substantial promise to address these needs.

This technical framework describes the baseline requirements for the use of Payment Tokens within the existing payment ecosystem through the establishment of a Token Programme. Payment Tokens are surrogate values that replace the PAN in the payment ecosystem. Payment Tokens are designed to provide transparency to payment ecosystem stakeholders when accepting and processing Payment Tokens.

Other forms of tokenisation exist in the ecosystem which are not addressed in this technical framework. They are commonly referred to as acquirer / merchant / issuer tokens and are used by a variety of entities and serve a number of different purposes, including data protection. They focus on enhanced data protection for PAN-based transactions and can reduce the size and scope of the Payment Card Industry (PCI) Cardholder Data Environment. This technical framework does not preclude or seek to restrict their use.

Payment Tokens may be used with Cardholder Verification Methods (CVMs) for EMV Based Applications and remain implementation specific. Approaches to CVMs may include signature, PIN, Consumer Device CVM (CD-CVM) or no CVM. This technical framework does not define the usage of, or additional requirements relating to, CVM implementation for Payment Token usage scenarios. CVMs requirements are defined by existing entities in the payment ecosystem and should be observed accordingly.

A Payment Token provides improved protection when its use is limited to a specific domain(s), such as a Merchant, Consumer Device or Token Presentment Mode (represented by the POS Entry Mode). These underlying usage controls, known as the Token Domain Restriction Controls, are a fundamental benefit of Payment Tokens and an important security differentiator in contrast to PANs. Token Domain Restriction Controls allow for the creation of specific constraints for the use of a Payment Token and are applied during Token Processing. An example is the prevention of the successful use of a Payment Token outside of a specific

usage scenario or Token Presentment Mode (for example, whether the Cardholder is physically present at a Merchant location to perform Token Presentment).

The document EMV® Payment Tokenisation – A Guide to Use Cases ("A Guide to Use Cases") describes common use cases for Payment Tokens that are in part defined by the specific Token Domain Restriction Controls applied to each Payment Token. Each use case example illustrates how various Token Domain Restriction Controls can be used to constrain the usage of a Payment Token.

Steps may be taken to ensure that the Payment Token, as a surrogate value, is replacing a PAN that was issued by the Card Issuer to the legitimate Cardholder, interacting with the Token Requestor. This process is known as Identification and Verification (ID&V) and results in the setting of the Token Assurance Method.

Payment Tokens provide benefits for all stakeholders in the payment ecosystem. Examples include:

- Card Issuers and Cardholders may benefit from new and more secure ways to pay, improved transaction approval levels, and reduced risk of subsequent fraud in the event of a data breach in which Payment Tokens are exposed instead of PANs
- Acquirers and Merchants may experience a reduced threat of online attacks and data breaches, as Payment Token data stores will be less appealing targets given the limitation of Payment Tokens to a specific domain(s). Acquirers and Merchants may also benefit from the Token Domain Restriction Controls that Payment Tokens offer

This technical framework introduced the Payment Account Reference (PAR) as a means to minimise the need to receive or store Full PAN. More specifically, in order to achieve the benefits of Payment Tokenisation and minimise the fraud impact of account data compromise, it is critical that Merchants and the broader acceptance community not receive the Full PAN in the authorisation response messages. Dependency on ubiquitous availability of Full PAN extends into many other solutions that facilitate fraud and risk analysis solutions for Merchants, and broader requirements of local law. Payment Tokenisation can create new challenges for entities within the acceptance community that rely on Full PAN to drive payment processing and value added services.

Cardholders may have many Payment Tokens affiliated with the same underlying PAN since each Payment Token may have its own Token Domain Restriction Controls that are unique to its environment, Consumer Device or Token Requestor. This means that entities within the acceptance community can perform or process transactions with multiple Payment Tokens for the same underlying PAN without an easy way to determine a linkage between these transactions or to those performed on the underlying PAN.

The transition from a dependency on ubiquitous availability of Full PAN can be accomplished by providing PAR as an alternative mechanism that meets the needs of Merchants and the broader acceptance community. It enables the ability to link tokenised transactions with transactions associated with the underlying PAN.

EMV® Payment Tokenisation – A Guide to Use Cases is an informational supplement that is intended to be read in conjunction with this technical framework. It describes relationship models and use case examples common to Payment Tokenisation.

Payment Tokenisation is interoperable generically across EMV technologies. The use of Payment Tokenisation does not preclude the use of other EMV technologies.

1.3 Audience

This technical framework is intended for use by all participants in the payment ecosystem, such as Card Issuers, Merchants, Acquirers, Payment Systems, Payment Networks, Payment Processors, BIN Controllers and Third Party Service Providers.

1.4 References

The latest version of any reference, including all published amendments, applies unless a publication date is explicitly stated.

1.4.1 Normative References

The standards in Table 1.1 contain provisions that are referenced in this technical framework.

Table 1.1: Normative References

Reference	Publication Name
ISO/IEC 7812-1:2017, ISO/IEC 7812-2:2017	Identification cards — Identification of issuers: Part 1: Numbering system Part 2: Application and registration procedures
ISO 8583	Financial transaction card originated messages — Interchange message specifications (1987, 1993, 2003 and other variants where appropriate)
ISO 9564-1	Financial services -- Personal Identification Number (PIN) management and security -- Part 1: Basic principles and requirements for PINs in card-based systems
ISO 13491	Banking — Secure cryptographic devices, all parts

Reference	Publication Name
ISO 20022 ATICA	Acquirer to Issuer Card Messages - Version 2 Message Definition Report - Part 2
PCI DSS	Payment Card Industry Data Security Standard

1.4.2 Published EMVCo Documents

The documents in Table 1.2 are related to or are associated with Payment Tokenisation.

Table 1.2: EMVCo References

Reference	Publication Name
Transaction Types	EMV® Best Practices Document – Recommendations for EMV Processing for Industry-Specific Transaction Types
EMV® 3-D Secure	EMV® 3-D Secure – Protocol and Core Functions Specification
SB-197	SB-197: Tokenisation Data Objects – Token Requestor ID and Last 4 Digits of PAN
A Guide to Use Cases	EMV® Payment Tokenisation – A Guide to Use Cases
FAQ	EMV® Payment Tokenisation FAQ
SRC	EMV® Secure Remote Commerce Specification
Use Case Submission Template	EMV® Payment Tokenisation – Use Case Submission Template (requires an EMVCo Associate membership)
SB-178	SB-178: Tokenisation Data Objects – Payment Account Reference (PAR)
PAR White Paper	EMV® White Paper on Payment Account Reference

For further information, including registration procedures, please refer to www.emvco.com.

1.5 Definitions

The following terms are used in this technical framework. They apply only to the context of this technical framework and are not representative of other uses outside of the scope of this technical framework.

Table 1.3: 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 Section 3.11 BIN Controller for further details.
BIN Controller Identifier	A unique identifier consisting of four uppercase Alphanumeric Roman characters assigned by EMVCo to Registered BIN Controllers.
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.
Cardholder-Initiated Transaction	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.
Card Issuer	A financial institution or its Third Party Service Provider that provides Cardholders with a Payment Account represented by one or more PANs.
Card Issuer Aggregator	A specific Payment Tokenisation Aggregator role that facilitates some or all Payment Token related activities by acting as a service provider on behalf of one or more Card Issuers.
Card Verification Number	A security number used to authenticate the presence of the card. Examples include CAV2 / CVC2 / CVV2 / CID / CVN2.
Consumer	Any individual that enters a relationship with an entity where validated account credentials are used to access services.

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.
ID&V	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.
ID&V Actor	The entity performing the ID&V Method(s) as part of ID&V.
ID&V Method	An individual action through which an ID&V Actor may verify a previously established identity as part of ID&V.
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).
Merchant-Initiated Transaction	An authorisation request that relates to a previous Cardholder-Initiated Transaction but conducted without the Cardholder present, and without any Cardholder validation performed.

Term	Definition
PAN Authorisation	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.
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.
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 technical framework refers to the overall concept, rather than any specific component, e.g. PAR Data, PAR Field.
PAR Data	Refers to a specific Payment Account Reference value generated in the format specified in Table 9.1.
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 system 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 this technical framework.
Payment Tokenisation Aggregator	A role within the Payment Tokenisation ecosystem that facilitates some or all Payment Token related activities by acting as a service provider on behalf of one or more Payment Tokenisation roles.
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.
Registered Token Service Provider	A Token Service Provider that has successfully registered with EMVCo and is in receipt of an assigned Token Service Provider Code.
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 Authorisation	The process within Token Processing whereby a Payment Token and related data are used to facilitate a subsequent PAN Authorisation.
Token Assurance	The performance of ID&V within Payment Tokenisation.
Token Assurance Data	Supporting information for the Token Assurance Method.
Token Assurance Method	An updatable value that allows the Token Service Provider to communicate the ID&V performed. It is determined or updated as a result of the ID&V Method(s) and ID&V Actor.

Term	Definition
Token Assurance Method Category	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 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 Control Fields	Fields containing data that may be used to restrict Payment Token use to the appropriate Token Domains using Token Domain Restriction Controls.
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.
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 Generation	The process whereby a Payment Token is generated and is assigned a value associated with a Token BIN or Token BIN Range.
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 Payment Request / Response	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.

Term	Definition
Token Presentment	The interaction of the Cardholder and Merchant which leads to the Payment Token being presented for payment through Token Processing.
Token Presentment Mode	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	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 are delivered to the Token Location.
Token Reference ID	A substitute for the Payment Token that does not expose information about the Payment Token or the underlying PAN.
Token Request	The process whereby a Token Requestor requests a Payment Token from the Token Service Provider.
Token Request Indicator	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 Issuer of the reason that the account status check is being performed.

Term	Definition
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 Requestor Aggregator	A specific Payment Tokenisation Aggregator role that facilitates some or all Payment Token related activities by acting as a service provider on behalf of one or more Token Requestors.
Token Requestor ID	An 11-digit numeric value that identifies each unique combination of Token Requestor and Token Domain(s) for a given Token Service Provider.
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 Service Provider Code	A unique three-digit value, assigned by EMVCo, to a Registered Token Service Provider.
Token User	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 Payment Token provided by a Token Requestor.
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.

1.6 Notational Conventions

1.6.1 Abbreviations

The abbreviations listed in Table 1.4 are used in this technical framework.

Table 1.4: Abbreviations

Abbreviation	Description
AML	Anti-Money Laundering
BIN	Bank Identification Number (term for IIN as defined in ISO/IEC 7812)
CD-CVM	Consumer Device CVM
CDE	Cardholder Data Environment
CVM	Cardholder Verification Method
EMV 3DS	EMV® 3-D Secure
HCE	Host Card Emulation
ICC	Integrated Circuit Card
ID&V	Identification and Verification
IEC	International Electrotechnical Commission
IIN	Issuer Identification Number
ISO	International Organization for Standardization
NFC	Near Field Communication
OTP	One-Time Password
PAN	Primary Account Number
PAR	Payment Account Reference
PCI	Payment Card Industry
PCI SSC	Payment Card Industry Security Standards Council

Abbreviation	Description
POS	Point Of Sale
TEE	Trusted Execution Environment

1.6.2 Terminology and Conventions

The following words are used often in this technical framework and have a specific meaning:

SHALL / SHALL NOT

Indicates mandatory requirements of this technical framework.

SHOULD / SHOULD NOT

Indicates guidelines recommended by this technical framework.

1.7 Further Information

Additional Payment Token information can be found at www.emvco.com.

2 Constraints of the Ecosystem

This technical framework is designed to work within a number of constraints of the payment ecosystem, including roles of various entities, transaction flows and data definitions. The constraints include the following:

- This technical framework is not intended to supersede or interfere with any international, regional, national, or local laws and regulations
- Payment Tokens must preserve all product attributes of the PAN including product type, e.g. debit or credit
- Token BIN or Token BIN Ranges will be made available to the parties participating in Token Processing to support routing decisions
- Token BINs or Token BIN Ranges are managed distinctly from traditional BINs or BIN ranges to provide ecosystem transparency and to avoid collision or conflict between PANs and Payment Tokens
- Ongoing changes to Payment Token / Token Expiry Date affiliation with the underlying PAN / PAN Expiry Date due to lifecycle management events, such as underlying PAN updates, lost or stolen devices, and deactivation of the Payment Token, are accommodated
- The policies and processes of a Token Programme should minimise the impact on the existing payment processing environment in which Payment Tokenisation will be provided, e.g. Card Issuer portfolio conversions, Merchant conversions, and local network / on-us transaction routing
- Merchant-Initiated Transactions only occur after an original Cardholder-Initiated Transaction
- PAR Data is generated using a method that cannot be reverse engineered to reveal PAN or Payment Token
- PAR Data is unique in its assignment to PAN
- PAR Data is not intended to be a PAN replacement or a consumer identifier
- PAR Data must be unique across all PAR Data governed by any Registered BIN Controller to ensure no collision or conflict
- PAR has been created and evaluated to address a defined set of specific conditions. Use of PAR Data is limited to:
    - Supporting, as a linkage mechanism, the reversal of transactions, e.g. returns and chargebacks
    - Complying with regulatory requirements, e.g. Anti-Money Laundering (AML)
    - Performing risk analysis, e.g. fraud detection and control services

- Performing other non-payment operational needs as defined by the Registered BIN Controller, e.g. supporting a loyalty programme for consumers that have opted in to the service

3 Payment Tokenisation Ecosystem

The implementation of Payment Tokenisation as outlined by this technical framework, and in a manner consistent with this 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 this technical framework. Payment Tokenisation specific roles may be performed by existing entities within the payment ecosystem or by newly-emerging entities. Entities may perform one or more Payment Tokenisation roles.

Each of the Payment Tokenisation roles are described in more detail in the subsequent sub-sections.

3.1 Cardholder

Cardholders will continue in their current role. Payment Tokenisation does not impact the existing Cardholder and Card Issuer relationship. Cardholders will continue to be issued PANs representing the Payment Account. In most cases, a Cardholder is not expected to know that a Payment Token has been issued to represent an underlying PAN of the Payment Account. Optionally, the Token Requestor or Card Issuer may choose to make a Cardholder aware of the Payment Token.

As part of establishing Token Assurance, Cardholders may be required to participate in ID&V.

Cardholders will generally be unaware of PAR Data. This will not adversely impact the ability of Cardholders to transact.

3.2 Card Issuer

Card Issuers will continue in their current role in terms of owning the Payment Account relationship with the Cardholder(s), authorisation and ongoing risk management in the Payment Tokenisation ecosystem.

Card Issuers need to coordinate with their Registered BIN Controllers to understand the applicability and the governance of the PAR Field and PAR Data as implemented by the Payment Networks.

3.3 Merchant

Merchants will continue in their current role processing transactions, including Payment Token based transactions. This includes authorisation, capture and exception processing.

Merchants will need to implement any Merchant requirements defined by the Merchant's Acquirer or Payment Processor, including the support of Payment Tokenisation specific fields and interfaces.

Merchants may receive a Payment Token and related data, including the Token Expiry Date, during Token Presentment in any of the following scenarios:

- From the Cardholder using the Cardholder's Consumer Device
- As a Token Requestor either directly or via an intermediary
- As a Token User via the Token Requestor's interfaces

A Payment Token is constrained by its Token Domain Restriction Controls. Examples include constraining the use of a Payment Token:

- To a single Merchant
- To a specific Token Presentment Mode
- For a single Cardholder-Initiated Transaction and subsequent Merchant-Initiated Transactions

Merchants may implement the PAR Field and PAR Data in their payment processing environment based on requirements established by the Merchant's Acquirer or Payment Processor.

3.4 Acquirer

Acquirers will continue in their current role, processing all transactions, including Payment Token based transactions. This includes authorisation, capture, clearing, and exception processing. Additional Payment Tokenisation specific fields may be used to support Token Processing as defined in the interfaces governed by the Payment Networks or Acquirer.

Acquirers may implement the PAR Field and PAR Data in their payment processing environment as defined by the Payment Networks the Acquirer supports.

3.5 Payment System

Payment Systems will continue in their current role and may elect to support Payment Tokenisation in accordance with this technical framework. Payment Systems that support Payment Tokenisation are responsible for defining the policies, processes and registration programmes that comprise their Token Programme.

Payment Systems need to consider the business, technical and processing implications and communicate their requirements to all appropriate stakeholders.

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.

3.6 Payment Network

Payment Networks will continue in their current role and may elect to support the implementation of Token Processing functions within a Token Programme.

Payment Networks are responsible for defining and publishing the authorisation, clearing, and exception processing message interfaces and Payment Tokenisation specific fields that impact Token Processing in various Payment Tokenisation scenarios.

Payment Networks are responsible for supporting the implementation of the PAR Field in their message specification in accordance with Registered BIN Controllers.

3.7 Token Service Provider

The Token Service Provider is a Payment Tokenisation specific role. Token Service Providers are 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 Field and PAR Data in provisioning requests
- Token Requestor registry functions
- De-Tokenisation and Tokenisation
- Application of Token Domain Restriction Controls during Token Processing

Token Service Providers may engage with a variety of types of Token Requestor as part of their ongoing participation in a Token Programme.

3.8 Token Requestor

The Token Requestor is a Payment Tokenisation specific role. Token Requestors register with one or more Token Service Providers in order to request Payment Tokens. Token Requestor registration is managed in accordance with the policies and processes of each Token Programme.

Token Requestors vary in nature and may support a variety of usage scenarios. Upon registering with a Token Service Provider, Token Requestors will be assigned one or more unique Token Requestor IDs. Multiple Token Requestor IDs can be assigned to a Token Requestor to support different usage scenarios. Token Requestors are responsible for using the appropriate Token Requestor ID when requesting Payment Tokens.

Token Requestors can request Payment Tokens for their own use or for use by one or more Token Users. Usage of Payment Tokens is constrained by their Token Domain Restriction Controls. Token Requestors are responsible for managing both Payment Tokens and any Token Users they support.

3.9 Token User

The Token User is a Payment Tokenisation specific role. Token Users initiate Token Payment Requests with Payment Tokens which have been received from Token Requestors. The Token User will have a relationship with one or more Token Requestors. Token Requestors may define requirements for the use of Payment Tokens which they provide to Token Users. The use of each Payment Token is constrained by its Token Domain Restriction Controls.

3.10 Payment Tokenisation Aggregator

The Payment Tokenisation Aggregator is a Payment Tokenisation specific role. Payment Tokenisation Aggregators integrate with one or more Token Service Providers in order to facilitate some or all Payment Token related activities by acting as a service provider on behalf of one or more Payment Tokenisation roles or existing ecosystem entities. Payment Tokenisation Aggregator registration is managed in accordance with the policies and processes of each Token Programme.

This technical framework identifies the following specific types of Payment Tokenisation Aggregator:

- Token Requestor Aggregator
- Card Issuer Aggregator

3.11 BIN Controller

BIN Controllers will continue in their current role, determining the rules for use of the IINs (commonly referred to as BINs) under their control from which PANs are generated. A BIN Controller is either an:

- ISO IIN Blockholder

- ISO IIN Card Issuer

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

If the BIN Controller supports PAR as a linkage mechanism, it will register with EMVCo to receive a BIN Controller Identifier. Registered BIN Controllers will then determine the governance of the PAR Field and PAR Data for the BINs under their jurisdiction. Registered BIN Controllers will define how the unique characters of PAR Data will be generated and will communicate to their constituents the generation method for PAR Data along with the specific usage for PAR Data for Payment Tokens and underlying PANs.

Registered BIN Controllers may also determine the requirements for PAR Data as it relates to PAN and the presence on PAN-related messages.

Card Issuers who have been assigned BIN(s) by an ISO IIN Blockholder must follow the PAR Field and PAR Data governance and requirements of the ISO IIN Blockholder that is also the Registered BIN Controller for those BINs assigned by the ISO IIN Blockholder.

There is no expectation that PAR Data generation methods will be consistent across Registered BIN Controllers.

3.12 Illustrative Payment Token Process Overviews

The following diagrams (Figure 3.1 and Figure 3.2) provide high-level overviews of two of the processes involved in the Payment Tokenisation ecosystem. There are many different implementations for the various processes. Each diagram only shows one potential implementation, which is not intended to be definitive.

Figure 3.1 gives an example flow for Token Request where the Merchant is performing the role of the Token Requestor, with optional ID&V carried out by the Card Issuer in conjunction with the Token Service Provider.

Figure 3.1: Token Request Overview

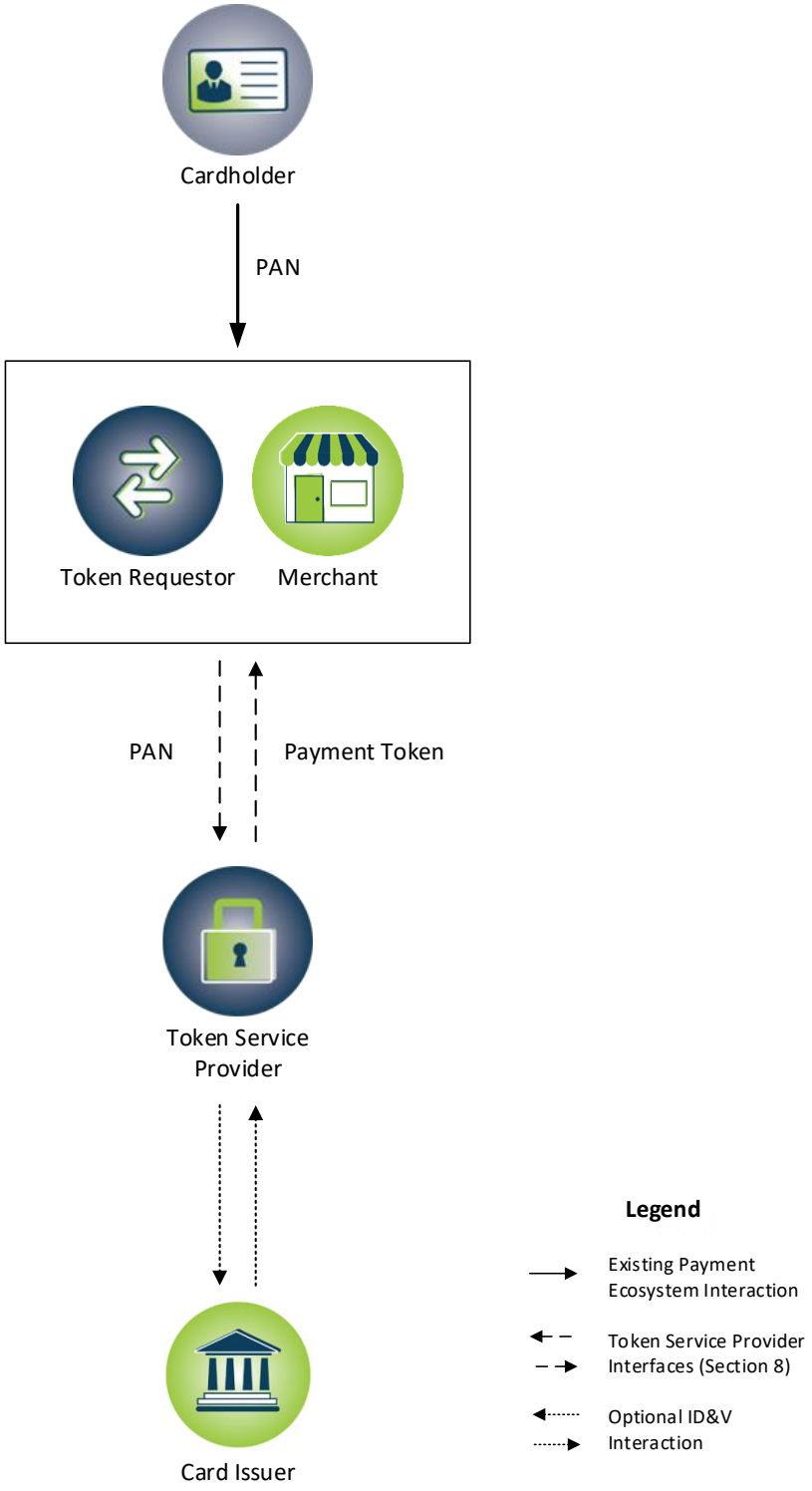
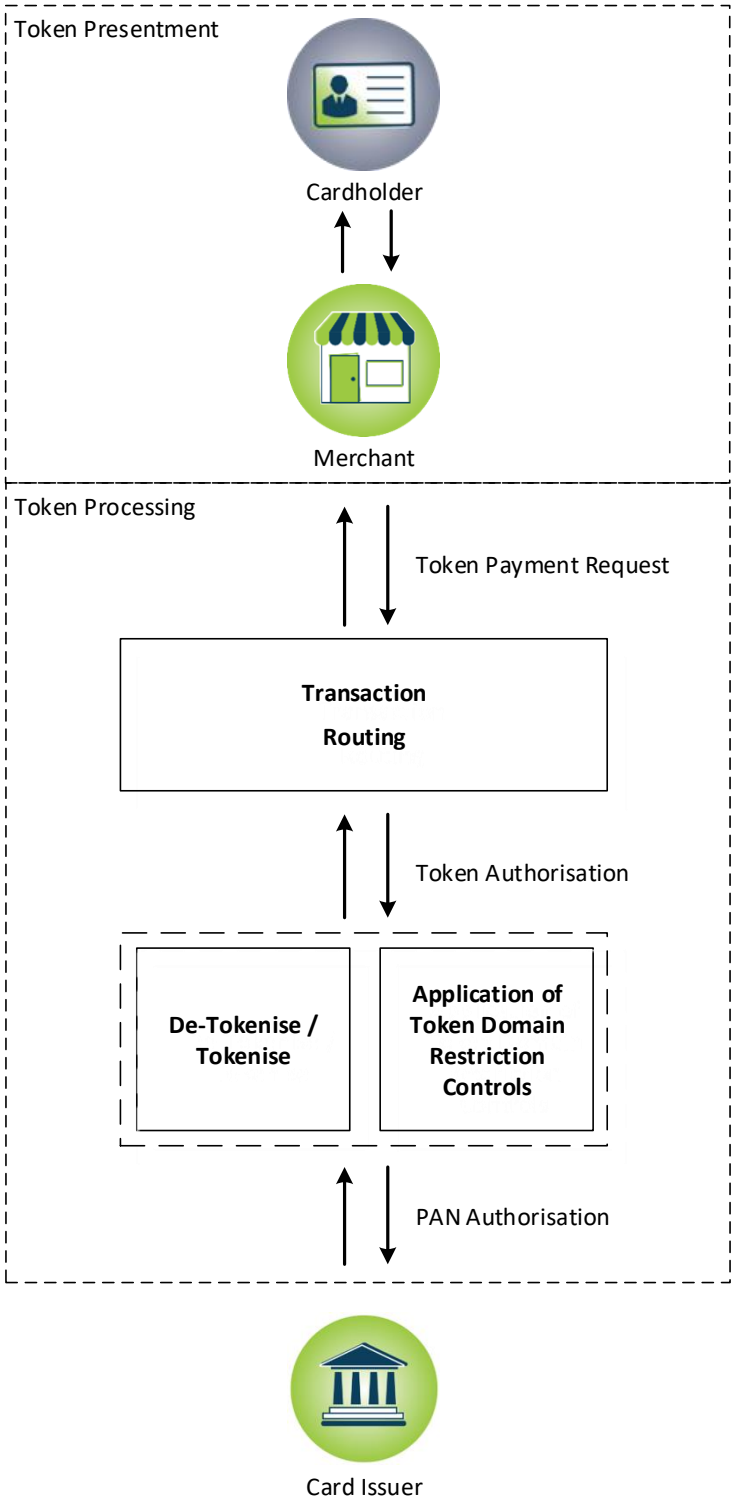


Figure 3.2 gives an example of how a Payment Token transaction might occur. The figure only includes those roles that are specific to Payment Tokenisation. All existing transaction processing roles continue as normal.

Figure 3.2: Payment Token Transaction Overview



4 Token Programme

A Token Programme is comprised of the:

- Policies, processes and registration programmes that facilitate generation and issuance of Payment Tokens by Token Service Providers to registered Token Requestors using designated Token BIN or Token BIN Ranges
- Policies and processes for De-Tokenisation, and the application of Token Domain Restriction Controls during Token Processing

An entity introducing Payment Tokenisation to an existing payment ecosystem is responsible for defining the policies, processes and registration programmes that comprises its Token Programme.

Authorised entities, including Token Service Providers and Token Requestors, will need to adhere to the relevant policies, processes, and registration programmes when operating within a Token Programme.

The following minimum policies should be considered in order to establish and maintain a Token Programme:

- Affiliation of Payment Tokens / Token Expiry Dates with underlying PANs / PAN Expiry Dates for use in Token Processing
- Registration and approval of Token Requestors, Token Service Providers and other authorised entities
- Determination of Token Assurance Methods to indicate the ID&V performed
- Security requirements and controls related to the Token Vault, Token Provisioning and Token Processing
- Permissible Token Domain Restriction Controls
- Requirements for Payment Tokenisation and PAN lifecycle management

The following minimum processes should be considered in order to support Payment Tokenisation within a Token Programme:

- Numeric management of PANs and Payment Tokens
- Issuance of Payment Tokens, including Token Assurance, Token Generation, Token Issuance, Token Location and Token Provisioning
- Ongoing operation and maintenance of a Token Vault
- Application of security and related controls
- Token Requestor registry functions, including Token Requestor IDs
- Application of Token Domain Restriction Controls
- Token Processing, including the application of Token Domain Restriction Controls

- Payment Tokenisation and PAN related lifecycle management requirements
- Support of Token Programme interfaces
- Token Programme reporting requirements
- Requirements for authorised entities

Specific requirements can extend to entities that perform Payment Tokenisation roles, which may be outside the EMVCo considerations for a Token Programme. In establishing a Token Programme, consideration should be given to understanding any potential impacts on these entities.

EMVCo does not evaluate, approve or otherwise endorse specific Token Programmes.

4.1 Numeric Management

BINs cannot be used solely for the purpose of differentiating between products, services or technologies. Payment Tokens must be created from existing licensed or otherwise assigned Token BINs by utilising designated ranges within a BIN or defined and distributed by existing ISO IIN Blockholders or ISO IIN Card Issuer in a similar manner.

Token Programme considerations for numeric management include policies and processes to:

- Assign numeric values that can be identified as Token BINs or Token BIN Ranges by managing the allocation of Payment Tokens to BINs including the Payment Token assignment methodology
- Establish requirements for affiliating Payment Tokens / Token Expiry Dates with underlying PANs / PAN Expiry Dates
- Ensure that Payment Tokens are managed distinctly from PANs
- Assign Token BINs and or Token BIN Ranges from which Payment Tokens are generated using a methodology that will preserve any product-related attributes of the BIN or BIN Range from which the underlying PAN has been issued
- Ensure the preservation of product-related attributes associated with a PAN are consistent with product-related attributes assigned to the PAN's affiliated Payment Tokens

4.2 Issuance of Payment Tokens

Token Programme considerations for the issuance of Payment Tokens include policies and processes for:

- Token Assurance

- Token Generation
- Token Issuance
- Token Provisioning

This includes any implications of specific technologies and processes.

4.2.1 Token Assurance

Token Assurance involves performing ID&V prior to Token Issuance to verify that the Cardholder is the rightful user of the PAN. The initial Token Assurance Method value is determined at the time of the Token Request and is based on the ID&V performed. The Token Assurance Method may be updated subsequent to Token Issuance.

Token Programme considerations for Token Assurance include:

- Establishing the Token Assurance policies and processes
- Establishing policies for the Token Service Provider to set a Token Assurance Method from the Token Assurance Method Categories that are to be supported within the Token Programme
- Determining the mapping of the ID&V Method(s) to the Token Assurance Method Categories and included them within the established policies

4.2.2 Token Generation

Token Generation occurs before Token Issuance. It is the process whereby a Payment Token and its associated Token Expiry Date are created for a specific underlying PAN, for use by a specific Token Requestor in specific Token Domain(s), as identified the Token Requestor ID.

Token Programme considerations for Token Generation include the minimum Token Generation:

- Policy requirements, including when Payment Tokens and related data can be generated
- Process requirements, based on the Token Request from the Token Requestor

4.2.3 Token Issuance

Token Issuance occurs after the Payment Token has been generated. It is the process whereby a Payment Token and related data are issued in preparation for Token Provisioning.

Token Programme considerations for Token Issuance include any minimum or recommended:

- Token Issuance policy and process requirements
- Token Locations eligible for Token Provisioning for a given Token Requestor

4.2.4 Token Provisioning

Token Provisioning occurs after Token Issuance. It is the process whereby a Payment Token and related data are delivered to the Token Location.

Token Programme considerations for Token Provisioning include:

- Defining the minimum Token Provisioning policy requirements, including the Payment Token and related data sent to the Token Requestor and physical and logical security
- Defining the minimum Token Provisioning process requirements, including the confirmation actions by the Token Requestor
- Defining any user interface requirements, including the acceptable interfaces for transmission of the Payment Token and related data
- Determining if PAR is available for provisioning and identifying the means to source the data according to the governance of the relevant Registered BIN Controller(s)
- Facilitating Token Provisioning using technology created or licensed that interfaces with terminals, wallet environments or other payment technologies

4.3 Token Vault

The Token Vault provides the mechanism for Payment Token / Token Expiry Date affiliation with the underlying PAN / PAN Expiry Date. Token Vaults need to maintain all Payment Token(s) / Token Expiry Date(s) that are affiliated with a given PAN / PAN Expiry Date throughout the lifecycle of both the underlying PAN and the Payment Token(s).

Token Programme considerations for the Token Vault include defining the:

- Minimum Token Vault policy requirements providing the affiliation of the Payment Token / Token Expiry Date with the underlying PAN / PAN Expiry Date, including any related data
- Minimum Token Vault process requirements, including the ongoing operation and maintenance of data managed in the Token Vault
- Minimum non-functional requirements, including, but not limited to, the availability of systems and performance expectations of the Token Vault
- Security and control requirements used to ensure strong physical and logical security of the Token Vault

4.4 Payment Tokenisation Aggregators

Payment Tokenisation Aggregators provide aggregation services for Payment Token related activities.

Token Programme considerations for Payment Tokenisation Aggregators include defining:

- Policies and processes for the registration of Payment Tokenisation Aggregators
- Information requirements so that a Payment Tokenisation Aggregator can uniquely identify the authorised entity it is acting on behalf of

4.5 Security and Related Controls

Due to the sensitive nature of the data maintained and managed within the Token Programme appropriate physical and logical security requirements are necessary.

Token Programme considerations for security and related controls include defining:

- Security and control requirements for entities that are:
  - Participating in the Token Programme
  - Interacting with other entities participating in the Token Programme
- Allowable communication channels for secure transmission of:
  - Payment Token and related data
  - Cardholder data

4.6 Token Requestor Registry Functions

The Token Requestor registry functions as a repository of information about the supported Token Locations, Token Domains and corresponding Token Domain Restriction Controls that are associated with each Token Requestor.

Token Programme considerations for Token Requestor registry functions include defining policies and processes for:

- Enrolment, approval, initial registration and ongoing maintenance of entities as Token Requestors
- Collection, review, risk assessment and approval of Token Requestor registrations
- Conducting due diligence on a potential Token Requestor. This may include established Know Your Customer (KYC) information as well as other policy-related requirements as defined by the international, regional, national or local laws and regulations
- Evaluating and approving specific usage scenario(s) supported by the Token Requestor
- Assigning Token Requestor IDs to registered Token Requestors.

- The publication of a registry reflecting all registered Token Requestors
- The communication of the Token Domain Restriction Controls associated with each Token Requestor

Considerations also include defining:

- Relevant Token Domain Restriction Controls that will be associated with each Token Domain and usage scenario for a Token Requestor
- Applicable Token Location and usage scenario that are permitted and supported for each Token Requestor

4.6.1 Token Requestor ID

The Token Requestor ID uniquely identifies each unique combination of Token Requestor and Token Domain(s) for each Registered Token Service Provider.

Token Programme considerations for Token Requestor IDs includes policies and processes for the assignment of unique Token Requestor IDs.

4.7 Token Domain Restriction Controls

Token Domain Restriction Controls are intended to ensure that any exposure of Payment Tokens does not result in significant levels of subsequent fraud. Token Domain Restriction Controls are established at the time of Token Issuance and may be modified post Token Issuance. Payment Tokens are constrained to specific usage scenarios based on the Token Domain Restriction Controls in place at the time of the transaction. The application of Token Domain Restriction Controls during Token Processing ensures that Payment Tokens are constrained to the permitted usage scenarios.

Token Domain Restriction Controls may vary based on usage scenarios and Token Domains, using data such as Merchant Identifiers and POS Entry Modes. This is to ensure that Token Domain Restriction Controls are consistently applied across the Token Programme.

Example Token Domain Restriction Controls include:

- Use of the Payment Token with particular Token Presentment Modes and usage scenarios, such as contactless or e-commerce
- Use of the Payment Token at a uniquely identified Merchant
- The presence and verification of a Token Cryptogram that is unique to each transaction
- Allowing the Payment Token to be used by multiple Token Users with which the Token Requestor has a direct relationship
- Constraining the use of the Payment Token to a single Cardholder-Initiated Transaction and any subsequent Merchant-Initiated Transactions

A Payment Token may be issued for use across multiple usage scenarios, according to its Token Domain Restriction Controls. For example, the same Payment Token may be used for a Point of Sale transaction (e.g. Proximity at Point of Sale use case) and also used for an in-application transaction (e.g. In-Application using a Consumer Device use case).

Token Programme considerations for Token Domain Restriction Controls include defining which Token Domain Restriction Controls are to be established and subsequently applied during Token Processing.

4.8 Token Processing

The policies and processes of the Token Programme need to ensure that it operates in a manner which preserves interoperability and the ongoing integrity of traditional processing of payment transactions including authorisation, clearing, and exception processing. Therefore, the Token Programme and related Token Vault solutions need to be integrated with these payment transaction processes in the applicable Payment Network(s).

The Token Domain Restriction Controls are applied during Token Processing in accordance with the policies and processes of the Token Programme.

Token Programme considerations for Token Processing include defining:

- Requirements for the application of Token Domain Restriction Controls during Token Processing
- Policies and processes that create transparency to facilitate transaction routing of Payment Tokens by clearly distinguishing Payment Token from PANs
- Policies and processes that ensure routing and account range tables can clearly distinguish Token BINs and Token BIN Ranges from traditional BINs and BIN ranges in order to ensure the underlying integrity of transaction processing
- Transaction processing requirements for Payment Tokens and related data to be available within the transaction message that traverses a Payment Network or transaction interface
- Requirements for De-Tokenisation during Token Processing to the retrieve the underlying PAN. This includes defining and communicating interfaces that enable De-Tokenisation

Token Programme considerations for Token Processing include establishing:

- Fields necessary to enable the application of Token Domain Restriction Controls in Token Processing
- Policies and processes for the presence of Payment Token related fields and data in transaction messages

4.9 Payment Tokenisation Lifecycle Management

Once a Payment Token is created and affiliated with an underlying PAN, various events can affect the function of a Payment Token. These events, commonly referred to as lifecycle management events, need to be managed as part of the Token Programme.

Token Programme considerations for Payment Tokenisation lifecycle management include:

- PAN lifecycle management events and requirements to ensure accurate content in the Token Vault
- Payment Token lifecycle management events and requirements to ensure accurate content in the Token Vault to facilitate Token Processing
- Token Provisioning lifecycle management events
- Payment Token lifecycle management policies for Token Provisioning related data

4.10 Interfaces

Within a Token Programme, consideration of appropriate interface requirements is necessary. This includes:

- Determining the minimum interface requirements and the minimum data requirements necessary to support consistency and integrity in these interfaces
- Defining the specific characteristics and requirements unique to the Token Programme to support Token Requests, Token Generation, Token Issuance and Token Provisioning, and Payment Tokenisation lifecycle management

Token Service Providers will support both the minimum interface requirements and the minimum data requirements to support Token Requestors and Card Issuer programmes.

4.11 Reporting

Within a Token Programme, consideration of appropriate reporting requirements is necessary. This includes:

- Requirements that indicate the integrity and performance of the Token Programme
- Policies and processes to support auditing and reconciliation of the various functions, within the Token Programme

4.12 Authorised Entities

The integrity of the Token Programme relies on only authorised entities participating in the Token Programme. Participation can include, but is not limited to:

- Token Service Providers and associated third parties
- Token Requestors and associated Token Requestor Aggregators
- Card Issuers and associated Card Issuer Aggregators

Token Programme considerations for authorised entities include:

- Defining registration polices and processes
- Defining initial and ongoing participation criteria
- Evaluating authorised entities against these initial and on-going criteria
- Ensuring compliance of authorised entities to security and related controls

5 Payment Tokenisation Requirements

This section describes the baseline requirements for Payment Tokenisation.

5.1 Token Service Provider

The Token Service Provider is a role within the Payment Tokenisation ecosystem that is carried out by entities authorised to provide Payment Tokens to registered Token Requestors within a Token Programme. Token Service Providers are responsible for a number of discrete functions which can include, are not limited to:

- Registering with EMVCo
- Registration and management of Token Requestors
- Issuance of Payment Tokens, including Token Assurance, Token Generation, Token Issuance and Token Provisioning
- Maintenance of security and related controls
- Establishing Token Domain Restriction Controls
- Support and management of Token Processing, including De-Tokenisation and the application of Token Domain Restriction Controls

Token Service Providers are responsible for integrating into relevant Token Programmes. This includes building and managing interfaces that integrate with Token Requestors and Card Issuers.

A Token Service Provider SHALL operate a Token Vault in accordance with the policies and processes of the relevant Token Programme and the requirements specified in Section 5.6 Token Vault.

In addition to the requirements in this section (Section 5.1 Token Service Provider), Token Service Providers SHALL comply with the relevant requirements in:

- Section 6 Token Assurance Method
- Section 7.3 Token Service Provider
- Section 8 Token Service Provider Interfaces
- Section 10 Token Processing

5.1.1 Token Service Provider Registration

To aid Payment Tokenisation ecosystem transparency, traceability and global interoperability, EMVCo manages a Token Service Provider Code registration process. This provides unique

identification of each Registered Token Service Provider and avoids collisions of Token Requestors IDs between Token Service Providers.

In compliance with Token Programme policies, Token Service Providers SHOULD register with EMVCo when providing services for one or more separate and legally distinct entities. Upon successful registration EMVCo will assign a unique Token Service Provider Code and publish the assigned code within the list of currently registered Token Service Provider Codes on the EMVCo website.

Assignment of a Token Service Provider Code alone is not sufficient to perform Token Service Provider functions in a Token Programme. The Token Service Provider may have additional programme and participation requirements defined in the Token Programme beyond those defined in this technical framework.

Note that EMVCo does not evaluate, approve or otherwise endorse Token Service Providers.

Please visit www.emvco.com for details of the:

- EMVCo registration process to obtain a Token Service Provider Code
- Currently registered Token Service Provider Codes.

5.1.2 Registration and Management of Token Requestors

Token Service Providers are responsible for registration and management of participating Token Requestors according to each Token Programme's policies and processes.

The Token Requestor registration process SHALL include the usage scenarios that the Token Requestor intends to support, including any appropriate Token Domain information.

The Token Service Provider SHALL establish the applicable Token Domain Restriction Controls according to Token Programme policies.

The relevant information relating to the Token Domain Restriction Controls SHALL be stored in the Token Vault and communicated according to the Token Programme policies.

The Token Service Provider, in accordance with the Token Programme policies SHALL manage the assignment of the Token Requestor ID(s) based on the usage scenario and Token Domains that the Token Requestor supports.

The Token Service Provider SHOULD provide the relevant Token Requestor registration information according to Token Programme policies, including, but not limited to, the requested Token Assurance Method.

The Token Service Provider SHALL be responsible for the ongoing management of a registered Token Requestor and its associated Token Requestor ID(s).

Token Requestor registration with the applicable Token Service Provider is optionally facilitated through a Token Requestor Aggregator acting on behalf of the Token Requestor.

5.1.3 Issuance of Payment Tokens

The issuance of Payment Tokens and the sequence of events are defined by the policies and processes of the Token Programme. A number of steps are discussed in the following sub-sections. The order of these steps does not dictate any particular sequence of events.

5.1.3.1 Token Assurance

Token Assurance involves performing ID&V prior to Token Issuance to verify that the Cardholder is the rightful user of the PAN.

The Token Service Provider SHALL:

- Manage the Token Assurance Method associated with each registered Token Requestor, based on usage scenarios
- Manage the Types of ID&V Method(s) applied during Token Assurance
- Enable the Token Assurance Method to be updated subsequent to Token Issuance

The ID&V associated with a Token Request SHALL be based on the established Token Assurance Method agreed to by the Token Requestor and the Token Service Provider.

5.1.3.2 Token Generation

Token Generation is the process of creating a Payment Token and its associated Token Expiry Date and affiliating it with a specific underlying PAN and PAN Expiry Date, for use by a specific Token Requestor and Token Domain(s), as identified by the Token Requestor ID.

The Token Service Provider SHALL facilitate the generation of a Payment Token and related data. A Payment Token may be generated:

- In response to a Token Request from a registered Token Requestor with a valid Token Requestor ID
- In advance of a Token Request from a registered Token Requestor with a valid Token Requestor ID

The Payment Token is then affiliated with the underlying PAN contained in the Token Request.

Token Generation SHALL be performed using only assigned Token BINs or Token BIN Ranges to ensure that there is no possibility of generating Payment Tokens that collide or conflict with a PAN.

The Token Service Provider SHALL provide the Token Vault with the Payment Token / Token Expiry Date affiliated with the underlying PAN / PAN Expiry Date.

5.1.3.3 Token Issuance

Token Issuance is the process of issuing a Payment Token and related data in preparation for Token Provisioning.

The Token Service Provider SHALL manage Token Requests based on the Token Requestor ID. Token Service Providers SHALL manage the issuance of Payment Tokens. Payment Tokens SHALL only be issued through the response to a Token Request from a registered Token Requestor with a valid Token Requestor ID.

Token Issuance SHALL include the generation of all necessary data.

Additional Token Issuance and Token Provisioning must occur when additional Token Locations are requested. Token Service Providers must not fulfil requests for additional Token Locations for a given Token Requestor unless allowed by the policies and processes of the Token Programme.

5.1.3.4 Token Provisioning

Token Provisioning is the process of delivering a Payment Token and related data to the Token Location.

Token Provisioning SHOULD be carried out by the Token Service Provider or by other authorised entities on its behalf. The methodologies associated with Token Provisioning may be proprietary to each Token Programme and are outside the scope of this technical framework.

The Token Service Provider SHOULD enable provisioning of PAR Data with a Payment Token as defined by the Registered BIN Controller (see Section 7.3 Token Service Provider).

5.1.4 Security and Related Controls

Due to the sensitive nature of the data maintained and managed by the Token Service Provider, appropriate physical and logical security requirements are necessary.

As defined in the Token Programme, the Token Service Provider SHALL maintain:

- Appropriate security controls
- Physical and logical security of the information within its system(s)

5.1.5 Token Domain Restriction Controls

Token Domain Restriction Controls are used to constrain a Payment Token to its intended use.

As defined in the Token Programme, the Token Service Provider SHALL:

- Enable Token Domain Restriction Controls
- Use the Token Requestor ID as part of the identification and configuration of the Token Doman Restrictions Controls for the issued Payment Token

5.1.6 Token Processing

Token Processing utilises existing Payment Network transactions, authorisation message types and structures.

As defined in the Token Programme, the Token Service Provider SHALL:

- Support and manage Token Processing requirements
- Support De-Tokenisation

5.2 Token Requestor

The Token Requestor is a role within the Payment Tokenisation ecosystem that is carried out by registered entities who request Payment Tokens from Token Service Providers. Token Requestors may be assigned multiple Token Requestor IDs to support Token Domain Restriction Controls and Token Locations. The assignment of Token Requestor IDs can be influenced by associated usage scenarios.

Token Requestors SHALL:

- Register and integrate with Token Service Providers in accordance with each Token Programme's requirements
- Use the appropriate Token Requestor ID in applicable Payment Token related activities that include but are not limited to Token Requests, Token Cryptogram Request and Payment Token lifecycle management events

Token Requestors SHOULD be aware of PAR Data in order to make it available to Merchants.

Token Requestors can request Payment Tokens for their own use or for use by one or more Token Users. Usage of Payment Tokens is constrained by their Token Domain Restriction Controls. Token Requestors are responsible for managing both Payment Tokens and any Token Users they support.

When requesting Payment Tokens for use by one or more Token Users, the Token Requestor SHALL:

- Manage the Payment Tokens and Token Users, including associated Payment Token related activities
- Support the necessary Token User and Token Payment Request processing requirements

Token Requestors may use Token Requestor Aggregators to facilitate some or all Payment Token related activities.

5.2.1 Token Requestor ID

A Token Requestor ID is an 11-digit numeric value set by the Token Service Provider in accordance with the Token Programme's requirements.

The Token Requestor ID SHALL comply with the following convention:

- Positions 1-3: Token Service Provider Code, unique to each Registered Token Service Provider
- Positions 4-11: Assigned to the Token Requestor

5.3 Token User

The Token User is a role within the Payment Tokenisation ecosystem using Payment Tokens received from Token Requestors.

A Token User SHALL:

- Have a relationship with one or more Token Requestor(s)
- Adhere to Token Requestor requirements when using a Payment Token received from the Token Requestor
- Include the Payment Token and Payment Token related data in Token Payment Request messages

5.4 Payment Tokenisation Aggregator

The Payment Tokenisation Aggregator is a category of roles within the Payment Tokenisation ecosystem. The following specific Payment Tokenisation Aggregator roles are carried out by registered entities who provide aggregation services in accordance with the Token Programme policies and processes:

- Token Requestor Aggregator
- Card Issuer Aggregator

This technical framework does not preclude other types of Payment Tokenisation Aggregator.

5.4.1 Token Requestor Aggregator

The Token Requestor Aggregator is authorised to integrate with a Token Service Provider to perform Payment Token related activities on behalf of one or more Token Requestors. Token Requestor Aggregators perform Payment Token related activities that include performing Token Requests. Additional activities may include, but are not limited to, Token Cryptogram Request and Payment Token lifecycle management events.

Token Requestor Aggregators SHALL:

- Register in accordance with each Token Programme's requirements
- Indicate which Token Requestor they are servicing by providing the corresponding Token Requestor ID in each Token Request or other Payment Token related activities

If a Token Requestor does not register directly with a Token Service Provider then the Token Requestor Aggregator SHOULD facilitate the registration of the Token Requestor in order to receive a Token Requestor ID

When an entity is performing the role of Token Requestor Aggregator it SHALL NOT:

- Be assigned a Token Requestor ID in its role as a Token Requestor Aggregator
- Be considered a Token Requestor in its own right

5.4.2 Card Issuer Aggregator

The Card Issuer Aggregator is authorised to integrate with a Token Service Provider to perform Payment Token related activities on behalf of one or more Card Issuers. Card Issuer Aggregators perform Payment Token related activities that may include, but are not limited to, supporting Token Requests, facilitation of ID&V processes and Payment Token lifecycle management events.

Card Issuer Aggregators SHALL:

- Register in accordance with each Token Programme's requirements
- Provide sufficient information to allow the Token Service Provider to identify which PAN or Card Issuer they are servicing in support of Payment Token related activity

When an entity is performing the role of Card Issuer Aggregator it SHALL NOT be considered a Card Issuer in its own right.

5.5 Additional Stakeholders

The following stakeholders have specific requirements placed on them by Payment Tokenisation.

5.5.1 Payment Networks

Payment Networks may elect to support Token Processing functions within a Token Programme.

Payment Networks that support a given Payment Tokenisation usage scenario for a specific Token Programme SHALL implement all of the fields defined in this technical framework. This includes all of the required, conditional and optional fields, and those that are further defined

in the Token Programme within the context of its proprietary message specifications enabling support of Token Processing steps incorporating Token Payment Request, Token Authorisation and PAN Authorisation. Proprietary message specification changes are notified through existing communication channels.

5.5.2 Acquirers

Acquirers need to be aware that additional Payment Tokenisation specific fields may be used to support Token Processing.

Acquirers SHOULD implement any required, conditional or optional fields as referenced in this technical framework, and further defined by the supporting Payment Network's message specification.

5.5.3 Card Issuers

Card Issuers need to be aware that additional Payment Tokenisation specific fields may be used to support Token Processing.

Card Issuers SHOULD:

- Implement any required, conditional or optional fields as referenced in this technical framework, and further defined by the supporting Payment Network's message specification
- Provide PAN lifecycle management events through established interfaces

Card Issuers may use Card Issuer Aggregators to facilitate some or all Payment Token related activities.

5.6 Token Vault

Token Vaults include a variety of sensitive storage and processing functions associated between the Payment Token / Token Expiry Date affiliated with the underlying PAN / PAN Expiry Date and storage of the association between a Payment Token and its assigned Token Domain Restriction Controls. These operations require appropriate levels of security to protect the integrity of processing and ensure data assets are secured.

A Token Vault SHALL:

- Provide the capability for generation and issuance of Payment Tokens
- Establish and maintain the Payment Token / Token Expiry Date affiliated with the underlying PAN / PAN Expiry Date
- Provide underlying security and related processing controls as defined in the Token Programme

- Be protected by strong physical and logical security measures per industry standards and compliance validation processes
- Store the association between the Payment Token and its assigned Token Domain Restriction Controls

5.7 Token Location

The Token Location provides the data storage approach and any accompanying security architecture for the Payment Token and related data.

Token Locations are defined in Table 5.1.

Table 5.1: Token Locations

Token Location	Description
00	Not specified
01	Remote storage: e.g. a single Merchant's card-on-file data store
02	EMVCo and Payment System type approved secure element / ICC
03	Local device storage: e.g. Payment Token and related data stored using the data storage mechanisms of a Consumer Device, such as when utilising HCE
04	Local hardware secured storage: e.g. using a TEE to ensure appropriately restricted access to data
05	Remote hardware secured storage: e.g. ISO 13491 compliant storage
06	Shared storage: e.g. e-commerce multi-merchant wallet accessing a card-on-file data store
07	Temporary storage: e.g. guest checkout
08 – 99	Reserved for future use

The Token Location SHALL NOT change during the life of the Payment Token when it is used as a Token Domain Restriction Control.

6 Token Assurance Method

Token Assurance Methods are defined by the policies and processes of the Token Programme. These enable the communication of the ID&V Actor and ID&V Method associated with the Payment Token and its underlying PAN for secure Token Processing.

In the context of this technical framework, ID&V is the verification of a previously-established identity. The establishment of identity is outside of the scope of this technical framework.

This technical framework addresses the following components of the Token Assurance Method:

- Token Assurance Method Categories
- ID&V Methods
- ID&V Actors
- Token Assurance Data

These are used by the Token Service Provider to determine and verify the Token Assurance Method for a given Payment Token.

Token Service Providers maintain two fields that are used to communicate Token Assurance and the ID&V Methods performed:

- Token Assurance Method
- Token Assurance Data

6.1 Token Assurance Concepts

Token Assurance is performed prior to Token Issuance and results in the setting of the Token Assurance Method. It can be updated once the Payment Token has been issued.

6.1.1 Setting the Token Assurance Method

The Token Assurance Method is set when issuing a Payment Token.

The Token Service Provider SHALL set a Token Assurance Method value for the Payment Token, based on the ID&V Method(s) and ID&V Actor utilised.

Individual ID&V Methods may be used singularly or in combination and are mapped, by the Token Service Provider, into a specific Token Assurance Method Category. The Token Assurance Method Category is then used in conjunction with the ID&V Actor(s) that performed the ID&V Method(s) to determine the Token Assurance Method.

The Token Service Provider SHALL ensure that the Token Assurance Method accurately represents:

- Whether ID&V was performed
- The ID&V Actor(s) involved
- The ID&V Method(s) performed, according to verification of the evidence provided in the Token Assurance Data
- The association of the ID&V Method(s) to the Token Assurance Method Category

Where ID&V is performed, it SHALL be performed on the Cardholder associated with the PAN, regardless of whether the Token Request was initiated with a PAN, a Payment Token, or a Token Reference ID (see Section 8.1.1.2 Token Request with Payment Token). When a Token Request is initiated with a Payment Token or Token Reference ID, the underlying PAN SHALL be made available to the ID&V Actor(s) so that the relevant ID&V Method(s) can be performed on it.

6.1.2 Token Assurance Data

Token Assurance Data consists of supporting information for the Token Assurance Method. Its contents depend on the context in which it is provided.

ID&V Methods are performed by ID&V Actors. Token Requestors and Token Service Providers coordinate the ID&V. The Token Service Provider will verify both the ID&V performed and the outcomes resulting from the ID&V.

The details of what constitutes Token Assurance Data are outside the scope of this technical framework, but examples include:

- Cryptogram
- Authorisation code
- Billing address
- Shipping address
- Postal code
- Card Verification Number
- Fraud risk score that is provided by the Token Requestor
- Account verification results

When requesting a Payment Token from the Token Service Provider, the Token Requestor SHALL provide Token Assurance Data representing either:

- Verifiable evidence of the ID&V Method(s) performed and their outcomes *or*
- Any data required to allow the Token Service Provider to coordinate Token Assurance

6.1.3 Communicating the Token Assurance Method

The Token Service Provider SHALL ensure that the Token Assurance Method and Token Assurance Data are passed, where necessary, to the Card Issuer and Token Requestor.

6.1.4 Updating the Token Assurance Method

The Token Assurance Method value is always set during Token Issuance. It may be updated during the Payment Token's lifecycle.

When updating the Token Assurance Method, the Token Service Provider SHALL use the methodology defined within the Token Programme.

6.2 Default Token Assurance Method Categories

There are two default Token Assurance Method Categories. A Payment Token with one of the default Token Assurance Methods can still be used to initiate Token Payment Requests.

The Token Service Provider SHALL set the Token Assurance Method values in the following scenarios as defined in Table 6.1.

Table 6.1: Default Token Assurance Method Categories

Token Assurance Method Category	Description
Spaces	No Value Set
00	ID&V Not Performed

6.3 Token Assurance Method Structure

The Token Assurance Method is divided into three independent ranges as defined in Table 6.2.

Table 6.2: Token Assurance Method Structure

Token Assurance Method Category Range	Description
01 – 19	Common
20 – 89	Token Programme Specific

Token Assurance Method Category Range	Description
90 – 99	Reserved for future EMVCo use

The first range, 01 – 19, is a common EMVCo-defined Token Assurance Method Category range that represents two commonly recognised categories of ID&V Actors and a set of common Token Assurance Method Categories. Certain values within this range are reserved for future use by EMVCo and SHALL NOT be defined by any other entity. The Token Service Provider SHALL recognise the following common categories of ID&V Actors for the common Token Assurance Method Category range:

- Non-Card Issuer ID&V Actors
- Card Issuer ID&V Actors

The second range, 20 – 89, is Token Programme specific and SHOULD have a structure defined within the Token Programme. This SHOULD be used to accommodate Token Assurance Method needs that extend beyond the EMVCo-defined common Token Assurance Method Category range.

The third range, 90 – 99, is reserved for future use by EMVCo.

6.4 Common Token Assurance Method Category Range

The Token Assurance Method Categories in the common range are defined in the following tables.

For Non-Card Issuer ID&V Actors, the Token Service Provider SHALL recognise the Token Assurance Method Categories defined in Table 6.3.

Table 6.3: Non-Card Issuer Token Assurance Method Categories

Token Assurance Method Category	Description
01	Non-Card Issuer Interactive Cardholder Authentication - 1 Factor
02	Non-Card Issuer Interactive Cardholder Authentication - 2 Factor
03	Non-Card Issuer Risk Oriented Non-Interactive Cardholder Authentication
04 – 09	Reserved for future EMVCo use for non-Card Issuer Token Assurance Method Categories

For Card Issuer ID&V Actors, the Token Service Provider SHALL recognise the Token Assurance Method Categories defined in Table 6.4.

Table 6.4: Card Issuer Token Assurance Method Categories

Token Assurance Method Category	Description
10	Card Issuer Account Verification
11	Card Issuer Interactive Cardholder Authentication - 1 Factor
12	Card Issuer Interactive Cardholder Authentication - 2 Factor
13	Card Issuer Risk Oriented Non-Interactive Cardholder Authentication
14	Card Issuer Asserted Authentication
15 – 19	Reserved for future EMVCo use for Card Issuer Token Assurance Method Categories

6.5 ID&V Method Assignment to Recognised Token Assurance Method Categories

It is the responsibility of the Token Service Provider, in accordance with the policies of the Token Programme, to map ID&V Methods into the common Token Assurance Method Categories.

Where the ID&V Actor is not the Token Service Provider, the results SHALL be reported by the Token Requestor to the Token Service Provider using the Token Assurance Data.

Recognised authentication-related solutions such as EMV® 3-D Secure may be used in Token Assurance and therefore apply to different Token Assurance Method Categories.

When Cardholder authentication is performed using ID&V Methods that could be determined to meet the criteria of more than one Token Assurance Method Category, the Token Assurance Method Category SHALL be determined in accordance with the policies of the Token Programme.

6.5.1 Card Issuer Account Verification

ID&V Methods mapped to this Token Assurance Method Category can only be performed by an ID&V Actor which is a Card Issuer. These ID&V Methods provide basic account verification checks to validate if the PAN is active and valid at the Card Issuer. Example Account Verification ID&V Methods and their equivalents include:

- Zero or single unit of currency authorisation
- Card Verification Number validation
- Postal code and address verification

These Account Verification ID&V Methods can be initiated by any entity, but can only be performed by the Card Issuer.

6.5.2 Interactive Cardholder Authentication – 1 Factor

ID&V Methods mapped to this Token Assurance Method Category may be performed by any ID&V Actor. The verification performed is equivalent to a 1 Factor Interactive Cardholder Authentication, meaning that the Cardholder is directly involved in the verification process. Examples include, but are not limited to:

- Verification of a user name and password.
  - The user name and password are both classed as something the Cardholder “knows” and is a 1 Factor verification
- Verification of an online biometric
  - The biometric is something the Cardholder “is” and is a 1 Factor verification

Note that a 1 Factor authentication of a Consumer Device is not Interactive Authentication and therefore does not fall into this category.

6.5.3 Interactive Cardholder Authentication – 2 Factor

ID&V Methods mapped to this Token Assurance Method Category may be performed by any ID&V Actor. The verification performed is equivalent to a 2 Factor Interactive Cardholder

Authentication, meaning that the Cardholder is directly involved in the verification process and verification is performed in two out of the following three Factors A, B or C:

- Factor A – verification of what the Cardholder “has” in their possession
- Factor B – verification of what the Cardholder “knows”
- Factor C – verification of what the Cardholder “is”

An example of an existing payment ecosystem method capable of supporting 2 Factor authentication is EMV® 3-D Secure.

6.5.4 Risk Oriented Non-Interactive Cardholder Authentication

ID&V Methods mapped to this Token Assurance Method Category may be performed by any ID&V Actor. These methods involve the use of risk and authentication data maintained by the ID&V Actor and provided to the ID&V Actor by the Token Requestor to perform a risk-oriented assessment.

Examples include, but are not limited to:

- Account age and history
- Bill to / ship to addresses and contact information
- IP address
- Consumer Device Information
- Geo location
- Transaction velocity

An example of an existing payment ecosystem method supporting a risk oriented authentication is the use of EMV® 3-D Secure in a risk-based mode, that is, without an interactive Cardholder authentication challenge.

Risk Oriented Non-Interactive Cardholder Authentication needs to be performed by an established entity with sufficient historic risk data to enable an effective risk decision.

6.5.5 Card Issuer Asserted Authentication

ID&V Methods mapped to this Token Assurance Method Category can only be performed by an ID&V Actor which is a Card Issuer. These ID&V Methods involve the Card Issuer asserting that the underlying authentication is sufficient and trusted due to the existence of a previously established Card Issuer approved authentication method.

The Card Issuer verification of the Cardholder may be performed using methods that include, but are not limited to:

- Established mobile banking verification of the Cardholder
- In-person authentication, e.g. using government approved identification

7 Payment Account Reference

This section describes a common set of requirements for the implementation of PAR as a linkage mechanism between Token Processing transactions where the full underlying PAN is not available and transactions associated with the Payment Token's underlying PAN. See Section 2 Constraints of the Ecosystem for further details of the intended use of PAR. Any use of PAR Data outside of the EMVCo defined use will require additional evaluation by the relevant BIN Controller.

Entities having responsibilities associated with the introduction of PAR include Registered BIN Controllers, Token Service Providers, Token Requestors, Payment Processors, Payment Networks, Card Issuers, Acquirers and Merchants. For any given implementation of PAR, under the governance of the Registered BIN Controller, the PAR Field and PAR Data may affect all Payment Token services, including Token Provisioning and Token Processing.

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 Table 9.1.

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 this 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. The PAR Field and PAR Data may also be included in current PAN-based transactions in which Payments Token(s) have been previously generated for the PAN.

Payment Tokens affiliated with the same underlying PAN will consistently have the same PAR Data assigned.

PAR Data is unique in its assignment to a given PAN and is not intended to be a PAN replacement or a consumer identifier.

All PAR implementations SHALL NOT replace or interfere with any international, regional, national or local laws and regulations; those governing requirements supersede any industry specification or standard.

7.1 Creation and Assignment

The following requirements for the creation and assignment of PAR Data ensure its use as a linkage mechanism between the PAN and its affiliated Payment Tokens.

PAR Data SHALL:

- Be generated using a method that cannot be reverse engineered to determine underlying PAN or Payment Token information
- Comply with the data format defined in Table 9.1
- Be directly associated with the Payment Account as represented by the PAN
- Be the same for a PAN regardless of the number of instances where the PAN is embossed, encoded or personalised
- 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
- Have the same value when assigned to a single PAN used by multiple Cardholders on the same Payment Account
- Only be used for the specific limitations identified in Section 2 Constraints of the Ecosystem
- Be an unintelligible value with the exception of the BIN Controller Identifier

PAR Data SHALL NOT be:

- Used as a consumer identifier
- Capable of being used to derive underlying PAN attributes that identify product type
- Used to route transactions

7.2 BIN Controller

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 that support Payment Tokenisation and PAR as a linkage mechanism SHALL:

- Register with EMVCo to receive BIN Controller Identifier
- Be responsible for PAR Field and PAR Data governance

- Define rules governing the use of PAR Data for its implementations within the payment ecosystem
- Ensure that PAR Data is generated using their EMVCo-assigned BIN Controller Identifier
- Define the generation method of the last 25 characters of the PAR Data
- Ensure the global uniqueness of PAR Data assignment to PANs generated from BINs under its control to ensure no collision or conflict
- Identify the entities that are permitted to participate in PAR Data generation and assignment for BINs under their control
- Require PAR Data in all relevant Token Processing response messages
- Require PAR Data in all relevant PAN-based payment processing response messages when Payments Token(s) have been previously generated for the PAN
- Provide a PAR Enquiry Function to facilitate retrieval of PAR Data for the Merchants, Acquirers, Payment Processors and others in the acceptance community before, during, and after a transaction

7.3 Token Service Provider

Specific usage scenario differences will determine where PAR Data is provisioned by Token Service Providers.

Token Service Providers SHOULD provision PAR Data with a Payment Token as defined by the Registered BIN Controller under the following conditions:

- PAR Data provisioned to an EMV Based Application (e.g. for use at Point of Sale) SHALL utilise EMV Tag ‘9F24’ to identify PAR Data
- PAR Data provisioned to a non-EMV Based Application where the application does not support EMV based transactions with EMV tagged fields (e.g. for use in e-commerce) SHALL NOT utilise EMV Tag ‘9F24’ but SHOULD be included in an accessible field

Token Service Providers SHOULD pass PAR Data in response to a successful Token Request.

Token Service Providers SHALL provide PAR Data in De-Tokenisation enquiries, if PAR Field and PAR Data are supported by the Token Service Provider.

7.4 Token Requestors

When a Payment Token is used to initiate a Token Payment Request as an EMV based transaction, the PAR Data will be available for transmission and identified as PAR Data by

EMV Tag ‘9F24’ so that it may be passed during Token Processing. The Token Requestor may not be aware that PAR Data is passed in a Token Payment Request when PAR Data is stored in an EMV Based Application.

When a Payment Token is used to initiate a Token Payment Request as a non-EMV based transaction, the Token Requestor SHALL pass PAR Data to the Merchant when PAR Data is included with the Payment Token in the related data.

7.5 Transaction Processing

Payment Networks are responsible for supporting the implementation of PAR in accordance with Registered BIN Controllers.

Payment Networks SHOULD:

- Follow the Token Processing and payment processing requirements as defined and communicated by the Registered BIN Controllers
- Determine the Token Processing and payment processing messaging requirements for supporting PAR

Payment Networks will ensure an ISO-defined field for PAR Data is available in their message specifications, which may include authorisation, capture, clearing and exception messages:

- Registered BIN Controllers SHALL determine PAR Data availability requirements in Token Processing and all payment processing messages
- Transactions that are PAN-based or Payment Token based SHALL NOT be initiated with PAR Data alone
- Payment Networks SHALL make the PAR Field available to Acquirers and Payment Processors in authorisation transaction responses resulting from Payment Token or PAN-based transactions that have an affiliated Payment Token
- Payment Networks SHOULD support the PAR Field in authorisation request messages, capture files, clearing, and exception messages resulting from Payment Token or PAN-based transactions that have an affiliated Payment Token
- Registered BIN Controllers SHALL enable a PAR Enquiry Function that may be available for retrieval of PAR Data for Merchants, Acquirers, Payment Processors, and others in the acceptance community before, during and after a transaction

7.5.1 EMV Terminal Processing

EMVCo has defined EMV Tag ‘9F24’ for the identification of PAR Data provisioned in an EMV Based Application.

The Terminal SHOULD:

- Be able to support the EMV Tag without disruption to the Terminal

- Be capable of receiving PAR Data using either the READ RECORD response or GET PROCESSING OPTIONS response of an EMV-based transaction
- Pass PAR Data to the Merchant's POS system
- Pass PAR Data with other EMV data to the Merchant's Payment Processor or Acquirer

7.5.2 Merchant Processing

Acquirers and Payment Processors enable PAR Field and PAR Data availability for Merchants.

Where the Merchant accepts Payment Tokens and is not a Token Requestor, PAR Data may be available as follows:

- When provisioned in an EMV Based Application, PAR Data is identified at the point of sale through EMV Tag '9F24'
- When provisioned in a non-EMV Based Application, PAR Data is passed by the Token Requestor with the Payment Token in the related data
- Through a PAR Enquiry Function
- In the authorisation response from the Acquirer or Payment Processor

A Merchant may rely on its Acquirer or Payment Processor to provide specific requirements defining PAR Field and PAR Data availability in authorisation and capture processing.

7.5.3 Acquiring Processing

Payment Networks define PAR Field and PAR Data availability for Acquirers and Payment Processors.

Acquirers and Payment Processors SHOULD:

- Rely on Payment Networks for specific requirements that define PAR Field and PAR Data availability in authorisation, capture, clearing and exception messages
- Make PAR Field and PAR Data available to Merchants and other Payment Processors in transaction responses from Payment Networks
- Be aware that PAR Data may be:
  - Read from EMV Tag '9F24'
  - Passed as part of Token Provisioning
  - Retrieved via a PAR Enquiry Function

Acquirers and Payment Processors may elect to receive PAR Data as defined by the Payment Network.

- Prior to Token Processing, PAR Data support will require that the Acquirer or Payment Processor evaluate their message formats to support PAR Data in incoming Token Processing requests:
  - Merchants SHOULD pass PAR Data to the Acquirer or Payment Processor in the Token Processing message format
  - Acquirers or Payment Processors SHOULD use the PAR Enquiry Function to retrieve PAR Data if PAR Data is not available
- During Token Processing:
  - Acquirers or Payment Processors SHOULD receive PAR Data in the Token Authorisation Response
  - PAR Data SHALL NOT be used to determine transaction routing to a Payment Network

7.5.4 Card Issuer Processing

The availability and assignment guidelines will be provided by the Registered BIN Controller. Card Issuers SHOULD:

- Have access to the assigned PAR Data for each PAN
- Return the PAR Data in transaction responses as defined by the Registered BIN Controller and implemented by the Payment Network
- Provide PAR Data to Token Service Providers for Token Provisioning in accordance to the governance requirements of the Registered BIN Controller
- Provide PAN lifecycle management events to the Registered BIN Controller

7.5.5 Other Processing

Other entities not specifically referenced in this technical framework may elect to receive PAR Data based on their participation within the payment ecosystem according to the other non-payment operational needs as defined by the Registered BIN Controller.

7.6 Data Security Considerations

PAR Data is not a substitute for PAN or Payment Tokens in terms of enabling payment transactions or routing. The PCI SSC has determined that PAR Data is not considered Account Data as defined by PCI DSS and has published an FAQ on its website, www.pcisecuritystandards.org.

For clarity, although PAR Data is not considered Account Data as defined by PCI DSS, PAR Data SHOULD be protected in accordance with national, regional or local laws and

regulations, plus any additional requirements of a given Payment System or Token Programme.

8 Token Service Provider Interfaces

This section establishes the common fields of any external interface that each Token Service Provider supports.

The Token Service Provider SHALL implement one or more secure methods of interaction with participating entities using the Payment Token service, including implementing appropriate access security controls. The following are examples of the authenticated methods through which these interactions may occur:

- Application Programming Interfaces (APIs) including web services
- ISO 8583 / ISO 20022 ACTICA message exchange through an existing Payment Network interface
- File / batch

Interfaces SHALL only be supported from recognised, authorised and authenticated sources.

The interfaces SHOULD be implemented and made available by the Token Service Provider to be used by all participating entities that interact with the Token Service Provider.

Payment Tokenisation Aggregators SHOULD use the interfaces made available by the Token Service Provider when interacting with the Token Service Provider.

This technical framework does not provide for technical level implementation detail of each of the interfaces or specify in detail the interfaces that will be implemented by each Token Service Provider.

This section does not address Token Processing. For more information, refer to Section 10 Token Processing.

Each of the following subsections describes a specific Payment Token related operation. Each operation SHALL have one or more defined interfaces and / or messages to carry it out.

8.1 Token Request and Issuance

This interface is used by a registered Token Requestor to request a Payment Token from the Token Service Provider. In order to request a Payment Token, the Token Requestor needs to provide a PAN or a Payment Token / Token Reference ID.

The Token Request interface may support:

- Real-time requests that require issuance of a Payment Token and Token Expiry Date for each Token Request
- Bulk requests through a secure interface file where multiple Payment Tokens and Token Expiry Dates are generated and returned to the Token Requestor.

Where a PAN-based interface (for example, see Section 9 Payment Token Fields Used in ISO 8583 and 20022 ATICA Messages) is repurposed for Token Request, a Payment Tokenisation Indicator SHOULD be included in the message to indicate the intent to reuse the PAN-based interface. The addition of the Payment Tokenisation Indicator explicitly identifies the PAN-based interface is being used as part of Token Request rather than for its original purpose.

If the request is successful, a Payment Token is returned in the response to the request.

8.1.1 Input Fields

The input fields for a Token Request depend on whether it is being made with a:

- PAN
- Payment Token or Token Reference ID

8.1.1.1 Token Request with PAN

The Token Service Provider SHALL provide a common method that a registered Token Requestor can use to submit a request through the defined interface to input the PAN and PAN Expiry Date and receive a Payment Token and Token Expiry Date in response.

The Token Service Provider SHALL implement appropriate controls and processes to generate a Payment Token and Token Expiry Date based on the input PAN and PAN Expiry Date.

Required, conditional and optional fields are shown in Table 8.1. This table does not preclude the use of other implementation-specific fields.

Table 8.1: Fields for Token Request with PAN

Field Name	Length	Format	R/C/O	Description
Token Requestor ID	11	Numeric	R	Uniquely identifies the pairing of the Token Requestor submitting this request with a specific Token Domain. Refer to Table 9.1 for a detailed description.
PAN	Variable (up to 19)	Numeric	R	PAN for which the Payment Token is requested.
PAN Expiry Date	4	Numeric	R	Expiry Date of the PAN for which the Payment Token is requested.

Field Name	Length	Format	R/C/O	Description
Token Assurance Method	2	Numeric	O	Indicates the Token Assurance Method Category that the Token Requestor would like to achieve. May be present if a specific Token Assurance Method Category is being requested.
Token Location	2	Numeric	C	Required unless inherent in the Token Requestor interface. Indicates the storage location of the Payment Token.
Token Assurance Data	Variable	Implementation Specific	C	Data as necessary to support the requested / agreed Token Assurance Method. This may include Cardholder data. Required if the requested / agreed Token Assurance Method requires Token Assurance Data. Refer to Section 6 Token Assurance Method for more details on Token Assurance Data. Specific examples of Token Assurance Data are given in Section 6.1.2 Token Assurance Data.
Consumer Device Information	Variable	Alphanumeric	O	Attributes of the Consumer Device that may be used to identify the specific device where a Payment Token is stored. Examples include secure element ID and / or characteristics of the device such as MAC address, operating system version, language etc.

R – Required, C – Conditional, O – Optional

Implementation of field formats is defined by each Token Service Providers' interface

8.1.1.2 Token Request with Payment Token / Token Reference ID

The Token Service Provider SHALL provide a common method that a registered Token Requestor can use to submit a request through the defined interface to input a Payment Token and Token Expiry Date or, if allowed by the policies of the Token Programme, to input a Token

Reference ID, and receive a new Payment Token and Token Expiry Date in response. Input is limited to Payment Tokens / Token Reference IDs issued by the same Token Service Provider.

When the Token Requestor is NOT the same as the Token Requestor associated with the input Payment Token or Token Reference ID, the Token Service Provider SHALL require the Token Requestor to include the Token Request Authorisation provided by the Token Requestor associated with the original Payment Token.

Required, conditional and optional fields are shown in Table 8.2. This table does not preclude the use of other implementation-specific fields.

Table 8.2: Fields for Token Request with a Payment Token / Token Reference ID

Field Name	Length	Format	R/C/O	Description
Token Requestor ID	11	Numeric	R	Uniquely identifies the pairing of the Token Requestor submitting this request with a specific Token Domain. Refer to Table 9.1 for a detailed description.
Token Request Authorisation	Variable	Implementation Specific	C	The authorisation of the original Token Requestor granting the input Token Requestor rights to request a Payment Token. Required if the Token Requestor is not the same as the Token Requestor associated with the Payment Token or Token Reference ID passed in the Payment Token field.
Payment Token	Variable (up to 19)	Numeric	C	Payment Token from which the new Payment Token is requested. Required if a Token Reference ID is not passed.
Token Expiry Date	4	Numeric	C	Token Expiry Date of the Payment Token from which the new Payment Token is requested. Required if a Payment Token is used in the request.

Field Name	Length	Format	R/C/O	Description
Token Reference ID	Variable	Implementation Specific	C	Reference identifier for the Payment Token from which the new Payment Token is requested. Required if a Payment Token is not passed.
Token Assurance Method	2	Numeric	O	Indicates the Token Assurance Method Category that the Token Requestor would like to achieve. May be present if a specific Token Assurance Method Category is being requested.
Token Location	2	Numeric	C	Required unless inherent in the Token Requestor interface. Indicates the storage location of the Payment Token.
Token Assurance Data	Variable	Implementation Specific	C	Data as necessary to support the requested / agreed Token Assurance Method. This may include Cardholder data. Required if the requested / agreed Token Assurance Method requires Token Assurance Data. Refer to Section 6 Token Assurance Method for more details on Token Assurance Data. Specific examples of Token Assurance Data are given in Section 6.1.2 Token Assurance Data.
Consumer Device Information	Variable	Alphanumeric	O	Attributes of the Consumer Device that may be used to identify the specific device where a Payment Token is stored. Examples include secure element ID and / or characteristics of the device such as MAC address, operating system version, language etc.

R – Required, C – Conditional, O – Optional

Implementation of field formats is defined by each Token Service Providers' interface

8.1.2 Output Fields

For any Token Request, the interface SHALL provide a response message with the required, conditional and optional fields that are shown in Table 8.3. This table does not preclude the use of other implementation-specific fields.

Table 8.3: Fields for Response to Token Request

Field Name	Length	Format	R/C/O	Description
Request Status	1	Numeric	R	Indicates success or failure of the request.
Reason Code	Variable	Alphanumeric	C	Provides information on the reason that the request failed. Required if Request Status is not successful.
Payment Token	Variable (up to 19)	Numeric	C	The Payment Token that is generated by the Token Service Provider. Required if Request Status is successful.
Token Expiry Date	4	Numeric	C	The Token Expiry Date that is generated by the Token Service Provider. Required if Request Status is successful.
Token Assurance Method	2	Numeric or Space Character	C	The Token Assurance Method Category assigned as a result of the ID&V performed. Required if Request Status is successful.
Token Reference ID	Variable	Implementation Specific	O	Reference identifier for the Payment Token which can optionally be provided to the Token Requestor.
Payment Account Reference	29	Alphanumeric[1]	C	The Payment Account Reference associated with the underlying PAN. Required if Request Status is successful and if PAR Field and PAR Data are supported by the Token Service Provider.

R – Required, C – Conditional, O – Optional

Implementation of field formats is defined by each Token Service Providers' interface

[1] Alphanumeric fields consist of uppercase Alphanumeric Roman characters

8.2 Token Assurance Method Update

This interface is used for situations where, after the issuance of a Payment Token, updated ID&V is performed and an updated Token Assurance Method assigned to the Payment Token.

8.2.1 Input Fields

The Token Service Provider SHALL provide a common method that an authenticated entity can use to submit a request through the defined interface to input a Payment Token and receive an updated Token Assurance Method in response.

Required, conditional and optional fields are shown in Table 8.4. This table does not preclude the use of other implementation-specific fields.

Table 8.4: Fields for Token Assurance Method Update Request

Field Name	Length	Format	R/C/O	Description
Payment Token	Variable (up to 19)	Numeric	R	The Payment Token.
Token Requestor ID	11	Numeric	R	Uniquely identifies the pairing of the Token Requestor submitting this request with a specific Token Domain. Refer to Table 9.1 for a detailed description.
Token Assurance Method	2	Numeric	O	Indicates the Token Assurance Method that the Token Requestor would like to achieve. May be present if Token Requestor is requesting a specific Token Assurance Method.

Field Name	Length	Format	R/C/O	Description
Token Assurance Data	Variable	Alphanumeric	C	Data as necessary to support the requested Token Assurance Method. This may include Cardholder data. Refer to Section 6 Token Assurance Method for more details on Token Assurance Data. Specific examples of Token Assurance Data are given in Section 6.1.2 Token Assurance Data.
Consumer Device Information	Variable	Alphanumeric	O	Attributes of the Consumer Device that may be used to identify the specific device where a Payment Token is stored. Examples include secure element ID and / or characteristics of the device such as MAC address, operating system version, language etc.

R – Required, C – Conditional, O – Optional

Implementation of field formats is defined by each Token Service Providers' interface

8.2.2 Output Fields

The interface SHALL provide a response message with the required, conditional and optional fields that are shown in Table 8.5. This table does not preclude the use of other implementation-specific fields.

Table 8.5: Fields for Response to Token Assurance Method Update Request

Field Name	Length	Format	R/C/O	Description
Request Status	1	Numeric	R	Indicates success or failure of the request.
Reason Code	Variable	Alphanumeric	C	Provides information on the reason that the request failed. Required if Request Status is not successful.
Payment Token	Variable (up to 19)	Numeric	O	May be present if Request Status is successful.

Field Name	Length	Format	R/C/O	Description
Token Assurance Method	2	Numeric or Space Characters	C	The Token Assurance Method assigned as a result of the ID&V performed. Required if Request Status is successful.

R – Required, C – Conditional, O – Optional

Implementation of field formats is defined by each Token Service Providers' interface

8.3 De-Tokenisation without Verification

The De-Tokenisation without Verification interface provides the necessary mechanism to exchange the Payment Token by returning the underlying PAN and PAN Expiry Date to the authenticated entity. No transaction-specific validation is performed on this request and is not used in Token Processing.

The ability to retrieve an underlying PAN and PAN Expiry Date in exchange for its affiliated Payment Token and Token Expiry Date without verification is restricted to specifically authorised entities, individuals, applications, or systems.

8.3.1 Input Fields

The Token Service Provider SHALL provide a common method that an authenticated entity can use to submit a request through the defined interface to input a Payment Token and Token Expiry Date and receive the underlying PAN and PAN Expiry Date in response without any transaction-specific validation being performed.

Required, conditional and optional fields are shown in Table 8.6. This table does not preclude the use of other implementation-specific fields.

Table 8.6: Fields for De-Tokenisation without Verification Request

Field Name	Length	Format	R/C/O	Description
Payment Token	Variable (up to 19)	Numeric	R	The Payment Token being submitted for De-Tokenisation.
Token Expiry Date	4	Numeric	R	The Token Expiry Date.

Field Name	Length	Format	R/C/O	Description
Token Requestor ID	11	Numeric	O	Uniquely identifies the Token Requestor of the Payment Token. May be present if available to the entity submitting the request.
Payment Account Reference	29	Alphanumeric[1]	O	The PAR Data associated with the Payment Token. May be present if available to the entity submitting the request.

R – Required, C – Conditional, O – Optional

Implementation of field formats is defined by each Token Service Providers' interface

[1] Alphanumeric fields consist of uppercase Alphanumeric Roman characters

8.3.2 Output Fields

The interface SHALL provide a response message with the required, conditional and optional fields that are shown in Table 8.7. This table does not preclude the use of other implementation-specific fields.

Table 8.7: Fields for Response to De-Tokenisation without Verification Request

Field Name	Length	Format	R/C/O	Description
Request Status	1	Numeric	R	Indicates success or failure of the request.
Reason Code	Variable	Alphanumeric	C	Provides information on the reason that the request failed. Required if Request Status is not successful.
PAN	Variable (up to 19)	Numeric	C	The underlying PAN of the Payment Token submitted for De-Tokenisation. Required if Request Status is successful.
PAN Expiry Date	4	Numeric	C	The expiry date of the underlying PAN. Required if Request Status is successful.

Field Name	Length	Format	R/C/O	Description
Payment Account Reference	29	Alphanumeric[1]	C	The Payment Account Reference associated with the underlying PAN. Required if Request Status is successful and if PAR Field and PAR Data are supported by the Token Service Provider.

R – Required, C – Conditional, O – Optional

Implementation of field formats is defined by each Token Service Providers' interface

[1] Alphanumeric fields consist of uppercase Alphanumeric Roman characters

8.4 De-Tokenisation with Verification

The De-Tokenisation with Verification interface provides the necessary mechanism to exchange the Payment Token and Token Expiry Date by returning the underlying PAN and PAN Expiry Date to the authenticated entity, whilst performing any required verification of the Payment Token and applying the Token Domain Restriction Controls associated with the Payment Token.

8.4.1 Input Fields

The Token Service Provider SHALL provide a common method that an authenticated entity can use to submit a request through the defined interface to input a Payment Token and Token Expiry Date and receive the underlying PAN and PAN Expiry Date in response.

Required, conditional and optional fields are shown in Table 8.8. This table does not preclude the use of other implementation-specific fields.

Table 8.8: Fields for De-Tokenisation with Verification Request

Field Name	Length	Format	R/C/O	Description
Payment Token	Variable (up to 19)	Numeric	R	The Payment Token being submitted for De-Tokenisation.
Token Expiry Date	4	Numeric	R	The Token Expiry Date.
Token Requestor ID	11	Numeric	O	Uniquely identifies the Token Requestor of the Payment Token. May be present if available to the entity submitting the request.

Field Name	Length	Format	R/C/O	Description
Transaction Data	Variable	Implementation Specific	C	Other transaction data as necessary for the Token Service Provider to execute the request, content is proprietary to the Token Service Provider. Required if De-Tokenisation is taking place within Token Authorisation.
Payment Account Reference	29	Alphanumeric[1]	O	The PAR Data associated with the Payment Token. May be present if available to the entity submitting the request.

R – Required, C – Conditional, O – Optional

Implementation of field formats is defined by each Token Service Providers' interface

[1] Alphanumeric fields consist of uppercase Alphanumeric Roman characters

8.4.2 Output Fields

The interface SHALL provide a response message with the required, conditional and optional fields that are shown in Table 8.9. This table does not preclude the use of other implementation-specific fields.

Table 8.9: Fields for Response to De-Tokenisation with Verification Request

Field Name	Length	Format	R/C/O	Description
Request Status	1	Numeric	R	Indicates success or failure of the request.
Reason Code	Variable	Alphanumeric	C	Provides information on the reason that the request failed. Required if Request Status is not successful.
PAN	Variable (up to 19)	Numeric	C	The underlying PAN of the Payment Token submitted for De-Tokenisation. Required if Request Status is successful.
PAN Expiry Date	4	Numeric	C	The expiry date of the underlying PAN. Required if Request Status is successful.

Field Name	Length	Format	R/C/O	Description
Transaction Data	Variable	Implementation Specific	C	Transaction data as necessary to continue the transaction, content is proprietary to the Token Service Provider. Required if De-Tokenisation is taking place within Token Authorisation.
Payment Account Reference	29	Alphanumeric[1]	C	The Payment Account Reference associated with the underlying PAN. Required if Request Status is successful and if PAR Field and PAR Data are supported by the Token Service Provider.

R – Required, C – Conditional, O – Optional

Implementation of field formats is defined by each Token Service Providers' interface

[1] Alphanumeric fields consist of uppercase Alphanumeric Roman characters

8.5 Token Cryptogram Request

The Token Cryptogram Request interface allows an authorised entity to request a Token Cryptogram by providing a Payment Token and Token Expiry Date or a Token Reference ID.

If the request is successful, then a Token Cryptogram is provided in the response to the request. If a Token Reference ID is provided in the input, then the corresponding Payment Token is also provided in the response to the request.

8.5.1 Input Fields

If supported, the Token Service Provider SHALL:

- Provide a common method that an authorised entity can use to submit a request through the defined interface to input a Payment Token and Token Expiry Date or a Token Reference ID and receive a Token Cryptogram in response.
- Implement appropriate controls and processes to generate a Token Cryptogram

Required, conditional and optional fields are shown in Table 8.10. This table does not preclude the use of other implementation-specific fields.

Table 8.10: Fields for Token Cryptogram Request

Field Name	Length	Format	R/C/O	Description
Payment Token	Variable (up to 19)	Numeric	C	The Payment Token for which the Token Cryptogram is being requested. Optionally, a Token Reference ID may be submitted in place of the Payment Token and Token Expiry Date. Required if a Token Reference ID is not passed.
Token Expiry Date	4	Numeric	C	The Token Expiry Date. Required if a Payment Token is passed.
Token Reference ID	Variable	Implementation Specific	C	Reference identifier for the Payment Token for which the Token Cryptogram is being requested. Optionally, a Token Reference ID may be submitted in place of the Payment Token and Token Expiry Date. Required if a Payment Token is not passed.
Token Requestor ID	11	Numeric	C	Uniquely identifies the Token Requestor of the Payment Token. Required when available to the entity submitting the request.
Transaction Data	Variable	Implementation Specific	C	Transaction data as required by the Token Service Provider to execute the request. The content is proprietary to the Token Service Provider and, if the request is for Token Processing, includes whether this is a Cardholder-Initiated or Merchant-Initiated Transaction.

R – Required, C – Conditional, O – Optional

Implementation of field formats is defined by each Token Service Providers' interface

8.5.2 Output Fields

If supported, the interface SHALL provide a response message with the required, conditional and optional fields that are shown in Table 8.11. This table does not preclude the use of other implementation-specific fields.

Table 8.11: Fields for Response to Token Cryptogram Request

Field Name	Length	Format	R/C/O	Description
Request Status	1	Numeric	R	Indicates success or failure of the request.
Reason Code	Variable	Alphanumeric	C	Provides information on the reason that the request failed. Required if Request Status is not successful.
Payment Token	Variable (up to 19)	Numeric	C	Payment Token for which the Token Cryptogram was requested. Required if Request Status is successful and the Payment Token was not in the original request.
Token Expiry Date	4	Numeric	C	Expiry date of the Payment Token. Required if Request Status is successful and the Payment Token is provided in the response.
Token Cryptogram	Variable	Implementation Specific	C	The Token Cryptogram generated in response to the request. Required if Request Status is successful.
Transaction Data	Variable	Implementation Specific	C	Transaction data as necessary to continue the transaction. Content is proprietary to the Token Service Provider. Required if the Token Cryptogram has been requested for the purposes of Token Processing.

R – Required, C – Conditional, O – Optional

Implementation of field formats is defined by each Token Service Providers' interface

8.6 Payment Tokenisation Lifecycle Management

Payment Tokens may require ongoing management and updates due to changes to the PAN and PAN Expiry Date, as well as lifecycle management events that may require the affiliation of the Payment Token / Token Expiry Date with the underlying PAN / PAN Expiry Date to be deactivated.

The Token Service Provider SHALL provide lifecycle management event updates through the interfaces to manage changes that affect the issued Payment Token.

Payment Tokenisation lifecycle management may be required to support existing business-as-usual processes.

Table 8.12 provides a sample set of lifecycle management events that SHOULD be made available as interfaces by the Token Service Provider. Note that it is not a requirement that a Token Service Provider performs the actions described for each event: the actions performed for each event will be according to the policies and processes of the Token Programme.

Fields defined in previous sections will also be applicable to these interfaces.

Table 8.12: Lifecycle Management Events

#	Interface	Example Event / Description	Initiated By	Action Performed
1	Unlink Payment Token	• Lost or stolen device • Underlying PAN no longer valid • Token Requestor no longer carries the card-on-file • Lost or stolen PAN • Fraud alert on PAN • Fraud alert on Payment Token	Token Requestor Card Issuer Token Service Provider	The Payment Token / Token Expiry Date affiliation with the underlying PAN / PAN Expiry Date is unlinked.
2	Suspend Payment Token	• Temporary deactivation due to lost or stolen device	Token Requestor Card Issuer Token Service Provider	The Payment Token / Token Expiry Date affiliation with the underlying PAN / PAN Expiry Date is temporarily suspended.

#	Interface	Example Event / Description	Initiated By	Action Performed
3	Activate Payment Token	• First-time activation or resumption from temporary suspension of Payment Token / Token Expiry Date affiliation with the underlying PAN / PAN Expiry Date	Token Requestor Card Issuer Token Service Provider	The Payment Token / Token Expiry Date affiliation with the underlying PAN / PAN Expiry Date is activated.
4	Update Payment Token Attributes	• Ongoing management of the Token Assurance Method on the Payment Token • Updates to Payment Token attributes, such as Token Expiry Date	Token Requestor Card Issuer Token Service Provider	The Token Assurance Method is updated, based on the ID&V Method(s) performed, or as a result of internal operations. Updates to the Payment Token attributes, such as Token Expiry Date, are made to extend the use of the Payment Token.
5	Update PAN Attributes	• Updates to underlying PAN attributes, such as PAN Expiry Date	Card Issuer Token Service Provider	Updates to the PAN attributes, such as PAN Expiry Date, are made to extend the use of the Payment Token. This may also include PAR Data.

9 Payment Token Fields Used in ISO 8583 and 20022 ATICA Messages

The fields defined in this section represent:

- Existing ISO-recognised fields that have been repurposed for Payment Tokenisation
- Fields introduced as Payment Network specific fields until such time as they are adopted into ISO specifications

The fields associated with Payment Tokenisation can be used for both Token Processing and Token Provisioning. Requirements on how these fields may be used are provided in the following sections:

- Section 8 Token Service Provider Interfaces (Token Provisioning)
- Section 10 Token Processing

9.1 ISO-specific Fields

Table 9.1 represents the ISO-specific Payment Token fields used in Token Processing and / or Token Provisioning. ISO fields are provided for both ISO 8583 and for ISO 20022 ATICA.

Table 9.1: ISO-specific Payment Token Fields

Field Name	ISO Field	Length	Format	Description
Payment Token	8583: 2 20022 ATICA: Environment: Card / Tag: <PAN> Or Environment: Token / Tag: <PmtTkn>	Variable (up to19)	Numeric	Payment Tokens use the PAN-related field since the format is consistent with existing PAN length and format requirements.
Token Expiry Date	8583: 14 20022 ATICA: Environment: Card / Tag: <ExpiryDate> Or Environment: Token / Tag: <TknXpryDt>	4	Numeric	Token Expiry Date uses the PAN Expiry Date field since the format is consistent with existing PAN Expiry Date length and format requirements.

Field Name	ISO Field	Length	Format	Description
Last 4 Digits of PAN	8583: Payment Network Specific 20022 ATICA: Environment: Card / Tag: <PANFourLastDgts>	4	Numeric	Represents the last four digits of the underlying PAN affiliated with the Payment Token. Its purpose is to support customer service, e.g. digital wallet display or receipt creation.
PAN Product ID	8583: Payment Network Specific 20022 ATICA: Environment: Card / Tag: <CardPdctTp>	Variable	Alpha-numeric	Used for determining the type of underlying card product as defined by the Payment System. It may be included in cases where transparency of this information is necessary.
POS Entry Mode	8583: 22.1 (1987) 22.7 (1993) 22.1 (2003) 20022 ATICA: Environment: PointOfServiceContext1 / Tag: <CardDataNtryMd>	2	Numeric	Used to indicate the mode through which the Payment Token is presented for payment to the Merchant. 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 Requestor ID	8583: Payment Network Specific 20022 ATICA: Environment: Token / Tag: <TknRqstrId>	11	Numeric	Uniquely identifies the pairing of Token Requestor with the Token Domain. It is a unique 11-digit numeric value assigned by the Token Service Provider: • Positions 1-3: Token Service Provider Code, unique to each Token Service Provider • Positions 4-11: Assigned by the Token Service Provider for each Token Requestor and Token Domain

Field Name	ISO Field	Length	Format	Description
Token Assurance Method	8583: Payment Network Specific 20022 ATICA: Environment: Token / Tag: <TknAssrncMtd>	2	Numeric or Space Characters	The value representing the categorisation of the ID&V Method(s) performed and the ID&V Actor that performed it.
Token Assurance Data	8583: Payment Network Specific 20022 ATICA: Environment: Token / Tag: <TknAssrncData>	Variable	Payment Network Specific	One or more fields providing information in support of the categorisation for the Token Assurance Method.
Token Cryptogram	8583: Payment Network Specific 20022 ATICA: Environment: Verification / Tags: <VrfctnInf> / <Tp> / <Val>	Variable	Payment Network Specific	One or more fields that contains uniquely generated data to enable validation of the authorised use of the Payment Token.
Payment Account Reference	8583: 56 (1987) 112 (1993) 51 (2003) 20022 ATICA: Environment: Card / Tag: <PmtAcctRef>	29	Alpha-numeric[1]	Enables Merchants, Acquirers and Payment Processors to link transactions initiated with affiliated Payment Tokens to transactions based on the underlying PAN. 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

Field Name	ISO Field	Length	Format	Description
Original Transaction Reference	8583: Payment Network Specific 20022 ATICA: Environment: Transaction / Tags: <TxId> / <OrgnlDataElmts> / <TxRef>	Variable	Payment Network Specific	One or more fields that uniquely identify the original Cardholder-Initiated Transaction in a Merchant-Initiated Transaction request.
Merchant-Initiated Transaction Type	8583: Payment Network Specific 20022 ATICA: Environment: Transaction / Tag: <TxAttr>	Variable	Payment Network Specific	One or more fields that identify the business condition associated with a Merchant-Initiated Transaction. Defines the payment ecosystem specific transaction type or the type of standing instruction.
Merchant Identifiers	8583: Payment Network Specific 20022 ATICA: Environment: Acceptor / Tag: <Id>	Variable	Payment Network Specific	Uniquely identifies the Merchant and / or Token User during Token Processing.
Authentication Data	8583: Payment Network Specific 20022 ATICA: Payment Network Specific	Variable	Payment Network Specific	One or more fields that provide information to be used during authentication.

Field Name	ISO Field	Length	Format	Description
Token Request Indicator	8583: Payment Network Specific / ID&V specific 20022 ATICA: Environment: Token / Tag: <TknInittdInd>	Variable	Payment Network Specific / ID&V specific	Uniquely indicates that an existing PAN- based message is being used for a Token Request. Authorisation response messages can be used to return the relevant data. Note: whenever a Token Request Indicator is present, additional fields, including PAN, PAN Expiry Date, Payment Token, Token Expiry Date and Token Assurance Data, may also be present.

[1] *Alphanumeric fields consist of uppercase Alphanumeric Roman characters*

9.2 Field Considerations

This section describes the Payment Token fields that may be used in Token Processing. Token Processing fields will be mapped and flow through the existing messaging infrastructure. The Token Processing field and data requirements will vary based on the use of the Payment Token. The fields are described in Table 9.2.

Table 9.2: Token Processing Fields

Field Name	Comment
Payment Token	An existing payment processing field that is passed through the authorisation, capture, clearing, and exception messages in place of the PAN. After De-Tokenisation, the Payment Token is replaced with the underlying PAN. The PAN is then passed to the Card Issuer as part of the PAN Authorisation in this field. The Payment Token may optionally be passed to the Card Issuer as part of the PAN Authorisation using a Payment Network specific Token Processing field.

Field Name	Comment
Token Expiry Date	An existing payment processing field that is passed through the authorisation, capture, clearing, and exception messages in place of the PAN Expiry Date. After De-Tokenisation, the Token Expiry Date is replaced with the PAN Expiry Date. The PAN Expiry Date is then passed to the Card Issuer as part of PAN Authorisation request in this field. The Token Expiry Date may optionally be passed to the Card Issuer as part of PAN Authorisation using a Payment Network specific Token Processing field.
Last 4 Digits of PAN	A Payment Tokenisation specific field that is passed in: • The Token Authorisation response and the Token Payment Response • An EMV based transaction via EMV Tag '9F25'
PAN Product ID	An existing payment processing field that may optionally be passed as part of the Token Processing response. The PAN Product ID for a Payment Token is identical to the value assigned for the underlying PAN.
POS Entry Mode	An existing payment processing field that is passed through the authorisation, capture, clearing, and exception messages as a Token Control Field.
Token Requestor ID	A Payment Tokenisation specific field that is passed during Token Processing. It may optionally be passed through the authorisation, capture, clearing, and exception messages. It may be validated if present during Token Processing. It may optionally be available in: • An EMV based transaction via EMV Tag '9F19'. • A Non-EMV based transaction
Token Assurance Method	A Payment Tokenisation specific field that is passed during Token Processing. Is required to be passed in the authorisation response, capture and clearing messages.
Token Assurance Data	A Payment Tokenisation specific field that may optionally be passed during Token Processing.

Field Name	Comment
Token Cryptogram	A Payment Tokenisation specific field that is passed during Token Processing as a Token Control Field. The field contents depend on the type of transaction and associated usage scenario: • EMV based transactions will carry the Token Cryptogram in an existing EMV field • Non-EMV based transactions may use a non-EMV field
Payment Account Reference	A payment processing field that is passed through the authorisation, capture, clearing, and exception messages.
Original Transaction Reference	An existing payment processing field that is passed during Token Processing as a Token Control Field.
Merchant-Initiated Transaction Identifier	An existing payment processing field(s) that is passed during Token Processing as a Token Control Field.
Merchant Identifiers	An existing payment processing field(s) that is passed during Token Processing as a Token Control Field.

10 Token Processing

The implementation of a Token Programme based on this technical framework is not intended to change the traditional methods and transaction flows in which PANs are currently processed. To support the introduction of Payment Tokens there may be changes to the relevant message specifications.

This includes:

- Using existing fields
- Passing some Payment Token related data within existing fields
- Introducing Payment Tokenisation specific fields
- Ensuring that the Payment Network can recognise Payment Token transactions so that Payment Tokens are de-tokenised during transaction processing

Some of the Payment Tokenisation specific fields introduced in this technical framework are required in order to provide for consistency of implementation and interoperability throughout the payment ecosystem, while others are conditional or optional.

Various controls, including Token Domain Restriction Controls, are needed to manage and validate both the Payment Token and its usage. The required controls will be determined within each Token Programme.

It is the responsibility of the impacted Payment Networks to inform Card Issuers and Acquirers of changes to authorisation (and other) messages that support Payment Tokenisation, including identification of which fields have had their usage changed and which fields are new. Card Issuers need to be aware of the separation of responsibility when processing Payment Token transactions, since validation and verification of content within the message can be performed in conjunction with Card Issuers.

This section identifies the fields that can be present in transaction messages containing Payment Tokens. Presence in authorisation, capture, clearing and exception processing transactions depends on whether the field is considered required, conditional or optional. For each transaction message, additional fields will be present depending on the Payment Network that the transaction traverses and the requirements of the Payment System. This technical framework does not provide a complete or comprehensive list of fields and data used in each message, rather it provides context for the common transaction-based elements.

10.1 EMV Based Application Tags

EMVCo has defined the following tags for EMV Based Applications related to Payment Tokenisation:

- EMV Tag ‘9F24’ Payment Account Reference (PAR)
- EMV Tag ‘9F25’ Last 4 Digits of PAN
- EMV Tag ‘9F19’ Token Requestor ID

10.2 Authorisation Overview

Token Processing utilises existing Payment Network transactions, authorisation message types and structures as well as fields described in Section 9 Payment Token Fields Used in ISO 8583 and 20022 ATICA Messages. Implementation requirements may vary by Token Programme.

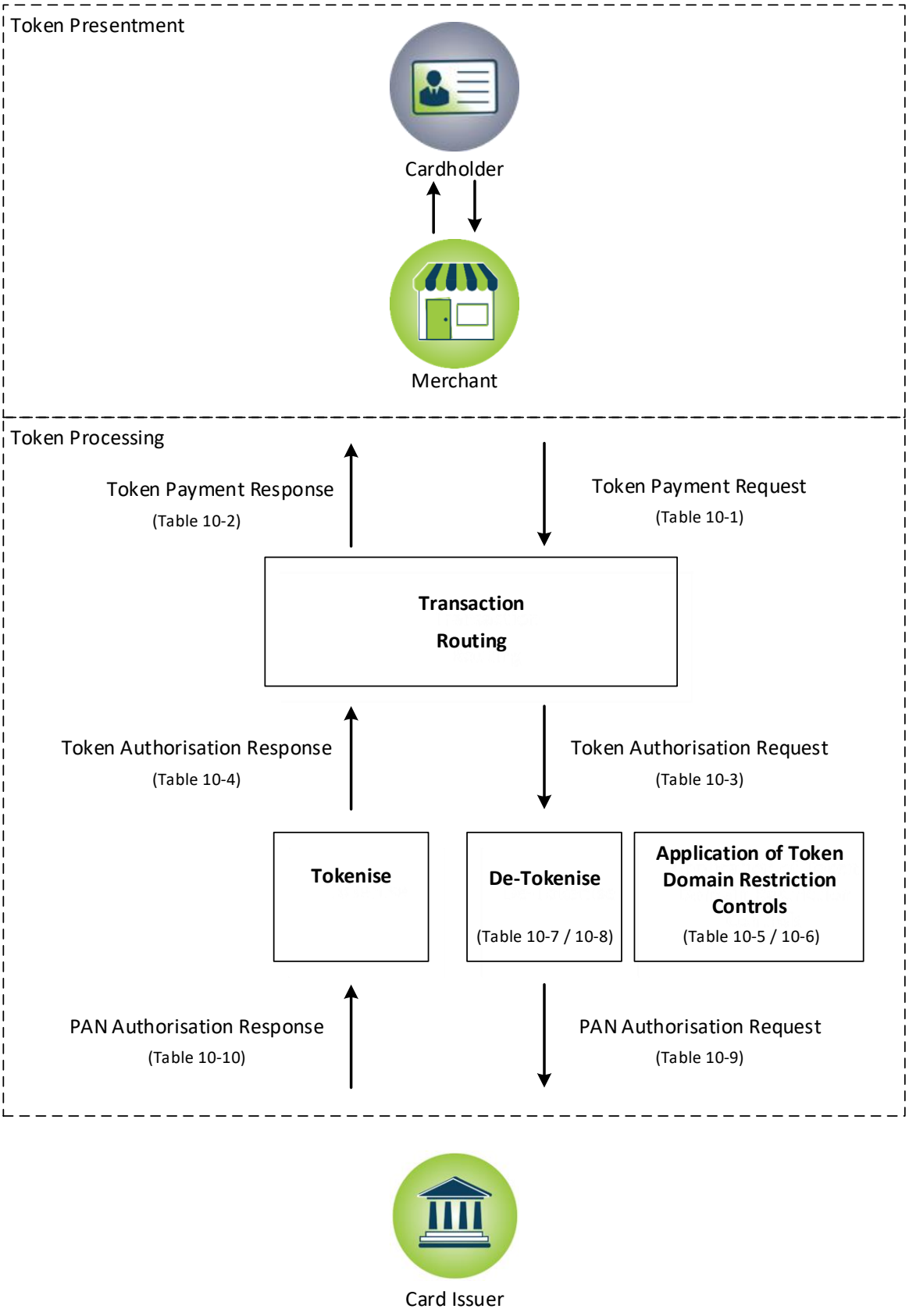
Token Processing follows Token Presentment and is divided into the following functions (see Figure 10.1: Illustrative Payment Token Processing Flow for Authorisations):

- 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 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 Payment Token and Token Expiry Date before the Token Authorisation Response.

The basic authorisation flow is shown in Figure 10.1.

Figure 10.1: Illustrative Payment Token Processing Flow for Authorisations



10.3 Routing and Account Range Tables

Routing and account range tables need to clearly distinguish Token BINs and Token BIN Ranges from traditional PAN BINs and PAN BIN ranges in order to ensure the underlying integrity of payment processing. This requires the assignment of Token BINs and Token BIN Ranges that are unique and distinct from traditional BINs and BIN ranges which will preserve any product-related attributes of the BIN or BIN Range of the underlying PAN and are flagged accordingly in all routing and account range tables.

10.4 Transaction Processing Considerations

Token Processing includes the application of the Token Domain Restriction Controls.

Requirements for Token Processing are:

- Token Control Fields and related data SHALL be validated in the incoming Token Authorisation
- If an online PIN is used with a Payment Token, such as ISO 9564-1 PIN Block Format 0 or Format 3, the PIN Block SHALL include the Payment Token in place of the PAN. The Card Issuer will receive the PIN Block with the PAN or Payment Token, as appropriate, for validation

10.4.1 Payment Network

The Payment Network may interface with the Token Service Provider in order to verify the state of the Payment Token / Token Expiry Date affiliation with the underlying PAN / PAN Expiry Date in the Token Vault for the affiliated Payment Token.

The Payment Network SHOULD be aware that a Payment Token transaction may include a Token Cryptogram and authentication data.

10.4.2 Types of Transaction

All transactions are the result of an originating interaction between a Cardholder and Merchant where an implicit acceptance agreement is entered into by the parties. This agreement results in two different types of transaction initiation.

The first type is the Cardholder-Initiated Transaction, where the Cardholder directly presents a payment credential. Cardholder-Initiated Transactions may use various authentication and verification features. A Token Cryptogram is required for EMV based and application based

commerce in Cardholder-Initiated Transactions and is optional for all other Cardholder-Initiated Transactions.

The second type is the Merchant-Initiated Transaction, which is always the result of a previous Cardholder interaction, represented by the original Cardholder-Initiated Transaction. The nature of the Merchant-Initiated Transaction is governed by two factors:

- Industry-specific authorisation practices that are the result of an original Cardholder-Initiated Transaction and extends the initial Cardholder-Initiated Transaction
- Standing instructions that provide express permission for additional purchases

Multiple standing instruction Merchant-Initiated Transactions using a Payment Token can result from a single Cardholder-Initiated Transaction regardless of the original payment credential that was presented by the Cardholder.

Merchant-Initiated Transactions are considered card-not-present or Cardholder-not-present transactions. Payment Token related data (such as Token Cryptograms) associated with the original Cardholder-Initiated Transaction SHOULD NOT be re-used for the application of Token Domain Restriction Controls for any subsequent Merchant-Initiated Transactions.

To increase transaction security, a Token Programme may require that each separate Merchant-Initiated Transaction has a unique Token Cryptogram which is part of the Token Domain Restriction Controls. Token Cryptograms associated with a Merchant-Initiated Transaction SHOULD be unique to that transaction. Token Cryptograms associated with a specific Merchant-Initiated Transaction SHOULD NOT be re-used for the application of Token Domain Restriction Controls for any other Merchant-Initiated Transactions.

10.5 Token Payment Request

The Token Payment Request is the first leg and the Token Payment Response is the last leg of any transaction, starting with the interaction between the Cardholder and the Merchant and ending with the successful completion of the transaction. The transaction message fields and data are governed by the entities between which the Token Payment Request and its associated Response traverse.

The Cardholder interacting with a Terminal, website or application will result in Token Processing related data being passed to the Merchant.

For the purposes of Token Processing, the fields and data included in Token Payment Requests are defined in Table 10.1. These are included with other transaction fields that are created and passed following existing message standards.

Table 10.1: Fields Included in Token Payment Requests

Field Content	Field Name	R/C/O	Condition / Option	Comment
Payment Token	PAN	R		
Token Expiry Date	PAN Expiry Date	R		
Token Presentment Mode	POS Entry Mode	R		Token Control Data
Token Cryptogram	Payment Network Specific	C	Required for EMV based and application based commerce in Cardholder-Initiated Transactions Optional for all other Cardholder-Initiated Transactions and Merchant-Initiated Transactions, based on the policies of each Token Programme	Generated and passed in appropriate cryptogram field Token Control Data
Token Requestor ID	Payment Network Specific	O	May be present if received by the Terminal or sourced by the Merchant directly from Token Requestor related interactions	
Merchant Identifiers	Payment Network Specific	O	May be present for e-commerce transactions	Token Control Data

Field Content	Field Name	R/C/O	Condition / Option	Comment
Payment Account Reference	Payment Account Reference	O	May be present if received by the Terminal or sourced by the Merchant directly from Token Requestor related interactions	

R – Required, C – Conditional, O – Optional

For the purposes of Payment Token Processing, the fields and data included in Token Payment Responses are defined in Table 10.2. These are included with other transaction fields that are created and passed following existing message standards.

Table 10.2: Fields Included in Token Payment Responses

Field Content	Field Name	R/C/O	Condition / Option	Comment
Payment Token	PAN	R		Value must match the Payment Token value in the Token Payment Request
Last 4 Digits of PAN	Payment Network Specific	C	Required when agreed by Acquirer and Merchant	
PAN Product ID	Payment Network Specific	C	Required when agreed by Acquirer and Merchant	
Token Assurance Method	Payment Network Specific	C	Required when agreed by Acquirer and Merchant	
Payment Account Reference	Payment Account Reference	C	Required when agreed by Acquirer and Merchant	

R – Required, C – Conditional, O – Optional

10.6 Token Authorisation Processing

Token Authorisation Processing minimally involves the interaction between the Acquirer and the Payment Network. Upon receipt of the Token Payment Request, the Acquirer will perform routine processing checks and pass the Token Processing related data and other relevant payment data to the Payment Network, including setting the Token Presentment Mode to indicate the specific method in which the Payment Token was input into the Terminal or other Merchant point of interaction.

Token Authorisation Processing consists of a Token Authorisation request and a Token Authorisation response. The Token Authorisation request process continues until De-Tokenisation has been completed. The relevant request data comes from the Token Payment Request and the relevant response data comes from the PAN Authorisation response.

For the purposes of Token Processing, the fields and data included in Token Authorisation requests are defined in Table 10.3. These are included with other transaction fields that are created and passed following existing message standards.

Table 10.3: Fields Included in Token Authorisation Requests

Field Content	Field Name	R/C/O	Condition / Option	Comment
Payment Token	PAN	R		
Token Expiry Date	PAN Expiry Date	R		
Token Presentment Mode	POS Entry Mode	R		Inserted by Acquirer Token Control Data
Token Cryptogram	Payment Network Specific	C	Required for EMV based and application based commerce in Cardholder-Initiated Transactions Optional for all other Cardholder-Initiated Transactions and Merchant-Initiated Transactions, based on the policies of each Token Programme	Token Control Data

Field Content	Field Name	R/C/O	Condition / Option	Comment
Token Requestor ID	Payment Network Specific	O	May be present if read from Terminal or sourced directly from Token Requestor and passed to the Acquirer	
Merchant Identifiers	Payment Network Specific	O	May be present for e-commerce transactions	Token Control Data
Payment Account Reference	Payment Account Reference	O	May be present if received by the Terminal or sourced by the Merchant directly from Token Requestor related interactions	

R – Required, C – Conditional, O – Optional

For the purposes of Token Processing, the fields and data included in Token Authorisation responses are defined in Table 10.4. These are included with other transaction fields that are created and passed following existing message standards.

Table 10.4: Fields Included in Token Authorisation Responses

Field Content	Field Name	R/C/O	Condition / Option	Comment
Payment Token	PAN	R		Original Token Authorisation request value must be restored in response. Replaced in response after De-Tokenisation and PAN Authorisation
Last 4 Digits of PAN	Payment Network Specific	R		Contains the last four digits of the underlying PAN
PAN Product ID	Payment Network Specific	C	Required if provided by Payment Network	Contains the Product ID of the underlying PAN

Field Content	Field Name	R/C/O	Condition / Option	Comment
Token Assurance Method	Payment Network Specific	C	Required if provided by Payment Network	Sourced from the Token Vault during De-Tokenisation
Payment Account Reference[1]	Payment Account Reference	R		

R – Required, C – Conditional, O – Optional

[1] Responsibility to populate based on requirements of the BIN Controller

10.7 Token Domain Restriction Controls

The application of Token Domain Restriction Controls depend upon the availability of specific Token Control Fields and Payment Token related data in Token Processing messages to restrict Payment Token use to the appropriate Token Domain(s). Token Service Providers and participating Payment Networks provide the Token Control Fields.

The content of the Token Control Fields is dependent on specific Token Domain Restriction Controls for the Payment Token and type of transaction (Cardholder-Initiated or Merchant-Initiated – see Table 10.5 and Table 10.6). There can be different Token Domain Restriction Controls based on transactions that are Cardholder-Initiated versus Merchant-Initiated.

To successfully apply the Token Domain Restriction Controls for a Cardholder-Initiated Transaction, contents of Token Control Fields and related data are driven by the direct Consumer and Merchant interaction. Cardholder-Initiated Transactions SHALL contain the relevant cryptography generated during the payment interaction. Token Cryptogram validation can be distributed to any entity with the necessary validation keys in accordance with Token Programme policies and processes.

To successfully apply the Token Domain Restriction Controls, a Merchant-Initiated Transaction SHOULD refer to the original Cardholder-Initiated Transaction using the Token Control Fields and related data as well as including identification of the type of Merchant-Initiated Transaction being presented.

To further extend the application of Token Cryptogram-based Token Domain Restriction Controls to Merchant-Initiated Transactions, a Merchant-Initiated Transaction SHOULD include a unique Token Cryptogram for each Merchant-Initiated Transaction. When Token Cryptograms are present in Merchant-Initiated Transactions, the Token Cryptogram SHALL contain the relevant cryptography generated during the preparation for Token Processing. Token Cryptogram validation can be distributed to any entity with the necessary validation keys in accordance with Token Programme policies and processes.

The results of the application of Token Domain Restriction Controls SHALL be made available to the Card Issuer.

10.7.1 Token Cryptogram

When present in a Cardholder-Initiated Transaction or Merchant-Initiated Transaction, Token Cryptograms SHALL be validated during Token Processing. This is to ensure the authenticity of the transaction and the integrity of the data used in the generation of the Token Cryptogram.

10.7.2 POS Entry Mode

POS Entry Mode Code field values SHALL be used to limit the use of Payment Tokens to only those values agreed between the Token Service Provider and the Token Requestor during or after Token Requestor registration.

10.7.3 Merchant Identifiers

When the Merchant is the Token Requestor, Merchant-related fields in the existing ISO messages (see Section 9 Payment Token Fields Used in ISO 8583 and 20022 ATICA Messages) SHOULD be used to constrain the use of a Payment Token. This is accomplished by comparing data in one or more transaction fields in the Token Processing messages with controls established in the Token Vault and associated with the Token Requestor.

Merchants that are Token Users SHOULD be identified by the Merchant Identifiers during Token Processing.

10.7.4 Original Transaction Reference

For Merchant-Initiated Transactions, the Original Transaction Reference refers to the original Cardholder-Initiated Transaction. This is an existing payment processing field that is passed during Token Processing. Original Transaction Reference field values SHOULD be used to limit the use of Payment Tokens in Merchant-Initiated Transactions.

10.7.5 Merchant-Initiated Transaction Identifier

The identification of a Merchant-Initiated Transaction SHOULD be present in accordance with the EMV® Best Practices Document – Recommendations for EMV® Processing for Industry-Specific Transaction Types.

10.7.6 Application of Token Domain Restriction Controls

The Token Control Fields for Cardholder-Initiated Transactions are listed in Table 10.5.

Table 10.5: Token Control Fields for Cardholder-Initiated Transactions

Token Control Field	R/C/O	Condition / Option	Comment
Token Cryptogram	C	Required for EMV based and application based commerce in Cardholder-Initiated Transactions Optional for all other Cardholder-Initiated Transactions	
POS Entry Mode	R		Indicates the Token Presentment Mode
Merchant Identifiers	O	May be present for e-commerce transactions	

R – Required, C – Conditional, O – Optional

The Token Control Fields for Merchant-Initiated Transactions are listed in Table 10.6.

Table 10.6: Token Control Fields for Merchant-Initiated Transactions

Token Control Field	R/C/O	Condition / Option	Comment
Token Cryptogram	O	Optional for all Merchant-Initiated Transactions	If used, each Token Cryptogram must be unique for each Merchant-Initiated Transaction
POS Entry Mode	R		Indicates Token Presentment Mode
Original Transaction Reference	C	Required if created for the original Cardholder-Initiated Transaction	Refers to the original Cardholder-Initiated Transaction
Merchant-Initiated Transaction Identifier	C	Required when used as a Token Domain Restriction Control	Identifies the transaction as a Merchant-Initiated Transaction

R – Required, C – Conditional, O – Optional

10.8 De-Tokenise

The Payment Token SHALL be de-tokenised to the underlying PAN in the incoming Token Authorisation prior to sending the PAN Authorisation to the Card Issuer.

This SHALL include a verification of the state of the Payment Token / Token Expiry Date affiliation with the underlying PAN / PAN Expiry Date maintained in the Token Vault, including expiry date validation, and successfully return the underlying PAN / PAN Expiry date when an active Payment Token is found. This process may also include other controls defined for the Payment Token.

It is possible that De-Tokenisation could be coupled with the application of Token Domain Restriction Controls or managed as an independent function as defined in Section 10.7 Token Domain Restriction Controls.

The fields and data required for De-Tokenisation are defined in Table 10.7.

Table 10.7: Fields Included in De-Tokenisation Requests

Field Content	Field Name	R/C/O	Condition / Option	Comment
Payment Token	PAN	R		
Token Expiry Date	PAN Expiry Date	R		

R – Required, C – Conditional, O – Optional

The results of successful De-Tokenisation will include retrieval of data contained in the Token Vault that SHALL be provided to the Card Issuer. The output from successful De-Tokenisation is defined in Table 10.8.

Table 10.8: Fields Included in De-Tokenisation Responses

Field Content	Field Name	R/C/O	Condition / Option	Comment
PAN	PAN	R		Underlying PAN from Token Vault
PAN Expiry Date	PAN Expiry Date	R		Expiry date associated with the underlying PAN. Replace Token Expiry Date with PAN Expiry Date

Field Content	Field Name	R/C/O	Condition / Option	Comment
Token Requestor ID	Payment Network Specific	R		Payment Token related data
Payment Token	Payment Network Specific	R		
Token Expiry Date	Payment Network Specific	O		Payment Token related data
Token Assurance Method	Payment Network Specific	R		Payment Token related data
Token Assurance Data	Payment Network Specific	O		Payment Token related data
Payment Account Reference	Payment Account Reference	C	Required if PAR Field and PAR Data are supported by the Token Service Provider	The Payment Account Reference associated with the underlying PAN

R – Required, C – Conditional, O – Optional

10.9 Tokenise

The value of the PAN field in the Token Authorisation response is restored to the Payment Token contained in the incoming Token Authorisation request.

Note that for some EMV based transactions, a response cryptogram using the Payment Token is generated, and returned in the Token Authorisation response using an existing field.

10.10 PAN Authorisation

Once a Payment Token has been de-tokenised, the final request step is to initiate a PAN Authorisation, destined for the Card Issuer's authorisation system. PAN Authorisation processing may include Payment Token related data. The Card Issuer completes the PAN-

level and account-level validation and the authorisation check, and returns the PAN in the authorisation response.

For the purposes of Token Processing, the fields and data associated with PAN Authorisation requests are defined in Table 10.9. These are included with other transaction fields that are created and passed following existing message standards.

Table 10.9: Fields Included in PAN Authorisation Requests

Field Content	Field Name	R/C/O	Condition / Option	Comment
PAN	PAN	R		Underlying PAN from Token Vault
PAN Expiry Date	PAN Expiry Date	R		Expiry date associated with the underlying PAN
Token Presentment Mode	POS Entry Mode	R		Payment Token related data
Token Requestor ID	Payment Network Specific	R		Payment Token related data
Payment Token	Payment Network Specific	R		
Token Expiry Date	Payment Network Specific	O		Payment Token related data
Token Assurance Method	Payment Network Specific	C	Required if provided by Payment Network	Payment Token related data
Token Assurance Data	Payment Network Specific	O		Payment Token related data
Payment Account Reference	Payment Account Reference	O	May be present if available to the Token Service Provider	The Payment Account Reference associated with the PAN

R – Required, C – Conditional, O – Optional

For the purposes of Token Processing, the fields and data associated with PAN Authorisation responses are defined in Table 10.10. These are included with other transaction fields that are created and passed following existing message standards.

Table 10.10: Fields Included in PAN Authorisation Responses

Field Content	Field Name	R/C/O	Condition / Option	Comment
PAN	PAN	R		
Payment Account Reference	Payment Account Reference	C	Required if PAR Field and PAR Data are supported	The Payment Account Reference associated with the PAN

R – Required, C – Conditional, O – Optional

10.11 Capture Processing

The overall capture processes performed by existing ecosystem entities are not impacted by this technical framework. These processes continue with Payment Tokenisation data and are performed by existing entities.

Entities who define Payment Tokenisation requirements for capture processing SHOULD accommodate the Payment Tokenisation fields applicable to the clearing message requirements in the capture file definition and processing.

A Merchant or other entity on its behalf populates the capture file using data from the authorisation process. The Payment Token SHALL be included in the existing PAN field of the capture file. Additional Payment Tokenisation fields SHOULD be included according to the applicable capture file message specifications.

Clearing message specifications SHOULD be used by Acquirers to determine the changes for their capture processing message specifications.

10.12 Clearing

The overall process of clearing performed by existing ecosystem entities is not impacted by Payment Tokenisation. These processes continue with Payment Tokenisation data and includes the addition of De-Tokenisation and an optional application of Token Domain Restriction Controls.

Clearing processes are Payment System dependent and use a variety of different models within a Payment Network, such as single message and dual message. For the purposes of

this technical framework, the clearing function is limited to reflect the PAN and Payment Token received by the Card Issuer.

Clearing messages flow from the Acquirer to the Payment Network and from the Payment Network to the Card Issuer. Payment Tokenisation may affect the entities involved in clearing message processing and impacts the associated clearing data. The extent of the impact may vary by Token Programme and is dependent on the implementation specific approaches.

The Payment Token SHALL be included in the existing PAN field of the clearing file by the Acquirer. Additional Payment Tokenisation fields SHALL be included according to the applicable clearing file message specifications.

The application of Token Domain Restriction Controls SHOULD be performed on each clearing file record containing a Payment Token.

De-Tokenisation SHALL be performed and provides the underlying PAN to the Card Issuer for posting to the Payment Account. The status of the Payment Token SHOULD be verified prior to onward notification of PAN information.

Each record in the clearing file SHALL be augmented with the underlying PAN during De-Tokenisation. The Payment Token SHOULD be included in the clearing file record.

Payment Tokenisation impacts to clearing message specifications SHALL be communicated by applicable Payment Networks.

10.13 Exception Processing

Chargeback messages are impacted by this technical framework. The extent of the impact varies by Payment System and will be defined in the chargeback message specifications communicated by participating Payment Networks as part of their implementation of Payment Tokenisation solutions that are based on this technical framework. It is the responsibility of the Payment Network to define the specific Card Issuer requirements for processing exception and chargeback messages.

The Payment Network SHALL send the chargeback record to the Acquirer, replacing the PAN with the Payment Token.

***** END OF DOCUMENT *****