EMV®*
Payment Tokenisation Specification

Technical Framework

Version 1.0
March 2014

* EMV is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo.

Contents

Figures

Tables

1 Introduction

The purpose of this document is to provide a detailed technical specification for industry-aligned and interoperable Payment Tokenisation solutions that will benefit Acquirers, Merchants, Card Issuers, and Cardholders.

This specification describes the Payment Tokenisation landscape, defines key roles of the entities necessary to support Payment Tokenisation, identifies impacts of this specification, specifies the required and optional data fields associated with Token requests, Token issuance and provisioning, transaction processing, and identifies necessary application programming interfaces (APIs).

This specification is also intended to provide a detailed description of the Payment Tokenisation ecosystem, terminology definitions, key responsibilities, and controls specific to each entity within the ecosystem. In addition, this document provides potential use cases, related transaction flows, and the standardisation of required and optional fields within these transaction flows across traditional payment functions, such as authorisation, capture, clearing, and exception processing.

1.1 Overview

The payments industry 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 unauthorised use of Cardholder account data and to reduce cross-channel fraud for card-not-present and emerging transaction environments which combine elements of card-present and card-not-present transactions. Payment Tokenisation systems hold substantial promise to address these needs.

Payment Tokens are surrogate values that replace the Primary Account Number (PAN) in the payments ecosystem. Payment Tokens may be used to originate payment transactions, while non-Payment Tokens may be used for ancillary processes, such as loyalty tracking. This specification describes the minimum requirements for the creation and use of Payment Tokens. While this specification does not address non-Payment Tokens, it does not preclude their use.

Payment Tokens may be used with all Cardholder Verification Methods (CVMs), including signature, online and offline PIN, and no CVM. If an online PIN is used with a Payment Token, in accordance to ISO 9564-1 PIN Block Format 0 or Format 3, the PIN Block would include the Payment Token in lieu of the PAN. The Token Service Provider (refer to Section 3.2 Token Service Provider) is responsible for ensuring that the Card Issuer receives the PIN Block with the PAN or Payment Token, as appropriate, for validation.

In order for Payment Tokens to provide improved protection against misuse, the Payment Token is limited to use in a specific domain, such as to a specific Merchant or channel. These underlying usage controls are a key benefit of Payment Tokens and this specification describes methods for their implementation.

Additionally, at the time a Payment Token is issued, steps may be taken to ensure that the Payment Token is replacing a PAN that was legitimately being used by the Token Requestor. This process is known as Identification and Verification (ID&V) and is performed each time a Payment Token is requested. Different types of ID&V may be performed, resulting in corresponding levels of Token Assurance. For example, no or minimal ID&V performed should result in a low assurance Payment Token, while a high level of ID&V would likely result in a high assurance Payment Token.

There are benefits for all stakeholders in the payments ecosystem that will help encourage adoption of Payment Tokens:

- 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 databases will be less appealing targets given their limitation to a specific domain. Acquirers and Merchants may also benefit from the higher assurance levels that Payment Tokens offer.
- Payment processing networks will be able to adopt an open specification that facilitates interoperability and helps reduce data protection requirements for the Payment Network and its participants.

1.2 Audience

This document is intended for use by all participants in the payment industry ecosystem, such as Card Issuers, Merchants, Acquirers, Payment Networks, Payment Processors, and third-party service providers.

1.3 Normative References

Table 1-1 lists references mentioned in this document that may be used to implement Token payment processing. The latest version applies unless a publication date is explicitly stated.

Table 1-1: Normative References

Reference	Document Title
ISO 7812	Identification cards — Identification of issuers
ISO 8583	Financial transaction card originated messages — Interchange message specifications
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
ISO 27001	Information technology — Security techniques — Information security management systems
PCI DSS	Payment Card Industry Data Security Standard

1.4 Terms

The terms SHALL and SHALL NOT indicate mandatory requirements of the specification. The terms SHOULD and SHOULD NOT indicate guidelines recommended by this specification.

1.5 Abbreviations

Table 1-2: Abbreviations

Abbreviation	Definition
API	Application Programming Interface
AVS	Address Verification Service

Abbreviation	Definition
ICC	Integrated Circuit Card
NFC	Near Field Communication
TEE	Trusted Execution Environment

1.6 Definitions

Table 1-3: Definitions

Term	Definition
3-D Secure	Protocol for Cardholder authentication in e-commerce
Agent	An entity appointed by the Card Issuer to perform specific functions on behalf of the Card Issuer. Some examples of these functions include card processing, Cardholder verification using the 3-D Secure protocol, and Token Service.
Bank Identification Number (BIN)	BINs are assigned by Payment Networks to Card Issuers. BINs are consistent with ISO 7812 requirements to identify the Payment Network based on the BIN and associated account ranges.
BIN Controller / Manager	An entity that controls the issuance and allocation of ISO BINs that will be used to issue Payment Tokens according to this specification.
Card	Any Cardholder device or form factor, such as a mobile phone, that can be used to initiate financial transactions.
Cardholder	Any individual that has been issued a financial account provisioned to a Card by a Card Issuer

Term	Definition
Card Acceptor	The entity that initiates a payment transaction and presents transaction data to the Acquirer, typically a Merchant
Card Acceptor ID	The identification value for the Card Acceptor.
Card Issuer	A financial institution or its Agent that issues the Card to Cardholders.
Card Issuer Access Control Server (ACS)	The Card Issuer's Agent that provides a 3-D Secure service for ID&V.
De-Tokenisation	The process of redeeming a Payment Token for its associated PAN value based on the Payment Token to PAN mapping stored in the Token Vault. The ability to retrieve a PAN in exchange for its associated Payment Token should be restricted to specifically authorised entities, individuals, applications, or systems.
Identification and Verification (ID&V)	A valid method through which an entity may successfully validate the Cardholder and the Cardholder's account in order to establish a confidence level for Payment Token to PAN / Cardholder binding. Examples of ID&V methods are: • Account verification message • Risk score based on assessment of the PAN • Use of one time password by the Card Issuer or its Agent to verify the Cardholder
Payment Network	An electronic payment system used to accept, transmit, or process transactions made by payment cards for money, goods, or services, and to transfer information and funds among Issuers, Acquirers, Payment Processors, Merchants, and Cardholders.

Term	Definition
Payment Processor	An entity that provides payment processing services for Acquirers and / or Issuers. A Payment Processor may in addition to processing provide operational, reporting and other services for the Acquirer or Card Issuer.
Payment Token	Payment Tokens can take on a variety of formats across the payments industry. For this specification, the term Payment Token refers to a surrogate value for a PAN that is a 13 to 19-digit numeric value that must pass basic validation rules of an account number, including the Luhn check digit. Payment Tokens are generated within a BIN range that has been designated as a Token BIN Range and flagged accordingly in all appropriate BIN tables. Payment Tokens must not have the same value as or conflict with a real PAN.
Primary Account Number (PAN)	A variable length, 13 to 19-digits, ISO 7812-compliant account number that is generated within account ranges associated with a BIN by a Card Issuer.
Requested Token Assurance Level / Assigned Token Assurance Level	The Requested Token Assurance Level is requested from the Token Service Provider by the Token Requestor. Requested Token Assurance Level is a field included in the Token Request. The Assigned Token Assurance Level is the actual value assigned by the Token Service Provider as the result of the ID&V process and is provided back to the Token Requestor in response to the Token Request.

Term	Definition
Token Assurance Level	A value that allows the Token Service Provider to indicate the confidence level of the Payment Token to PAN / Cardholder binding. It is determined as a result of the type of Identification and Verification (ID&V) performed and the entity that performed it. It may also be influenced by additional factors such as the Token Location. The Token Assurance Level is set when issuing a Payment Token and may be updated if additional ID&V is performed. The Token Assurance Level value is defined by the Token Service Provider.
Token BIN	A specific BIN or range within a BIN that has been designated only for the purpose of issuing Payment Tokens and is flagged accordingly in BIN tables.
Token BIN Range	A unique identifier that consists of the leading 6 to 12 digits of the Token BIN. The Token BIN Range may be designed to carry the same attributes as the associated Card Issuer card range and will be included in the BIN routing table distributed to the participating Acquirers and Merchants to support routing decisions.
Token Cryptogram	A cryptogram generated using the Payment Token and additional transaction data to create a transaction-unique value. The calculation and format may vary by use case.
Token Domain	The types of transactions for which a Payment Token may be used. Token Domains may be channel-specific (e.g. NFC only), Merchant-specific, digital wallet-specific, or a combination of any of the above.

Term	Definition
Token Domain Restriction Controls	A set of parameters established as part of Payment Token issuance by the Token Service Provider that will allow for enforcing appropriate usage of the Payment Token in payment transactions. Some examples of the controls are: • Use of the Payment Token with particular presentment modes, such as contactless or e-commerce • Use of the Payment Token at a particular Merchant that can be uniquely identified • Verification of the presence of a Token Cryptogram that is unique to each transaction
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 transaction processing to ensure interoperability and minimise the impact of Tokenisation implementation. The Token Expiry Date is a 4-digit numeric value that is consistent with the ISO 8583 format.
Token Interoperability	The process to ensure that the processing and exchanging of transactions between parties through existing interoperable capabilities is preserved when using Payment Tokens with new fields and field values that are defined in this specification.
Token Issuance	The process by where a Payment Token is created and delivered to a Token Requestor. Payment Tokens may be issued for multiple use or for single use.

Term	Definition
Token Location	An indication of the intended mode of storage for a Payment Token and any related data, provided by a Token Requestor when requesting a Payment Token from a Token Service Provider. The security of this location may influence the Token Assurance Level that can be assigned to a Payment Token. Due diligence of the security provided by Token Requestors is the responsibility of each Token Service Provider and assignation of a location type to each Token Requestor will be at the discretion of each Token Service Provider. Currently identified location types are: • Remote storage: An example would be a card-on-file database • EMVCo / Payment Network type approved secure element / ICC • Local Device storage: An example would be Payment Token data stored using the standard data storage mechanisms of a consumer controlled device • Local hardware secured storage: An example would be using a TEE to ensure appropriately restricted access to data • Remote hardware secured storage: An example would be ISO 13491 compliant storage More categories of storage locations may be added over time.

Term	Definition
Token Presentment Mode	The mode through which a Payment Token is presented for payment. This information will resolve to an existing field called Point of sale (POS) Entry Mode as defined in ISO 8583 messages and that will be enhanced to include new potential values as part of this specification. Each Payment Network will define and publish any new POS Entry Mode values as part of its existing message specifications and customer notification procedures. In addition to supporting existing values for contactless, new values may be defined, if not already in existence, by participating Payment Networks for: • Server initiated (Card-on-file use case) • Scan (Optical)
Token Processing	Transaction processing in which a Payment Token is present in lieu of the PAN and is processed from the point of interaction through to the Payment Network and Token Service Provider's Vault for De-Tokenisation in order to allow for transaction completion. Token Processing may span payment processes that include authorisation, capture, clearing, and exception processing.
Token Provisioning	The act of delivering the Payment Token and related values, potentially including one or more secret keys for cryptogram generation, to the Token Location.
Token Reference ID	A value used as a substitute for the Payment Token that does not expose information about the Payment Token or the PAN that the Payment Token replaces.

Term	Definition
Token Request	The process in which a Token Requestor requests a Payment Token from the Token Service Provider. As a consequence of this action, ID&V may be performed using a Token Request Indicator to show that the ID&V mechanism being used is for the purpose of a Token Request, rather than for some other purpose.
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) API to inform the Card Issuer of the reason that the account status check is being performed.
Token Requestor	An entity that is seeking to implement Tokenisation according to this specification and initiate requests that PANs be Tokenised by submitting Token Requests to the Token Service Provider. Each Token Requestor will be registered and identified uniquely by the Token Service Provider within the Tokenisation system.
Token Requestor Registration	A Token Service Provider function that formally processes Token Requestor applications to participate in the Token Service programme. The Token Service Provider may collect information pertaining to the nature of the requestor and relevant use of Payment Tokens to validate and formally approve the Token Requestor and establish appropriate Token Domain Restriction Controls. Successfully registered Token Requestors will be assigned a Token Requestor ID that will also be entered and maintained within the Token Vault.

Term	Definition
Token Service	A system comprised of the key functions that facilitate generation and issuance of Payment Tokens from the Token BINs, and maintain the established mapping of Payment Tokens to PAN when requested by the Token Requestor. It also includes the capability to establish the Token Assurance Level to indicate the confidence level of the Payment Token to PAN / Cardholder binding. The service also provides the capability to support Token Processing of payment transactions submitted using Payment Tokens by de-tokenising the Payment Token to obtain the actual PAN.
Token Service Provider	An entity that provides a Token Service comprised of the Token Vault and related processing. The Token Service Provider will have the ability to set aside licensed ISO BINS as Token BINs to issue Payment Tokens for the PANs that are submitted according to this specification.
Token Vault	A repository, implemented by a Tokenisation system that maintains the established Payment Token to PAN mapping. This repository is referred to as the Token Vault. 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 by the Token Service Provider to apply domain restrictions or other controls during transaction processing.
Tokenisation	A process by which the Primary Account Number (PAN) is replaced with a surrogate value called a Payment Token. Tokenisation may be undertaken to enhance transaction efficiency, improve transaction security, increase service transparency, or to provide a method for third-party enablement.

1.7 Further Information

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

2 Constraints

2.1 Constraints of the Ecosystem

This specification is designed to work within a number of constraints of the payments ecosystem, including roles of various entities, the transaction flows, definitions, and associated use cases. These constraints include the following:

- This specification is not intended to replace or interfere with any international, national, regional or local laws and regulations; those governing requirements supersede any industry standard.
- This specification does not preclude existing Acquirer or other third-party implemented Payment Token solutions in which these entities generate Payment Tokens and perform Payment Token to PAN mapping within their ecosystem.
- Additional data (e.g. Full or Partial PAN) may be provided to the Acquirer and / or Merchant based on each Payment Network's policy and business requirements. It is important to note that delivering the Full PAN to Merchants could lessen the value the token brings to the Merchant.
- Product attributes, such as product type (for example, debit or credit), are preserved for Tokenised transactions to ensure continuity of existing business requirements related to the transparency of product attributes to payment industry participants.
- Token BIN Ranges and assignment of Payment Tokens from these BIN ranges will be made available to the parties accepting the transaction to make routing decisions.
- The ongoing changes to Payment Token to PAN mapping due to lifecycle events, such as PAN updates, lost or stolen devices, and deactivation of the Payment Token due to customer relationship termination with the Token Requestor, will be accommodated by the Token Service when implemented according to this specification.
- An entity providing a Token Service Provider capability must be cognisant of the payment processing environment in which that service will be provided and ensure that the introduction of Tokenisation into that environment by the Token Service Provider does not have an adverse effect on existing processes, e.g. Card Issuer portfolio conversions, Merchant conversions, and local network / on-us transaction routing.

3 Tokenisation Ecosystem Environment

3.1 Payment Token Ecosystem

The implementation of Payment Token solutions as outlined by this specification, and in a manner consistent with this specification itself, involves a number of roles within the ecosystem. Some are existing roles within the traditional payments industry, and others are new roles introduced by this specification.

The following diagrams provide an overview of the various roles involved in the Payment Token ecosystem. Each of the Payment Token roles and functions are described in more detail in subsequent sections.

Figure 1: Payment Token Provisioning Overview

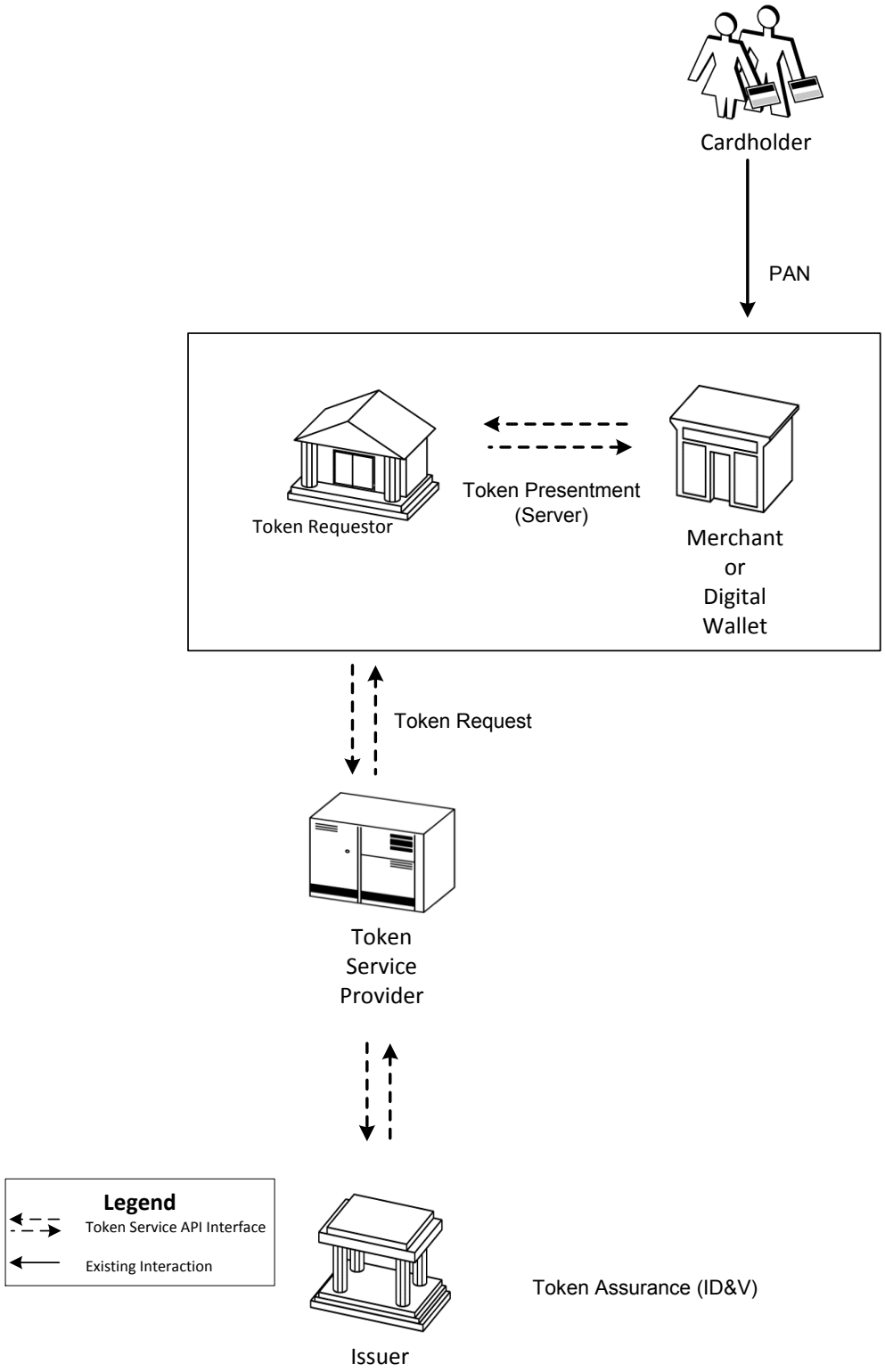
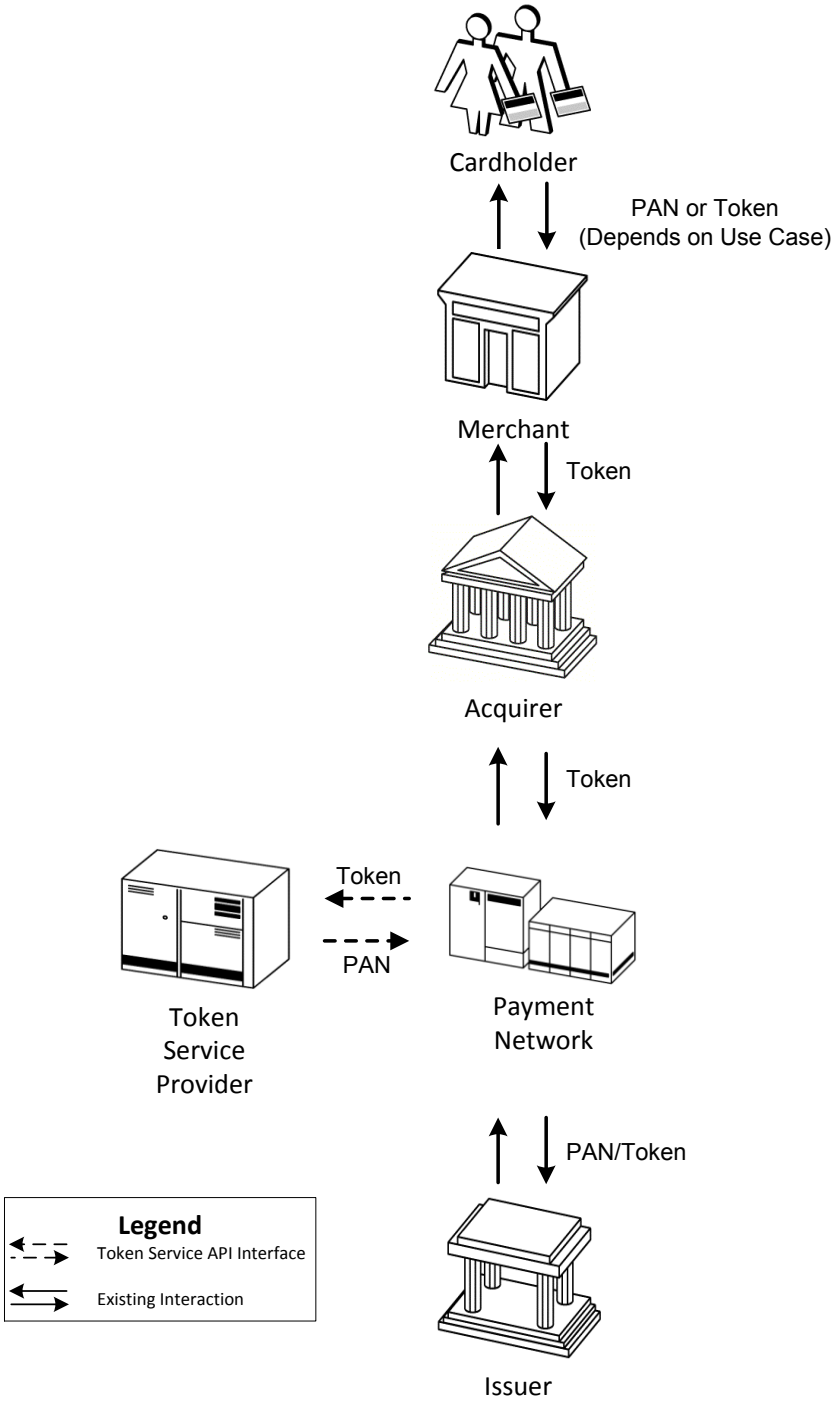


Figure 2: Payment Token Transaction Overview



3.2 Token Service Provider

Token Service Providers are entities within the Tokenisation ecosystem that are authorised to provide Payment Tokens to registered Token Requestors.

Token Service Providers are responsible for a number of discrete functions in their capacity as the authorised party for issuance of Payment Tokens. These responsibilities include, but are not limited to:

- Ongoing operation and maintenance of the Token Vault
- Payment Token generation and issuance
- Application of security and controls
- Payment Token provisioning
- Token Requestor registry functions

Token Service Providers are responsible for building and managing their own proprietary Token Requestor APIs, Token Vaults, Token provisioning platforms, and Token registries. This specification itself does not describe in detail the individual functional requirements that comprise each of these proprietary platforms and related systems. However, Token Service Providers SHALL ensure that Token BINs or Token BIN ranges are managed distinctly from traditional BINs or BIN ranges, in part to avoid any inadvertent overlap of PANs and Payment Tokens.

3.3 Cardholder

This specification does not change the role of the Cardholder. Cardholders will continue to be issued Cards and card accounts by their Card Issuer. In most cases, Cardholders are not expected to know that a Payment Token has been issued to represent their account. Optionally, Token Requestors may choose to make Cardholders aware and may also ask the Cardholders to participate in the ID&V process for Token Assurance.

3.4 Card Issuer

Card Issuers will continue to maintain their current role in terms of owning the account relationship with the Cardholder, as well as owning authorisation and ongoing risk management in the Payment Token ecosystem. Any Card Issuer-implemented Token Service SHOULD consider following this specification, in order to remain interoperable and consistent with solutions that are deployed using this specification.

3.5 Merchant

Merchants will continue to maintain their current role, but depending upon the specific use case, may be the recipient of a Payment Token in lieu of a PAN, such as in a NFC at point of sale use case. Merchants may also be a Token Requestor, such as in a Card-on-file use case. Use cases are defined in subsequent sections of this specification. Merchants will continue to process all transactions in the same manner as they do today, including authorisation and capture, and will need to implement any required or optional data elements as referenced in this specification and any processing requirements established by the Merchant's Acquirer or Payment Processor. In use cases where the Merchant is also a Token Requestor, the Merchant will need to accommodate the implementation of Token Service APIs that are referenced in this specification and subsequently implemented by a Token Service Provider as part of its solution.

For more information, refer to Section 9 Payment Token Transaction Flows.

3.6 Acquirer

Acquirers will process all transactions in the same manner as they do today, including authorisation, capture, clearing, and exception processing. Additional fields may be required to support the specification.

3.7 Payment Network

Payment Networks continue in their current role and may additionally perform the Token Service Provider function, including all of the associated roles defined for Token Service Providers within this specification.

Payment Networks performing as Token Service Providers are responsible for building and managing their own proprietary Token Requestor APIs, Token Vaults, Token provisioning platforms, and Token registries as outlined in Section 3.2 Token Service Provider. Payment Networks are also responsible for defining and publishing the authorisation, clearing, and exception processing message impacts of their Token Service.

Payment Networks that are not Token Service Providers SHOULD support the implementation of processing functions that allow for the exchange of messages with the Token Service Provider for De-Tokenisation purposes to ensure Payment Token Interoperability.

3.8 Token Requestor

Payment Token Requestors may be traditional participants within the payments industry or newly emerging participants. Potential Token Requestors include, but are not limited to:

- Card-on-file Merchants
- Acquirers, Acquirer Processors, and payment gateways on behalf of Merchants
- Payment enablers, such as original equipment manufacturer (OEM) device manufacturers
- Digital wallet providers
- Card Issuers

Token Requestors will be required to register with Token Service Providers and comply with their proprietary registry requirements, systems, and processes. After successful registration with a Token Service Provider, the Token Requestor will be assigned a Token Requestor ID.

Token Requestors, after registration with a given Token Service Provider and assignment of a Token Requestor ID, will implement the specified Token API. After the Token Requestor has installed the Token API in production, the Token Requestor will be able to initiate Payment Token Requests in accordance with the processes and technologies specified within the API. When Payment Token Requests initiated by a Token Requestor are processed by the Token Service Provider, Payment Tokens will be issued.

4 Payment Token Specification Data Elements

4.1 Data Elements

As part of this specification, the following data elements may be used in transactions that are initiated with a Payment Token. These data elements will be mapped and flow through the existing payment messaging infrastructure.

Although each data element may be Required, Conditional or Optional in the context of a particular message or API call, in order to ensure interoperability between Payment Networks, all participating Payment Networks SHALL support all of these data elements for transaction processing.

Table 4-1: Payment Token Specification Data Elements

Field Name	ISO 8583 Field	Length	Format	Comment
Payment Token	2	13-19	Numeric	The Payment Token number refers to a surrogate value for a PAN that is a 13 to 19-digit numeric value that passes basic validation rules of an account number, including the Luhn check digit. Payment Tokens are generated within a BIN range or Card range that has been designated as a Token BIN Range and flagged accordingly in all appropriate BIN tables. Payment Tokens are generated such that they will not have the same value as or conflict with a real PAN. **Transaction messages** • The Payment Token number will be passed through the authorisation, capture, clearing, and exception messages in lieu of the PAN. • The Payment Token number may optionally be passed from the Token

Field Name	ISO 8583 Field	Length	Format	Comment
				Service Provider to the Card Issuer as part of the authorisation request.
Token Expiry Date	14	4	Numeric	The expiration date of the Payment Token that is generated by and maintained in the Token Vault. The Token Expiry Date field carries a 4-digit numeric value that is consistent with the ISO 8583 format. **Transaction messages** • The Token Expiry Date is passed in lieu of PAN Expiry Date. • The value is replaced by the Token Service Provider with the PAN Expiry Date which is then passed to the Card Issuer as part of the authorisation request.
Last 4 Digits of PAN	Payment Network Specific	4	Numeric	The last four digits of the PAN to be provided optionally through the Acquirer to the Merchant for customer service usage such as being printed on the consumer receipt.
PAN Product ID	Payment Network Specific	3	Alpha-numeric	The PAN Product ID is an optional identifier used for determining the type of Card product that was tokenized. It may be included in cases where transparency of this information is necessary. **Transaction messages** The PAN Product ID may optionally be passed from the Token Service Provider to the Acquirer as part of the authorisation response.
POS Entry Mode	22	2	Numeric	This specification uses the POS Entry Mode field to indicate the mode through which the Payment Token is presented for

Field Name	ISO 8583 Field	Length	Format	Comment
				payment. Each Payment Network will define and publish any new POS Entry Mode values as part of its existing message specifications and customer notification procedures. **Transaction messages** POS Entry Mode is an existing field that will be passed through the authorisation, capture, clearing, and exception messages.
Token Requestor ID	Payment Network Specific	11	Numeric	This value uniquely identifies the pairing of Token Requestor with the Token Domain. Thus, if a given Token Requestor needs Tokens for multiple domains, it will have multiple Token Requestor IDs, one for each domain. It is an 11-digit numeric value assigned by the Token Service Provider and is unique within the Token Vault: • Positions 1-3: Token Service Provider Code, unique to each Token Service Provider • Positions 4-11: Assigned by the Token Service Provider for each requesting entity and Token Domain **Transaction messages** Token Requestor ID can be optionally passed through the authorisation, capture, clearing, and exception messages.
Token Assurance Level	Payment Network Specific	2	Numeric	Token Assurance Level is a value that allows the Token Service Provider to indicate the confidence level of the Payment Token to PAN / Cardholder binding. It is determined as a result of the type of ID&V performed and the entity that performed it.

Field Name	ISO 8583 Field	Length	Format	Comment
				The Token Assurance Level is set when issuing a Payment Token and may be updated if additional ID&V is performed. It is a two-digit value ranging from **00** which indicates the Payment Token has no ID&V that has been performed to a value of **99** indicating the highest possible assurance. The specific method to produce the value is defined by the Token Service Provider. **Transaction messages** • Token Assurance Level will be provided by the Token Service Provider. • The value may be optionally passed to the Card Issuer as part of the authorisation request. • The value may optionally be passed to the Acquirer / Merchant in the authorisation response, capture, clearing, and exception processing messages.
Token Assurance Data	Payment Network Specific	Variable	Binary	This data provided by the Token Service Provider contains supporting information for the Token Assurance Level. **Transaction messages** This data may be optionally passed to the Card Issuer as part of the authorisation request.
Token Cryptogram	Payment Network Specific	Variable	Binary	This cryptogram is uniquely generated by the Token Requestor to validate authorised use of the Token. The cryptogram will be carried in different fields in the transaction message based on the type of transaction and associated use case: • NFC contactless transactions will carry

Field Name	ISO 8583 Field	Length	Format	Comment
				the Token Cryptogram in existing chip data fields. • Other transactions, such as those originating from a digital wallet, may carry the Token Cryptogram in an existing field. **Transaction messages** The Token Cryptogram will be passed in the authorisation request and validated by the Token Service Provider and / or the Card Issuer.
The following Data Element is used only as an optional field during ID&V between the Token Service Provider and the Issuer				
Token Request Indicator	Payment Network Specific / ID&V process specific	Variable	Payment Network Specific / ID&V process specific	An indicator used to indicate that the message is intended to authenticate the Cardholder during a Payment Token Request.

5 Token Service Provider Requirements

5.1 Introduction

This section describes the requirements that Token Service Providers need to implement to provide a Token Service that is consistent with this specification. Multiple responsibilities are assigned to Token Service Providers, including the Token Vault, Token Issuance, Token Assurance using ID&V methods, Token Service APIs, Token Processing functions, and Token Lifecycle Management.

Although the specification describes a direct relationship between Token Requestors and a Token Service Provider, it does not preclude an intermediary entity acting as an aggregator or gateway, providing representation for that Token Requestor to multiple Token Service Providers, so long as Token Domain Restriction Controls are maintained.

5.2 Token Vault Requirements

The Token Service Provider SHALL develop and operate a Token Vault that will provide the capability for generation and issuance of Payment Tokens, establish and maintain the Payment Token to PAN mapping, and provide underlying security and related processing controls, such as domain restrictions during transaction processing. The Token Vault provides the mechanism for Payment Token to PAN mapping to be made available during transaction processing such as authorisation, capture, clearing, and exception processing. Token Vaults need to maintain all associated Payment Tokens mapped to a given PAN throughout its lifecycle.

5.2.1 Payment Token Generation

The Token Service Provider generates Payment Tokens in response to Payment Token Requests. Payment Token generation SHALL be performed using only assigned Token BINs or range within BINs to ensure there is no possibility of generating Payment Tokens that conflict with a PAN. At the time of Payment Token generation, the Token Service Provider SHALL identify and store the Payment Token to PAN mapping for use in subsequent transaction processing in the Token Vault. The Token Vault SHALL also associate each generated Payment Token with the Token Requestor that initiated the request by capturing and storing the Token Requestor ID.

Traditional processing of business functions including authorisation, clearing, and exception processing will need to be integrated with the applicable Payment Network and related Token Vault solutions to ensure Token Service is performed in a manner that preserves interoperability and the ongoing integrity of these transaction processes.

Any Card Issuer-implemented Token Service SHOULD consider following this specification for interoperability and consistency with solutions that are deployed using this specification.

Payment Tokens that are generated SHALL include a Token Expiry Date. The Token Expiry Date SHALL meet the format requirements of a PAN Expiry Date. Payment Tokens SHALL be generated using Token BINs in such a way as to ensure the preservation of product and other attributes of the PAN throughout all existing transaction processes.

Payment Tokens that are generated in response to a Payment Token Request from a given Token Requestor are only valid for transactions within the Token Domain to which the Payment Token has been issued.

5.2.2 Payment Token Issuance and Provisioning

Payment Tokens SHALL be issued through the response to the Token Request from only a registered Token Requestor recognised by the Token Service Provider with a valid Token Requestor ID. Payment Token Requests SHALL be subject to a designated ID&V assurance method based on the Requested Assurance Level agreed to by the Token Requestor and the Token Service Provider.

Payment Token issuance may also involve provisioning of the Payment Token to the Token Requestor. Payment Token provisioning occurs after the Payment Token has been generated and the assurance steps are completed. The methodologies associated with the provisioning may be proprietary to each Token Service Provider and are outside the scope of this specification.

Payment Token provisioning is performed through an interface between the Token Requestor and the Token Service Provider.

Token Service Providers may also opt to implement Payment Token issuance and provisioning through the use of specially designated and flagged ISO 8583-based authorisation request messages to perform the Payment Token Request and transport ID&V information to the Token Service Provider for subsequent processing. In such a case, ISO 8583-based authorisation response messages can be used to return the Payment Token and associated Token Expiry Date back to the Token Requestor.

5.2.3 Security and Controls

Due to the sensitive nature of the data mappings that are stored and managed in them, Token Vaults SHALL be protected by strong physical and logical security measures per industry standards.

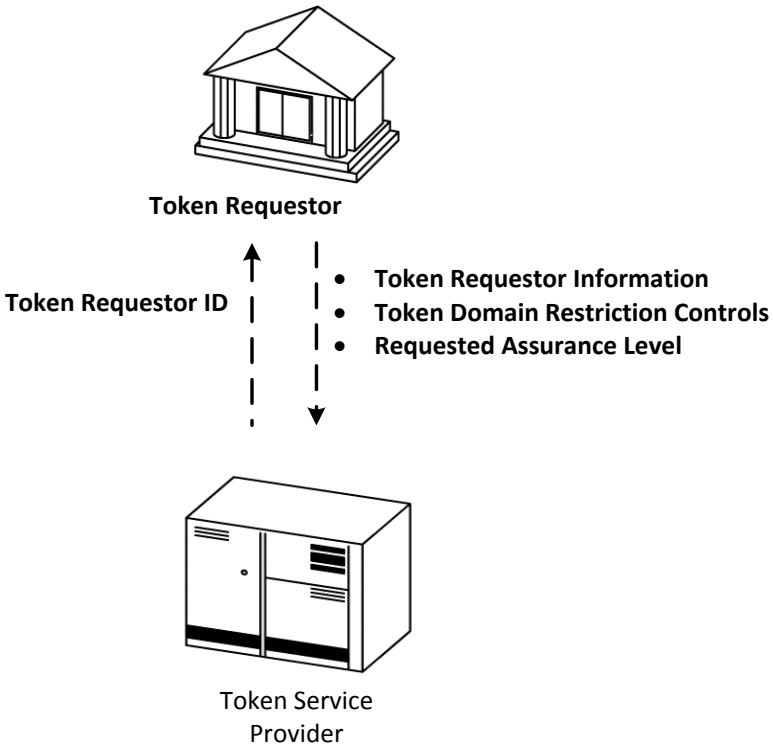
Token Service Providers, in conjunction with payment transaction processing, SHALL be responsible for restricting Token-based transactions to the appropriate domain associated with a given Token Requestor as determined at the time of Token Requestor registration.

Token Requestor Registration ensures the integrity of the Token Service by enrolling, approving, and registering entities as Token Requestors. The Token Service Provider SHALL assign at least one unique Token Requestor ID to a given Token Requestor, and SHALL be responsible for lifecycle management of Token Requestors and their associated Token Requestor IDs. As part of the registration, the Token Service Provider SHOULD also capture the requested Token Assurance Level and Token Domain Restriction Controls associated with a given Token Requestor and ensure that these domain restrictions are made available to the Token Vault to apply such restrictions during Payment Token transaction processing.

5.2.4 Token Requestor Registration

The Token Service Provider SHALL establish a process to register the entities that request designation as a Token Requestor. Entities that choose to be recognised as a Token Requestor for multiple Token Service Providers may register separately with each Token Service Provider, according to the proprietary processes established by each Token Service Provider.

Figure 3: Token Requestor Registration Process



Each Token Service Provider determines the information collected from the Token Requestor and establishes its own proprietary processes for collection, review, and approval. Information collected may include, among others, typical Know Your Customer (KYC) information, as well as Payment Token use cases that the enrolling Token Requestor will support, including any appropriate domain restrictions and other transaction controls that may be required to be implemented within the Token Vault.

The outcome of the registration function is an approval or decline decision on the registration application of the prospective Token Requestor. Approved Token Requestors are assigned a unique Token Requestor ID. Domain restrictions and other transaction controls SHALL be communicated to and coordinated with the Token Vault for implementation.

5.2.5 Token Assurance

The Token Service Provider SHALL determine the expected level of assurance associated with each approved Token Requestor, and based on use cases, define what types of ID&V are applied during the Payment Token Request and approval processes. The initial Token Assurance Level will be determined at time of Payment Token Request and be based on the type and outcome of the ID&V process. The Token Assurance Level may be updated subsequent to Payment Token issuance.

5.2.6 Token Domain Restriction Controls

To ensure that Payment Tokens are used as intended by the Token Requestor, additional controls are needed to manage and validate the underlying usage of the Payment Tokens. These controls SHALL be defined and implemented by the Token Service Provider based on conditions, including use cases and Token Domains, such as Merchant identifiers and POS Entry Modes that are identified during the Token Requestor registration process. These Token Domain Restriction Controls are intended to ensure that any exposure of Payment Tokens does not result in significant levels of subsequent fraud. The permitted Token Domain Restriction Controls for a given Token Requestor are driven in part by the Payment Token use cases specified at time of Token Requestor Registration and approved by the Token Service Provider. These Token Domain Restriction Controls SHALL be stored in the Token Vault or in a location with equivalent security protections. The actual Token Domain Restriction Controls are applied and executed by the Token Service Provider and its proprietary Token Vault.

5.2.6.1 Token Requestor ID

Each Token Requestor ID assigned by a Token Service Provider SHALL be unique and not conflict with other assigned Token Requestor IDs from that same Token Service Provider or another Token Service Provider.

Each Token Requestor SHALL be assigned a Token Requestor ID, one for each domain. It is an 11-digit numeric value assigned by the Token Service Provider with the following convention:

- Positions 1-3: Token Service Provider code, unique to each Token Service Provider
- Positions 4-11: Assigned by Token Service Provider for each requesting entity and Token Domain

A Token Service Provider code is assigned to each Token Service Provider and maintained by EMVCo. See the EMVCo website for additional information: www.emvco.com.

The Token Requestor ID is an underlying control data element that SHOULD be present in transactions. In use cases where the Token Requestor ID is passed to the Merchant, these transactions SHOULD not be permitted to successfully process if the Token Requestor ID present in the transaction does not match the Token Requestor ID for that Payment Token stored in the Token Vault.

5.2.6.2 POS Entry Modes

Other controls that are designed to restrict transactions associated with a specific Token Requestor include the use of POS Entry Mode values that are carried in the POS Entry Mode Code field to limit the use of Tokens to only those POS Entry Modes agreed to during Token Requestor Registration.

5.2.6.3 Merchant Information

In use cases where the Merchant may be the Token Requestor, Merchant-related data elements, such as the Card Acceptor ID in combination with Acquirer-identifying data elements, SHOULD be used to limit the use of a Payment Token by comparing these fields in the transaction processing messages with controls established in the Token Vault per information ascertained during Token Requestor Registration. One such use case would be Tokenisation of PANs held by Card-on-file Merchants.

5.2.7 Reports and Raw Data

The Token Service Provider SHOULD have the ability to provide reports or data output to reporting tools regarding approved, pending, or declined Token Requests, including any assigned Token Requestor IDs.

The Token Service Provider SHOULD also have the ability to provide data output related to Token-based transactions to reporting tools and applications and present the Payment Token and / or PAN as appropriate in the reporting output. Should Token Requestors be revoked or assigned new Token Requestor IDs, this information SHOULD also be subject to reporting and audit and be reconcilable with the Token Vault.

5.3 Acquirer Requirements

Acquirers SHOULD implement any required or optional data elements as referenced in this specification, and further defined by the supporting Payment Network's message specifications.

5.4 Payment Network Requirements

Payment Networks SHALL implement all of the fields, including both required and optional fields, defined in this specification within the context of their proprietary message specifications and communicate those changes through existing communication channels.

6 Token Assurance ID&V Methods

6.1 General

The Token Assurance ID&V Methods provide a set of functionalities and services that allow for a trusted association of the Payment Token to a PAN from an authorised Cardholder, in order to support secure and reliable payment transactions initiated with Payment Tokens.

This specification addresses key components of the Token Assurance Level, including ID&V methods, Token Assurance Levels derived from ID&V methods, and supporting Token Assurance Data.

The ID&V steps taken at the time of Token Issuance / Provisioning, along with the domain in which a Payment Token is used, are essential elements that determine the Token Assurance Level. The Token Assurance Level in turn may be used by the Token Service Provider to establish particular programmes, transaction classifications, or other proprietary business delineations. Any such programmes or classifications are outside the scope of this specification.

Two new data elements are used to communicate Payment Token Assurance and the ID&V steps performed on that Payment Token maintained by the Token Service Provider:

- Token Assurance Level
- Token Assurance Data

Each Token Service Provider SHALL implement methods and processes to communicate the Token Assurance Level and Token Assurance Data to the Card Issuer regarding the assurance level and the strength of the ID&V performed on that Payment Token to PAN / Cardholder binding.

6.2 Card Issuer Assurance Concepts and ID&V Methods

ID&V methods may be used singularly or in combination to provide a specific Token Assurance Level. These levels range from no assurance to high assurance depending on the ID&V methodology performed and the Token Service Provider that confirms the result of the assessment. The following are examples of ID&V methods:

- Account verification
- Token Service Provider risk score
- Token Service Provider risk score with Token Requestor data

- Card Issuer authentication of the Cardholder

Alternatively, ID&V need not be performed. In this case, a Token Requestor is offering no assurance of the authenticity of the use of card data and is merely requesting a Payment Token to represent that data.

Additional methods may be implemented at the discretion of the Token Service Provider.

The Token Service Provider SHALL implement one or more ID&V methods. Additionally, the Token Service Provider SHALL ensure that the ID&V method(s) appropriate for the Token Assurance Level are always performed when issuing a Token.

ID&V steps may be performed by the Token Service Provider, the Token Requestor, or a third party. In instances where the ID&V steps are performed by an entity other than the Token Service Provider, verifiable evidence SHALL be provided to prove that the steps were performed and the resulting outcomes were provided. Verifiable evidence may consist of any value provided to the Token Service Provider by the ID&V processing entity that the Token Service Provider may validate. The details of what constitutes verifiable evidence are outside the scope of this specification, but examples include a cryptogram or an authorisation code. These requirements apply to all ID&V methods, with the exception of conditions in which the ID&V is not performed. The Token Service Provider SHALL set the Token Assurance Level to the appropriate value on the basis of the ID&V performed (00 = no ID&V, 99 = highest assurance), and the Token storage and usage information provided by the Token Requestor at the time of Token Requestor Registration.

The following table provides derived Token Assurance Level based on ID&V steps performed. Additional ID&V methods may be defined in future supplements or revisions to this specification.

Table 6-1: ID&V Examples

ID&V Assurance Method	Assurance Performed By	Potential Uses
No ID&V performed	None	Card-on-file account number replacement with Token
Account verification ($0 authorisation, with or without AVS and Card Verification Numbers)	Token Requestor Token Service Provider	Card-on-file account number replacement with Token
Risk score derived from Token Service Provider	Token Service Provider	Medium assurance level supported with Token authentication data

ID&V Assurance Method	Assurance Performed By	Potential Uses
Risk score derived from Payment Token user data combined with Payment Network data	Token Service Provider	Medium to high assurance level supported with Token authentication data
Card Issuer authentication of the Cardholder	Card Issuer or Agent	High assurance level supported with Token authentication data to specific channel or domain

6.2.1 No ID&V Performed

The Token Assurance Level SHALL be set to the value of No Assurance when a Payment Token has been issued without any ID&V step performed at the time of Token Issuance. Depending on the Token use case and Token Service Provider rules, the Payment Token can still be used to initiate payment transaction, but will not carry any Token Assurance. Additional restrictions for using Tokens with no assurance level are explained in later sections of this specification.

6.2.2 Account Verification

This ID&V assurance method provides a basic account verification check to validate if the PAN is active and valid at the Card Issuer. Verification methods may include, but are not restricted to:

- $0 authorisation
- Card Verification Number validation
- Postal code and address verification, where supported

The account verification method may be initiated by either the Token Requestor and reported to the Token Service Provider through Token Service API, or by the Token Service Provider at the time of the Token issuance.

6.2.3 Token Service Provider Assurance

This ID&V assurance method involves the use of risk and authentication data maintained by the Token Service Provider to perform a risk-based assessment of the likelihood that the request to Tokenise a PAN is assured with sufficient level of confidence.

The Token Service Provider SHOULD establish and maintain assessment techniques and tools to support the risk-based assessment.

The Token Service Provider defines the methods to communicate the assurance level to the applicable parties including the Card Issuer.

6.2.4 Token Service Provider Assurance with Requestor Data

This ID&V assurance method involves the use of data elements provided by the Token Requestor that could be predictive of fraud. Examples of data elements include, but are not limited to:

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

The Token Service Provider SHOULD have appropriate assessment techniques and tools in place to implement this ID&V method and SHOULD combine the resulting ID&V data with the Token Service Provider risk and authentication data related to the PAN to determine the assigned Token Assurance Level. The Card Issuer may be involved in this process.

The Token Service Provider defines methods to communicate the assurance level and the ID&V steps performed to the applicable parties, including the Card Issuer.

6.2.5 Card Issuer Verification of the Cardholder

This ID&V method involves interacting with the Card Issuer or its Agent to perform the Cardholder verification to satisfy the assurance necessary to complete the binding of the Payment Token to the PAN. Methods used for verification SHOULD be designed to provide an acceptable user experience based on the device type; for example, mobile phone or computer; the Cardholder may use during the authentication process. Device guidelines SHOULD be created and followed to ensure a consistent user experience.

Card Issuer authentication SHOULD be designed to leverage input data and scores from the Token Requestor in order for the Card Issuer to deliver the most intelligent experience possible to the consumer. The use of this data will, in many cases, allow the Card Issuer to have confidence that the genuine and authorised Cardholder is in fact requesting the Payment Token without having to add extra steps to the process.

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

- Use of a 3-D Secure ACS
- Mobile banking verification of the Cardholder with an authentication code
- Federated login systems
- API functionality capable of generating, delivering, and validating data from the Token Requestor
- One-time password (OTP), activation code, or other shared secret between the Card Issuer and the Cardholder
- Two-way email confirmation

When the Card Issuer determines that there is a need to verify the consumer requesting the Payment Token through an explicit verification; for example, using an OTP or activation code; the shared secret SHOULD be delivered to the consumer through an out-of-band channel.

The Card Issuer may use a plurality of methods for Cardholder authentication; however, the following methods SHOULD NOT be used for ID&V:

- Static authentication data
- Enrolment in an authentication service at the time of Cardholder authentication

In contrast, one-time passwords SHOULD be used for Cardholder authentication by the Card Issuer or its Agent.

The Card Issuer or its Agent SHOULD use the following standards for one-time passwords:

- In order to balance between security and convenience, OTPs SHOULD have a length of at least 6 and no more than 8 characters
- OTPs SHOULD be generated in a manner such that they are not predictable
- Preferred method for delivery is a secure channel from the Card Issuer to the consumer device, such as a mobile banking application installed on the consumer device

Additional methods may also be used at the discretion of the Card Issuer, but SHOULD follow similar methodology as defined in this specification.

7 Token Service Provider APIs

7.1 General

This section establishes the common data elements of the interface that each Token Service Provider SHALL support for the APIs externally available at a specific Token Service Provider.

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.

This specification 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.

The Token Service Provider SHALL implement a secure method of interaction with participating entities using the Token Service.

This section of this specification does not address the Token Processing interfaces. For more information, refer to Section 9 Payment Token Transaction Flows.

7.2 Token Service Participating Endpoints

The Token Service Provider SHALL provide the capability to establish and use the standard interfaces or APIs with the entities that are authenticated through a secured method of interaction with the Token Service. The following are examples of the authenticated methods through which these interactions may occur:

- Web services
- ISO 8583 message exchange through an existing Payment Network interface
- File / batch

The following are examples of the entities that may participate and use the Token Service interfaces:

- Token Requestor
- Acquirer
- Payment Network
- Other networks
- Merchant

- Acquirer and Card Issuer Processors
- Card Issuer
- Card Issuer 3-D Secure ACS

7.3 Interface Categories

This section describes the interfaces and messages that will be implemented by the Token Service Provider to provide the Token Service. These interfaces are classified into the following categories:

- Token Request and Issuance
- Token Assurance (ID&V)
- De-Tokenisation
- Token Routing
- Token Lifecycle Management

Each of these categories SHALL have one or more defined interfaces and / or messages to carry out a specific Token-related operation.

7.3.1 Token Request and Issuance

The Token Service Provider SHALL provide a standard method that a registered Token Requestor can use to submit a request through the standard interface to input the original payment credential and receive a Payment Token in response.

The Token Service Provider SHALL implement appropriate controls and processes to generate a Token based on the input PAN. Additionally, assurance steps may be performed based on the request. Where such assurance steps involve mechanisms also used for other purposes (e.g. 3-D Secure), a Token Request Indicator SHOULD be used to indicate that the mechanism is being used as part of a Token Request.

The Token Request interface may support real-time requests that require issuance of a Payment Token for each PAN requested, or in-bulk requests through a secure interface file where Tokens are generated and issued in bulk quantities and returned to the Token Requestor.

7.3.1.1 Input Data Elements

The input to this request SHALL minimally contain the following data elements:

- Token Requestor ID

- PAN
- PAN Expiry Date

A Requested Assurance Level is present if a particular assurance level is being requested.

The Token Location provides information about where the Token data will be stored. The security of this location may influence the assurance level that can be assigned to a Token. Due diligence of the security provided by Token Requestors is the responsibility of each Token Service Provider and assignation of a location type to each Token Requestor will be at the discretion of each Token Service Provider. Token Location SHALL not change during the life of the Payment Token.

Currently identified location types are:

- Remote storage: e.g. a card-on-file database
- EMVCo / Payment Network type approved secure element / ICC
- Local Device storage: e.g. Token data stored using the standard data storage mechanisms of a consumer controlled device
- Local hardware secured storage: e.g. using a TEE to ensure appropriately restricted access to data
- Remote hardware secured storage: e.g. ISO 13491 compliant storage

The Protocol provides information about how the Token Requestor is communicating with the Cardholder. The security of the communication channel used may influence the assurance level that can be assigned to a Payment Token.

Account Verification Results contains the result of a previously performed account verification transaction, such as $0 auth with or without address verification.

Optional Cardholder data elements may include additional data such as, but not limited to, bill to / ship to address and postal code to carry out the Token Assurance ID&V method. This is not an exhaustive list and is likely to grow in future.

Device Information is 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.

Table 7-1: Data Elements for Token Request

Field Name	Length	Format	R/C/O	Description
Version Number	3	N.N	R	Version number of this message

Field Name	Length	Format	R/C/O	Description
Token Requestor ID	11	Numeric	R	Refer to Table 4-1: Payment Token Specification Data Elements for a detailed description.
Length of PAN	2	Numeric	R	Length of PAN field
PAN	Variable (from 13 to 19 digits)	Numeric	R	PAN for which the Payment Token is requested
PAN Expiry Date	4	Numeric	R	PAN Expiry Date for which the Payment Token is requested
Requested Token Assurance Level	2	Numeric	O	Present if an assurance level is being requested, refer to Table 1-3: Definitions for a detailed description.
Token Location	2	Numeric	C	Required unless inherent in the Token Requestor API. Indicates the storage location of the Payment Token: • 01 – Remote storage • 02 – EMVCo / Payment Network type approved secure element / ICC • 03 – Local Device storage • 04 – Local hardware secured storage • 05 – Remote hardware secured storage • 06 – 99 Reserved for future use

Field Name	Length	Format	R/C/O	Description
Protocol	2	Numeric	C	Required unless inherent in the Token Requestor API. Describes what protocol the Token Requestor is using to communicate with the Cardholder. Values are Token Service Provider specific and may include values for: • Mobile App API • Browser
Account Verification Results	2	Numeric	O	Indicates the results of account verification, if performed, e.g. Pass, Fail (values will be Payment Network specific)
Account Verification Reference Length	2	Numeric	R	Length of the Account Verification Reference, will contain zero (0) if not present
Account Verification Reference	Variable	Alphanumeric	O	Reference to the Account Verification transaction performed by the Token Requestor. Note: The reference should contain sufficient information to determine the type of authentication performed, if necessary.
Token Requestor Risk Score	4	Numeric	O	Fraud risk score that is provided by the Token Requestor
Address Mismatch Indicator	2	Numeric	O	Populated if shipping and billing addresses are different
Length of Cardholder Data	4	Numeric	R	Length of Cardholder data, will contain zero (0) if not present

Field Name	Length	Format	R/C/O	Description
Cardholder Data	Variable	Alphanumeric	C	Data as necessary to support the Requested Assurance Level. Examples include, but are not limited to: • Billing address • Shipping address • Postal code • CAV2 / CVC2 / CVV2 / CID Refer to Section 6 Token Assurance ID&V Methods for details on ID&V methods.
Device Information Length	2	Numeric	R	Length of Device Information, will contain zero (0) if not present
Device Information	Variable	Alphanumeric	O	Attributes of the device that may be used to identify it

R – Required, C – Conditional, O – Optional

Implementation of field formats is defined by each Token Service Providers API

7.3.1.2 Output Data Elements

The interface SHALL provide a response message that contains the following data elements in the response:

- Status of the request – Successful or failure
- Reason code – Code indicating the type of failure

For successful requests, the following additional data elements SHALL be returned in the response:

- Payment Token
- Payment Token Expiry Date

When a Token Assurance Method has been performed at the time of the Token Request, the interface may optionally provide the Assigned Token Assurance Level calculated for that Payment Token.

Table 7-2: Data Elements for Response to Token Request

Field Name	Length	Format	R/C/O	Description
Version Number	3	N.N	R	Version number of this message
Request Status	1	Numeric	R	Indicates success or failure of the request
Reason Code Length	2	Numeric	R	Length of Reason Code, will contain zero (0) if not present
Reason Code	Variable	Alphanumeric	C	Present if Request Status is not successful
Token Length	2	Numeric	R	Length of Payment Token, will contain zero (0) if not present
Payment Token	Variable (from 13 to 19 digits)	Numeric	C	Present if Request Status is successful, the Payment Token is generated by the Token Service Provider.
Token Reference ID Length	2	Numeric	R	Length of Token Reference ID, will contain zero (0) if not present
Token Reference ID	Variable	Numeric	O	A reference identifier for the Payment Token
Token Expiry Date	4	Numeric	C	Present if Request Status is successful, the Token Expiry Date is generated by the Token Service Provider.
Assigned Token Assurance Level	2	Numeric	C	Present if Request Status is successful and ID&V has been requested, refer to Table 4-1: Payment Token Specification Data Elements for a detailed description.

R – Required, C – Conditional, O – Optional

Implementation of field formats is defined by each Token Service Providers API

7.3.2 Token Assurance Level Method Update

This method is used for situations where after the issuance of a Payment Token, the Token Requestor wishes to have an updated assurance level assigned to the Payment Token.

7.3.2.1 Input Data Elements

The input to this request SHALL minimally contain the following data elements:

- Payment Token
- Token Expiry Date
- Token Requestor ID

A Requested Assurance Level is present if a particular assurance level is being requested.

Optional Cardholder data elements may include additional data such as, but not limited to, bill to / ship to address and postal code to carry out the Token Assurance ID&V method. This is not an exhaustive list and may be expanded in the future.

Table 7-3: Data Elements for Token Assurance Level Update Request

Field Name	Length	Format	R/C/O	Description
Version Number	3	N.N	R	Version number of this message
Token Length	2	Numeric	R	Length of Payment Token
Payment Token / Token Reference ID	Variable (from 13 to 19 digits)	Numeric	R	The Payment Token or a reference identifier for the Token
Token Requestor ID	11	Numeric	R	A unique value assigned to the registered business entity that is requesting the Payment Token

Field Name	Length	Format	R/C/O	Description
Requested Token Assurance Level	2	Numeric	C	Indicates the level of validation the Token Requester would like to be performed. Present if Token Requestor is requesting a specific Token Assurance Level (rather than just a, assurance level re-evaluation.
Account Verification Results	2	Numeric	O	Indicates the results of account verification, if performed, e.g. Pass, Fail (values will be Payment Network specific)
Account Verification Reference Length	2	Numeric	R	Length of the Account Verification Reference, will contain zero (0) if not present
Account Verification Reference	Variable	Alphanumeric	O	Reference to the Account Verification transaction performed by the Token Requestor. Note: The reference should contain sufficient information to determine the type of authentication performed, if necessary.
Token Requestor Risk Score	4	Numeric	O	Fraud risk score that is provided by the Token Requestor
Address Mismatch Indicator	1	Boolean	O	Indication of whether or not shipping and billing addresses are different
Length of Cardholder Data	4	Numeric	R	Length of Cardholder data, will contain zero (0) if not present

Field Name	Length	Format	R/C/O	Description
Cardholder Data	Variable	Alphanumeric	C	Data as necessary to support the Requested Assurance Level. Examples include, but are not limited to: • Billing address • Shipping address • Postal code • CAV2 / CVC2 / CVV2 / CID Refer to Section 6 Token Assurance ID&V Methods for details on ID&V methods.
Device Information Length	2	Numeric	R	Length of Device Information, will contain zero (0) if not present
Device Information	Variable	Alphanumeric	O	Attributes of the device that may be used to identify it

R – Required, C – Conditional, O – Optional

Implementation of field formats is defined by each Token Service Providers API

7.3.2.2 Output Data Elements

The interface SHALL provide a response message that contains the following data elements in response:

- Status of the request – Successful or failure
- Reason code – Code explaining the type of failure

For successful requests, the additional data elements shown in the following table are returned in the response.

Table 7-4: Data Elements for Response to Token Assurance Level Update Request

Field Name	Length	Format	R/C/O	Description
Version Number	3	N.N	R	Version number of this message

Field Name	Length	Format	R/C/O	Description
Request Status	1	Numeric	R	Indicates success or failure of the request
Reason Code Length	2	Numeric	R	Length of Reason Code, will contain zero (0) if not present
Reason Code	Variable	Alphanumeric	C	Present if Request Status is not successful
Token Length	2	Numeric	R	Length of Payment Token
Payment Token	Variable (from 13 to 19 digits)	Numeric	R	Present if Request Status is successful, the Payment Token is generated by the Token Service Provider.
Assigned Token Assurance Level	2	Alphanumeric	R	Present if Request Status is successful and ID&V has been requested.

R – Required, C – Conditional, O – Optional

Implementation of field formats is defined by each Token Service Providers API

7.3.3 De-tokenisation Query

The De-Tokenisation Query interface provides the necessary mechanism to exchange the Payment Token by returning the mapped original PAN and PAN Expiry Date credential to the authenticated entity.

No transaction specific validation is performed on this request: its purpose is to make the original card details available to a trusted party and is not used in transaction processing.

The Token Service Provider SHALL implement appropriate access security controls, in particular, the Token Service Provider SHALL ensure that the request is received from a recognised, authorised and authenticated source.

7.3.3.1 Input Data Elements

The input to this request contains the data elements shown in the following table.

Table 7-5: Data Elements for De-Tokenisation Query Request

Field Name	Length	Format	R/C/O	Description
Version Number	3	N.N	R	Version number of this message
Token Requestor ID	11	Numeric	C	Present when available to De-Tokenisation requestor. Refer to Table 4-1: Payment Token Specification Data Elements for a detailed description.
Token Length	2	Numeric	R	Length of Payment Token
Payment Token	Variable (from 13 to 19 digits)	Numeric	R	The issued Payment Token
Token Expiry Date	4	Numeric	R	The issued Payment Token Expiry Date

R – Required, C – Conditional, O – Optional

Implementation of field formats is defined by each Token Service Providers API

7.3.3.2 Output Data Elements

The interface SHALL provide a response message that contains the following data elements:

- Status of the request – Successful or failure
- Reason code – Code explaining the type of failure

For successful requests, the following additional data elements are returned in the response:

- PAN
- PAN Expiry Date

Table 7-6: Data Elements for Response to De-Tokenisation Query Request

Field Name	Length	Format	R/C/O	Description
Version Number	3	N.N	R	Version number of this message
Request Status	1	Numeric	R	Indicates success or failure of the request
Reason Code Length	2	Numeric	R	Length of Reason Code, will contain zero (0) if not present
Reason Code	Variable	Alphanumeric	C	Present if Request Status is not successful
PAN Length	2	Numeric	C	Present if Request Status is successful, with length of PAN field
PAN	Variable (from 13 to 19 digits)	Numeric	C	Present if Request Status is successful, with PAN
PAN Expiry Date	4	Numeric	C	Present if Request Status is successful, with PAN expiry date

R – Required, C – Conditional, O – Optional

Implementation of field formats is defined by each Token Service Providers API

7.3.4 De-tokenisation With Verification

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

7.3.4.1 Input Data Elements

The input to this request contains the data elements shown in the following table

Table 7-7: Data Elements for De-Tokenisation With Verification Request

Field Name	Length	Format	R/C/O	Description
Version Number	3	N.N	R	Version number of this message
Token Requestor ID	11	Numeric	C	Must be included when available to De-Tokenisation requestor. Refer to Table 4-1: Payment Token Specification Data Elements for a detailed description.
Token Length	2	Numeric	R	Length of Payment Token
Payment Token	Variable (from 13 to 19 digits)	Numeric	R	The issued Payment Token
Token Expiry Date	4	Numeric	R	The issued Payment Token Expiry Date
Length of Transaction Data Elements	3	Numeric	R	Length of Transaction Data Elements field, will contain zero (0) if not present
Transaction Data Elements	Variable	Implementation Dependent	O	Other transaction data elements as necessary for the Token Service Provider to execute the request, content is proprietary to the Token Service Provider

R – Required, C – Conditional, O – Optional

Implementation of field formats is defined by each Token Service Providers API

7.3.4.2 Output Data Elements

The interface SHALL provide a response message that contains the following data elements:

Table 7-8: Data Elements for Response to De-Tokenisation With Verification Request

Field Name	Length	Format	R/C/O	Description
Version Number	3	N.N	R	Version number of this message
Request Status	1	Numeric	R	Indicates success or failure of the request
Reason Code Length	2	Numeric	R	Length of Reason Code, will contain zero (0) if not present
Reason Code	Variable	Alphanumeric	C	Present if Request Status is not successful
PAN Length	2	Numeric	C	Present if Request Status is successful, with length of PAN field
PAN	Variable (from 13 to 19 digits)	Numeric	C	Present if Request Status is successful, with PAN
PAN Expiry Date	4	Numeric	C	Present if Request Status is successful, with PAN expiry date
Length of Transaction Data Elements	3	Numeric	R	Length of Transaction Data Elements field, will contain zero (0) if not present
Transaction Data Elements	Variable	Implementation Dependent	O	Transaction data elements as necessary to continue the transaction, content is proprietary to the Token Service Provider

R – Required, C – Conditional, O – Optional

Implementation of field formats is defined by each Token Service Providers API

7.3.5 Token Lifecycle Management

Payment Tokens may require ongoing management and updates due to changes to the PAN and PAN Expiry Date, as well as events that may require the mapping to be deactivated.

The Token Service Provider SHALL provide lifecycle updates through the interfaces to manage changes that affect the issued Payment Token. These interfaces may be used by multiple parties, including Token Requestors, Card Issuers and Payment Networks.

Token Lifecycle Management may be required to support existing business-as-usual processes such as Card Issuer portfolio conversion.

The following table provides a sample set of lifecycle 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 at the discretion of the Token Service Provider.

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

Table 7-9: Lifecycle Events

#	Interface	Example Event / Description	Initiated By	Action Performed
1	Unlink Token	• Lost or stolen device • Original credential 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 Payment Network	The Payment Token is unlinked from the PAN and the mapping is disabled for further use.
2	Suspend Token	• Temporary deactivation due to lost or stolen device	Token Requestor Card Issuer Payment Network	The Payment Token to PAN mapping is temporarily suspended and further use will be withheld.
3	Activate Token	• First-time activation or resume Payment Token to PAN mapping from temporary suspension	Token Requestor Card Issuer Payment Network	The Payment Token to PAN mapping is activated.

#	Interface	Example Event / Description	Initiated By	Action Performed
4	Update Token Assurance	• Ongoing management of the Token Assurance Level on the Payment Token	Token Requestor Card Issuer Payment Network Token Service Provider	The Token Assurance Level is updated for the Payment Token to PAN mapping based on the ID&V method performed, or as a result of internal operations.
5	Update PAN Attributes	• Updates to original credential, 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 to PAN mapping.

8 Payment Token Processing

8.1 General

This specification includes the use of existing data fields, the inclusion of Payment Token-related data within current fields, as well as new fields, some of which are required in order to provide for consistency of implementation and interoperability throughout the payments system. Other new fields introduced as part of this specification are optional.

The presence of fields associated with Payment Tokenisation within the transaction processing types will vary by use case as highlighted in Section 9 Payment Token Transaction Flows.

8.2 Routing and Account Range Tables

Routing and account range tables need to clearly distinguish Token BINs and Token BIN Ranges from traditional BINs and BIN ranges in order to ensure the underlying integrity of Payment Token transaction processing. This requires the Token Service Provider to assign Token BINs and Token BIN Ranges that are unique and distinct from traditional BINs and BIN ranges which are flagged accordingly in all routing and account range tables.

8.3 Transaction Authorisations

Transaction authorisation messages, specifically request messages that flow from Merchant to Acquirer, Acquirer to Payment Network, and Payment Network to Card Issuer, and all corresponding response messages, are impacted by this specification. The extent of the impact varies by use case and will be defined in the authorisation message specifications communicated by participating Payment Networks as part of their implementation of Tokenisation solutions based on this specification.

The following are key requirements for Payment Token transaction processing:

- The Token Service Provider SHALL validate the Payment Token in the incoming authorisation message against data elements, including Token Requestor ID (if available), and provide the result to the Payment Network of the validity of the Payment Token within the Token Domain Restriction Controls.

- The Payment Network SHOULD use the Token Service Provider to map the Payment Token to the PAN in the incoming authorisation message prior to sending the message to the Card Issuer, and SHALL always map the PAN back to the Payment Token in any response messages sent back to the Acquirer (except in cases where the Card Issuer is acting as the Token Service Provider).
- The Token Service Provider SHOULD indicate to the Payment Network any changes in Payment Token status such as when Payment Tokens that have been deemed as lost / stolen and / or have been marked as suspended.

8.4 Token Domain Restriction Controls During Transactions

Token Service Providers and participating Payment Networks provide the capability to apply specific Token Domain Restriction Controls as defined for a given Token Requestor and use case. The Token Domain Restriction Controls depend upon the availability of specific control-related data elements in the transaction processing messages and underlying data integrity, as these data elements will be critical to ensuring controlled usage of Payment Tokens. Domains may encompass one or more channels, so long as the Token Domain Restriction Controls can be fully enforced to prevent cross-channel fraud.

8.5 Capture Processing

The impact of this specification on capture processing is defined by such entities as Acquirers or Payment Processors based on the clearing requirements associated with participating Payment Networks. The clearing requirements defined in this specification, and implemented within the context of the clearing systems operated by the Payment Networks, determine the definition of any impact to capture processing for Acquirers or Payment Processors and related Merchants.

8.6 Clearing

Clearing messages that flow from the Acquirer to Payment Network, and Payment Network to Card Issuer, are impacted by this specification. The extent of the impact varies by use case and will be defined in the clearing message specifications communicated by participating Payment Networks as part of their implementation of Payment Tokenisation solutions that are based on this specification. These clearing-related specifications determine the changes defined by Acquirers and Payment Processors to their capture processing message specifications.

8.7 Exception Processing

Chargeback messages that flow from the Card Issuer to Payment Network, and Payment Network to Acquirer, are impacted by this specification. The extent of the impact varies by use case 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 specification.

9 Payment Token Transaction Flows

9.1 General

The implementation of a Token Service based on this specification is not intended to change the traditional methods and flows in which payment transactions using PANs are currently processed. The introduction of Payment Tokens, however, does require the passing of data in some new data elements, carrying some Token-related data within existing data elements, and ensuring the Payment Network can recognise Payment Token transactions in order to ensure that Payment Tokens are de-tokenized by the appropriate Token Service Provider during transaction processing. The impact of this specification on Payment Token transaction flows must be examined separately for each potential use case to understand the underlying requirements.

It is the responsibility of each Token Service Provider to inform Card Issuers of any changes to authorisation (and other) messages, specifically which fields have had their usage changed and which fields are new. It is also the responsibility of each Token Service Provider to ensure Card Issuers are aware of the separation of responsibility when processing Payment Token transactions, for example in the NFC at point of sale use-case the Token Service Provider may authenticate the validity of a Payment Token but the Card Issuer must still check for Cardholder verification if needed.

The sample use cases defined in this specification include mobile NFC at POS, mobile / digital wallet e-commerce, Card-on-file e-commerce, and scan at point of sale. Depending on the use case, there are different levels of impacts to authorisation, presentment, and chargeback transaction processing, and the underlying message requirements. Each of these use cases is examined with regard to the use of existing fields, the presence of Payment Token data in current fields, and new data fields, both required and optional, including Payment Token control fields used to support Token Domain Restriction Controls by the Token Service Provider in conjunction with the Payment Network(s). The following figures identify some of the key data elements that may or may not be present in authorisation, capture, clearing, and exception processing transactions, depending on the use case and whether the data element is considered required or optional. For each message, additional data fields will be present depending on use-case, payment brand etc. The figures do not attempt to present a complete list of data elements used in each message.

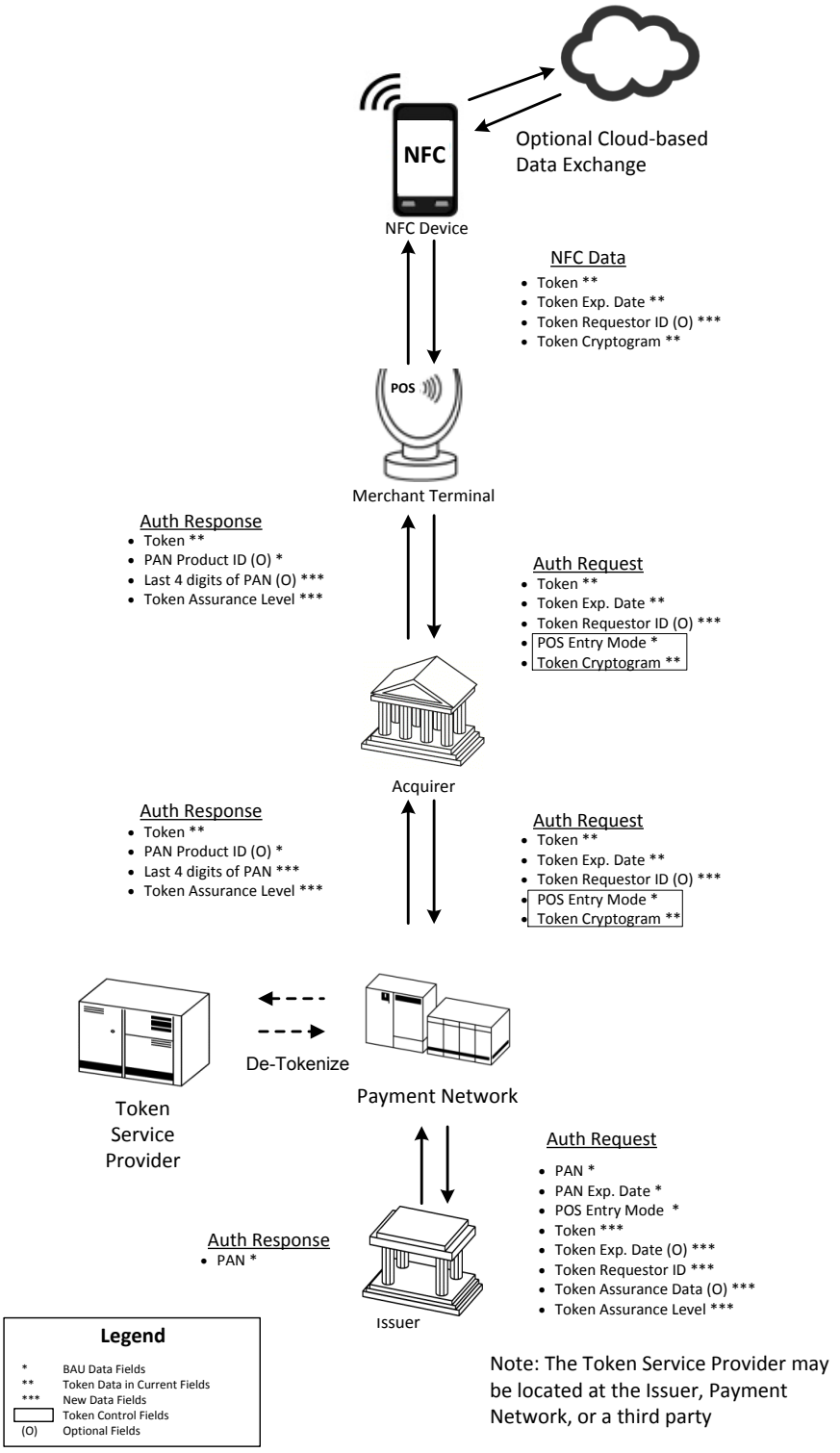
The use-cases presented are examples only and are not required to be supported, nor are they intended to be an exhaustive list of possible use-cases. This specification can be used to serve more use cases, in addition to those presented here.

9.2 Use Case 1: Mobile NFC at Point of Sale

In this use case, a Payment Token is stored within an NFC-enabled mobile device or alternatively in a remote server and delivered just-in-time to the device. Token Provisioning can be accomplished by the Token Requestor interfacing with the Token Service Provider. When a transaction is initiated, the mobile device and / or remote server will generate a contactless transaction including the Payment Token, Token Expiry Date, Token Cryptogram, and other chip data elements, and pass the transaction to the Merchant's point of sale terminal via the NFC interface.

The impacts defined for this use case are shown in the following figure.

Figure 4: Mobile NFC at Point of Sale Flow



The following steps explain the flow of the standard Payment Token data fields in the authorisation message when the mobile device is used at an NFC-enabled point of sale terminal.

1. The mobile device will interact with the NFC terminal through the payment application and pass the following key Payment Token data elements to the Merchant terminal:
    a. Payment Token will be passed in the existing PAN field.
    b. Token Expiry Date will be passed in the PAN Expiry Date field.
    c. Token Cryptogram will be generated based on the Token data elements and will be passed in the Chip Cryptogram field. (The cryptogram may be a full chip cryptogram, or an abbreviated Track 2 equivalent cryptogram.)
    d. Token Requestor ID will be passed as an optional field.
    e. All other contactless data elements will be created and passed following the contactless data standards.

NOTE

The Token Cryptogram generated from the mobile device along with POS Entry Mode will serve as the Domain Restriction Control fields that will be used by the Token Service Provider to validate the integrity of the transaction using that Payment Token.

2. The Merchant terminal will pass the contactless authorisation request to the Acquirer, carrying all of the standard Payment Token data fields and contactless data elements; POS Entry Mode will be set to indicate contactless transaction.
3. The Acquirer will perform routine processing checks and pass the Token data fields and the contactless data to the Payment Network.
4. The Payment Network will interface with the Token Service Provider to:
    a. Retrieve the PAN.
    b. Verify the state of the Payment Token to PAN mapping in the Token Vault for the active Payment Token, and other controls that may be defined for that Payment Token.
    c. Validate the Token Cryptogram and validate the Token Domain Restriction Controls for that Payment Token (alternatively the Card Issuer may validate the cryptogram if it has the necessary keys).
    d. Retrieve the Token Requestor ID if it was not provided in the authorisation message.
5. The Payment Network will send the authorisation request to the Card Issuer, with the following changes to the authorisation request message:

a. Replace Payment Token with PAN.

b. Replace Token Expiry Date with PAN Expiry Date.

c. Add an indicator that conveys to the Card Issuer that an on-behalf-of validation has been completed by the Token Service Provider of that Payment Token.

d. The following Payment Token-related fields are passed to the Card Issuer in the authorisation request:

i. Payment Token

ii. Token Expiry Date (Optional)

iii. Token Assurance Data (Optional)

iv. Token Assurance Level

v. Token Requestor ID

vi. POS Entry Mode Code

6. The Card Issuer completes the account-level validation and the authorisation check, and sends the PAN back in the authorisation response to the Payment Network.
7. The Payment Network (possibly in communication with the Token Service Provider) may generate a response cryptogram and will replace the PAN with the Payment Token based on the mapping, and will pass the following required fields to the Acquirer as part of the authorisation response, in addition to other standard data elements:

a. Payment Token

b. Token Assurance Level

c. Last 4 digits of PAN

d. PAN Product ID (Optional)

8. The Acquirer will pass the authorisation response to the Merchant.
9. The consumer will be notified of the success or failure of the transaction.

NOTE

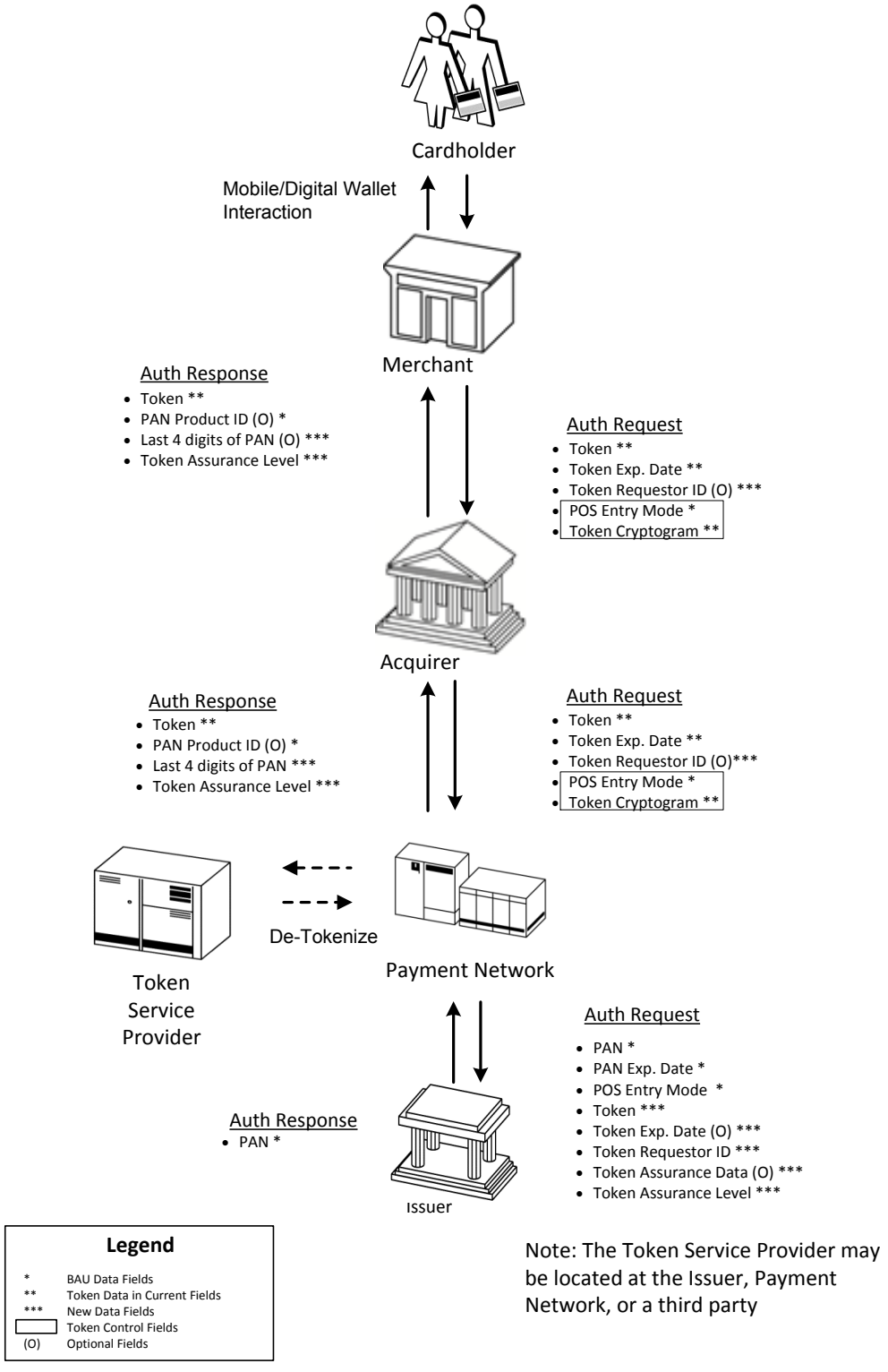
This use case also accommodates use of a Payment Token loaded into a contact and / or contactless chip at time of issuance. Such a Payment Token would be different from the PAN embossed/printed on the Card and encoded on the magnetic stripe.

9.3 Use Case 2: Mobile / Digital Wallet E-Commerce

This use case refers to scenarios where a Cardholder initiates payment to an e-commerce site using a mobile / digital wallet to transfer payment and other order information. The wallets may be operated by Card Issuers, Payment Networks, or third parties; and the digital wallet operator will likely be the Token Requestor. In this use case, the wallet operator uses Payment Tokenisation so as to no longer need to store the PAN in the wallet platform for security or other business rationales. When a Cardholder initiates payment at an e-commerce Merchant that supports the wallet, the wallet will pass a Payment Token in lieu of the PAN along with additional Payment Token-related fields through the wallet API to the Merchant. Merchants will initiate authorisations using the Payment Token and accompanying Token Expiry Date carried within the existing fields for PAN and PAN Expiry Date. Split shipments and recurring payments may be supported using the Payment Network's existing processes, although de-Tokenisation and Token Domain Restriction Controls will need to be performed as well.

The impacts defined for this use case are shown in the following figure.

Figure 5: Authorisation – Mobile / Digital Wallet E-Commerce Flow



The following steps explain the flow of the standard Payment Token data fields in the authorisation message when a consumer initiates an e-commerce transaction using a Merchant application or digital wallet in the mobile device to make a purchase.

1. The Merchant application / digital wallet in the mobile device will interact with the payment application and pass the following key Payment Token data elements to the Merchant platform:
    a. Payment Token will be passed in the existing PAN field.
    b. Token Expiry Date will be passed in the PAN Expiry Date field.
    c. Token Cryptogram will be generated based on the Payment Token data elements and will be passed in the Token Cryptogram field.
    d. Token Requestor ID will be passed as an optional field.
    e. All other required data elements will be created and passed along.
2. The Merchant platform will pass the authorisation request to the Acquirer, carrying all the standard Payment Token fields; POS Entry Mode will be set to indicate e-commerce transaction.
3. The Acquirer will perform processing checks on the data elements, and pass the Payment Token data fields to the Payment Network.
4. The Payment Network will interface with the Token Service Provider to:
    a. Retrieve the PAN.
    b. Verify the state of the Payment Token to PAN mapping in the Token Vault for the active Payment Token, and other controls that may be defined for that Payment Token.
    c. Validate the Token Cryptogram and validate the Token Domain Restriction Controls for that Payment Token (alternatively the Card Issuer may validate the cryptogram if it has the necessary keys).
    d. Retrieve the Token Requestor ID if it was not provided in the authorisation message.
5. The Payment Network will send the authorisation request to the Card Issuer, with the following changes to the authorisation request message:
    a. Replace Payment Token with PAN.
    b. Replace Token Expiry Date with PAN Expiry Date.
    c. Add an indicator that conveys to the Card Issuer that an on-behalf-of validation has been completed by the Token Service Provider of that Payment Token.

d. The following Token-related fields are passed to the Card Issuer in the authorisation request:

   i. Payment Token

   ii. Token Expiry Date (Optional)

   iii. Token Assurance Data (Optional)

   iv. Token Assurance Level

   v. Token Requestor ID

   vi. POS Entry Mode Code

6. The Card Issuer completes the account-level validation and the authorisation checks, and sends an authorisation response to the Payment Network.
7. The Payment Network will replace the PAN with the Payment Token based on the mapping, and will pass the following required fields to the Acquirer as part of the authorisation response, in addition to other standard data elements:

   a. Payment Token

   b. Token Assurance Level

   c. Last 4 digits of PAN

   d. PAN Product ID (Optional)

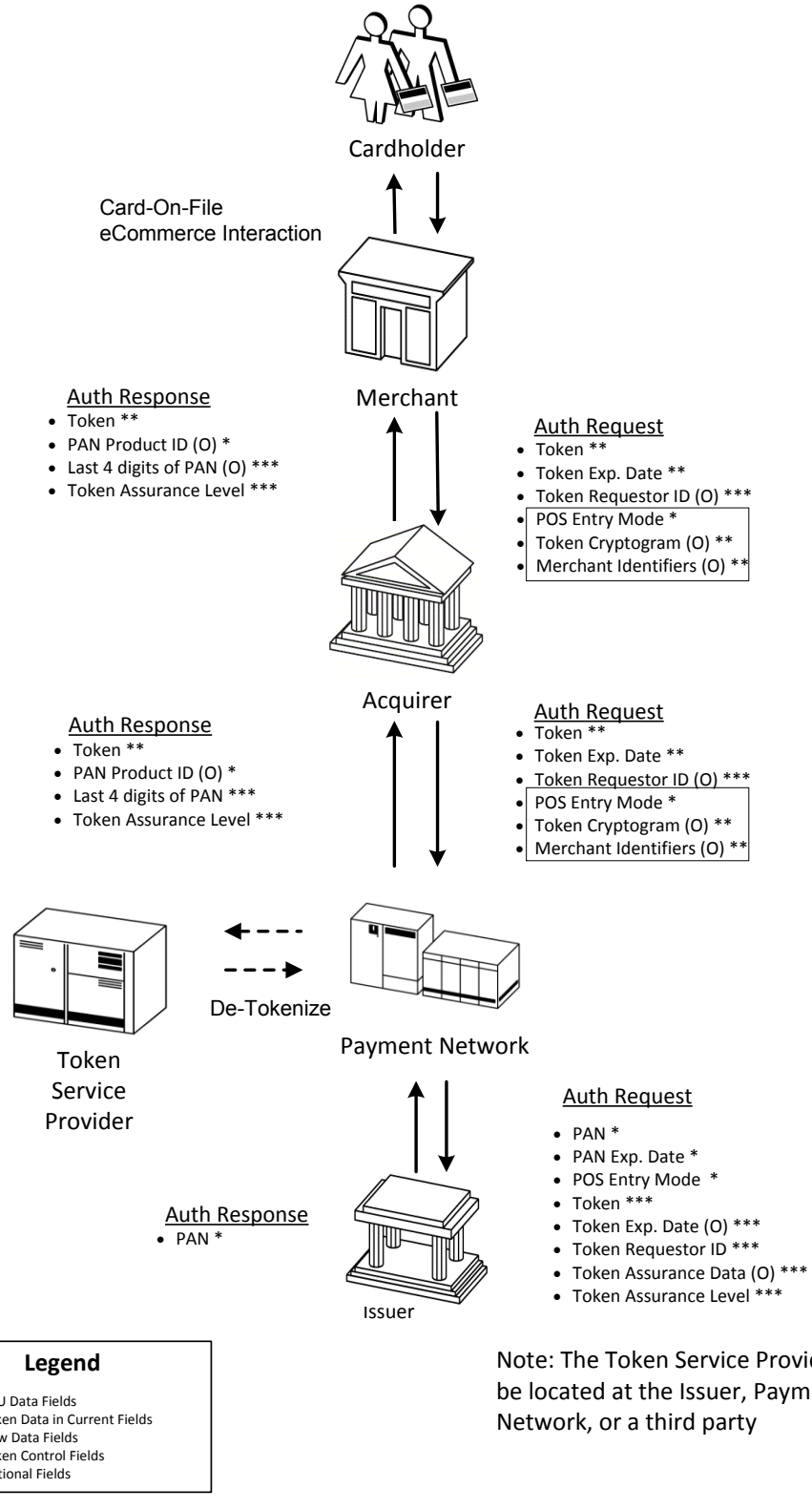
8. The Acquirer will pass the authorisation response to the Merchant.
9. The consumer will be notified of the success or failure of the transaction.

9.4 Use Case 3: Card-On-File E-Commerce

This use case refers to scenarios where an e-commerce Merchant that has payment card data on file in a database seeks to remove the underlying security exposure of storing card data by replacing the PANs with Payment Tokens. In such scenarios, these Merchants will likely be the Token Requestor. Once Payment Tokens are returned to these Card-on-file Merchants, all subsequent e-commerce transactions that are processed will use the Payment Token and the Token Expiry Date in lieu of the PAN and PAN Expiry Date fields.

The impacts defined for this use case are shown in the following figure.

Figure 6: Authorisation – Card-On-File E-Commerce Flow



The following steps explain the flow of the standard Payment Token data fields in the authorisation message when a consumer initiates an e-commerce purchase with a Card-on-file Merchant.

1. The Cardholder logs in with the Card-on-file Merchant and initiates an e-commerce purchase. The Merchant website passes the following key Payment Token data elements to the Merchant platform:
    a. Payment Token will be passed in the existing PAN field.
    b. Token Expiry Date will be passed in the PAN Expiry Date field.
    c. Token Requestor ID will be passed as an optional field.
    d. Token Cryptogram will be generated based on the Payment Token data fields and passed (Optional).
    e. All other Merchant identifier data will be created and passed (Optional).

NOTE

The Token Requestor ID and related Merchant identifiers will serve as the Domain Restriction Control fields that are to be used to validate the integrity of the transaction.

2. The Merchant platform will pass the authorisation request to the Acquirer, carrying all the standard Payment Token data fields and any required Merchant-specific identifiers; POS Entry Mode will be set to indicate e-commerce transaction.
3. The Acquirer will perform processing checks on the data elements, and pass the Payment Token data fields including Token Cryptogram to the Payment Network.
4. The Payment Network will interface with the Token Service Provider to:
    a. Retrieve the PAN.
    b. Verify the state of the Payment Token to PAN mapping in the Token Vault for the active Payment Token, and other controls that may be defined for that Payment Token.
    c. Validate the Token Cryptogram and validate the Token Domain Restriction Controls for that Payment Token (alternatively the Card Issuer may validate the cryptogram if it has the necessary keys).
    d. Retrieve the Token Requestor ID if it was not provided in the authorisation message.
5. The Payment Network will send the authorisation request to the Card Issuer, with the following changes to the authorisation request message:
    a. Replace Payment Token with PAN.
    b. Replace Token Expiry Date with PAN Expiry Date.

c. Add an indicator that conveys to the Card Issuer that an on-behalf-of validation has been completed by the Token Service Provider of that Payment Token.

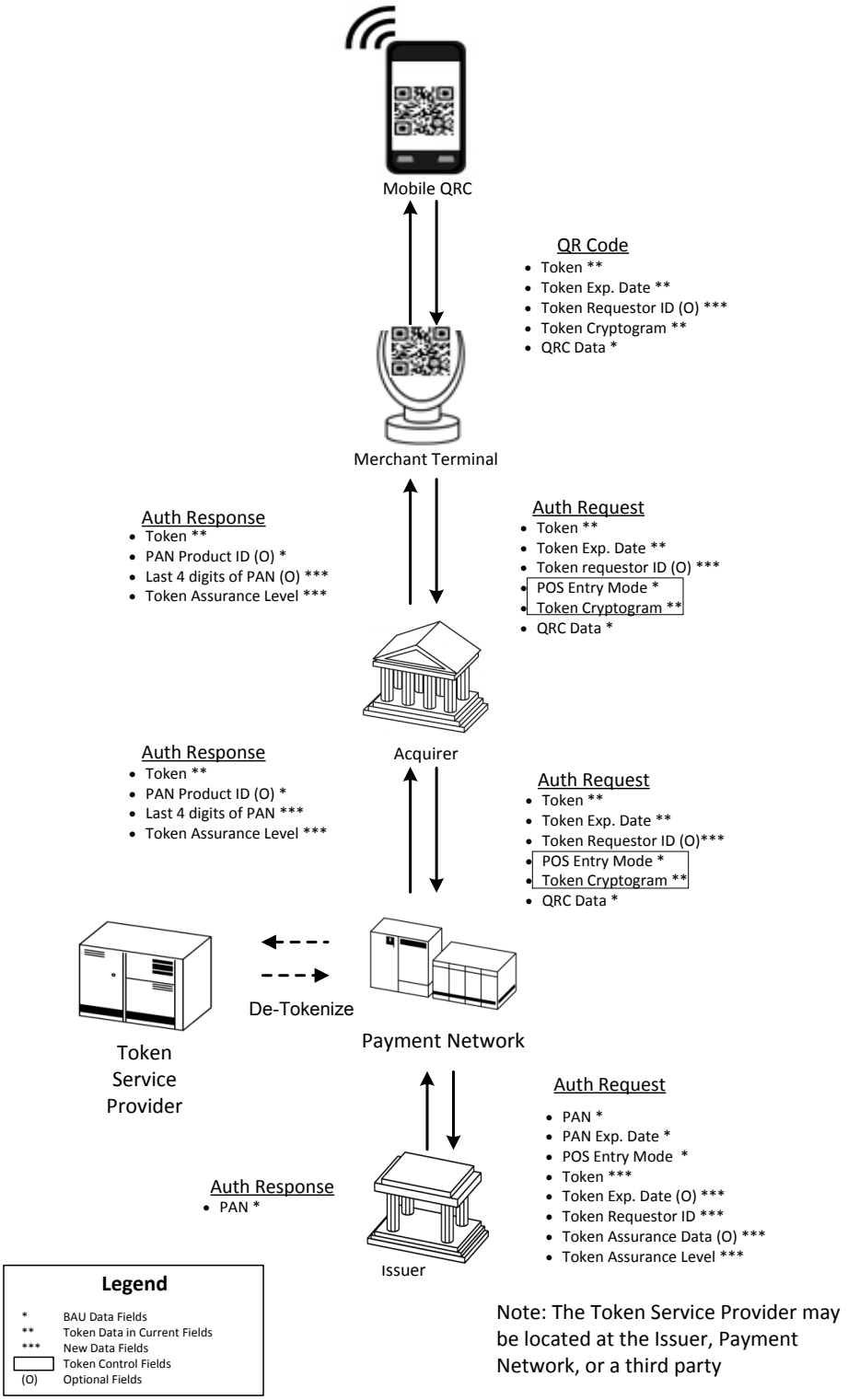
6. The following Payment Token-related fields are passed to the Card Issuer in the authorisation request:
    a. Payment Token
    b. Token Expiry Date (Optional)
    c. Token Assurance Data (Optional)
    d. Token Assurance Level
    e. Token Requestor ID
    f. POS Entry Mode Code
    g. The Card Issuer completes the account-level validation and the authorisation checks, and sends an authorisation response to the Payment Network.
7. The Payment Network will replace the PAN with the Payment Token based on the mapping, and will pass the following fields to the Acquirer as part of the authorisation response, in addition to other standard data elements:
    a. Payment Token
    b. Token Assurance Level
    c. Last 4 digits of PAN
    d. PAN Product ID (Optional)
8. The Acquirer will pass the authorisation response to the Merchant.
9. The consumer will be notified of the success or failure of the transaction.

9.5 Use Case 4: Scan at Point of Sale

The mobile quick response code (QR) at point of sale use case refers to the enablement of mobile devices to initiate QR code-based payments at Merchant locations that can accept this form of payment at the point of sale. In this use case, an application in the mobile device generates a dynamic QR code every time a payment is initiated in a secure manner. When a transaction is initiated, the mobile device will generate a transaction including the Payment Token, Token Expiry Date, and Token Cryptogram elements, and any other data from the QR code, and pass it to the Merchant's point of sale terminal.

The impacts defined for this case are shown in the following figure.

Figure 7: Scan at Point of Sale Flow



The following steps explain the flow of the standard Payment Token data fields in the authorisation message when a mobile device is used to present the Payment Token using a QR code at the point of sale.

1. The mobile device will interact with the Merchant terminal that is enabled to read QR codes, and pass the following key Payment Token data elements to the Merchant terminal:
    a. Payment Token will be passed in the existing PAN field.
    b. Token Expiry Date will be passed in the PAN Expiry Date field.
    c. Token Cryptogram may be generated based on the Payment Token data elements.
    d. Token Requestor ID will be passed as an optional field.
    e. All other QR data elements will be created and passed into respective transaction data fields.

NOTE

The Token Cryptogram is generated and when present will serve as the Domain Restriction Control field that will be used by the Token Service Provider to validate the integrity of the transaction using that Token.

2. The Merchant terminal will pass the authorisation request to the Acquirer, carrying all the standard Payment Token fields as shown in the previous figure; POS Entry Mode will be set to indicate a QR Code based transaction.
3. The Acquirer will perform standard processing checks, and pass the Payment Token data fields to the Payment Network.
4. The Payment Network will interface with the Token Service Provider to:
    a. Retrieve the PAN.
    b. Verify the state of the Payment Token to PAN mapping in the Token Vault for the active Payment Token, and other controls that may be defined for that Payment Token.
    c. Validate the Token Cryptogram and validate the Token Domain Restriction Controls for that Payment Token (alternatively the Card Issuer may validate the cryptogram if it has the necessary keys).
    d. Retrieve the Token Requestor ID if it was not provided in the authorisation message.
5. The Payment Network will send the authorisation request to the Card Issuer, with the following changes to the authorisation request message:

a. Replace Payment Token with PAN.

b. Replace Token Expiry Date with PAN Expiry Date.

c. Add an indicator that conveys to the Card Issuer that an on-behalf-of validation has been completed by the Token Service Provider of that Payment Token.

d. The following Payment Token-related fields are passed to the Card Issuer in the authorisation request:

i. Payment Token

ii. Token Expiry Date (Optional)

iii. Token Assurance Data (Optional)

iv. Token Assurance Level

v. Token Requestor ID

vi. POS Entry Mode Code

6. The Card Issuer completes the account-level validation and the authorisation checks, and sends an authorisation response to the Payment Network.
7. The Payment Network will replace the PAN with the Payment Token based on the mapping, and will pass the following to the Acquirer as part of the authorisation response, in addition to other standard data elements:

a. Payment Token

b. Payment Token Assurance Level

c. Last 4 digits of PAN

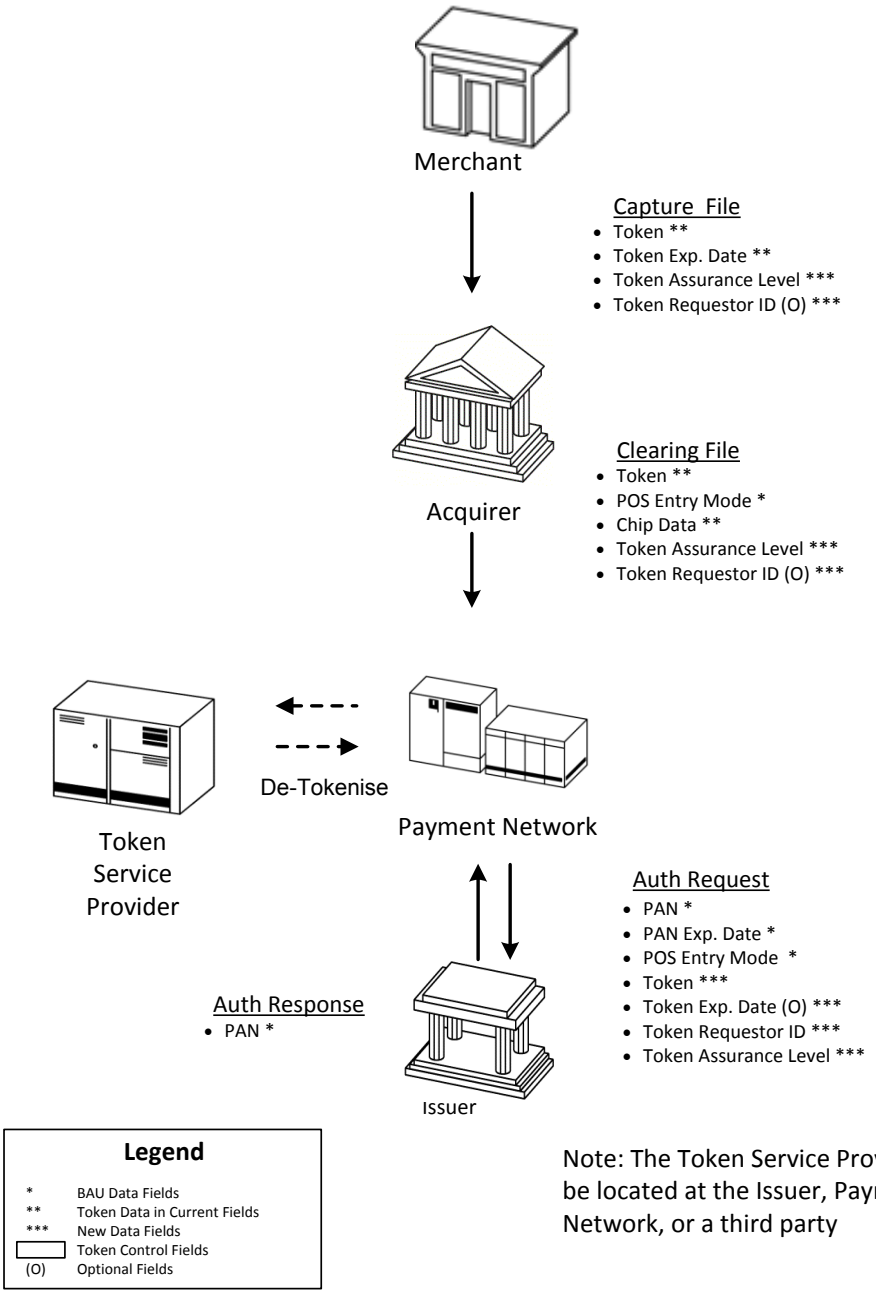
d. PAN Product ID (Optional)

8. The Acquirer will pass the authorisation response to the Merchant.
9. The consumer will be notified of the success or failure of the transaction.

9.6 Capture and Clearing Flow

The following figure shows the capture and clearing process for a Payment Token transaction.

Figure 8: Capture and Clearing Flow



The following steps describe the flow of the standard Payment Token data fields in the capture and clearing process as part of the transaction lifecycle.

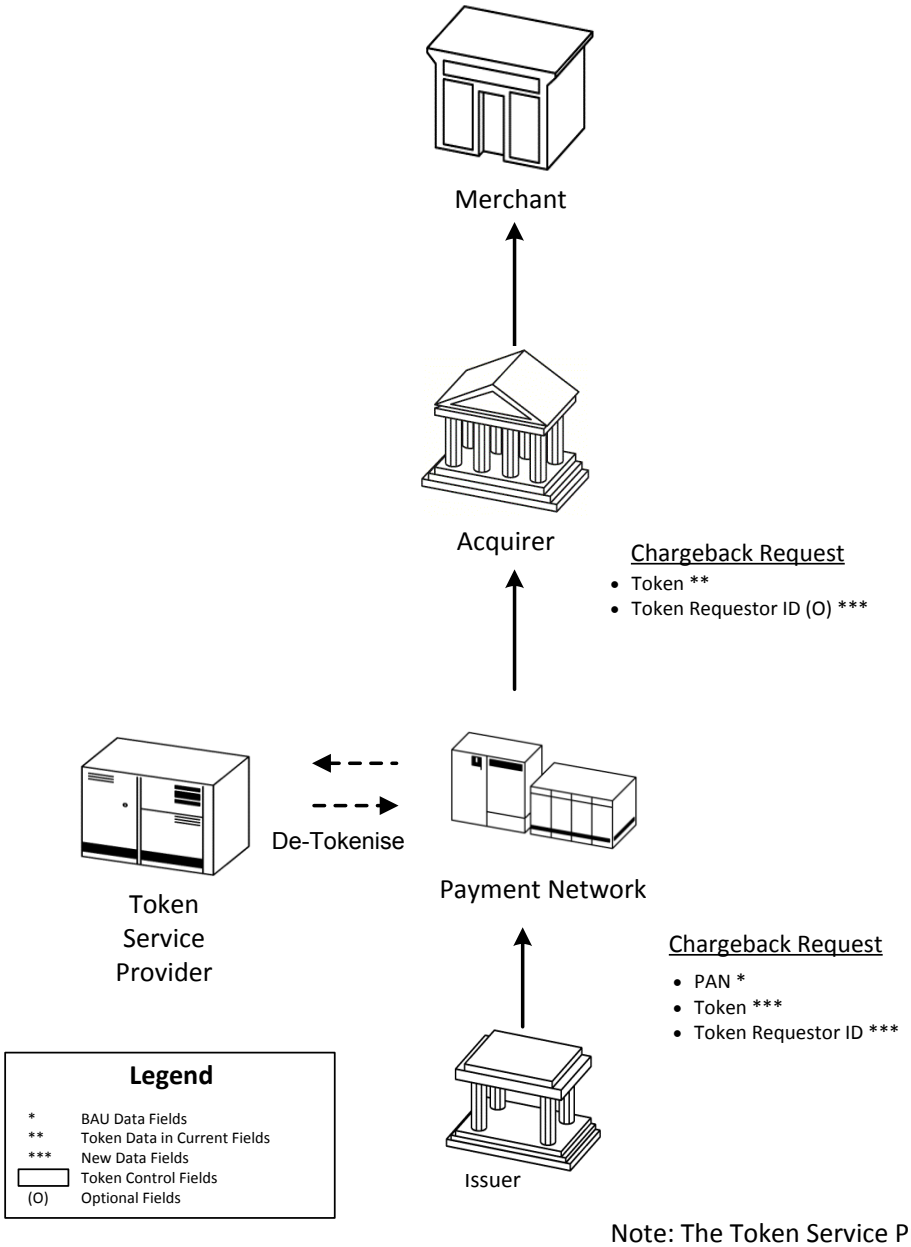
1. The information for Capture File processing is created by the Acquirer based on the information provided by the consumer during transaction initiation. The Payment Token will be passed in the existing PAN field of the Capture File, along with other standard Payment Token data elements, and sent to the Acquirer.

2. The Acquirer will perform processing checks on the data elements, and will use the following Payment Token data fields to create the Clearing File to be sent to the Payment Network:
    a. Payment Token will be passed in the existing PAN field.
    b. POS Entry Mode will be set to the standard POS Entry Mode for the channel-specific transaction, and included in the Clearing File.
    c. Token Assurance Level will be included in the Clearing File and will be a new data field that will be introduced for Payment Token transactions.
    d. Token Requestor ID will be passed as an optional field in the Clearing file.
3. The Payment Network will interface with the Token Service Provider to:
    a. Retrieve the PAN.
    b. Verify the state of the Payment Token to PAN mapping in the Token Vault for the active Payment Token, and other controls that may be defined for that Payment Token.
    c. Validate the Token Domain Restriction Controls for the Payment Token.
4. The Payment Network will send the Clearing File to the Card Issuer, with the following information:
    a. Replace Payment Token with PAN.
    b. Add an indicator that conveys to the Card Issuer that an on-behalf-of validation has been completed by the Token Service Provider of that Payment Token.
    c. Pass the following Payment Token-related fields in the Clearing File. These are new fields sent optionally to the Card Issuer in the Clearing File:
        i. Payment Token
        ii. Token Exp. Date (Optional)
        iii. Token Requestor ID
        iv. Token Assurance Level
5. The Card Issuer performs validation on the Clearing File and completes the clearing process.

9.7 Exception Flow

The following figure shows the Token Processing flow for a chargeback request.

Figure 9: Chargeback Data Elements Flow



Note: The Token Service Provider may be located at the Issuer, Payment Network, or a third party

The following steps explain the flow of the standard Payment Token data fields in the exception handling process of the transaction lifecycle.

1. The Card Issuer typically files for a chargeback after validating that the original transaction is a valid chargeback, and that the Card Issuer has the appropriate chargeback rights.
2. The Card Issuer files for a chargeback and provides the following Payment Token data fields to create the chargeback record to be sent to the Payment Network:
    a. PAN that was used in the original purchase transaction.
    b. Payment Token will be a new data element introduced in the chargeback record that can be provided.
    c. Token Requestor ID will be optionally passed by the Card Issuer
3. The Payment Network will interface with the Token Service Provider to:
    a. Retrieve the PAN.
    b. Verify the state of the Payment Token to PAN mapping in the Token Vault for the active Payment Token, and other controls that may be defined for that Payment Token.
    c. If the Payment Token is not sent by Card Issuer, retrieve the Payment Token for the transaction that is being disputed to send to the Acquirer.
4. Send the chargeback record to the Acquirer with the following information:
    a. Replace PAN with Payment Token.
    b. Token Requestor ID will be passed as an optional field
5. The Acquirer performs validation on the chargeback record, and based on the investigation of the case, moves to another phase of dispute handling or resolves the chargeback.

*** END OF DOCUMENT ***