EMV®
Payment Tokenisation

A Guide to Use Cases

Version 2.2.1

January 2023

Legal Notice

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

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

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

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

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

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

Revision Log – Version 2.2.1

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

- Addition of new use case variation: Token Service Provider in the Issuer Domain (Section 9.4)

Contents

Figures

Tables

1 Introduction

This document, EMV Payment Tokenisation – A Guide to Use Cases (referred to as "A Guide to Use Cases"), is an informational supplement to the EMV Payment Tokenisation Specification – Technical Framework, (referred to as the "Technical Framework"). It describes relationship models and use case examples common to the Technical Framework and is intended to be read in conjunction with the Technical Framework.

The Technical Framework describes a common baseline set of roles and associated functions for Payment Tokenisation that can be adopted to meet the unique payment ecosystem requirements of international, regional, national or local implementations.

1.1 Scope

A Guide to Use Cases describes a limited number of use case examples, some of which are based on established EMV-defined technology:

- Proximity at Point of Sale (Section 8.2)
- Online Wallet (Section 8.3)
- In-Application using a Consumer Device (Section 8.4)
- Card-On-File E-Commerce (Section 8.5)
- E-Commerce Guest Checkout (Section 8.6)
- Third Party Service Provider (Section 8.7)

Section 9 Use Case Variations provides some potential differences and variations to these initial use cases:

- Payment Tokenisation Aggregator (Section 9.1)
- Bulk Token Request (Section 9.2)
- Token Reference IDs (Section 9.3)
- Token Service Provider in the Issuer Domain (Section 9.4)

Section 10 Payment Tokenisation Lifecycle Management describes Payment Token lifecycle management events and provides a limited number of lifecycle management use case examples:

- Merchant Deletion of Payment Credential (Section 10.5)
- Lost / Stolen Consumer Device (Section 10.6)
- PAN Replacement (Section 10.7)

Section 11 Payment Tokenisation and Other EMV Technologies provides use case examples involving Payment Tokenisation and other EMV Technologies:

- SRC E-Commerce Transaction (Section 11.2)
- SRC Guest Checkout Section (11.3)
- Card-On-File E-Commerce with EMV 3DS Payment Authentication Section (11.5)

Section 12 Payment Account Reference describes how Payment Account Reference (PAR) can link transactions made using both Payment Tokens and PAN and provides a limited number of use case examples:

- Transit Open Loop Payments (Section 12.1)
- Merchant Loyalty Schemes Section (12.2)

1.2 Overview

A Guide to Use Cases introduces relationship models which describe potential relationships between the Payment Tokenisation roles. Various common use case examples are given, which include unique relationship models for each use case and example flows for the Issuance of a Payment Token and for transactions. The relationship models and use case examples presented are intended to provide guidance for Payment Tokenisation within existing payment ecosystems and the considerations associated with various usage scenarios. The relationship models and use case examples are neither definitive nor exhaustive since the associated usage scenarios may require additional considerations not provided here. The guidance provided in A Guide to Use Cases does not supersede the Technical Framework or policies and processes defined by a Token Programme.

The relationship models are introduced in the following sections:

- Section 2 Token Programme Participants introduces the Token Programme Participants which feature in the relationship models
- Section 3 Relationship Model Descriptions introduces the basic relationship model, including how the Token Programme Participants fit into the models along with existing payment ecosystem participants such as Merchants
- The basic relationship model is described in more detail in the following sections. Each provides a detailed look at how the relationship model applies to specific common functions. Each model describes the specific relationships between the potential Token Programme Participants, describing the relationship itself and its function
    - Section 4 Token Issuance and Token Provisioning
    - Section 5 Token Presentment
    - Section 6 Token Processing

- Section 7 Payment Token Characteristics describes the characteristics of a Payment Token and how they might be determined for a specific use case

The remainder of A Guide to Use Cases describes specific use case examples as follows:

- Section 8 Use Case Examples takes the detailed relationship models from Sections 4, 5 and 6 and applies them to specific use cases. Each use case example has a specific example of a Token Issuance / Token Provisioning flow (issuance flow) and a Token Presentment / Token Processing flow (transaction flow). These flows are based on defined preconditions, setup activities and other flow assumptions
- Section 9 Use Case Variations takes the detailed relationship models from Sections 4, 5 and 6 and shows how they may vary depending on the particular use case variation
- Section 10 Payment Tokenisation Lifecycle Management shows how the relationship model applies to lifecycle management. It describes how existing relationships between the potential Token Programme Participants are used for lifecycle management and the function(s) of those relationships
- Section 11 Payment Tokenisation and Other EMV Technologies shows how Payment Tokenisation can be used with other EMV Technologies, such as Secure Remote Commerce (SRC) and EMV® 3-D Secure (EMV 3DS). It describes how Payment Tokenisation roles map to entities / functions in the other EMV Technology
- Section 12 Payment Account Reference provides examples of how Payment Account Reference (PAR) can link transactions made using both Payment Tokens and PAN

1.3 Audience

A Guide to Use Cases is intended for use by all participants in the payment ecosystem, such as Card Issuers, Merchants, Acquirers, Payment Systems, Payment Networks, Payment Processors, and third-party service providers.

1.4 References

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

1.4.1 Published EMVCo Documents

The documents in Table 1.1 contain provisions that are referenced in this guide and are available from www.emvco.com.

Table 1.1: EMVCo References

Reference	Publication Name
EMV 3DS	EMV® 3-D Secure – Protocol and Core Functions Specification
EMV Contactless	EMV® Contactless Specifications for Payment Systems
PAR White Paper	EMV® White Paper on Payment Account Reference
QR Code	EMV® QR Code Specification for Payment Systems (EMV QRCPS) – Merchant-Presented Mode
SRC	EMV® Secure Remote Commerce Specification
Technical Framework	EMV® Payment Tokenisation Specification – Technical Framework
Transaction Types	EMV® Best Practices Document – Recommendations for EMV Processing for Industry-Specific Transaction Types

1.5 Definitions

For a list of defined terms used in A Guide to Use Cases, please refer to Table 1.3 in Section 1.5 of the Technical Framework.

1.6 Notational Conventions

1.6.1 Abbreviations

The abbreviations listed in Table 1.2 are used in A Guide to Use Cases.

Table 1.2: Abbreviations

Abbreviation	Description
ACS	Access Control Server
API	Application Programming Interface
AReq	Authentication Request
ARes	Authentication Response

Abbreviation	Description
CDE	Cardholder Data Environment
DS	Directory Server
ICC	Integrated Circuit Card
ID&V	Identification and Verification
MST	Magnetic Secure Transmission
NFC	Near Field Communication
PAN	Primary Account Number
PAR	Payment Account Reference
PCI	Payment Card Industry
PCI DDS	Payment Card Industry Data Security Standard
POS	Point Of Sale
QR	Quick Response
SDK	Software Development Kit

1.6.2 Terminology and Conventions

A Guide to Use Cases uses the following words which have a specific meaning:

Assumptions

Assumptions for a given example flow are specific to that example flow, but not the wider use case. Different assumptions are part of the same use case but would refer to a different example flow.

Consumer / Cardholder

The terms Consumer and Cardholder are defined terms, as defined in the Technical Framework. They are used here in the following way.

A Consumer may have access to multiple payment credentials (representing underlying Payment Accounts). Each use case flow begins with an interaction involving a Consumer. Whenever a Consumer selects a specific payment credential (represented by a PAN), the Consumer then assumes the role of the Cardholder for the remainder of that use case.

Entity (Role)

When an entity is performing a specific Payment Tokenisation role, this is denoted by writing the role in parenthesis after the entity. For example, when a mobile payment application is performing the role of a Token Requestor, it is written as mobile payment application (Token Requestor).

Preconditions

Preconditions for a given example flow are those which must occur in order for the use case to exist.

Usage Scenario

A specific instance of Technical Framework usage that has common, distinct characteristics such as technologies used, Token Presentment Mode utilised, etc. This is usually representing the presentment, acceptance and intended payment offering to Consumers/Cardholders in the ecosystem.

Relationship Model

A construct that describes relationships between each specific Payment Tokenisation role and describes the common set of functions.

Use Case

A specific example of utilisation of the Technical Framework within a usage scenario, showing specifics of relationships and interactions between Payment Tokenisation roles. It includes an example issuance flow showing Token Issuance / Token Provisioning and an example transaction flow showing Token Presentment / Token Processing.

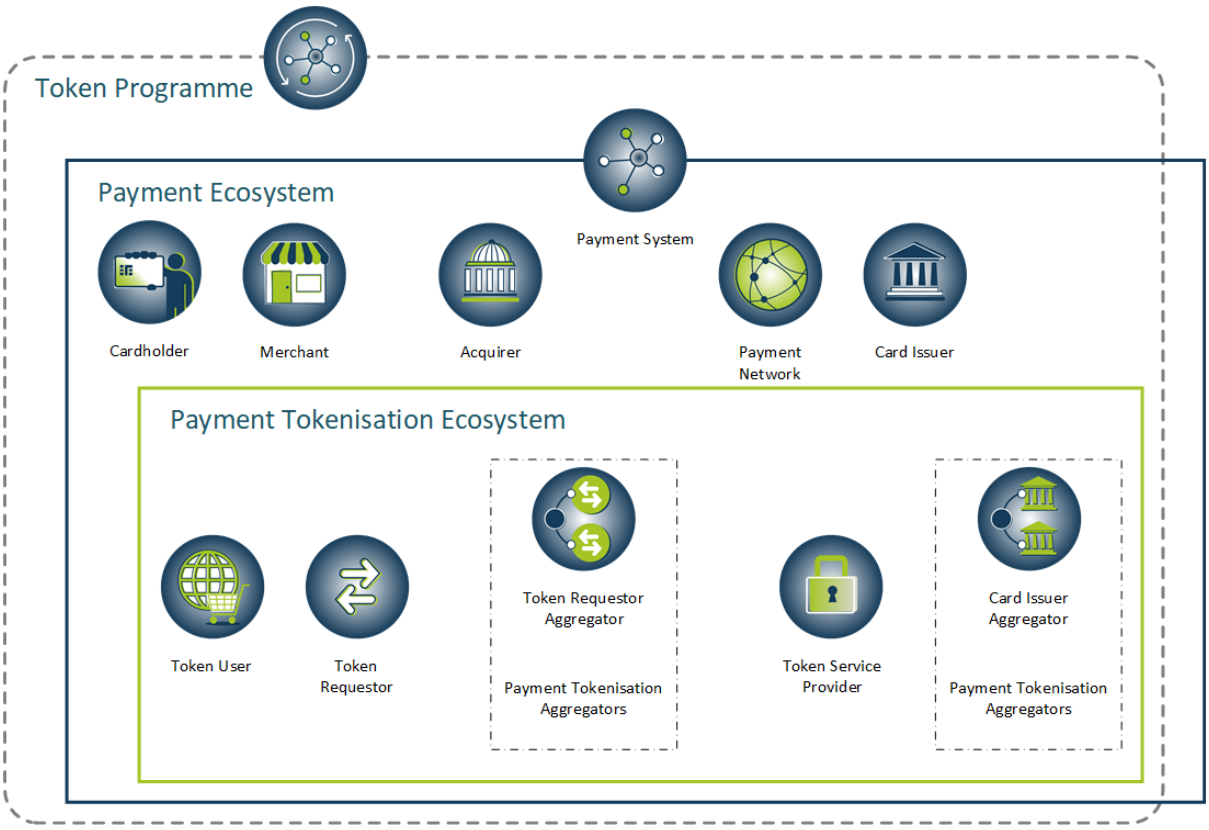
1.7 Further Information

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

2 Token Programme Participants

The Token Programme has an overarching responsibility, defining the processes, policies and registration programmes for the establishment and operation of a Payment Tokenisation ecosystem. Token Programme support of a usage scenario will include policies and processes to support the specifics of each use case. Each Token Programme may support some or all of the use cases contained within A Guide to Use Cases, as well as support use cases not described here. Figure 2.1 provides an overview of the Payment Tokenisation ecosystem.

Figure 2.1: Payment Tokenisation Ecosystem Overview

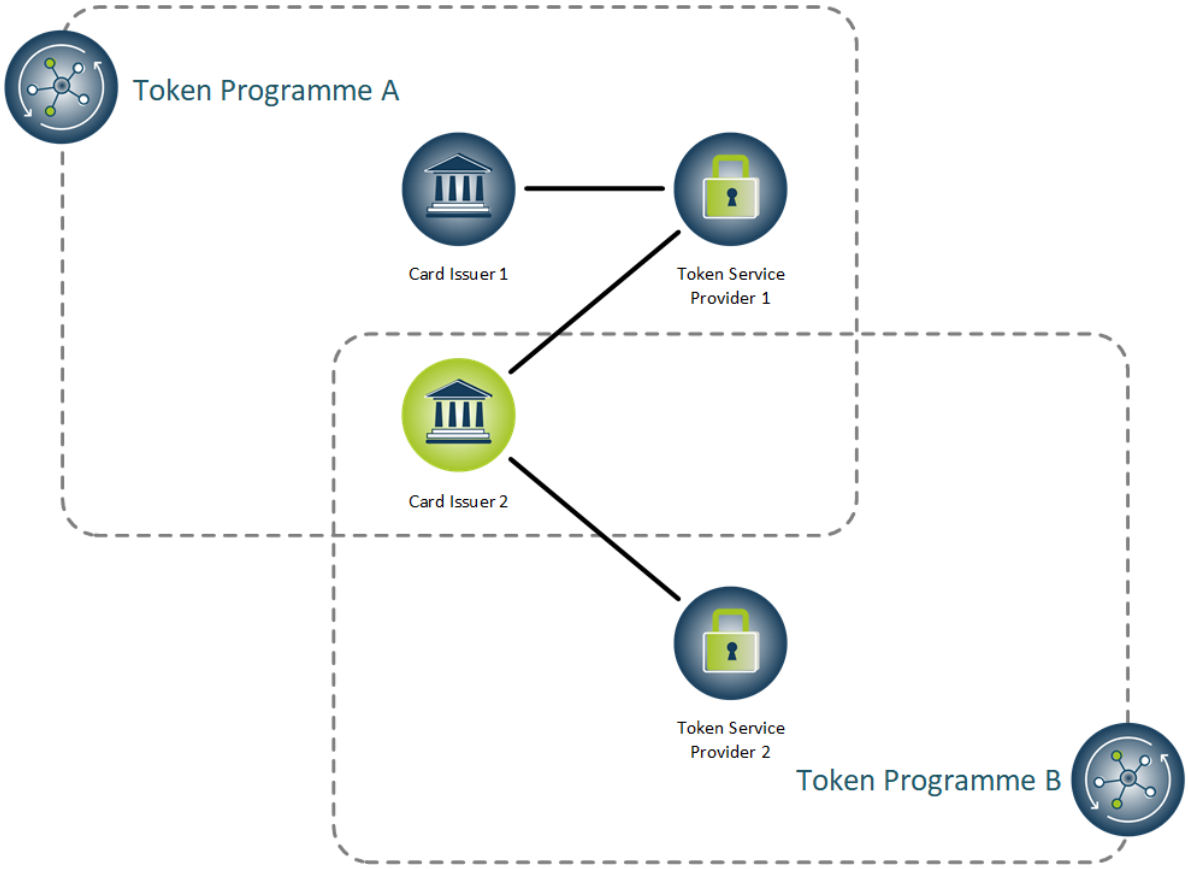


2.1 Card Issuers

A Token Programme includes participation of one or more Card Issuers. A Card Issuer that supports multiple Payment Systems may participate in multiple Token Programmes. This is illustrated in Figure 2.2, which shows an example of Card Issuers participating in one or more Token Programmes and interacting with one or more Token Service Providers. Card Issuer 2, which is shown in green, participates in both Token Programme A and Token Programme B, whereas Card Issuer 1 only participates in Token Programme A.

Card Issuers that participate in multiple Token Programmes for a given use case will support the policies, processes and registration programmes of each Token Programme for that use case.

Figure 2.2: Card Issuers

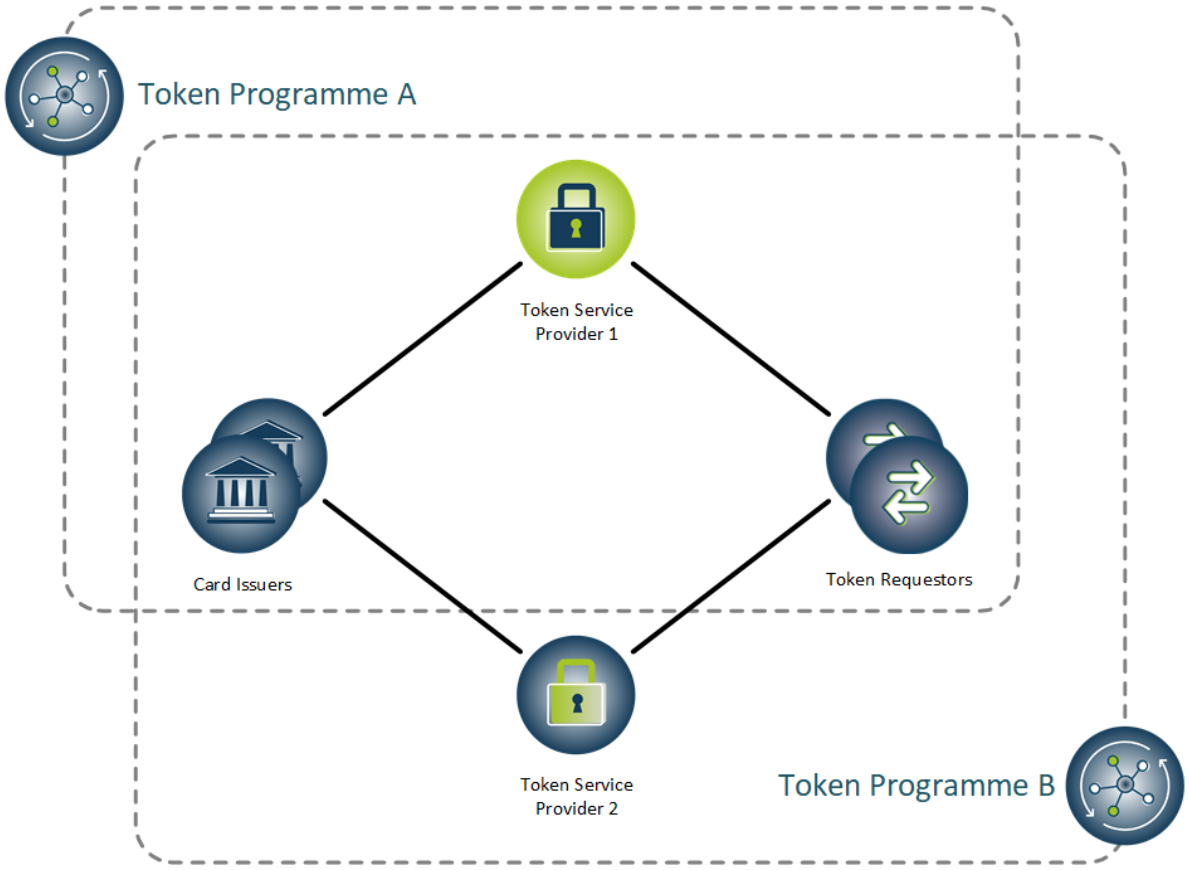


2.2 Token Service Providers

The Technical Framework supports a variety of ways for Token Service Providers to participate in a Token Programme. The participation of a Token Service Provider or multiple Token Service Providers is subject to the policies of the Token Programme. Token Service Providers may provide support to a single or multiple Card Issuer(s) and participate in one or more Token Programmes.

This is illustrated in Figure 2.3, where Token Service Provider 1, which is shown in green, participates in both Token Programme A and Token Programme B, whereas Token Service Provider 2 only participates in Token Programme B.

Figure 2.3: Token Service Providers

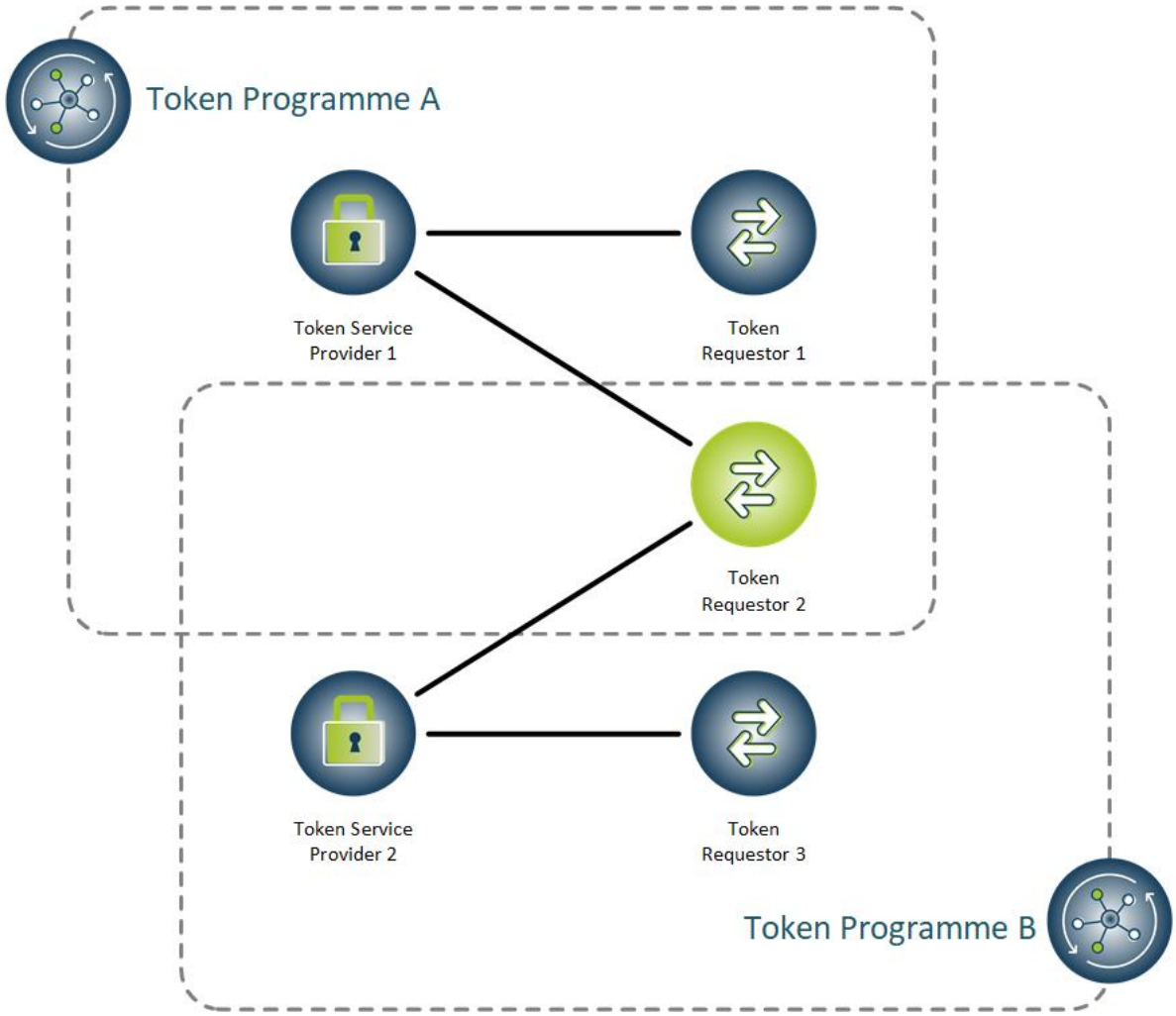


2.3 Token Requestors

Token Requestors may support a wide variety of use cases and may have a variety of relationships with Token Service Providers. Each Token Service Provider registers Token Requestors in accordance to the established processes of each Token Programme.

Token Requestors may participate in one or more Token Programmes. This is illustrated by Token Requestor 2 (shown in green in Figure 2.4), which particpates in both Token Programme A and B whereas Token Requestor 1 and 3 only particpate in a single Token Programme (A and B respectively). This provides one example of the possible relationships between Token Service Providers and Token Requestors. For purposes of simplicity, the Card Issuers shown in Figure 2.3 have not been included in Figure 2.4.

Figure 2.4: Token Requestors



2.4 Token Users

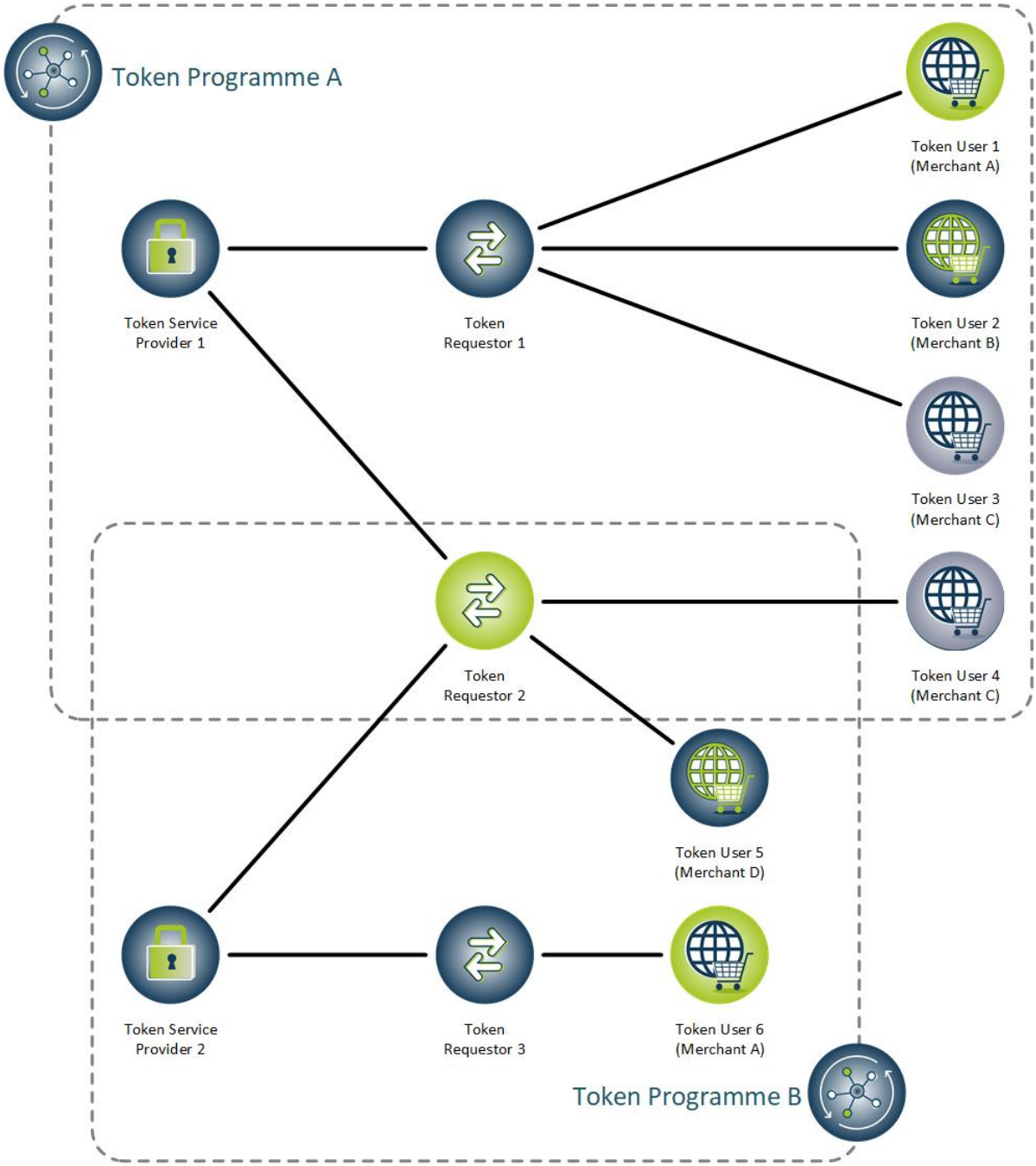
The Token User is a Payment Tokenisation specific role. Token Users initiate Token Payment Requests with Payment Tokens which have been received from Token Requestors. The Token User will have a relationship with one or more Token Requestors. Token Requestors may define requirements for the use of Payment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

An example of the possible relationships between Token Users and Token Requestors is shown in Figure 2.5. In this figure, Merchant A is shown in green and participates in two distinct Token Programmes. When participating in Token Programme A, Merchant A interacts with Token Requestor 1 as Token User 1, while the same Merchant A interacts with Token Requestor 3 as Token User 6 when participating in Token Programme B.

A second relationship example is illustrated by Merchant C, which is shown in grey. Merchant C only participates in Token Programme A, but interacts with two Token Requestors. It

interacts with Token Requestor 1 as Token User 3 and with Token Requestor 2 as Token User 4.

Figure 2.5: Token Users



2.5 Payment Tokenisation Aggregators

The Payment Tokenisation Aggregator is a Payment Tokenisation specific role. Payment Tokenisation Aggregators interact with one or more Token Service Providers in order to facilitate some or all Payment Token related activities by acting as a service provider on behalf of one or more Payment Tokenisation roles or existing ecosystem entities. The Technical Framework identifies the following specific types of Payment Tokenisation Aggregator. These are:

- Token Requestor Aggregator
- Card Issuer Aggregator

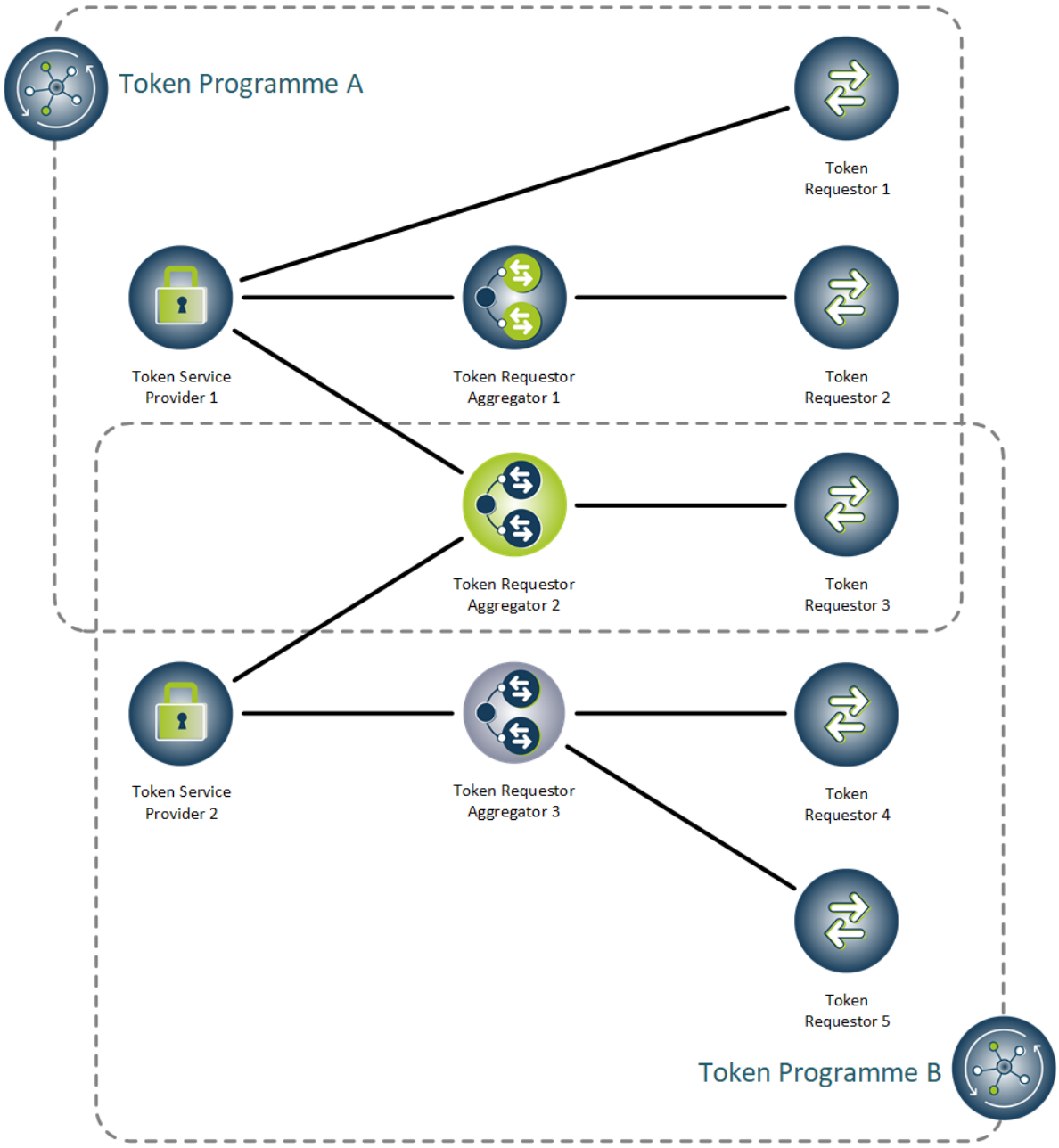
2.5.1 Token Requestor Aggregators

Figure 2.6 shows several possible relationships. Token Requestor Aggregator 1 is shown in blue and only participates in Token Programme A, interacting with Token Requestors and Token Service Providers that are only participating in Token Programme A. Similarly, Token Requestor Aggregator 3 is shown in grey and only participates in Token Programme B, interacting with Token Requestors and Token Service Providers that are only participating in Token Programme B.

In contrast, Token Requestor Aggregator 2 is shown in green and participates in both Token Programme A and B. When Token Requestor Aggregator 2 is interacting with Token Service Provider 1, it is participating in Token Programme A, while when interacting with Token Service Provider 2, it is participating in Token Programme B. In this example, Token Requestor Aggregator 2 is interacting with Token Requestor 3 in both these cases, with Token Requestor 3 participating in both Token Programme A and B.

In addition, Figure 2.6 shows Token Service Provider 1 interacting directly with Token Requestor 1, while it interacts with Token Requestor 2 through Token Requestor Aggregator 1 (blue) and with Token Requestor 3 through Token Requestor Aggregator 2 (green). In contrast, Token Service Provider 2 only interacts with Token Requestors through Token Requestor Aggregators.

Figure 2.6: Token Request Aggregators



2.5.2 Card Issuer Aggregators

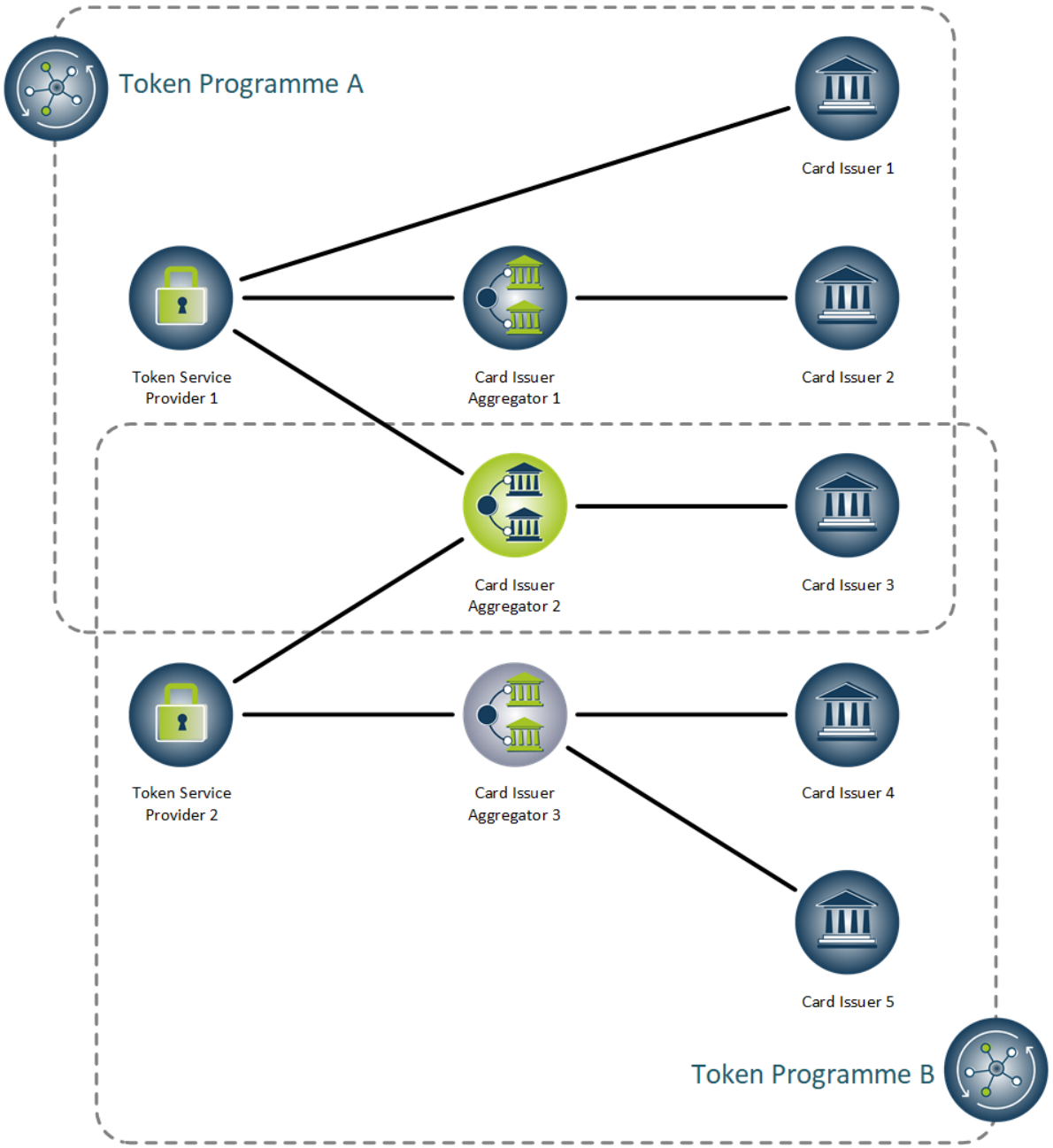
Figure 2.7 shows several possible relationships. Card Issuer Aggregator 1 is shown in blue and participates in Token Programme A, only interacting with Card Issuers and Token Service Providers that are participating in Token Programme A. Similarly, Card Issuer Aggregator 3 is shown in grey and participates in Token Programme B, only interacting with Card Issuers and Token Service Providers that are participating in Token Programme B.

In contrast, Card Issuer Aggregator 2 is shown in green and participates in both Token Programme A and B. When Card Issuer Aggregator 2 is interacting with Token Service

Provider 1, it is participating in Token Programme A, while when interacting with Token Service Provider 2, it is participating in Token Programme B. In this example, Card Issuer Aggregator 2 is interacting with Card Issuer 3 in both these cases, with Card Issuer 3 participating in both Token Programme A and B.

In addition, Figure 2.7 shows Token Service Provider 1 interacting directly with Card Issuer 1, while it interacts with Card Issuer 2 through Card Issuer Aggregator 1 (blue) and with Card Issuer 3 through Card Issuer Aggregator 2 (green). In contrast, Token Service Provider 2 only interacts with Card Issuers through Card Issuer Aggregators.

Figure 2.7: Card Issuer Aggregators



3 Relationship Model Descriptions

The introduction of Payment Tokenisation into an existing payment ecosystem requires consideration of usage scenarios. Within each Token Programme, many functions may be common across usage scenarios. These common functions are associated with processes that are grouped as follows:

- Token Issuance and Token Provisioning
- Token Presentment
- Token Processing

Each process is comprised of functions performed in usage scenarios that may be applied as guidelines for use case examples (for a definition of usage scenarios and use cases, see Section 1.6.2 Terminology and Conventions). Not all processes may be present in any given usage scenario or use case example.

The Technical Framework identifies a number of roles within the Payment Tokenisation ecosystem that carry out these functions and processes. Some are existing roles within the traditional payment ecosystem, and others are Payment Tokenisation specific roles defined by the Technical Framework.

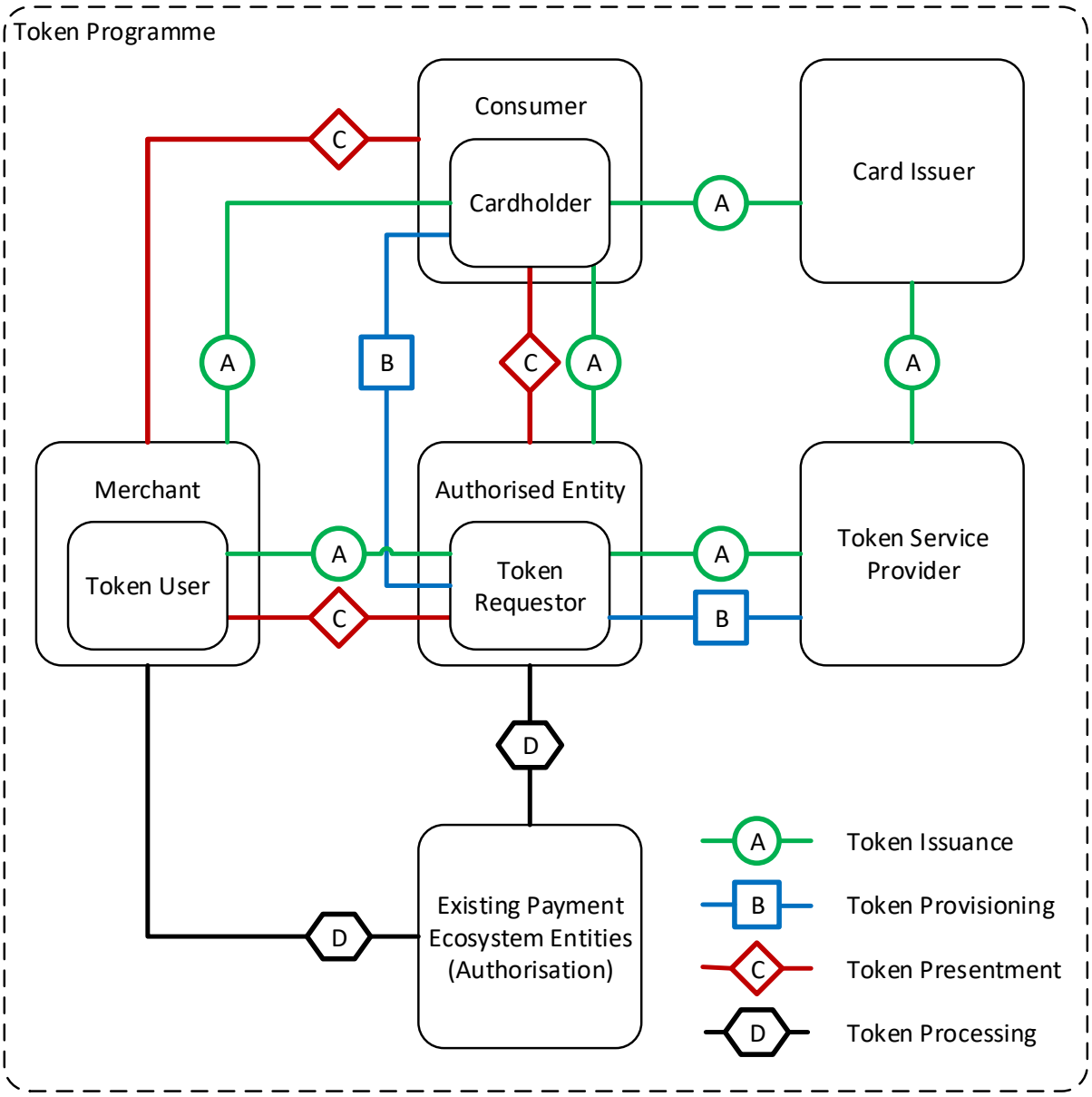
A Guide to Use Cases introduces a number of examples showing models demonstrating relationships between roles associated with Payment Tokenisation that represent the potential processes and functions performed. Some existing relationships are utilised by Payment Tokenisation, while others are specific to Payment Tokenisation. Each relationship is managed in accordance with the policies, processes and registration programmes of a specific Token Programme. Each example relationship model has a number of characteristics which have typical outcomes associated with specific use cases.

3.1 Relationship Model Diagram

Figure 3.1 displays all relationship models in a single diagram (for a definition of relationship model, see Section 1.6.2 Terminology and Conventions). These represent the various processes, showing the potential placement of the various Payment Tokenisation roles within the Payment Tokenisation ecosystem. This diagram represents a common configuration for Payment Tokenisation roles and their relationships by identifying the roles as boxes and relationships as lines.

Note that not all roles and relationships may be present in any given usage scenario.

Figure 3.1: Payment Token Ecosystem Relationship Model



This diagram establishes a baseline representation which is the basis for the more detailed relationship model diagrams introduced in the following sections:

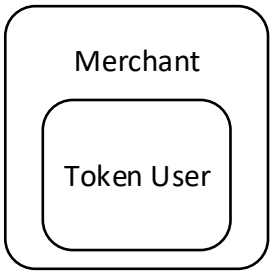
- Section 4 Token Issuance and Token Provisioning
- Section 5 Token Presentment
- Section 6 Token Processing

3.2 Understanding the Relationship Model Diagram

In Section 3.1 Relationship Model Diagram, the single diagram in Figure 3.1 gives all potential relationships between the various Payment Tokenisation roles within the Payment Tokenisation ecosystem.

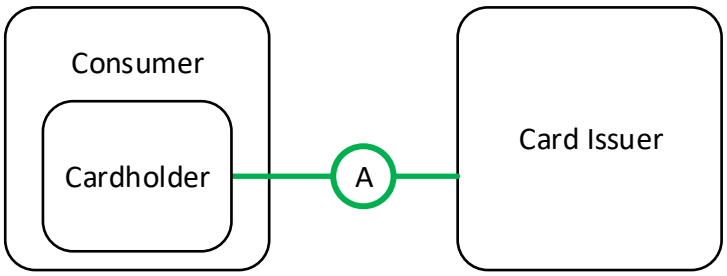
Where applicable, known entities that commonly perform the Payment Tokenisation role are included. Sometimes an additional, inner box is present within a larger, outer box. This occurs when an entity performs a specific role at some point during the process. For example, Figure 3.2 shows the Merchant / Token User. This is an example of a Merchant (shown by the outer box) performing the Payment Tokenisation role of Token User (shown by the inner box). When this is described in any text accompanying the figure, it is written as Merchant (Token User).

Figure 3.2: Example Roles



The lines in Figure 3.1 represent relationships between entities/roles and not flows. Relationships can exist between entities, between roles and between entities and roles. These are denoted by the lines in the relationship diagrams, which may join the outer boxes or the inner boxes, depending on the precise relationship being described. For example, Figure 3.3 shows the relationship between the Cardholder (not the Consumer) and the Card Issuer.

Figure 3.3: Example Relationships

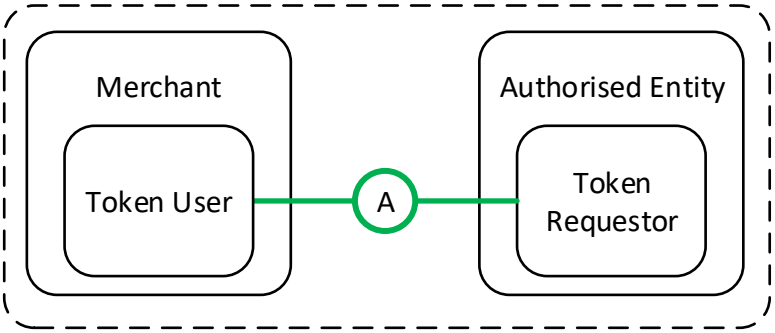


In certain relationship model diagrams, both a Token Requestor and a Token User are shown surrounded by a dashed line. This indicates that in certain use case examples, both roles can be present, while in other use cases, only the Token Requestor role is present.

An example is given in Figure 3.4, where both the Token User and the Token Requestor are shown, with a Merchant performing the role of Token User and an Authorised Entity performing

the role of Token Requestor. The relationship shown between the Token User and Token Requestor will not be present in use case examples which do not have a Token User.

Figure 3.4: Token User Example



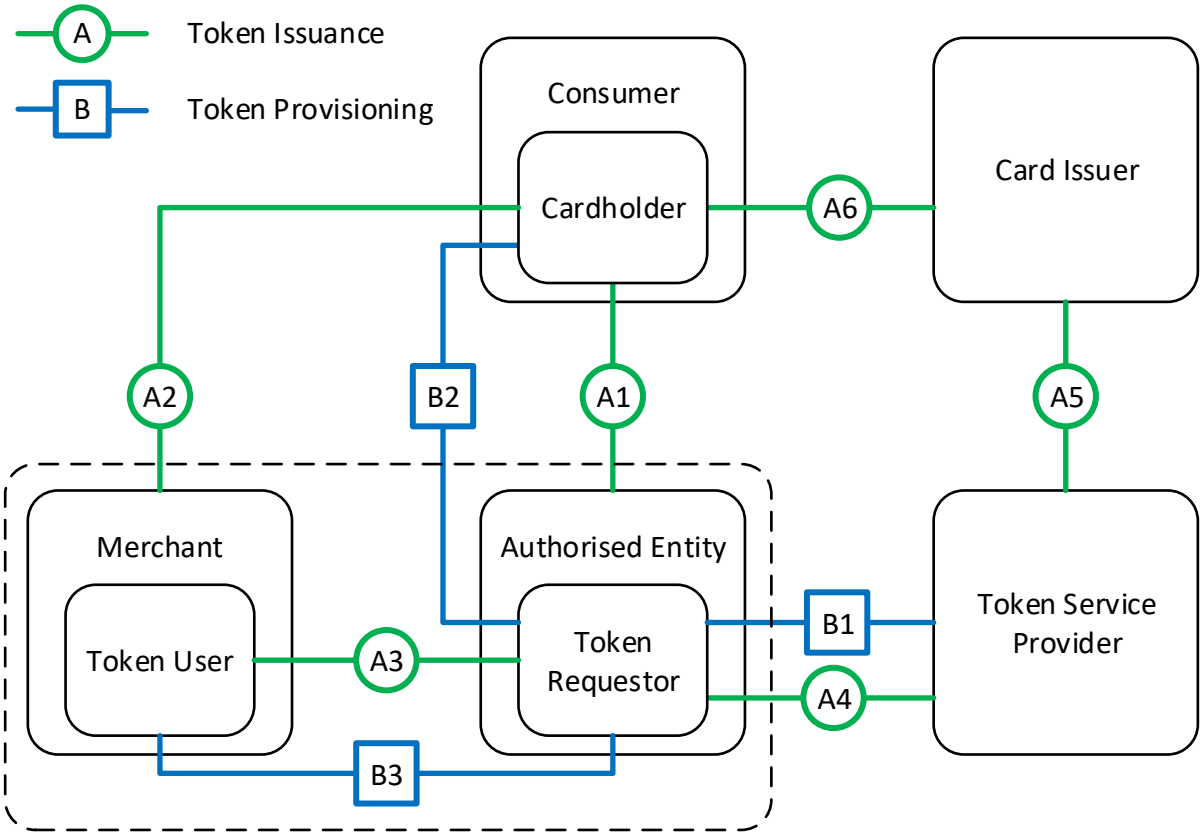
4 Token Issuance and Token Provisioning

Token Issuance and Token Provisioning occurs after Token Generation in response to a Token Request from a registered Token Requestor with a valid Token Requestor ID. Considerations for the issuance of Payment Tokens include policies and processes for Token Assurance, Token Generation, Token Issuance, and Token Provisioning. This includes any implications of specific technologies and processes.

4.1 Token Issuance and Token Provisioning Relationships and Functions

The possible relationships for Token Issuance and Token Provisioning are shown in Figure 4.1 and are dependent on the specific usage scenario. Not all relationships may be present in any given usage scenario. Note that the relationships in the figure do not imply flows between the entities shown and the numbers do not represent any specific order. Each relationship and how it may be utilised within Payment Tokenisation is described in the text following the figure, along with its function.

Figure 4.1: Token Issuance (A) and Token Provisioning (B) Relationships



Note that certain relationships only apply to a limited number of use cases, while other relationships do not vary by use case (although they are not necessarily present in all use cases). These instances are noted in the individual relationship descriptions.

4.1.1 A1. Cardholder – Authorised Entity (Token Requestor)

Relationship: The Cardholder may have an existing relationship with the authorised entity (Token Requestor) which can be utilised for Payment Tokenisation.

Function: The Cardholder provides a PAN and related data to the authorised entity (Token Requestor) which triggers the Token Issuance Process. How the PAN and related data are provided depends on the Use Case. The authorised entity (Token Requestor) may involve the active participation of the Cardholder in Token Assurance as described in the Technical Framework, Section 6 Token Assurance Method. There are many Token Assurance Method variations possible within a use case and any Cardholder interaction for performing ID&V is outside the scope of the use case examples.

4.1.2 A2. Cardholder – Merchant (Token User)

This relationship only applies when the Merchant is performing the role of Token User (see Section 8.7 Third Party Service Provider).

Relationship: The Cardholder may have an existing relationship with the Merchant (Token User) which can be utilised for Payment Tokenisation.

Function: The Cardholder provides a PAN and related data to the Merchant (Token User) which triggers the Token Issuance Process. How the PAN and related data are provided depends on the Use Case.

4.1.3 A3. Merchant (Token User) – Authorised Entity (Token Requestor)

This relationship only applies when the Merchant is performing the role of Token User (see Section 8.7 Third Party Service Provider).

Relationship: The Merchant (Token User) has an existing relationship with the authorised entity (Token Requestor) which can be utilised for Payment Tokenisation.

Function: The Merchant (Token User) provides a PAN and related data to the authorised entity (Token Requestor), which triggers the Token Issuance process.

4.1.4 A4. Token Service Provider – Authorised Entity (Token Requestor)

Relationship: The Token Service Provider provides Token Issuance services to the authorised entity (Token Requestor) on behalf of a Card Issuer. For each Token Request, the authorised entity (Token Requestor) identifies itself using the applicable registered Token Requestor ID assigned by the Token Service Provider.

Function: The authorised entity (Token Requestor) initiates a Token Request with its assigned Token Requestor ID, using a PAN and related data.

4.1.5 A5. Card Issuer – Token Service Provider

This relationship does not vary by use case.

Relationship: The Card Issuer uses the Token Service Provider to provide Token Issuance and Token Provisioning services to Token Requestors.

Function: The Token Service Provider may involve the Card Issuer in Token Assurance. For all issuance flows, it is assumed that the Card Issuer is performing ID&V as part of Token Assurance.

4.1.6 A6. Card Issuer – Cardholder

This relationship does not vary by use case.

Relationship: The existing Card Issuer – Cardholder relationship is utilised for the issuance of Payment Tokens.

Function: The Card Issuer may involve the Cardholder in Token Assurance but any Cardholder interaction for performing ID&V is outside the scope of the use case examples.

4.1.7 B1. Token Service Provider – Authorised Entity (Token Requestor)

Relationship: The Token Service Provider provides Token Provisioning services to the authorised entity (Token Requestor) on behalf of a Card Issuer.

Function: After Token Issuance, the Token Service Provider delivers the Payment Token and related data to the authorised entity (Token Requestor), which, subject to the use case, either stores it in the Token Location or delivers it to the Token Location.

4.1.8 B2. Cardholder – Authorised Entity (Token Requestor)

This relationship only applies to the Proximity at Point of Sale (Section 8.2) and In-Application using a Consumer Device (Section 8.4) use cases.

Relationship: The authorised entity (Token Requestor) extends Token Provisioning services to the Cardholder.

Function: The authorised entity (Token Requestor) delivers the Payment Token and related data to the Token Location.

4.1.9 B3. Merchant (Token User) – Authorised Entity (Token Requestor)

This relationship only applies when the Merchant is performing the role of Token User (see Section 8.7 Third Party Service Provider).

Relationship: The authorised entity (Token Requestor) extends Token Provisioning services to the Merchant (Token User).

Function: The authorised entity (Token Requestor) delivers the Payment Token and related data to the Token Location.

4.1.10 Variations to Relationships

Figure 4.1 represents all possible roles and therefore explicitly shows separate Token User and Token Requestor (shown by the box with dashed lines in the figure). However, the role of Token User only applies to use cases where the Merchant is not the Token Requestor. See, for example:

- Section 8.3 Online Wallet
- Section 8.7 Third Party Service Provider.

For variations where there is no Token User role, see, for example:

- Figure 8.1 (Section 8.2 Proximity at Point of Sale)
- Figure 8.9 (Section 8.5 Card-On-File E-Commerce)

4.2 Token Issuance Characteristics

Characteristics for Token Issuance include consideration of the availability of the Cardholder at the time the Payment Token is requested and issued. The Token Service Provider will use information provided within the Token Request to facilitate Cardholder participation in any relevant Token Assurance steps that are taken.

How the Payment Token is issued depends on the use case and this drives the Token Issuance characteristics shown in Table 4.1.

Table 4.1: Token Issuance Characteristics

Characteristic	Description	Typical Outcomes
Cardholder Availability	Cardholder availability may be required before Token Issuance can take place.	• Required • Not Required

4.3 Token Provisioning Characteristics

Characteristics for Token Provisioning include the Token Location.

How the Payment Token is provisioned depends on the use case and this drives the Token Provisioning characteristics shown in Table 4.2.

Table 4.2: Token Provisioning Characteristics

Characteristic	Description	Typical Outcomes
Token Location	The location where the Payment Token and related data is provisioned. See Table 5.1 of the Technical Framework for defined Token Locations.	• 00 – 99

5 Token Presentment

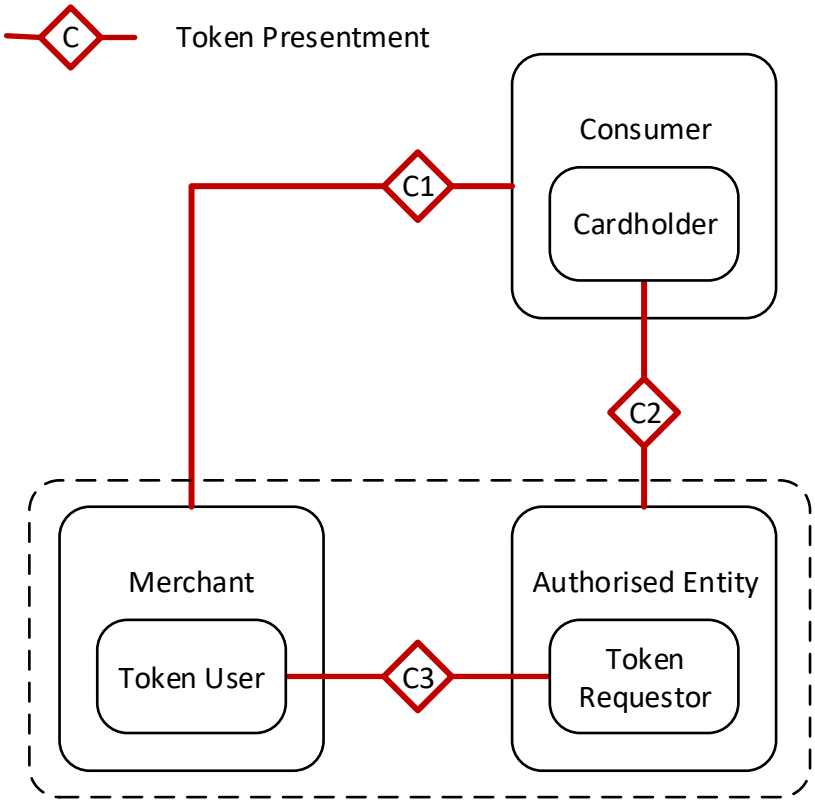
Token Presentment is the process of the Payment Token being presented or made available to the Merchant to start the Token Processing flow. Token Presentment occurs prior to Token Processing as shown in Figure 3.2 of the Technical Framework and follows existing PAN presentment modes for Cardholder-Initiated Transactions.

Merchant-Initiated Transactions do not have Token Presentment as a component of a use case since the Merchant will already possess the Payment Token. Therefore Merchant-Initiated Transactions start with Token Processing.

5.1 Token Presentment Relationships and Functions

The possible relationships for Token Presentment are shown in Figure 5.1 and are dependent on the specific usage scenario. Not all relationships may be present in any given usage scenario. Note that the relationships in the figure do not imply flows between the entities shown and the numbers do not represent any specific order. Each relationship and how it may be utilised within Payment Tokenisation is described in the text following the figure, along with its function.

Figure 5.1: Token Presentment Relationships



5.1.1 C1. Consumer / Cardholder – Merchant

Relationship: The existing Consumer / Cardholder – Merchant relationship is utilised for Cardholder-Initiated Transactions with a Payment Token. Whenever a Consumer selects a specific payment credential (represented by a PAN), the Consumer then assumes the role of the Cardholder for the remainder of that use case. The relationship between the Consumer and the Merchant (which may perform the role of Token User) may end on the completion of the specific Cardholder-Initiated Transaction or it may persist as a Merchant-managed Consumer account.

Function: The Consumer makes a purchase from the Merchant. Depending on the use case, the Cardholder then selects a payment credential, represented by a PAN (which has an affiliated Payment Token). This results in a Payment Token being received by the Merchant (which may perform the role of a Token User) or a Third Party Service Provider acting on behalf of the Merchant which leads to Token Processing for a Cardholder-Initiated Transaction. How this is achieved is use-case dependent.

5.1.2 C2. Cardholder – Authorised Entity (Token Requestor)

Relationship: The Cardholder may have an existing relationship with the authorised entity (Token Requestor) which can be utilised for Payment Tokenisation. It is not expected that the Cardholder will have any awareness of the role of Token Requestor.

Function: The Cardholder selects the payment credential (which has an affiliated Payment Token) from the authorised entity (Token Requestor).

5.1.3 C3. Merchant (Token User) – Authorised Entity (Token Requestor)

Relationship: The Merchant (Token User) has an existing relationship with the authorised entity (Token Requestor) which can be utilised for Payment Tokenisation. This relationship applies to all use cases where Token Requestors provide Payment Tokenisation services to Token Users.

Function: In use cases where the Merchant (Token User) initiates Token Processing, the necessary data is provided to the Merchant (Token User) by the Authorised Entity (Token Requestor). In use cases where the Authorised Entity (Token Requestor) initiates Token Processing, the necessary data is provided to Authorised Entity (Token Requestor) by the Merchant (Token User).

5.1.4 Variations to Relationships

Figure 5.1 represents all possible roles and therefore explicitly shows separate Token User and Token Requestor (shown by the box with dashed lines in the figure). However, the role of Token User only applies to use cases where the Merchant is not the Token Requestor. See, for example:

- Section 8.3 Online Wallet
- Section 8.4 In-Application using a Consumer Device

For variations where there is no Token User role, see, for example:

- Figure 8.1 (Section 8.2 Proximity at Point of Sale)
- Figure 8.9 (Section 8.5 Card-On-File E-Commerce)

5.2 Token Presentment Characteristics

Characteristics for Token Presentment include consideration of the Consumer access to the technology enabling Token Presentment and the acceptance environment.

How the Payment Token is presented depends on the use case and this drives the Token Presentment characteristics shown in Table 5.1.

Table 5.1: Token Presentment Characteristics

Characteristic	Description	Typical Outcomes
Token Presentment	How the Payment Token is presented to the Merchant during Token Presentment. For Proximity use cases, the Cardholder and / or Consumer Device is physically present, with the proximity bound by the range of the technology enabling the Merchant acceptance environment.	• Proximity • Non-proximity
Acceptance Environment	The Merchant acceptance environment at the time of Token Presentment.	• Physical • Non-physical

6 Token Processing

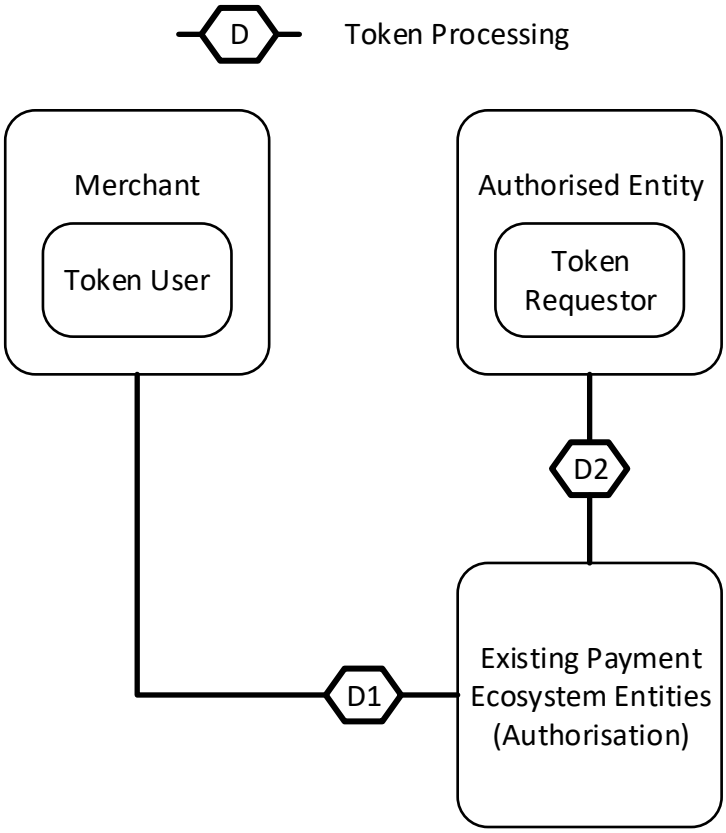
Token Processing occurs when the Payment Token and related data is processed to obtain an authorisation decision for a transaction as described in Section 10 of the Technical Framework.

6.1 Token Processing Relationships and Functions

The possible relationships for Token Processing are shown in Figure 6.1 and are dependent on specific usage scenarios. Not all relationships may be present in any given usage scenario. Note that the relationships in the figure do not imply flows between the entities shown and the numbers do not represent any specific order. Each relationship and how it may be utilised within Payment Tokenisation is described in the text following the figure, along with its function.

The existing payment ecosystem entities shown in the figure represent the existing entities in the payment ecosystem which undertake business-as-usual authorisation processes as described in Section 10.2 of the Technical Framework.

Figure 6.1: Token Processing Relationships



The two options for the relationship D are given in Section 6.1.1 D1. Merchant – Existing Payment Ecosystem Entities and 6.1.2 D2. Authorised Entity (Token Requestor) – Existing Payment Ecosystem Entities. In any given use case example, only one of these relationships is shown.

Note that certain relationships only apply to a limited number of use cases, while other relationships do not vary by use case (although they are not necessarily present in all use cases). These instances are noted in the individual relationship descriptions.

6.1.1 D1. Merchant – Existing Payment Ecosystem Entities

This relationship does not vary by use case.

Relationship: The Merchant (which may perform the role of Token User) utilises existing relationships to initiate Token Processing.

Function: The Merchant submits a Token Payment Request using the Payment Token and related data.

6.1.2 D2. Authorised Entity (Token Requestor) – Existing Payment Ecosystem Entities

The relationship does not vary by use case.

Relationship: The authorised entity (Token Requestor) utilises existing relationships to initiate Token Processing on behalf of the Merchant (which may perform the role of Token User).

Function: The authorised entity submits a Token Payment Request using the Payment Token and related data.

6.2 Token Processing Characteristics

Characteristics for Token Processing include consideration of the entity that initiates a Payment Token Request and the support of Token Control Fields.

How the Payment Token is processed depends on the use case and this drives the Token Processing characteristics shown in Table 6.1.

Table 6.1: Token Processing Characteristics

Characteristic	Description	Typical Outcomes
Token Payment Request	The entity responsible for submitting the Token Payment Request to obtain a PAN authorisation.	• Merchant • Third Party Service Provider

Characteristic	Description	Typical Outcomes
Token Control Fields	Token Control Fields are defined in the Technical Framework in Table 10-5 (Cardholder-Initiated Transactions) and Table 10-6 (Merchant-Initiated Transactions).	• See Technical Framework Tables 10-5 and 10-6.

7 Payment Token Characteristics

Payment Token integrity is achieved by considering the relationship model characteristics of each use case and establishing Token Programme policies and processes for:

- Token Assurance Method, based on Token Issuance and Token Provisioning relationship model characteristics
- Token Domain Restriction Controls, based on Token Presentment and Token Processing relationship model characteristics

The characteristics of a single Payment Token may vary, depending on the specific use case. For example, the same Payment Token may be used for:

- A Proximity at Point of Sale transaction (Proximity at Point of Sale use case)
- An in-app transaction where it is shared with a Merchant (Token User) (In-Application using a Consumer Device use case)

The different characteristics of a single Payment Token are given in Table 7.1. The stage at which the Payment Token characteristic applies in Figure 3.1 is shown in the final column of the table.

Table 7.1: Payment Token Characteristics

Characteristic	Description	Typical Outcomes
Payment Token Usage	Usage of the Payment Token based on considerations of Token Location and Token Domain Restriction Controls. • Device Specific: a Payment Token that has been issued for use with a specific Consumer Device • Merchant Specific: a Payment Token that has been issued for use at a specific Merchant (Token Requestor) • Guest Checkout: a Payment Token that is for use in a single Cardholder-Initiated Transaction (and any subsequent Merchant-Initiated Transactions) • Token User: a Payment Token that can be used by a Merchant (Token User) that is not the Token Requestor	• Device Specific • Merchant Specific • Guest Checkout • Token User

Characteristic	Description	Typical Outcomes
Token Assurance Method	Token Assurance will be determined based on the characteristics of the specific use case.	• Token Assurance Method Categories
Token Domain Restriction Controls	Common Token Domain Restriction Control categories available for specific use cases.	• Token Presentment Mode(s) • Device • Merchant(s)
Token Cryptogram	Use of a Token Cryptogram as a Token Control Field for specific use cases.	• Used • Not Used
Type of Transaction Initiation	The type of transaction initiation. Typically, the use cases described in A Guide to Use Cases result in a Cardholder-Initiated Transaction, which may result in subsequent Merchant-Initiated Transactions (described in the Merchant-Initiated Transaction use case, Section 8.8).	• Cardholder-Initiated Transaction • Merchant-Initiated Transaction

8 Use Case Examples

This Section describes the following use case examples:

- Proximity at Point of Sale (Section 8.2)
- Online Wallet (Section 8.3)
- In-Application using a Consumer Device (Section 8.4)
- Card-On-File E-Commerce (Section 8.5)
- E-Commerce Guest Checkout (Section 8.6)
- Third Party Service Provider (Section 8.7)
- Merchant-Initiated Transaction (Section 8.8)

8.1 Introduction

Each of the use case examples is discussed in the following terms.

8.1.1 Relationship Models

The use case examples are described in terms of the relationship models and their characteristics introduced in Section 3 Relationship Model Descriptions. Specifically, each use case is described in terms of the following relationships and their functions given in Sections:

- 4.1 Token Issuance and Token Provisioning Relationships and Functions
- 5.1 Token Presentment Relationships and Functions
- 6.1 Token Processing Relationships and Functions

Each use case is then described in terms of the following characteristics given in Sections:

- 4.2 Token Issuance Characteristics
- 4.3 Token Provisioning Characteristics
- 5.2 Token Presentment Characteristics
- 6.2 Token Processing Characteristics

The Payment Tokens issued and / or used in each use case are described in terms of the characteristics given in Section 7 Payment Token Characteristics.

8.1.2 Example Flows

Each use case example is illustrated with example flows describing a specific scenario. Example flows are provided, where applicable, for:

- Issuance of Payment Token (Token Issuance and Token Provisioning)

- Transaction (Token Presentment and subsequent Token Processing)

For all issuance flows, it is assumed that the Card Issuer is performing ID&V as part of Token Assurance. Any Cardholder interaction with the Card Issuer performing ID&V is outside the scope of the use case examples.

Each transaction flow is written for a Cardholder-Initiated Transaction. If any subsequent Merchant-Initiated Transactions occur, please refer to the Technical Framework for details on how these should be handled.

For all flows, a successful path is assumed (e.g. a Payment Token is successfully issued and provisioned, a transaction is authorised and the purchase is completed).

8.1.3 Payment Account Reference Data

In all use cases, Payment Account Reference (PAR) Data for a given Payment Token may be available to the Merchant as follows:

- In the PAR Field at the conclusion of Token Processing
- As the result of an enquiry process initiated by the Merchant

PAR Data may also be available via other methods as noted in the Token Processing Considerations section of each use case.

8.1.4 Proximity vs Non-proximity

The use case examples can be split into two broad categories where:

- The Cardholder physically interacts with the Merchant's acceptance environment (e.g. presenting a Consumer Device at a Point of Sale terminal). Examples of use cases which fall into this category include:
  - Proximity at Point of Sale (Section 8.2)
- The Merchant's Point of Sale terminal is not used to support the transaction (e.g. an e-commerce purchase at a Merchant's website). Examples of use cases which fall into this category include:
  - Online Wallet (Section 8.3)
  - In-Application using a Consumer Device (Section 8.4)
  - Card-On-File E-Commerce (Section 8.5)
  - E-Commerce Guest Checkout (Section 8.6)
  - Third Party Service Provider (Section 8.7)

Within each category, there are multiple potential use cases. A Guide to Use Cases presents a limited number of use case examples which illustrate these categories.

8.1.5 Digital Wallets

Some of the use case examples use digital wallets. A digital wallet is a service available to Cardholders to manage their access to payment credentials across multiple Merchants. Access is enabled through either an online user experience or the physical interaction of a Consumer Device with the Merchant's acceptance environment.

The following use case examples have digital wallets. To distinguish between the use cases, the digital wallet is referred to as:

- Mobile Payment Application (using EMV Based Applications)
  - Proximity at Point of Sale (Section 8.2)
  - In-Application using a Consumer Device (Section 8.4)
- Online Wallet (using Non-EMV Based Applications)
  - Online Wallet (Section 8.3)

The following use case examples do not have digital wallets:

- Card-On-File E-Commerce (Section 8.5)
- E-Commerce Guest Checkout (Section 8.6)
- Third Party Service Provider (Section 8.7)

8.2 Proximity at Point of Sale

This use case example assumes that a Cardholder is physically interacting with the Merchant Point of Sale (POS) terminal using a Consumer Device to make a purchase.

The Cardholder presents a Consumer Device with a mobile payment application provisioned with a Payment Token by the mobile payment application provider (Token Requestor). The Consumer Device communicates with the POS terminal using a proximity technology such as EMV Contactless, EMV QR Code or MST to transmit the Payment Token to the POS terminal. The Merchant uses this Payment Token for Token Processing.

The Cardholder is notified of the outcome of the transaction by the POS terminal and the mobile payment application.

This use case example covers:

- Token Issuance and Token Provisioning
- Token Presentment and Token Processing

8.2.1 Use Case Overview – Problems Addressed & User Experience

Proximity payments offer opportunities for faster transactions by leveraging proximity interfaces in acceptance locations where speed of transactions and interoperability with

mobile device-based proximity payment solutions is desired. Security is enhanced by initiating payments with Payment Tokens to reduce risks of PAN exposure and compromise and by relying on Token Domain Restriction Controls to only allow Payment Tokens issued for proximity payments.

The main difference in the user experience is that the Consumer may need to activate the mobile payment application on the Consumer Device and select the payment credential to be used. Thereafter, the user experience will closely follow that of making an EMV Contactless transaction using a contactless-enabled card.

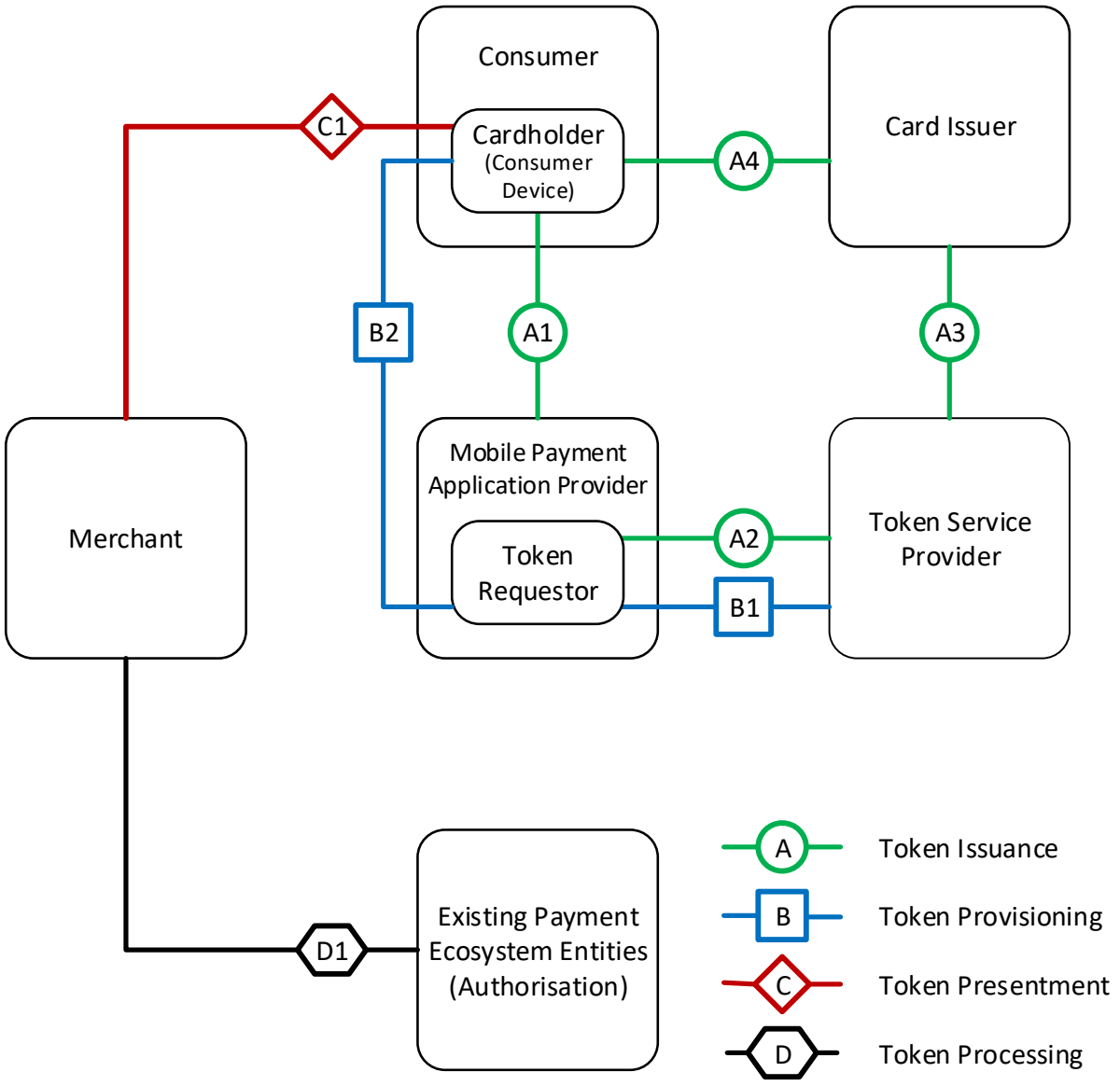
8.2.2 Use Case Relationships and Functions

The relationships for this use case example are shown in Figure 8.1. For a description of the baseline relationships and their functions, refer to the models given in Sections:

- 4.1 Token Issuance and Token Provisioning Relationships and Functions
- 5.1 Token Presentment Relationships and Functions
- 6.1 Token Processing Relationships and Functions

For this use case example, the mobile payment application provider is performing the role of the authorised entity described in Sections 4.1, 5.1 and 6.1. For each relationship shown in Figure 8.1, the specific nature of the relationship and its function is given in the text following the figure, along with a reference to the baseline relationship and function.

Figure 8.1: Proximity at Point of Sale – Use Case Relationships



Token Issuance and Token Provisioning

A1. Cardholder (Consumer Device) – Mobile Payment Application Provider (Token Requestor)

Relationship: The Cardholder (through the Cardholder's Consumer Device) has a relationship with the mobile payment application provider (Token Requestor).

Function: The Cardholder adds a payment credential by providing a PAN and related data to the mobile payment application provider (Token Requestor) via the mobile payment application on the Consumer Device, which triggers the Token Issuance process.

Reference: Section 4.1.1 A1. Cardholder – Authorised Entity (Token Requestor).

A2. Token Service Provider – Mobile Payment Application Provider (Token Requestor)

Relationship: The Token Service Provider has an existing relationship with the mobile payment application provider (Token Requestor) to enable Payment Tokenisation on behalf of a Card Issuer. The mobile payment application provider (Token Requestor) is identified by its Token Requestor ID assigned by the Token Service Provider.

Function: The mobile payment application provider (Token Requestor) makes a Token Request to the Token Service Provider using the PAN and related data (provided by the Cardholder via the mobile payment application).

Reference Section 4.1.4 A4. Token Service Provider – Authorised Entity (Token Requestor).

A3. Card Issuer – Token Service Provider

Relationship: The Card Issuer uses the Token Service Provider to provide Token Issuance and Token Provisioning services.

Function: The Token Service Provider may involve the Card Issuer in Token Assurance.

Note: This relationship does not vary by use case.

Reference: Section 4.1.5 A5. Card Issuer – Token Service Provider.

A4. Card Issuer – Cardholder (Consumer Device)

Relationship: The existing Card Issuer – Cardholder relationship is utilised for the issuance of a Payment Token.

Function: The Card Issuer may involve the Cardholder in Token Assurance.

Note: This relationship does not vary by use case.

Reference: Section 4.1.5 A5. Card Issuer – Token Service Provider.

B1. Token Service Provider – Mobile Payment Application Provider (Token Requestor)

Relationship: The Token Service Provider provides Token Provisioning services to the mobile payment application provider (Token Requestor) on behalf of a Card Issuer.

Function: The Token Service Provider delivers the Payment Token and related data to the mobile payment application provider (Token Requestor).

Reference: Section 4.1.7 B1. Token Service Provider – Authorised Entity (Token Requestor).

B2. Cardholder (Consumer Device) – Mobile Payment Application Provider (Token Requestor)

Relationship: The mobile payment application provider (Token Requestor) extends Token Provisioning services to the Cardholder.

Function: The mobile payment application provider (Token Requestor) delivers the Payment Token and related data to the Token Location of the Cardholder's Consumer

Device or a remote server where delivery to the Consumer Device takes place prior to commencing a transaction.

Reference: Section 4.1.8 B2. Cardholder – Authorised Entity (Token Requestor.

Token Presentment

C1. Cardholder (Consumer Device) – Merchant

Relationship: The existing Consumer – Merchant relationship is utilised for Cardholder-Initiated Transactions with a Payment Token and any subsequent Merchant-Initiated Transactions.

Function: The Consumer makes a purchase from the Merchant. The Cardholder may interact with the mobile payment application on the Consumer Device to select the payment credential (which has an affiliated Payment Token). The Cardholder's Consumer Device interacts with the Merchant's acceptance environment, which receives the Payment Token and related data from the Consumer Device.

Reference: Section 5.1.1 C1. Consumer / Cardholder – Merchant.

Token Processing

D1. Merchant – Existing Payment Ecosystem Entities

Relationship: The Merchant utilises existing relationships to initiate Token Processing

Function: The Merchant submits a Token Payment Request using the Payment Token and related data.

Note: This relationship does not vary by use case.

Reference: Section 6.1.1 D1. Merchant – Existing Payment Ecosystem Entities.

Other Relationships

In this use case there is no relationship between the Merchant and Token Requestor. This is because Merchant-specific integration with the Token Requestor is not required.

8.2.3 Use Case Characteristics

The use case characteristics are given in Table 8.1, Table 8.2, Table 8.3 and Table 8.4.

Table 8.1: Proximity at Point of Sale – Token Issuance Characteristics

Characteristic	Notes	Typical Outcomes
Cardholder Availability	The Cardholder must be available to interact with the Consumer Device.	• Required

Table 8.2: Proximity at Point of Sale – Token Provisioning Characteristics

Characteristic	Notes	Typical Outcomes
Token Location	See Table 5.1 of the Technical Framework for defined Token Locations.	EMV Contactless • 02, 03, 04 EMV QR Code • 01, 06, 07 MST • 02, 03, 04

Table 8.3: Proximity at Point of Sale – Token Presentment Characteristics

Characteristic	Notes	Typical Outcomes
Token Presentment	The Consumer Device presents the Payment Token to the Merchant, using EMV Contactless (for NFC), QR scanner (for QR Code), magnetic stripe reader (for MST) or other technologies to interact with the Merchant acceptance environment.	• Proximity
Acceptance Environment	The acceptance environment is a Merchant POS Terminal.	• Physical

Table 8.4: Proximity at Point of Sale – Token Processing Characteristics

Characteristic	Notes	Typical Outcomes
Token Payment Request	The Merchant submits the Token Payment Request to obtain a PAN authorisation.	• Merchant
Token Control Fields	Used to constrain the Payment Token to a specific Consumer Device and specific Token Presentment Mode(s).	• POS Entry Mode • Token Cryptogram

8.2.4 Payment Token Characteristics

The Payment Token characteristics are shown in Table 8.5.

Table 8.5: Proximity at Point of Sale – Payment Token Characteristics

Characteristic	Notes	Typical Outcomes
Payment Token Usage	The Payment Token is associated with a Consumer Device.	• Device Specific
Token Assurance Method	Typically, Card Issuer Token Assurance Method categories or Token Programme specific Assurance Method categories are used for this use case.	• 10 – 19 • 20 – 89
Token Domain Restriction Controls	The Payment Token is constrained to a specific Consumer Device and specific Token Presentment Mode(s).	• Token Presentment Mode(s) • Device
Token Cryptogram	A Token Cryptogram is used to ensure the integrity of the transaction-specific data.	• Used
Type of Transaction Initiation	Typically, the Cardholder uses a Consumer Device at the Merchant's proximity acceptance environment to initiate a transaction.	• Cardholder-Initiated Transaction

8.2.5 Issuance Flow

The following preconditions and assumptions apply to this specific flow.

Issuance Flow Preconditions

- The mobile payment application provider (Token Requestor) has registered with a Token Service Provider and has received a Token Requestor ID
- The mobile payment application is available on the Consumer Device
- The PAN that the Cardholder adds to the mobile payment application is eligible for Tokenisation

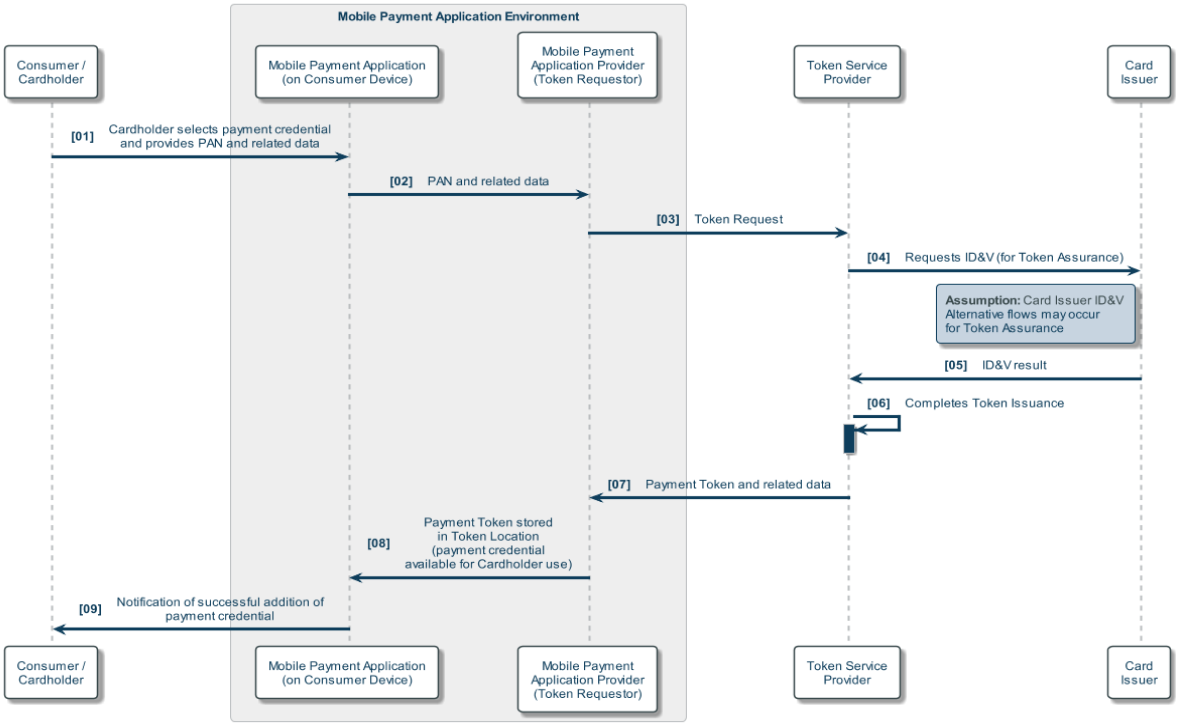
Issuance Flow Assumptions

- The Token Request is initiated by the mobile payment application provider (Token Requestor) based on an interaction with the Cardholder
- Token Assurance and the related ID&V is performed by the Card Issuer resulting in the Token Assurance Method value being set to one of the Card Issuer Token Assurance Method Categories
- The designated Token Location is 02 EMVCo and Payment System type approved secure element / ICC

Example Issuance Flow

Figure 8.2 shows an example issuance flow, with numbered steps which are explained following the figure.

Figure 8.2: Proximity at Point of Sale – Example Issuance Flow



01. The Cardholder selects a payment credential to add to the mobile payment application and provides the PAN and related data for the payment credential as required by the mobile payment application provider
02. The mobile payment application provides the PAN and related data to the mobile payment application provider
03. The mobile payment application provider (Token Requestor) uses the PAN and related data to initiate a Token Request to the Token Service Provider (using its Token Requestor ID)
04. The Token Service Provider carries out Token Assurance and requests that the Card Issuer undertakes ID&V
05. The Card Issuer responds to the Token Service Provider with its ID&V result
06. The Token Service Provider completes Token Issuance (this is on the assumption that the ID&V result indicates Card Issuer approval)
07. The Token Service Provider delivers a Payment Token and related data to the mobile payment application provider (Token Requestor) as part of Token Provisioning

08. The Payment Token and its related data are stored in the designated Token Location by the mobile payment application to complete Token Provisioning. The payment credential is now available in the mobile payment application for the Cardholder's future use

09. The Cardholder is notified of the successful addition of the payment credential by the mobile payment application. The Cardholder may not be aware of the Tokenisation process

8.2.6 Transaction Flow

The following preconditions and assumptions apply to this specific flow.

Transaction Flow Preconditions

- The Consumer Device supports a proximity payment technology such as NFC, MST or QR Code
- At least one of the supported proximity payment technologies has been enabled by the Consumer
- The Merchant POS terminal supports at least one of the proximity payment technologies enabled on the Consumer Device

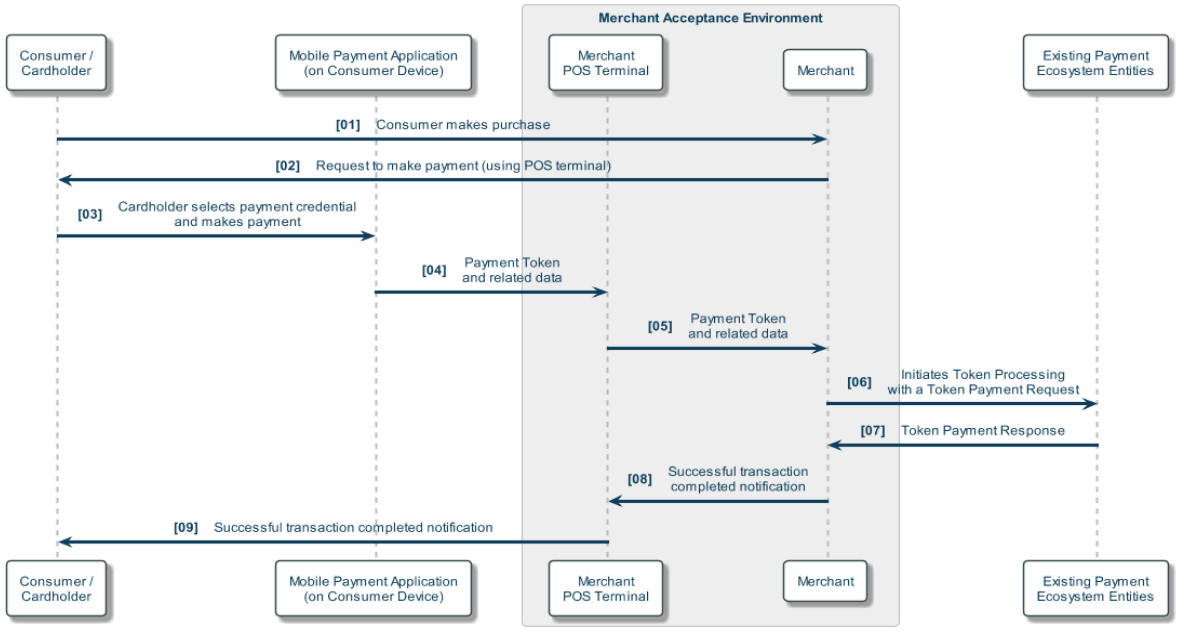
Transaction Flow Assumptions

There are no additional assumptions that apply to this specific flow.

Example Transaction Flow

Figure 8.3 shows an example transaction flow, with numbered steps which are explained following the figure.

Figure 8.3: Proximity at Point of Sale – Example Transaction Flow



01. The Consumer makes a purchase from a Merchant
02. The Merchant initiates a checkout process to request payment using the POS terminal
03. The Consumer selects a payment credential and makes a proximity payment using the mobile payment application on the Consumer Device
04. The Payment Token and related data are transmitted to the POS terminal
05. The POS terminal provides the Payment Token and related data to the Merchant
06. The Merchant initiates Token Processing by sending a Token Payment Request
07. The Merchant receives a Token Payment Response as a result of successful PAN Authorisation by the Card Issuer
08. The Merchant provides the results to the POS terminal
09. The Consumer receives confirmation from the POS terminal that the transaction was successful

Token Processing Considerations

Table 8.4 (Token Processing Characteristics) and Table 8.5 (Payment Token Characteristics) show the typical Token Control Fields (Table 8.4) which are used as part of the Token Domain Restriction Controls (Table 8.5). In these specific use case flows, the following Token Control Fields are used:

- POS Entry Mode: has an expected value that indicates a proximity transaction, used to constrain the Payment Token to a specific Token Presentment Mode
- Token Cryptogram: valid only for this transaction to prevent payment transactional data from being reused in another transaction. May be used to constrain the Payment Token to this specific Consumer Device

As well as the methods described in Section 8.1.3 Payment Account Reference Data (PAR Field and PAR Enquiry), PAR Data may be available to the Merchant:

- As part of the related data transmitted to the POS terminal using the EMV Tag ‘9F24’

8.2.7 Variations of User Experience

For this use case, the potential variations focus on the Token Presentment (Relationship C1 / Steps 3 & 4 of the transactional flow).

- NFC: the user experience will closely follow that of an EMV Contactless transaction on a contactless-enabled payment card. The Consumer Device will be held in proximity to the POS terminal
- MST: the Consumer Device will be held close to the magnetic stripe reader heads on the POS terminal to allow the mobile payment application to present the Payment Token and related data

- QR Codes: the mobile payment application on the Consumer Device displays a QR code that can then be read by a QR Code reader to complete the presentment of the Payment Token and related data

8.3 Online Wallet

This use case example assumes that a Consumer is interacting with the Merchant e-commerce environment to make a purchase.

The Cardholder uses an online wallet provisioned with a Payment Token by the online wallet provider (Token Requestor). When the online wallet is selected for payment, it interacts with the Merchant e-commerce environment to provide the Payment Token to the Merchant (Token User), which uses it for Token Processing.

The Cardholder is notified of the outcome of the transaction by the Merchant's e-commerce environment and can also be notified by the online wallet.

This use case example covers:

- Token Issuance and Token Provisioning
- Token Presentment and Token Processing

8.3.1 Use Case Overview – Problems Addressed & User Experience

In the case of an online wallet, a single Payment Token can be used by multiple Merchants (Token Users) and may be beneficial to and support scalability of Payment Tokenisation with Merchants that may not want to or have the ability to become a Token Requestor.

The Consumer will see a minor variation to the experience on the payment page by seeing their version of the online wallet as a payment option. The Consumer has an option to select the online wallet in addition to other payment methods, or depending on the level of integration, the payment credentials stored in the online wallet may be shown directly.

8.3.2 Use Case Relationships and Functions

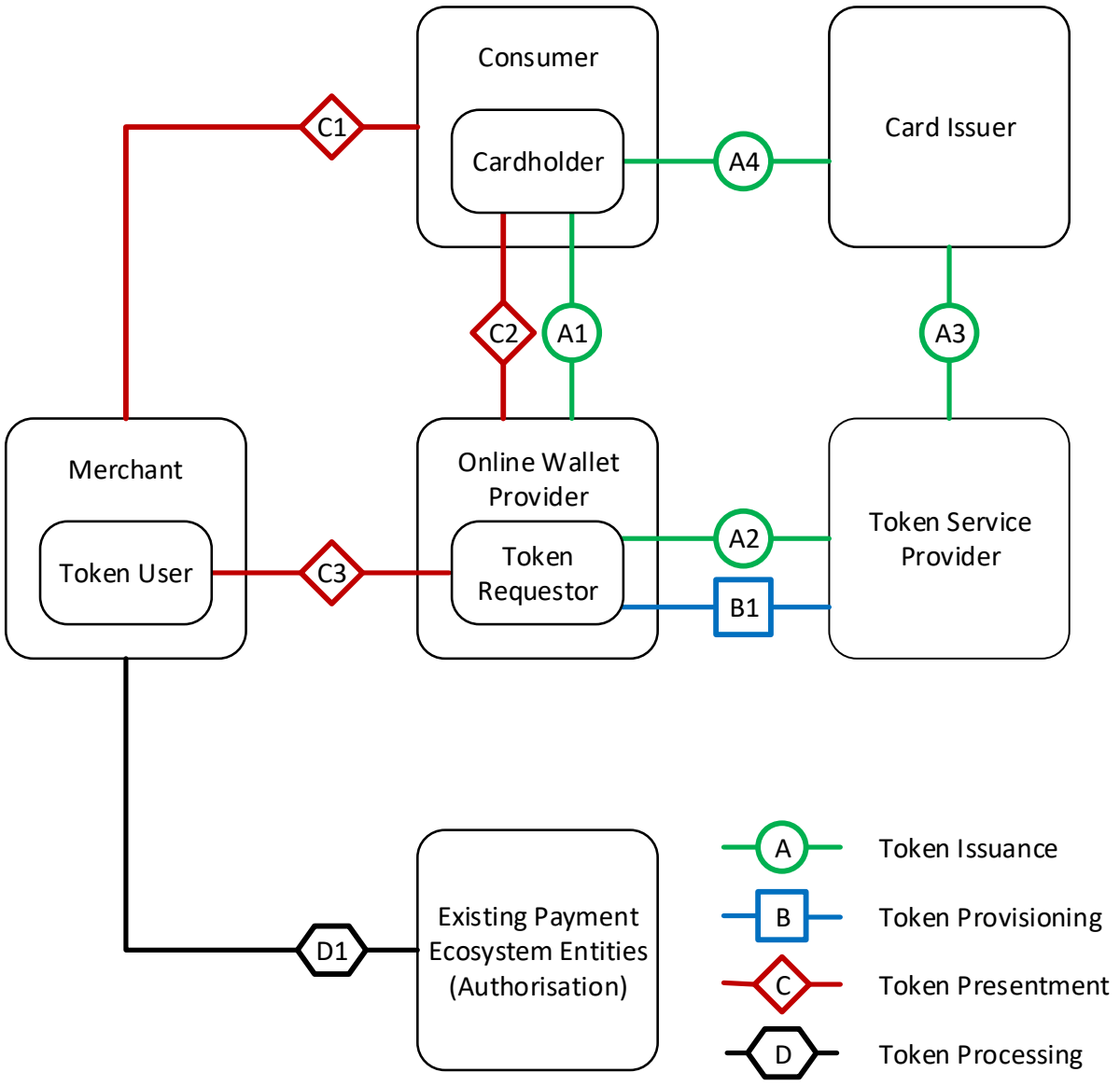
The relationships for this use case example are shown in Figure 8.4. For a description of the baseline relationships and their functions, refer to the models given in Sections:

- 4.1 Token Issuance and Token Provisioning Relationships and Functions
- 5.1 Token Presentment Relationships and Functions
- 6.1 Token Processing Relationships and Functions

For this use case example, the online wallet provider is performing the role of the authorised entity described in Sections 4.1, 5.1 and 6.1. For each relationship shown in Figure 8.4, the

specific nature of the relationship and its function is given in the text following the figure, along with a reference to the baseline relationship and function.

Figure 8.4: Online Wallet – Use Case Relationships



Token Issuance and Token Provisioning

A1. Cardholder – Online Wallet Provider (Token Requestor)

Relationship: The Cardholder has a relationship with an online wallet provider (Token Requestor).

Function: The Cardholder adds a payment credential by providing a PAN and related data to the online wallet provider (Token Requestor) via the online wallet, which triggers the Token Issuance process.

Reference: Section 4.1.1 A1. Cardholder – Authorised Entity (Token Requestor)

A2. Token Service Provider – Online Wallet Provider (Token Requestor)

Relationship: The Token Service Provider has an existing relationship with the online wallet provider (Token Requestor) to enable Payment Tokenisation on behalf of a Card Issuer. The online wallet provider (Token Requestor) is identified by its Token Requestor ID assigned by the Token Service Provider.

Function: The online wallet provider (Token Requestor) makes a Token Request to the Token Service Provider using the PAN and related data (provided by the Cardholder via the online wallet).

Reference: Section 4.1.4 A4. Token Service Provider – Authorised Entity (Token Requestor).

A3. Card Issuer – Token Service Provider

Relationship: The Card Issuer uses the Token Service Provider to provide Token Issuance and Token Provisioning services.

Function: The Token Service Provider may involve the Card Issuer in Token Assurance.

Note: This relationship does not vary by use case.

Reference: Section 4.1.5 A5. Card Issuer – Token Service Provider.

A4. Card Issuer – Cardholder

Relationship: The existing Card Issuer – Cardholder relationship is utilised for the issuance of a Payment Token.

Function: The Card Issuer may involve the Cardholder in Token Assurance.

Note: This relationship does not vary by use case.

Reference: Section 4.1.6 A6. Card Issuer – Cardholder.

B1. Token Service Provider – Online Wallet Provider (Token Requestor)

Relationship: The Token Service Provider provides Token Provisioning services to the online wallet provider (Token Requestor) on behalf of a Card Issuer.

Function: The Token Service Provider delivers the Payment Token to the online wallet provider (Token Requestor), which stores it in the Token Location.

Reference: Section 4.1.7 B1. Token Service Provider – Authorised Entity (Token Requestor).

Token Presentment

C1 Consumer – Merchant

Relationship: The existing Consumer – Merchant relationship is utilised for Cardholder-Initiated Transactions with a Payment Token and any subsequent Merchant-Initiated Transactions.

Function: The Consumer makes a purchase from the Merchant e-commerce environment.

Reference: Section 5.1.1 C1. Consumer / Cardholder – Merchant.

C2 Cardholder – Online Wallet Provider (Token Requestor)

Relationship: The Cardholder has a relationship with the online wallet provider (Token Requestor).

Function: Cardholder interacts with the online wallet to select the payment credential (which has an affiliated Payment Token).

Reference: Section 5.1.2 C2. Cardholder – Authorised Entity (Token Requestor).

C3 Merchant (Token User) – Online Wallet Provider (Token Requestor)

Relationship: The Merchant (Token User) has an existing relationship with the online wallet provider (Token Requestor).

Function: The Merchant e-commerce environment receives the Payment Token and related data from the online wallet.

Reference: Section 5.1.3 C3. Merchant (Token User) – Authorised Entity (Token Requestor).

Token Processing

D1. Merchant (Token User) – Existing Payment Ecosystem Entities

Relationship: The Merchant (Token User) utilises existing relationships to initiate Token Processing.

Function: The Merchant submits a Token Payment Request using the Payment Token and related data.

Note: This relationship does not vary by use case.

Reference: Section 6.1.1 D1. Merchant – Existing Payment Ecosystem Entities.

8.3.3 Use Case Characteristics

The use case characteristics are shown in Table 8.6, Table 8.7, Table 8.8 and Table 8.9.

Table 8.6: Online Wallet – Token Issuance Characteristics

Characteristic	Notes	Typical Outcomes
Cardholder Availability	The Cardholder must be available to interact with the online wallet.	• Required

Table 8.7: Online Wallet – Token Provisioning Characteristics

Characteristic	Notes	Typical Outcomes
Token Location	See Table 5.1 of the Technical Framework for defined Token Locations.	• 06 • 07

Table 8.8: Online Wallet – Token Presentment Characteristics

Characteristic	Notes	Typical Outcomes
Token Presentment	The online wallet presents the Payment Token to the Merchant (Token User).	• Non-proximity
Acceptance Environment	The acceptance environment is a Merchant e-commerce environment.	• Non-physical

Table 8.9: Online Wallet – Token Processing Characteristics

Characteristic	Notes	Typical Outcomes
Token Payment Request	The Merchant (Token User) submits the Token Payment Request to obtain a PAN authorisation.	• Merchant
Token Control Fields	Used to constrain the Payment Token to a specific Merchant (Token User), a specific Device and a specific Token Presentment Mode(s) at the time of a given transaction.	• POS Entry Mode • Merchant Identifiers • Token Cryptogram

8.3.4 Payment Token Characteristics

The Payment Token characteristics are shown in Table 8.10.

Table 8.10: Online Wallet – Payment Token Characteristics

Characteristic	Notes	Typical Outcomes
Payment Token Usage	The Payment Token can be used by a Merchant (Token User) that is not the Token Requestor.	• Token User
Token Assurance Method	Token Assurance is Token Programme specific and determined based on the detailed characteristics of this use case.	• Spaces / 00 • 01 – 19 • 20 – 89
Token Domain Restriction Controls	The Payment Token is constrained to specific Merchants (Token Users), a specific Device and specific Token Presentment Mode(s).	• Merchant(s) • Device • Token Presentment Mode(s)
Token Cryptogram	When a Token Cryptogram is used, it ensures the integrity of the transaction-specific data.	• Used • Not Used
Type of Transaction Initiation	Typically, the Cardholder uses a Merchant e-commerce environment to initiate a transaction.	• Cardholder-Initiated Transaction

8.3.5 Issuance Flow

The following preconditions and assumptions apply to this specific flow.

Issuance Flow Preconditions

- The online wallet provider (Token Requestor) has registered with the Token Service Provider and has received a Token Requestor ID
- The Merchant (Token User) has registered with the Token Requestor as a Token User
- The Cardholder has previously enrolled with the online wallet provider
- The PAN that the Cardholder adds to the online wallet is eligible for Tokenisation

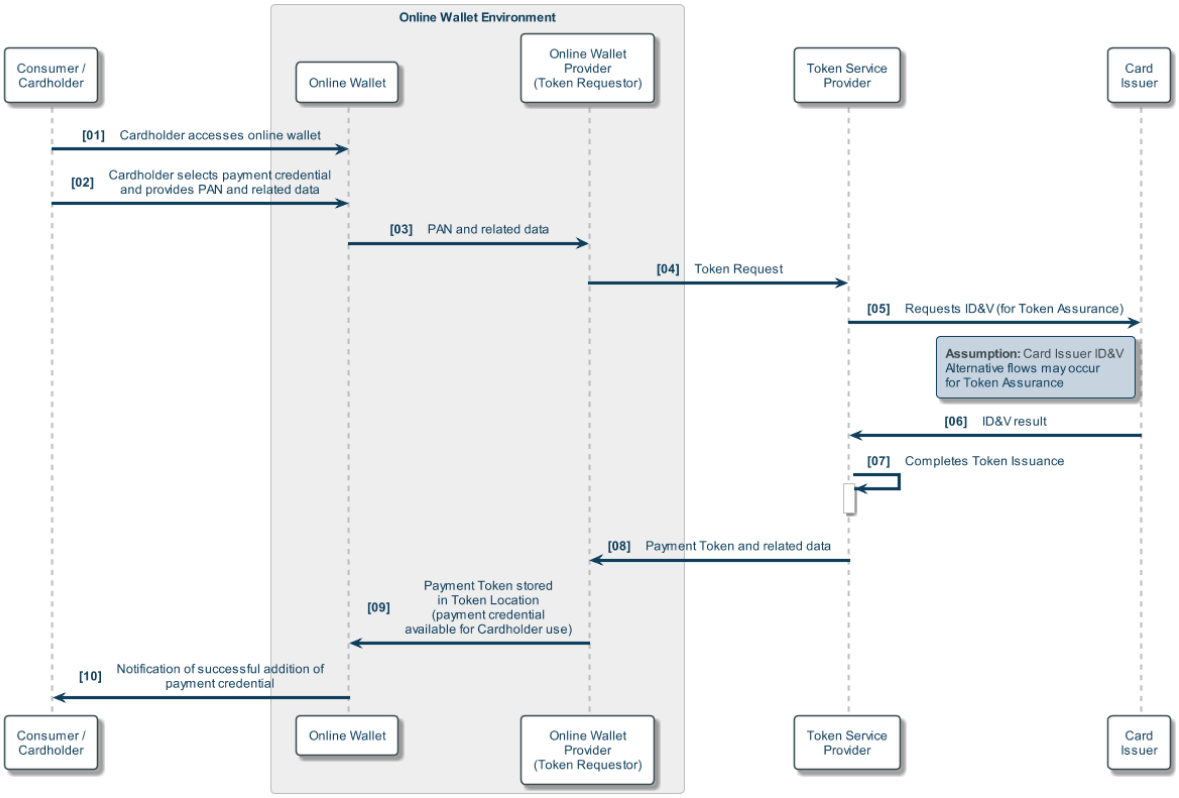
Issuance Flow Assumptions

- The Token Request is initiated by the online wallet provider (Token Requestor) based on an interaction with the Cardholder
- Token Assurance and the related ID&V is performed by the Card Issuer, resulting in the Token Assurance Method value being set to one of the Card Issuer Token Assurance Method Categories
- The designated Token Location is 06 Shared storage

Example Issuance Flow

Figure 8.5 shows an example issuance flow, with numbered steps which are explained following the figure.

Figure 8.5: Online Wallet – Example Issuance Flow



01. The Cardholder accesses the online wallet in accordance with the instructions provided by the online wallet provider
02. The Cardholder selects a payment credential to add to the online wallet and provides the PAN and related data for the payment credential as required by the online wallet provider
03. The online wallet provides the PAN and related data to the online wallet provider
04. The online wallet provider (Token Requestor) does not store the PAN and related data, instead using it to initiate a Token Request to the Token Service Provider (using its Token Requestor ID)
05. The Token Service Provider carries out Token Assurance and requests that the Card Issuer undertakes ID&V
06. The Card Issuer responds to the Token Service Provider with the ID&V result
07. The Token Service Provider completes Token Issuance (this is on the assumption that the ID&V result indicates Card Issuer approval)

08. The Token Service Provider delivers a Payment Token and related data to the online wallet provider (Token Requestor) as part of Token Provisioning
09. The Payment Token and its related data are stored in the designated Token Location by the online wallet to complete Token Provisioning. The payment credential is now available in the online wallet for the Cardholder's future use
10. The Cardholder is notified of the successful addition of the payment credential by the online wallet. The Cardholder may not be aware of the Tokenisation process

8.3.6 Transaction Flow

The following preconditions and assumptions apply to this specific flow.

Transaction Flow Preconditions

- The Merchant has enabled the online wallet within its e-commerce environment to provide payment credentials for the completion of transactions

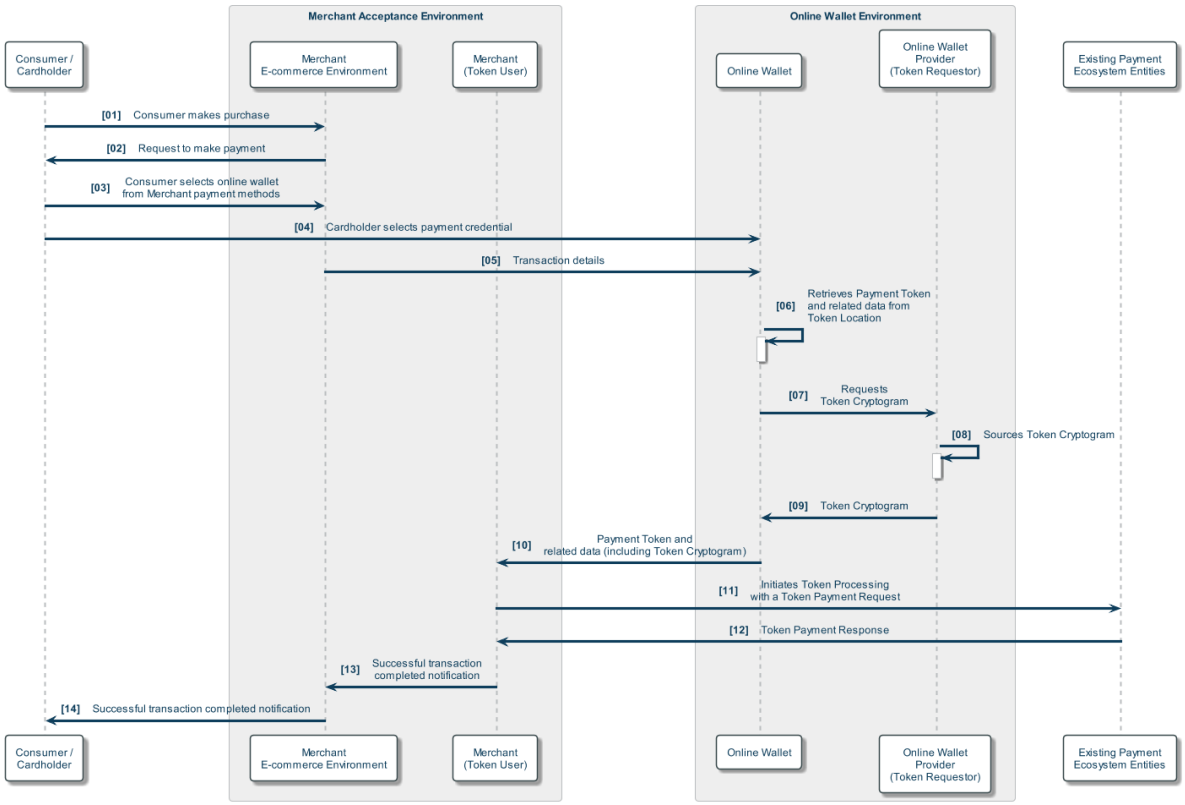
Transaction Flow Assumptions

- The Consumer selects a payment credential stored in the online wallet that is affiliated with a stored Payment Token
- The Payment Token is stored by the online wallet and is identified by the last four digits of the underlying PAN and digital card art
- A Token Cryptogram is used
- The online wallet provider (Token Requestor) sources the Token Cryptogram from the appropriate authorised entity
- The Merchant (Token User) initiates Token Processing using the Payment Token and related data (along with the provided Token Cryptogram) via existing relationships with the existing Payment Ecosystem Entities

Example Transaction Flow

Figure 8.6 shows an example transaction flow, with numbered steps which are explained following the figure.

Figure 8.6: Online Wallet – Example Transaction Flow



01. The Consumer makes a purchase from the Merchant e-commerce environment and initiates the checkout process
02. The Merchant e-commerce environment initiates the request for a payment credential to be selected
03. The Consumer chooses the online wallet from the options presented in the Merchant e-commerce environment
04. The Cardholder selects a previously stored payment credential from the online wallet
05. The Merchant e-commerce environment provides details of the transaction to the online wallet
06. The online wallet retrieves the Payment Token and related data from the Token Location.
07. The online wallet requests a Token Cryptogram from the online wallet provider (Token Requestor), passing the relevant transaction information to it
08. The online wallet provider (Token Requestor) sources the Token Cryptogram using the relevant transaction information passed by the online wallet
09. The online wallet provider (Token Requestor) provides the Token Cryptogram to the online wallet

10. The online wallet delivers the Payment Token and related data, along with the Token Cryptogram, to the Merchant (Token User)
11. The Merchant (Token User) initiates Token Processing by sending a Token Payment Request
12. The Merchant (Token User) receives a Token Payment Response as a result of successful PAN Authorisation by the Card Issuer
13. The Merchant provides the results to the Merchant e-commerce environment
14. The Cardholder receives confirmation from the Merchant e-commerce environment that the transaction was successful

Token Processing Considerations

Table 8.9 (Token Processing Characteristics) and Table 8.10 (Payment Token Characteristics) show the typical Token Control Fields (Table 8.9) which are used as part of the Token Domain Restriction Controls (Table 8.10). In these specific use case flows, the following Token Control Fields are used:

- POS Entry Mode: has an expected value that indicates an e-commerce transaction, used to constrain the Payment Token to a specific Token Presentment Mode
- Merchant identifier(s): represents the specific Merchant using the Payment Token for this transaction, used to constrain the Payment Token to this specific Merchant (Token User)
- Token Cryptogram: valid only for this transaction to prevent payment transactional data from being reused in another transaction

As well as the methods described in Section 8.1.3 Payment Account Reference Data (PAR Field and PAR Enquiry), PAR Data may be available to the Merchant:

- As part of the related data provided by the online wallet with the Payment Token

8.3.7 Variations of User Experience

Minor variations may occur due to the Merchant e-commerce environment used by the Cardholder, which are beyond the scope of the use case.

8.4 In-Application using a Consumer Device

This use case example assumes that a Consumer is interacting with a Merchant application on the Consumer Device to make a purchase.

The Cardholder uses a Consumer Device with a mobile payment application provisioned with a Payment Token by the mobile payment application provider (Token Requestor). When the mobile payment application is selected for payment, it interacts with the Merchant application

to provide the Payment Token to the Merchant (Token User). The Merchant uses this Payment Token for Token Processing.

The Cardholder is notified of the outcome of the transaction by the Merchant application and the mobile payment application.

This use case example covers:

- Token Presentment and Token Processing

This use case is linked to the Proximity at Point of Sale use case (Section 8.2). Both use cases have the same relationships and flows for Token Issuance and Token Provisioning. It is a precondition of this use case that Token Issuance and Token Provisioning has already occurred.

8.4.1 Use Case Overview – Problems Addressed & User Experience

In-Application transactions, often referenced as “In-App”, are intended to simplify e-commerce transactions and the checkout process for Consumers using a Consumer Device. This is useful as a Consumer Device has a relatively small screen and typical entry of payment / checkout data (e.g. billing address) may be neither easy or quick.

By reducing this friction, In-App transactions enable the Consumer to complete the transaction with minimal interactions and without leaving the Merchant’s shopping application. For the Merchant, it may reduce checkout failures or cart abandonment through the simplification of the experience and removal of Consumer friction.

The Consumer will see a minor variation to the experience by having an option to select the mobile payment application in addition to other payment methods.

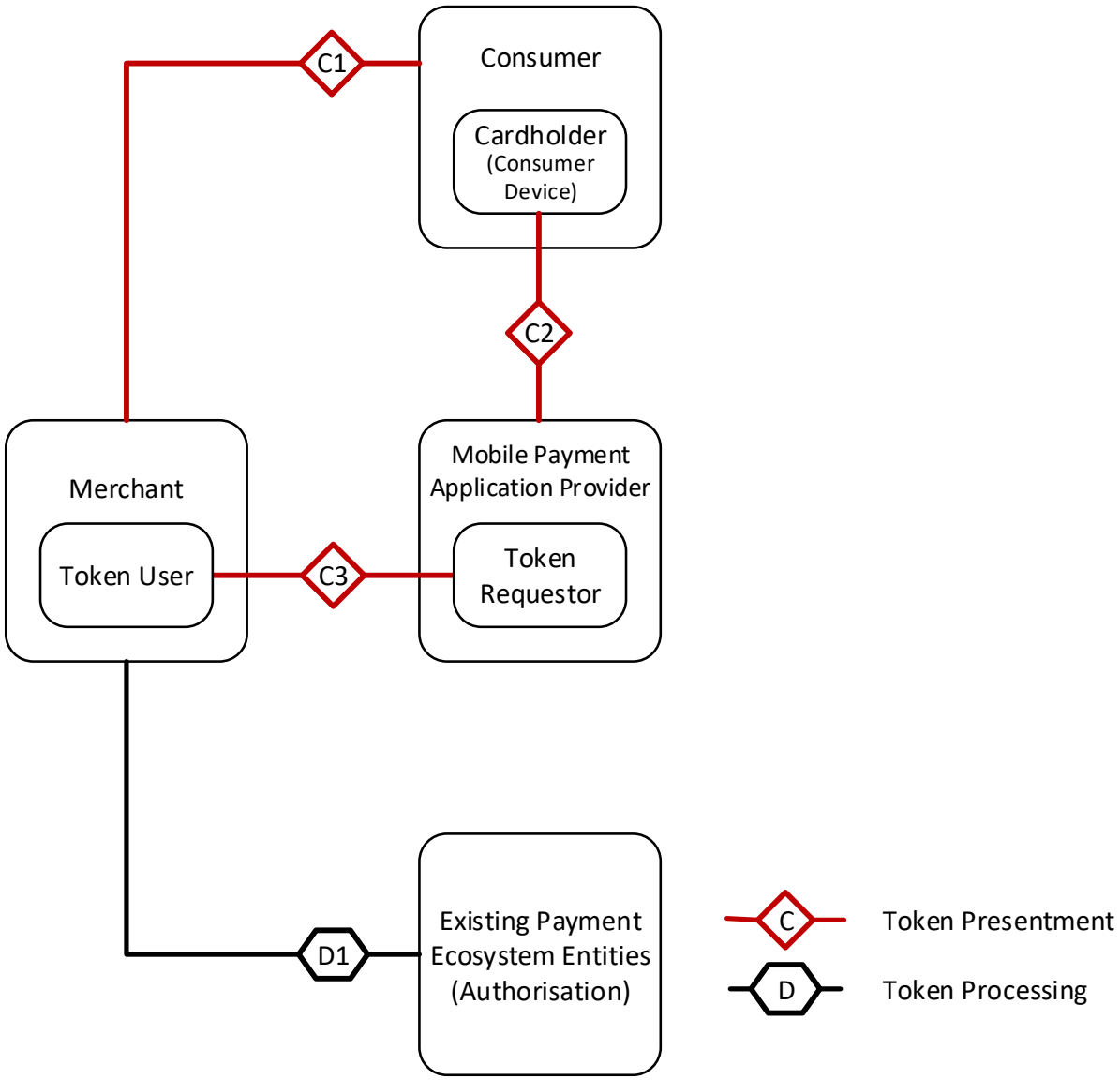
8.4.2 Use Case Relationships and Functions

The relationships for this use case example are shown in Figure 8.7. For a description of the baseline relationships and their functions, refer to the models given in Sections:

- 5.1 Token Presentment Relationships and Functions
- 6.1 Token Processing Relationships and Functions

For this use case example, the mobile payment application provider is performing the role of the authorised entity described in Sections 5.1 and 6.1. For each relationship shown in Figure 8.7, the specific nature of the relationship and its function is given in the text following the figure, along with a reference to the baseline relationship and function. Note that this use case is transactional and presupposes that a Payment Token has been provisioned to a mobile payment application on a proximity-enabled Consumer Device (Proximity at Point of Sale use case). Therefore, Token Issuance relationships and Token Provisioning relationships are not shown in Figure 8.7. The Token Issuance and Token Provisioning characteristics are not given in Section 8.4.3.

Figure 8.7: In-Application using a Consumer Device – Use Case Relationships



Token Presentment

C1 Consumer Device – Merchant

Relationship: The existing Consumer – Merchant relationship is utilised for Cardholder-Initiated Transactions with a Payment Token and any subsequent Merchant-Initiated Transactions.

Function: The Consumer makes a purchase from the Merchant application.

Reference: Section 5.1.1 C1. Consumer / Cardholder – Merchant.

C2 Cardholder (Consumer Device) – Mobile Payment Application Provider (Token Requestor)

Relationship: The Cardholder (through the Cardholder's Consumer Device) has a relationship with the mobile payment application provider (Token Requestor).

Function: The Cardholder interacts with the mobile payment application on the Consumer Device to select the payment credential (which has an affiliated Payment Token).

Reference: Section 5.1.2 C2. Cardholder – Authorised Entity (Token Requestor).

C3 Merchant (Token User) – Mobile Payment Application Provider (Token Requestor)

Relationship: The Merchant (Token User) has an existing relationship with the mobile payment application provider (Token Requestor).

Function: The Merchant application receives the Payment Token and related data from the mobile payment application. This is the Payment Token issued to the Consumer Device (Proximity at Point of Sale use case) but with different Token Domain Restriction Controls for this use case.

Reference: Section 5.1.3 C3. Merchant (Token User) – Authorised Entity (Token Requestor).

Token Processing

D1. Merchant (Token User) – Existing Payment Ecosystem Entities

Relationship: The Merchant (Token User) utilises existing relationships to initiate Token Processing.

Function: The Merchant submits a Token Payment Request using the Payment Token and related data.

Note: This relationship does not vary by use case.

Reference: Section 6.1.1 D1. Merchant – Existing Payment Ecosystem Entities.

8.4.3 Use Case Characteristics

The use case characteristics are given in Table 8.11 and Table 8.12. For the Token Issuance and Token Provisioning characteristics, see the Proximity at Point of Sale use case (Section 8.2.3).

Table 8.11: In-Application using a Consumer Device – Token Presentment Characteristics

Characteristic	Notes	Typical Outcomes
Token Presentment	The mobile payment application on the Consumer Device presents the Payment Token to the Merchant by interacting with the Merchant application.	• Non-proximity
Acceptance Environment	The acceptance environment is a Merchant application.	• Non-physical

Table 8.12: In-Application using a Consumer Device – Token Processing Characteristics

Characteristic	Notes	Typical Outcomes
Token Payment Request	The Merchant (Token User) submits the Token Payment Request to obtain a PAN authorisation.	• Merchant
Token Control Fields	Used to constrain the Payment Token to a specific Consumer Device and specific Token Presentment Mode(s).	• POS Entry Mode • Token Cryptogram

8.4.4 Payment Token Characteristics

The Payment Token characteristics are shown in Table 8.13.

Table 8.13: In-Application using a Consumer Device – Payment Token Characteristics

Characteristic	Notes	Typical Outcomes
Payment Token Usage	The Payment Token is associated with a Consumer Device and can be used by a Merchant (Token User) that is not the Token Requestor.	• Device Specific • Token User
Token Assurance Method	Token Assurance is Token Programme specific and determined based on the detailed characteristics of this use case.	• Spaces / 00 • 01 – 19 • 20 – 89
Token Domain Restriction Controls	The Payment Token is constrained to a specific Consumer Device and specific Token Presentment Mode(s).	• Token Presentment Mode(s) • Device
Token Cryptogram	A Token Cryptogram is used to ensure the integrity of the transaction-specific data.	• Used
Type of Transaction Initiation	Typically, the Cardholder uses a Merchant application on the Consumer Device to initiate a transaction.	• Cardholder-Initiated Transaction

8.4.5 Issuance Flow

The Issuance of the Payment Token follows the flow described in the Proximity at Point of Sale use case (Section 8.2.5 Issuance Flow).

8.4.6 Transaction Flow

The following preconditions and assumptions apply to this specific flow.

Transaction Flow Preconditions

- The Consumer has an account with the Merchant and has installed the Merchant application on a Consumer Device
- The Merchant application has been enabled to interact with a mobile payment application associated with the Consumer Device
- A Payment Token has been provisioned to the mobile payment application

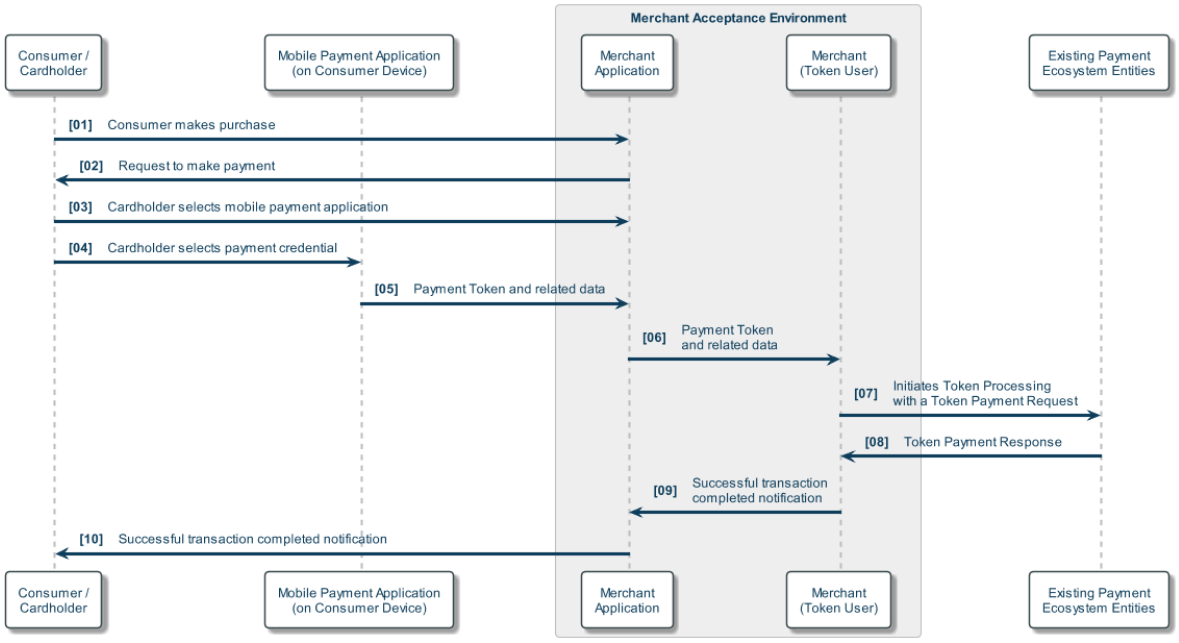
Transaction Flow Assumptions

- When the Consumer selects in-app payment, the Merchant application interacts with the mobile payment application to allow the Consumer to select a payment credential

Example Transaction Flow

Figure 8.8 shows an example transaction flow, with numbered steps which are explained following the figure.

Figure 8.8: In-Application using a Consumer Device – Example Transaction Flow



01. The Consumer makes a purchase using a Merchant application on the Consumer Device
02. The Merchant application initiates the request for the Consumer to select a method of payment
03. The Consumer selects the mobile payment application from the options presented in the Merchant application

04. The Cardholder selects the payment credential from the mobile payment application
05. The mobile payment application delivers the Payment Token and related data to the Merchant application
06. The Merchant application provides the Payment Token and related data to the Merchant (Token User)
07. The Merchant (Token User) initiates Token Processing by sending a Token Payment Request
08. The Merchant (Token User) receives a Token Payment Response as a result of successful PAN Authorisation by the Card Issuer
09. The Merchant provides the results to the Merchant application
10. Cardholder receives confirmation from the Merchant application that the transaction was successful

Token Processing Considerations

Table 8.12 (Token Processing Characteristics) and Table 8.13 (Payment Token Characteristics) show the typical Token Control Fields (Table 8.12) which are used as part of the Token Domain Restriction Controls (Table 8.13). In these specific use case flows, the following Token Control Fields are used:

- POS Entry Mode: has an expected value that indicates an in-application transaction, used to constrain the Payment Token to a specific Token Presentment Mode
- Token Cryptogram: valid only for this transaction to prevent payment transactional data from being reused in another transaction. May be used to constrain the Payment Token to this specific Consumer Device

As well as the methods described in Section 8.1.3 Payment Account Reference Data (PAR Field and PAR Enquiry), PAR Data may be available to the Merchant:

- As part of the related data passed by the mobile payment application

8.4.7 Variations of User Experience

Minor variations may occur for this use case due to mobile payment application and Merchant application related user interface / user experience differences, which are implementation specific.

8.5 Card-On-File E-Commerce

This use case example assumes that a Consumer, who has (or creates) an account with the Merchant, is interacting with the Merchant e-commerce environment to make a purchase and that the Consumer's payment credentials are stored by the Merchant.

The Cardholder provides the Merchant with details of the payment credential which the Merchant (Token Requestor) uses to obtain a Payment Token. The Payment Token is then stored by the Merchant (Token Requestor) to be used in transactions. The Cardholder selects a payment credential and the Merchant (Token Requestor) uses the affiliated Payment Token for Token Processing.

The Cardholder is notified of the outcome of the transaction by the Merchant e-commerce environment.

This use case example covers:

- Token Issuance and Token Provisioning
- Token Presentment and Token Processing

8.5.1 Use Case Overview – Problems Addressed & User Experience

E-Commerce merchants may offer to store a Consumer's payment credentials in conjunction with other data in an account in order to make purchases more convenient.

Replacing PANs with Payment Tokens:

- Enhances the underlying security of digital payments by potentially limiting the risk typically associated with compromised, unauthorised or fraudulent use of PANs
- Offers the ability to control or constrain usage to its intended use, e.g. a device or other domain through the use of Token Domain Restriction Controls
- Potentially reduces the scope of a Merchant's PCI DSS cardholder data environment (CDE)
- Reduces potential disruption due to PAN lifecycle management events

The user experience is essentially unchanged, with the Consumer selecting a payment credential (which has an affiliated Payment Token) for use during checkout. Once selected, the Merchant (Token Requestor) uses the affiliated Payment Token instead of the PAN. Typically, the Consumer will not be aware of the Tokenisation process.

8.5.2 Use Case Relationships and Functions

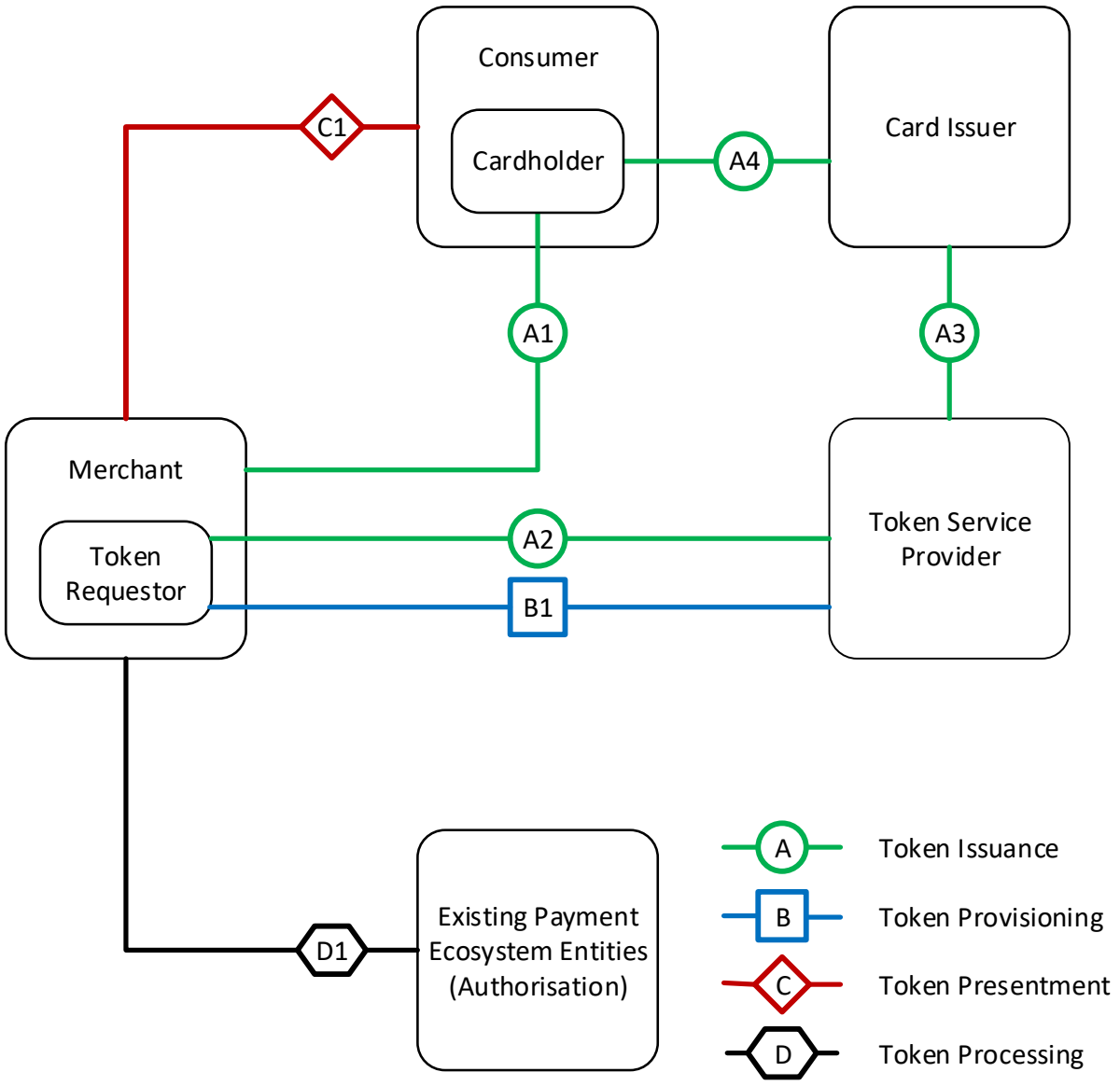
The relationships for this use case example are shown in Figure 8.9. For a description of the baseline relationships and their functions, refer to the models given in Sections:

- 4.1 Token Issuance and Token Provisioning Relationships and Functions
- 5.1 Token Presentment Relationships and Functions
- 6.1 Token Processing Relationships and Functions

For this use case example, the Merchant is performing the role of the authorised entity described in Sections 4.1, 5.1 and 6.1. For each relationship shown in Figure 8.9, the specific

nature of the relationship and its function is given in the text following the figure, along with a reference to the baseline relationship and function.

Figure 8.9: Card-On-File E-Commerce – Use Case Relationships



Token Issuance and Token Provisioning

A1. Cardholder – Merchant (Token Requestor)

Relationship: The Cardholder has (or establishes) a relationship with the Merchant (Token Requestor).

Function: The Cardholder adds a payment credential by providing a PAN and related data to the Merchant (Token Requestor) via the Merchant e-commerce environment which triggers the Token Issuance process.

Reference: Section 4.1.1 A1. Cardholder – Authorised Entity (Token Requestor).

A2. Token Service Provider – Merchant (Token Requestor)

Relationship: The Token Service Provider has an existing relationship with the Merchant (Token Requestor) to enable Payment Tokenisation on behalf of a Card Issuer. The Merchant (Token Requestor) is identified by its Token Requestor ID assigned by the Token Service Provider.

Function: The Merchant (Token Requestor) makes a Token Request to the Token Service Provider using the PAN and related data (provided by the Cardholder via the Merchant e-commerce environment).

Reference: Section 4.1.4 A4. Token Service Provider – Authorised Entity (Token Requestor).

A3. Card Issuer – Token Service Provider

Relationship: The Card Issuer uses the Token Service Provider to provide Token Issuance and Token Provisioning services.

Function: The Token Service Provider may involve the Card Issuer in Token Assurance.

Note: This relationship does not vary by use case.

Reference: Section 4.1.5 A5. Card Issuer – Token Service Provider.

A4. Card Issuer – Cardholder

Relationship: The existing Card Issuer – Cardholder relationship is utilised for the issuance of a Payment Token.

Function: The Card Issuer may involve the Cardholder in Token Assurance.

Note: This relationship does not vary by use case.

Reference: Section 4.1.6 A6. Card Issuer – Cardholder.

B1. Token Service Provider – Merchant (Token Requestor)

Relationship: The Token Service Provider provides Token Provisioning services to the Merchant (Token Requestor) on behalf of a Card Issuer.

Function: The Token Service Provider delivers the Payment Token to the Merchant (Token Requestor), which stores it in the Token Location.

Reference: Section 4.1.7 B1. Token Service Provider – Authorised Entity (Token Requestor).

Token Presentment

C1 Consumer – Merchant

Relationship: The existing Consumer – Merchant relationship is utilised for Cardholder-Initiated Transactions with a Payment Token and any subsequent Merchant-Initiated Transactions.

Function: The Consumer makes a purchase from the Merchant e-commerce environment. The Cardholder may interact with the Merchant e-commerce environment to select the payment credential (which has an affiliated Payment Token).

Reference: Section 5.1.1 C1. Consumer / Cardholder – Merchant.

Token Processing

D1. Merchant (Token Requestor) – Existing Payment Ecosystem Entities

Relationship: The Merchant (Token Requestor) utilises existing relationships to initiate Token Processing.

Function: The Merchant submits a Token Payment Request using the Payment Token and related data.

Note: This relationship does not vary by use case.

Reference: Section 6.1.1 D1. Merchant – Existing Payment Ecosystem Entities.

Other Relationships

In this use case, there is no Token User, and the Merchant fulfils the role of Token Requestor.

In comparison to the relationship model diagram in Figure 3.1, this means that the separate boxes showing the Merchant fulling the role of the Token User and the authorised entity fulfilling the role of Token Requestor have been merged into a single box (Merchant / Token Requestor) in Figure 8.9.

8.5.3 Use Case Characteristics

The use case characteristics are shown in Table 8.14, Table 8.15, Table 8.16 and Table 8.17.

Table 8.14: Card-On-File E-Commerce – Token Issuance Characteristics

Characteristic	Notes	Typical Outcomes
Cardholder Availability	Payment Tokens can be issued when the Cardholder is not available.	• Not Required

Table 8.15: Card-On-File E-Commerce – Token Provisioning Characteristics

Characteristic	Notes	Typical Outcomes
Token Location	See Table 5.1 of the Technical Framework for defined Token Locations.	• 01

Table 8.16: Card-On-File E-Commerce – Token Presentment Characteristics

Characteristic	Notes	Typical Outcomes
Token Presentment	The Merchant (Token Requestor) presents the Payment Token.	• Non-proximity
Acceptance Environment	The acceptance environment is a Merchant e-commerce environment.	• Non-physical

Table 8.17: Card-On-File E-Commerce – Token Processing Characteristics

Characteristic	Notes	Typical Outcomes
Token Payment Request	The Merchant submits the Token Payment Request to obtain a PAN Authorisation.	• Merchant
Token Control Fields	Used to constrain the Payment Token to a specific Merchant (Token Requestor) and a specific Token Presentment Mode.	• POS Entry Mode • Merchant Identifiers • Token Cryptogram

8.5.4 Payment Token Characteristics

The Payment Token characteristics are shown in Table 8.18.

Table 8.18: Card-On-File E-Commerce – Payment Token Characteristics

Characteristic	Note	Typical Outcomes
Payment Token Usage	The Payment Token is for use by a specific Merchant (Token Requestor).	• Merchant Specific
Token Assurance Method	Token Assurance is Token Programme specific and determined based on the detailed characteristics of this use case.	• Spaces / 00 • 01 – 19 • 20 – 89
Token Domain Restriction Controls	The Payment Token is constrained to a specific Merchant (Token Requestor) and a specific Token Presentment Mode.	• Merchant • Token Presentment Mode

Characteristic	Note	Typical Outcomes
Token Cryptogram	When a Token Cryptogram is used, it ensures the integrity of the transaction-specific data.	• Used • Not Used
Type of Transaction Initiation	Typically, the Cardholder uses a Merchant e-commerce environment to initiate a transaction.	• Cardholder-Initiated Transaction

8.5.5 Issuance Flow

The following preconditions and assumptions apply to this specific flow.

Issuance Flow Preconditions

- The Merchant (Token Requestor) has registered with the Token Service Provider and has received a Token Requestor ID
- The Merchant operates an e-commerce environment which can either be web-based or application-based
- The Consumer does not have an account with the Merchant and needs to create one before a payment credential can be added
- The PAN that the Cardholder adds to the account via the Merchant e-commerce environment is eligible for Tokenisation

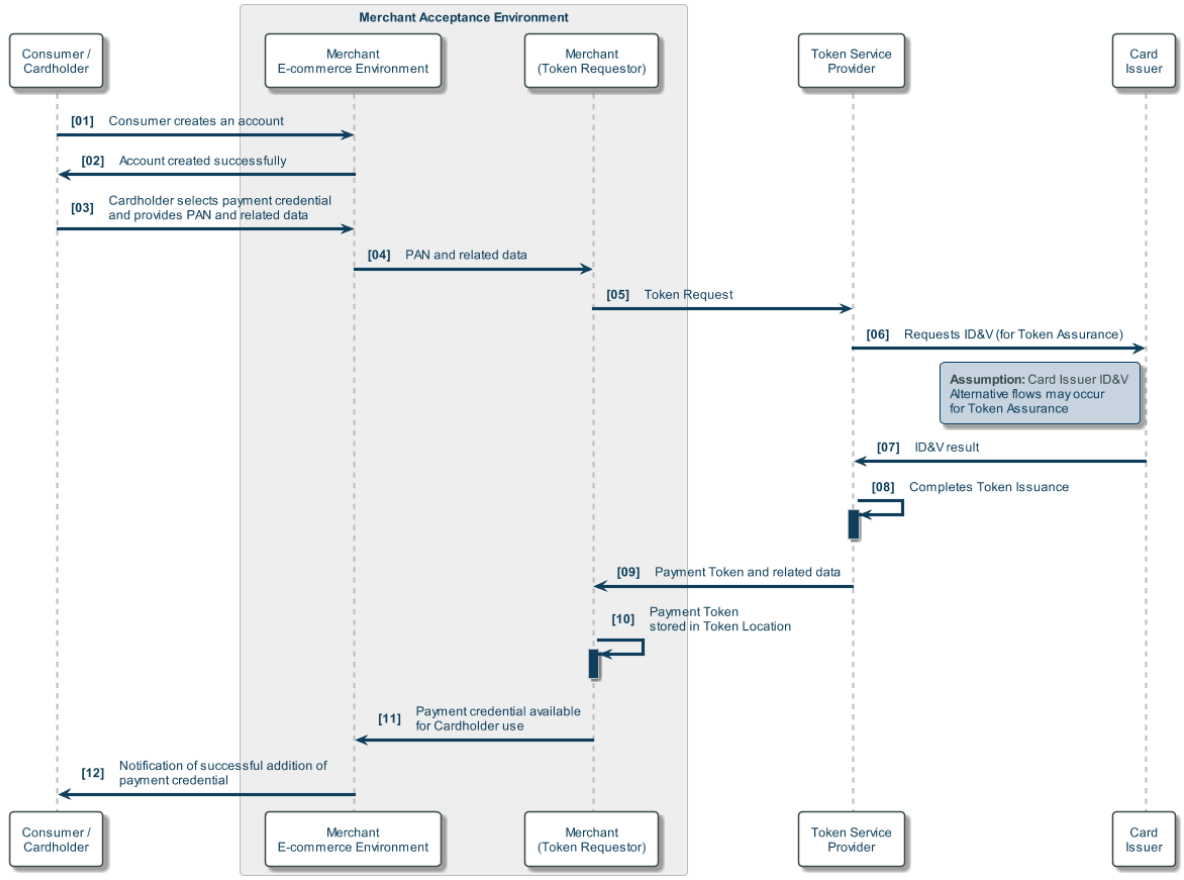
Issuance Flow Assumptions

- The Token Request is initiated by the Merchant (Token Requestor) based on an interaction with the Cardholder
- Token Assurance and the related ID&V is performed by the Card Issuer resulting in the Token Assurance Method value being set to one of the Card Issuer Token Assurance Method Categories
- The designated Token Location is 01 Remote storage

Example Issuance Flow

Figure 8.10 shows an example issuance flow, with numbered steps which are explained following the figure.

Figure 8.10: Card-On-File E-Commerce – Example Issuance Flow



01. The Consumer creates an account with the Merchant via its e-commerce environment
02. The Merchant e-commerce environment confirms that the account has been created
03. The Cardholder selects a payment credential to be added to the account and provides the PAN and related data as required by the Merchant e-commerce environment
04. The Merchant e-commerce environment provides the PAN and related data to the Merchant
05. The Merchant (Token Requestor) chooses not to store the PAN and related data and uses it to initiate a Token Request to the Token Service Provider (using its Token Requestor ID)
06. The Token Service Provider carries out Token Assurance and requests that the Card Issuer undertakes ID&V
07. The Card Issuer responds to the Token Service Provider with its ID&V result
08. The Token Service Provider completes Token Issuance (this is on the assumption that the ID&V result indicates Card Issuer approval)
09. The Token Service Provider delivers a Payment Token and its related data to the Merchant (Token Requestor) as part of Token Provisioning

10. The Payment Token and its related data are stored in the designated Token Location by the Merchant (Token Requestor) to complete Token Provisioning
11. The Merchant notifies the Merchant e-commerce environment that the payment credential is now available for the Cardholder's future use
12. The Cardholder is notified of the successful addition of the payment credential by the Merchant e-commerce environment. The Cardholder may not be aware of the Tokenisation process

8.5.6 Transaction Flow

The following preconditions and assumptions apply to this specific flow.

Transaction Flow Preconditions

There are no additional preconditions that apply to this specific flow.

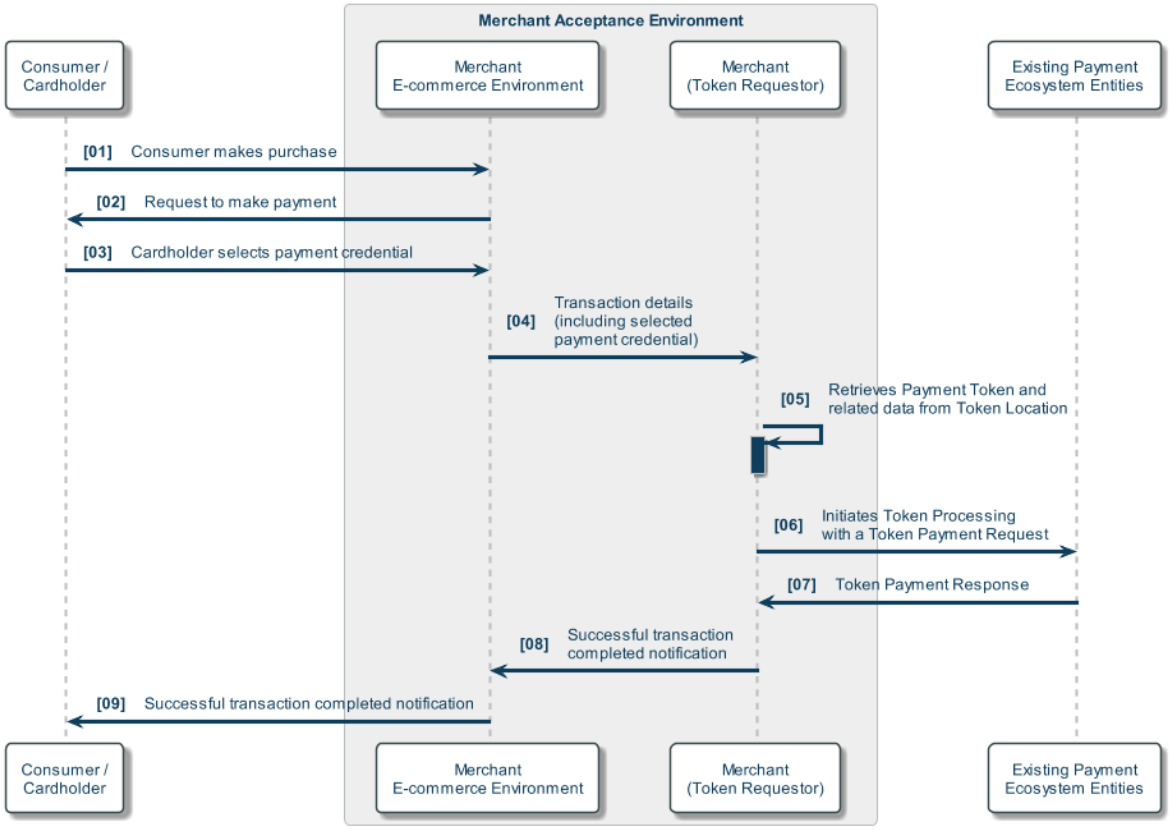
Transaction Flow Assumptions

- The Payment Token is stored by the Merchant (Token Requestor) and is identified in the Merchant e-commerce environment by the last four digits of the underlying PAN and digital card art
- The Consumer has accessed the account via the Merchant e-commerce environment
- The Consumer selects a payment credential stored in the account which has an affiliated Payment Token
- A Token Cryptogram is not used

Example Transaction Flow

Figure 8.11 shows an example transaction flow, with numbered steps which are explained following the figure.

Figure 8.11: Card-On-File E-Commerce – Example Transaction Flow



01. The Consumer makes a purchase from the Merchant e-commerce environment and initiates the checkout process
02. The Merchant e-commerce environment initiates the request for a payment credential to be selected
03. The Cardholder selects a previously stored payment credential from the account via the Merchant e-commerce environment
04. The Merchant e-commerce environment provides details of the transaction, including the selected payment credential, to the Merchant
05. The Merchant (Token Requestor) retrieves the Payment Token and related data from the Token Location
06. The Merchant initiates Token Processing by sending a Token Payment Request
07. The Merchant receives a Token Payment Response as a result of successful PAN Authorisation by the Card Issuer
08. The Merchant provides the results to the Merchant e-commerce environment
09. The Cardholder receives confirmation from the Merchant e-commerce environment that the transaction was successful

Token Processing Considerations

Table 8.17 (Token Processing Characteristics) and Table 8.18 (Payment Token Characteristics) show the typical Token Control Fields (Table 8.17) which are used as part of the Token Domain Restriction Controls (Table 8.18). In these specific use case flows, the following Token Control Fields are used:

- POS Entry Mode: has an expected value that indicates an e-commerce transaction, used to constrain the Payment Token to a specific Token Presentment Mode
- Merchant identifier(s): represents the specific Merchant (Token Requestor) using the Payment Token, used to constrain the Payment Token to a specific Merchant (Token Requestor)

As well as the methods described in Section 8.1.3 Payment Account Reference Data (PAR Field and PAR Enquiry), PAR Data may be available to the Merchant:

- As part of the Token Provisioning process

8.5.7 Variations of User Experience

Minor variations may occur for this use case due to possible differences related to whether the Consumer is interacting with a website or Merchant application, which will be Merchant and / or implementation specific.

8.6 E-Commerce Guest Checkout

This use case example assumes that a Consumer is interacting with the Merchant e-commerce environment using guest checkout to make a purchase. The details of the Consumer's payment credential are used by the Merchant for this specific purchase only.

The Cardholder provides the Merchant with details of the payment credential which the Merchant (Token Requestor) uses to obtain a Payment Token for this specific purchase only. The Merchant (Token Requestor) uses this Payment Token for Token Processing.

The Cardholder is notified of the outcome of the transaction by the Merchant e-commerce environment.

This use case example covers:

- Token Issuance and Token Provisioning
- Token Presentment and Token Processing

8.6.1 Use Case Overview – Problems Addressed & User Experience

E-Commerce Merchants have guest checkout options where the Merchant does not store any information beyond that necessary for the current transaction. Using a Payment Token to immediately replace a PAN and related data has the same benefits for the Merchants as

replacing PANs with Payment Tokens in a card-on-file scenario (see Section 8.5 Card-On-File E-Commerce).

The user experience is essentially unchanged with the Consumer entering details of the payment credential to be used.

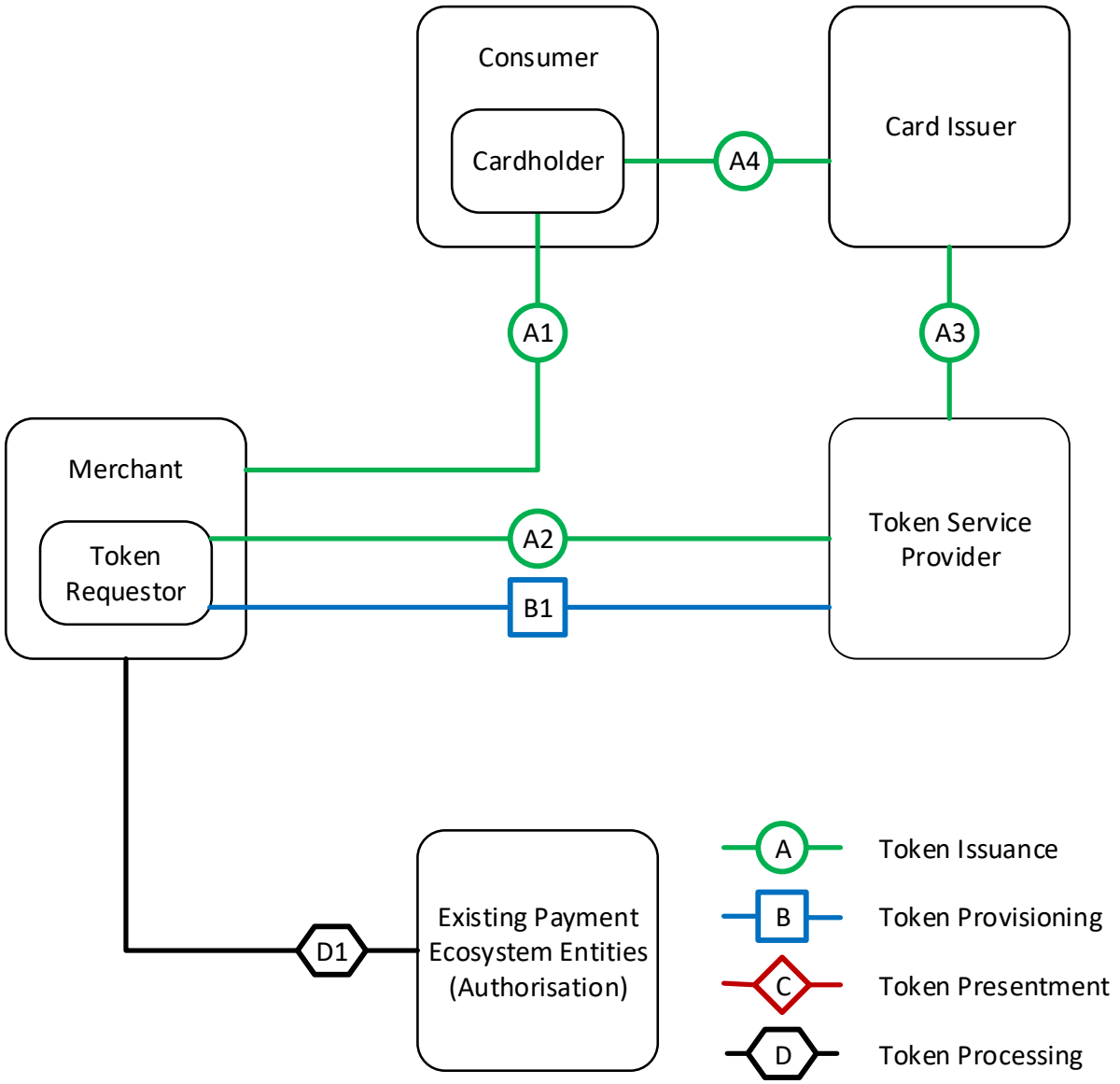
8.6.2 Use Case Relationships and Functions

The relationships for this use case example are shown in Figure 8.12. For a description of the baseline relationships and their functions, refer to the models given in Sections:

- 4.1 Token Issuance and Token Provisioning Relationships and Functions
- 5.1 Token Presentment Relationships and Functions
- 6.1 Token Processing Relationships and Functions

For this use case example, the Merchant is performing the role of the authorised entity described in Sections 4.1, 5.1 and 6.1. For each relationship shown in Figure 8.12, the specific nature of the relationship and its function is given in the text following the figure, along with a reference to the baseline relationship and function.

Figure 8.12: E-Commerce Guest Checkout – Use Case Relationships



Token Issuance and Token Provisioning

A1. Cardholder – Merchant (Token Requestor)

Relationship: The Cardholder has a temporary relationship with the Merchant (Token Requestor) for the duration of the single Cardholder-Initiated Transaction (and any subsequent Merchant-Initiated Transactions).

Function: The Cardholder uses a payment credential by providing a PAN and related data to the Merchant (Token Requestor) via the Merchant e-commerce environment which triggers the Token Issuance.

Reference: Section 4.1.1 A1. Cardholder – Authorised Entity (Token Requestor).

A2. Token Service Provider – Merchant (Token Requestor)

Relationship: The Token Service Provider has an existing relationship with the Merchant (Token Requestor) to enable Payment Tokenisation on behalf of a Card Issuer. The Merchant (Token Requestor) is identified by its Token Requestor ID assigned by the Token Service Provider.

Function: The Merchant (Token Requestor) makes a Token Request to the Token Service Provider using the PAN and related data (provided by the Cardholder via the Merchant e-commerce environment).

Reference: Section 4.1.4 A4. Token Service Provider – Authorised Entity (Token Requestor).

A3. Card Issuer – Token Service Provider

Relationship: The Card Issuer uses the Token Service Provider to provide Token Issuance and Token Provisioning services.

Function: The Token Service Provider may involve the Card Issuer in Token Assurance.

Note: This relationship does not vary by use case.

Reference: Section 4.1.5 A5. Card Issuer – Token Service Provider.

A4. Card Issuer – Cardholder

Relationship: The existing Card Issuer – Cardholder relationship is utilised for the issuance of a Payment Token.

Function: The Card Issuer may involve the Cardholder in Token Assurance.

Note: This relationship does not vary by use case.

Reference: Section 4.1.6 A6. Card Issuer – Cardholder.

B1. Token Service Provider – Merchant (Token Requestor)

Relationship: The Token Service Provider provides Token Provisioning services to the Merchant (Token Requestor) on behalf of a Card Issuer.

Function: The Token Service Provider delivers the Payment Token to the Merchant (Token Requestor), which stores it in the Token Location.

Reference: Section 4.1.7 B1. Token Service Provider – Authorised Entity (Token Requestor).

Token Processing

D1. Merchant – Existing Payment Ecosystem Entities

Relationship: The Merchant utilises existing relationships to initiate Token Processing.

Function: The Merchant submits a Token Payment Request using the Payment Token and related data.

Note: This relationship does not vary by use case.

Reference: Section 6.1.1 D1. Merchant – Existing Payment Ecosystem Entities.

Other Relationships

In this use case there is no Token Presentment relationship between the Consumer / Cardholder and the Merchant / Token Requestor.

Note: the Merchant (Token Requestor) facilitates Token Presentment on behalf of the Cardholder.

8.6.3 Use Case Characteristics

The use case characteristics are shown in Table 8.19, Table 8.20, Table 8.21 and Table 8.22.

Table 8.19: E-Commerce Guest Checkout – Token Issuance Characteristics

Characteristic	Notes	Typical Outcomes
Cardholder Availability	Payment Tokens can be issued when the Cardholder is not available.	• Not Required

Table 8.20: E-Commerce Guest Checkout – Token Provisioning Characteristics

Characteristic	Notes	Typical Outcomes
Token Location	See Table 5.1 of the Technical Framework for defined Token Locations.	• 07

Table 8.21: E-Commerce Guest Checkout – Token Presentment Characteristics

Characteristic	Notes	Typical Outcomes
Token Presentment	The Merchant (Token Requestor) presents the Payment Token.	• Non-proximity
Acceptance Environment	The acceptance environment is a Merchant e-commerce environment.	• Non-physical

Table 8.22: E-Commerce Guest Checkout – Token Processing Characteristics

Characteristic	Notes	Typical Outcomes
Token Payment Request	The Merchant submits the Token Payment Request to obtain a PAN Authorisation.	• Merchant

Characteristic	Notes	Typical Outcomes
Token Control Fields	Used to constrain the Payment Token to a specific Merchant (Token Requestor) and to constrain the use of the Payment Token to a single Cardholder-Initiated Transaction and any subsequent Merchant-Initiated Transactions.	• POS Entry Mode • Merchant Identifiers • Token Cryptogram

8.6.4 Payment Token Characteristics

The Payment Token characteristics are shown in Table 8.23.

Table 8.23: E-Commerce Guest Checkout – Payment Token Characteristics

Characteristic	Note	Typical Outcomes
Payment Token Usage	The Payment Token is for use by a specific Merchant (Token Requestor) and is constrained for use in a single Cardholder-Initiated Transaction and any subsequent Merchant-Initiated Transactions.	• Guest Checkout • Merchant Specific
Token Assurance Method	Token Assurance is Token Programme specific and determined based on the detailed characteristics of this use case.	• Spaces / 00 • 01 – 19 • 20 – 89
Token Domain Restriction Controls	The Payment Token is constrained to a specific Merchant (Token Requestor) and a specific Token Presentment Mode.	• Merchant • Token Presentment Mode
Token Cryptogram	When a Token Cryptogram is used, it ensures the integrity of the transaction-specific data.	• Used • Not Used
Type of Transaction Initiation	Typically, the Cardholder uses a Merchant e-commerce environment to initiate a transaction.	• Cardholder-Initiated Transaction

8.6.5 Issuance Flow

The following preconditions and assumptions apply to this specific flow.

Issuance Flow Preconditions

- Merchant (Token Requestor) has registered with the Token Service Provider and has received a Token Requestor ID
- The Merchant operates an e-commerce environment which can either be web-based or application-based
- The PAN that the Cardholder uses for the guest checkout on the Merchant e-commerce environment is eligible for Tokenisation

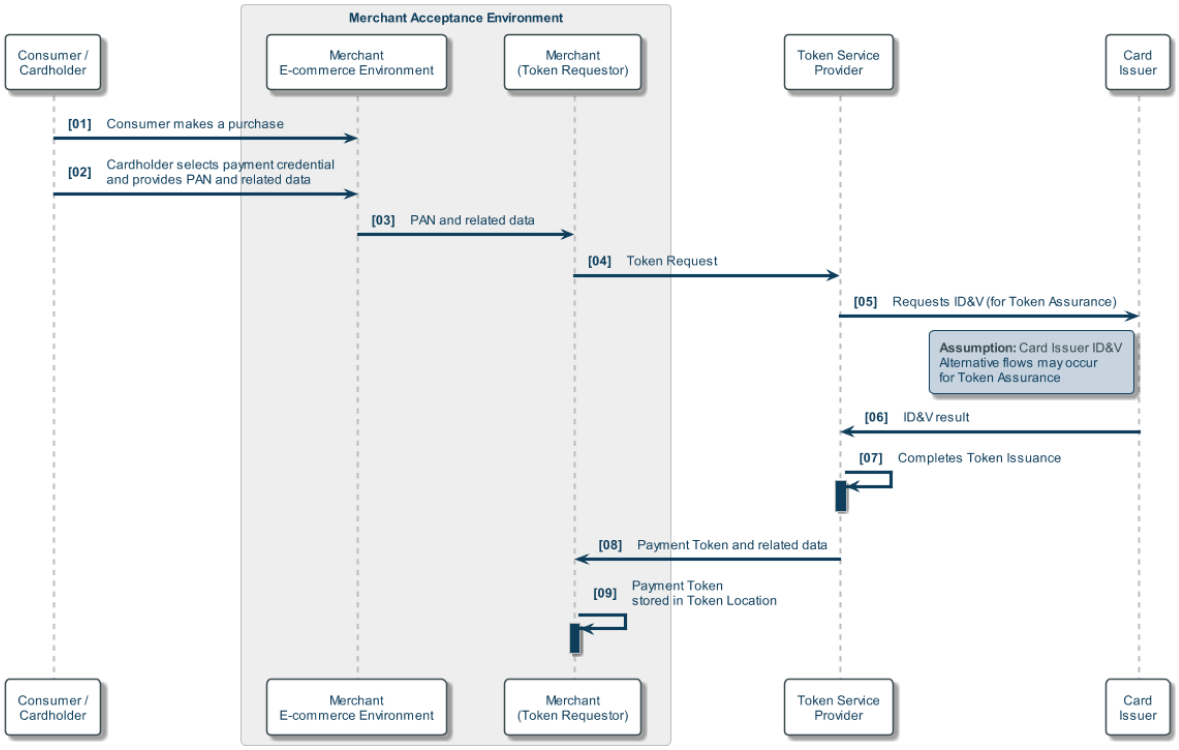
Issuance Flow Assumptions

- The Token Request is initiated by the Merchant (Token Requestor) based on an interaction with the Cardholder
- Token Assurance and the related ID&V is performed by the Card Issuer resulting in the Token Assurance Method value being set to one of the Card Issuer Token Assurance Method Categories
- The designated Token Location is 07 Temporary storage

Example Issuance Flow

Figure 8.13 shows an example issuance flow, with numbered steps which are explained following the figure.

Figure 8.13: E-Commerce Guest Checkout – Example Issuance Flow



01. The Consumer makes a purchase and chooses guest checkout on the Merchant e-commerce environment
02. The Cardholder selects a payment credential and provides the PAN and related data as required by the Merchant e-commerce environment
03. The Merchant e-commerce environment provides the PAN and related data to the Merchant
04. The Merchant (Token Requestor) chooses not to store the PAN and related data and uses it to initiate a Token Request to the Token Service Provider (using its Token Requestor ID)
05. The Token Service Provider carries out Token Assurance and requests that the Card Issuer undertakes ID&V
06. The Card Issuer responds to the Token Service Provider with its ID&V result
07. The Token Service Provider completes Token Issuance (this is on the assumption that the ID&V result indicates Card Issuer approval)
08. The Token Service Provider delivers a Payment Token and related data to the Merchant (Token Requestor) as part of Token Provisioning
09. The Payment Token and its related data are stored in the designated Token Location by the Merchant (Token Requestor) for the single transaction. The Cardholder may not be aware of the Tokenisation process

8.6.6 Transaction Flow

The following preconditions and assumptions apply to this specific flow.

Transaction Flow Preconditions

There are no additional preconditions that apply to this specific flow.

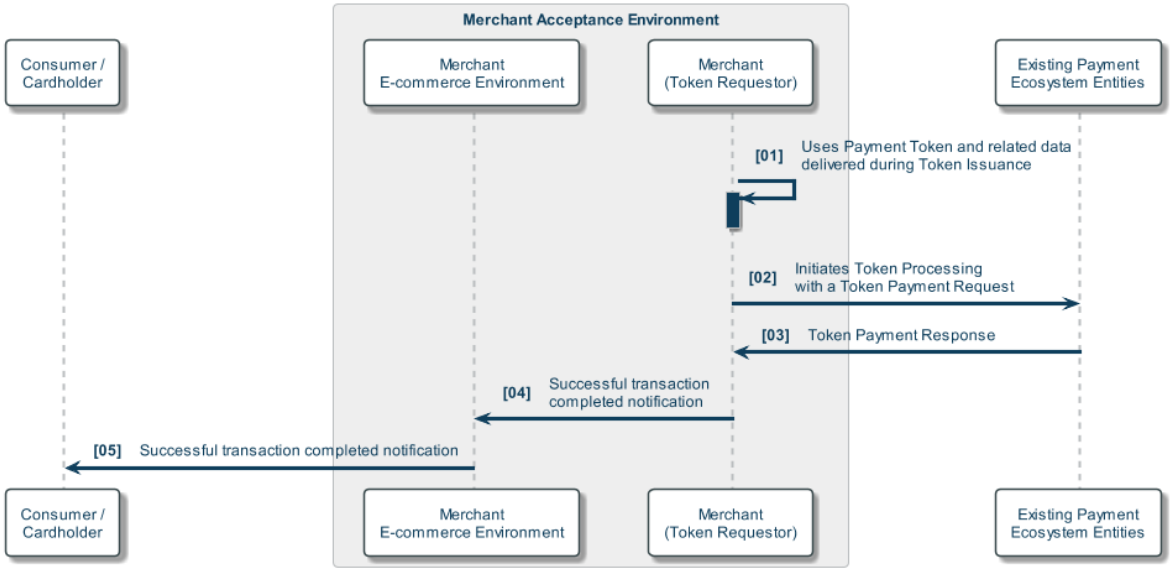
Transaction Flow Assumptions

- A Token Cryptogram is not used

Example Transaction Flow

Figure 8.14 shows an example transaction flow, with numbered steps which are explained following the figure.

Figure 8.14: E-Commerce Guest Checkout – Example Transaction Flow



01. The Merchant (Token Requestor) uses the Payment Token and related data which was received in response to the Token Request (see Section 8.6.5 Issuance)
02. The Merchant initiates Token Processing by sending a Token Payment Request
03. The Merchant receives a Token Payment Response as a result of successful PAN Authorisation by the Card Issuer
04. The Merchant provides the results to the Merchant e-commerce environment
05. The Cardholder receives confirmation from the Merchant e-commerce environment that the transaction was successful

Token Processing Considerations

Table 8.22 (Token Processing Characteristics) and Table 8.23 (Payment Token Characteristics) show the typical Token Control Fields (Table 8.22) which are used as part of the Token Domain Restriction Controls (Table 8.23). In these specific use case flows, the following Token Control Fields are used:

- POS Entry Mode: has an expected value that indicates an e-commerce transaction, used to constrain the Payment Token to a specific Token Presentment Mode
- Merchant identifier(s): represents the specific Merchant (Token Requestor) using the Payment Token for this transaction, used to constrain the Payment Token to this specific Merchant (Token Requestor)

Additional Payment Token restrictions may be applied to constrain the use of the Payment Token to a single Cardholder-Initiated Transaction and additional constraints on any Merchant-Initiated Transactions.

As well as the methods described in Section 8.1.3 Payment Account Reference Data (PAR Field and PAR Enquiry), PAR Data may be available to the Merchant:

- As part of the Token Provisioning process

8.6.7 Variations of User Experience

Minor variations may occur for this use case due to possible differences related to whether the Consumer is interacting with a website or Merchant application, which will be Merchant and / or implementation specific.

8.7 Third Party Service Provider

This use case example assumes that a Consumer is interacting with the Merchant e-commerce environment (web-based or application-based) to make a purchase and that the Merchant uses a Third Party Service Provider to enable Payment Tokenisation.

The Cardholder interacts with the Merchant to provide details of a payment credential. Token Requestor functionality is provided to the Merchant (Token User) by a Third Party Service Provider (Token Requestor) which uses the details to obtain a Payment Token. The Payment Token is then stored by the Merchant (Token User) to be used in transactions.

The Cardholder selects a payment credential at the time of purchase and the Merchant (Token User) retrieves the affiliated Payment Token. The Merchant (Token User) requests a Token Cryptogram from the Third Party Service Provider (Token Requestor) which it obtains from the Token Service Provider and provides to the Merchant (Token User). The Merchant (Token User) uses the Payment Token with the corresponding Token Cryptogram to initiate Token Processing.

The Cardholder is notified of the outcome of the transaction by the Merchant.

This use case example covers:

- Token Issuance and Token Provisioning
- Token Presentment and Token Processing

8.7.1 Use Case Overview – Problems Addressed & User Experience

Use of a Third Party Service Provider to enable Payment Tokenisation allows Merchants to gain the benefits of Payment Tokenisation without implementing multiple interfaces to perform the role of a Token Requestor. The Third Party Service Provider performs the role of Token Requestor for multiple Merchants (Token Users) and manages the various interfaces and interactions with the Token Servicer Provider(s). By using a single Third Party Service Provider (Token Requestor) to enable Payment Tokenisation, a Merchant (Token User) can potentially gain access to multiple Token Service Providers.

A single Payment Token can be used by multiple Merchants (Token Users) when managed by a Third Party Service Provider (Token Requestor) and may be beneficial to and support scalability of Payment Tokenisation and bring efficiency to the supply of Payment Tokens.

The user experience is essentially unchanged, with the Consumer selecting a stored payment credential (which has an affiliated Payment Token) for use during checkout. Once selected, the Merchant (Token User) uses the affiliated Payment Token instead of the PAN. Typically, the Consumer will not be aware of the Tokenisation process.

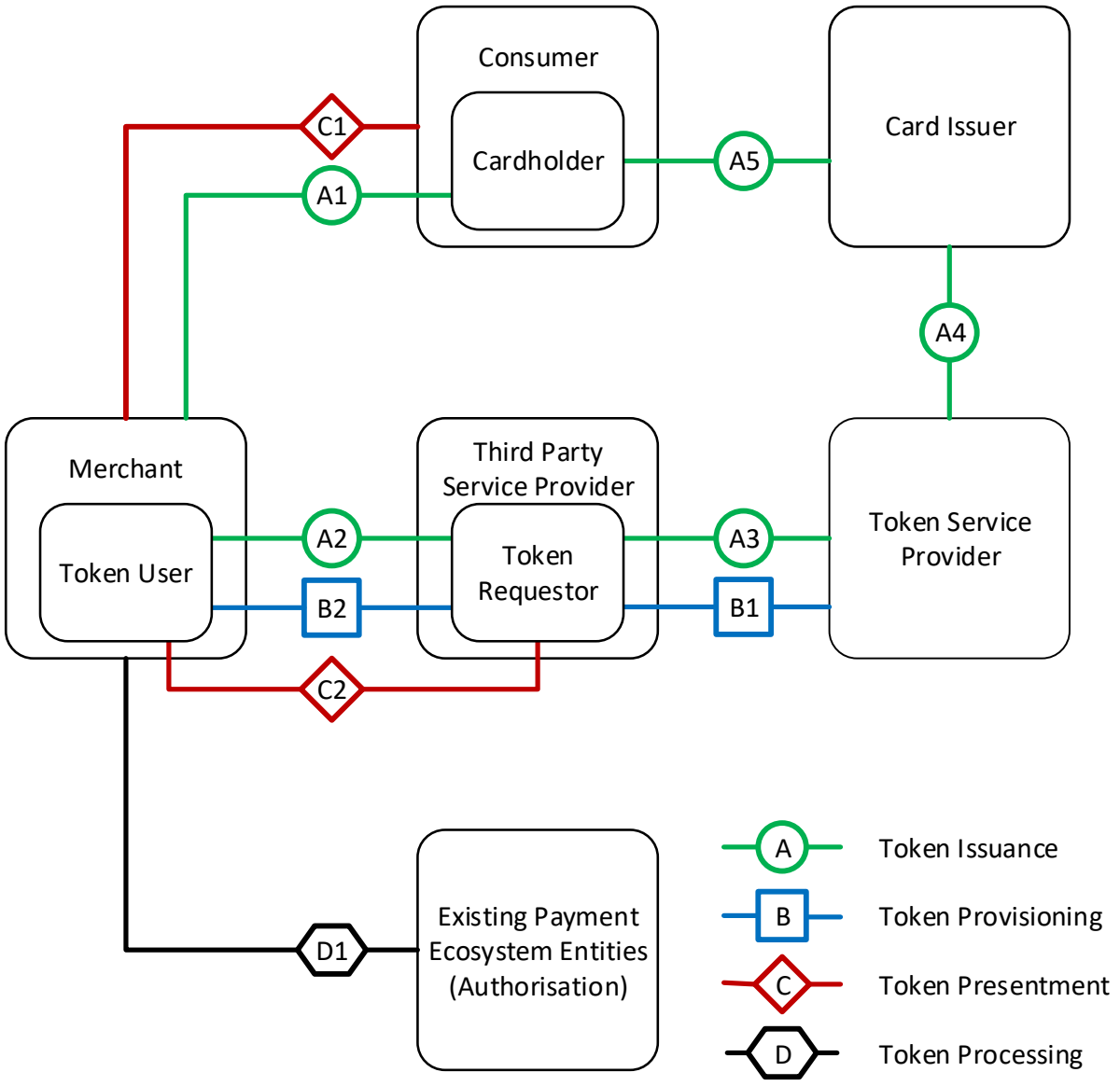
8.7.2 Use Case Relationships and Functions

The relationships for this use case example are shown in Figure 8.15. For a description of the baseline relationships and their functions, refer to the models given in Sections:

- 4.1 Token Issuance and Token Provisioning Relationships and Functions
- 5.1 Token Presentment Relationships and Functions
- 6.1 Token Processing Relationships and Functions

For this use case example, the Third Party Service Provider is performing the role of the authorised entity described in Sections 4.1, 5.1 and 6.1. For each relationship shown in Figure 8.15, the specific nature of the relationship and its function is given in the text following the figure, along with a reference to the baseline relationship and function.

Figure 8.15: Third Party Service Provider – Use Case Relationships



Token Issuance and Token Provisioning

A1. Cardholder – Merchant (Token User)

Relationship: The Cardholder has a relationship with the Merchant (Token User).

Function: The Cardholder adds a payment credential by providing a PAN and related data to the Merchant e-commerce environment.

Reference: Section 4.1.2 A2. Cardholder – Merchant (Token User).

A2. Merchant (Token User) – Third Party Service Provider (Token Requestor)

Relationship: The Merchant (Token User) has an existing relationship with a Third Party Service Provider (Token Requestor) to enable Payment Tokenisation.

Function: The Merchant (Token User) provides the PAN and the related data to the Third Party Service Provider (Token Requestor). In this use case example, the PAN has not previously been Tokenised by the Third Party Service Provider (Token Requestor), which triggers the Token Issuance process.

Reference: Section 4.1.3 A3. Merchant (Token User) – Authorised Entity (Token Requestor).

A3. Token Service Provider – Third Party Service Provider (Token Requestor)

Relationship: The Token Service Provider has an existing relationship with the Third Party Service Provider (Token Requestor) to enable Payment Tokenisation on behalf of a Card Issuer. The Merchant (Token Requestor) is identified by its Token Requestor ID assigned by the Token Service Provider.

Function: The Third Party Service Provider (Token Requestor) makes a Token Request to the Token Service Provider using the PAN and related data (provided by the Merchant (Token User)).

Reference Section 4.1.4 A4. Token Service Provider – Authorised Entity (Token Requestor).

A4. Card Issuer – Token Service Provider

Relationship: The Card Issuer uses the Token Service Provider to provide Token Issuance and Token Provisioning services.

Function: The Token Service Provider may involve the Card Issuer in Token Assurance.

Note: This relationship does not vary by use case.

Reference: Section 4.1.5 A5. Card Issuer – Token Service Provider.

A5. Card Issuer – Cardholder

Relationship: The existing Card Issuer – Cardholder relationship is utilised for the issuance of a Payment Token.

Function: The Card Issuer may involve the Cardholder in Token Assurance.

Note: This relationship does not vary by use case.

Reference: Section 4.1.6 A6. Card Issuer – Cardholder.

B1. Token Service Provider – Third Party Service Provider (Token Requestor)

Relationship: The Token Service Provider provides Token Provisioning services to the Third Party Service Provider (Token Requestor) on behalf of a Card Issuer.

Function: The Token Service Provider delivers the Payment Token to the Third Party Service Provider (Token Requestor).

Reference: Section 4.1.7 B1. Token Service Provider – Authorised Entity (Token Requestor).

B2. Merchant (Token User) – Third Party Service Provider (Token Requestor)

Relationship: The Third Party Service Provider (Token Requestor) extends Token Provisioning services to the Merchant (Token User).

Function: The Third Party Service Provider (Token Requestor) delivers the Payment Token and related data to the Merchant (Token User), who stores it in the Token Location until it is required for Token Processing.

Reference: Section 4.1.9 B3. Merchant (Token User) – Authorised Entity (Token Requestor.

Token Presentment

C1 Consumer – Merchant

Relationship: The existing Consumer – Merchant relationship is utilised for Cardholder-Initiated Transactions with a Payment Token and any subsequent Merchant-Initiated Transactions.

Function: The Consumer makes a purchase from the Merchant e-commerce environment. The Cardholder may interact with the Merchant e-commerce environment to select the payment credential (which has an affiliated

Payment Token).

Reference: Section 5.1.1 C1. Consumer / Cardholder – Merchant.

C2 Merchant (Token User) – Third Party Service Provider (Token Requestor)

Relationship: The Merchant (Token User) has an existing relationship with the Third Party Service Provider (Token Requestor) to provide Payment Tokenisation services.

Function: The Merchant (Token User) has previously been supplied with the Payment Token by the Third Party Service Provider (Token Requestor) during Token Provisioning (see B2). To enable the use of the Payment Token in Token Processing, the Merchant (Token User) receives a Token Cryptogram from the Third Party Service Provider (Token Requestor).

Reference: Section 5.1.3 C3. Merchant (Token User) – Authorised Entity (Token Requestor).

Token Processing

D1. Merchant (Token User) – Existing Payment Ecosystem Entities

Relationship: The Merchant (Token User) utilises existing relationships to initiate Token Processing.

Function: The Merchant submits a Token Payment Request using the Payment Token and related data.

Note: This relationship does not vary by use case.

Reference: Section 6.1.1 D1. Merchant – Existing Payment Ecosystem Entities.

8.7.3 Use Case Characteristics

The use case characteristics are shown in Table 8.24, Table 8.25, Table 8.26 and Table 8.27.

Table 8.24: Third Party Service Provider – Token Issuance Characteristics

Characteristic	Notes	Typical Outcomes
Cardholder Availability	Payment Tokens can be issued when the Cardholder is not available.	• Not Required

Table 8.25: Third Party Service Provider – Token Provisioning Characteristics

Characteristic	Notes	Typical Outcomes
Token Location	See Table 5.1 of the Technical Framework for defined Token Locations.	• 06

Table 8.26: Third Party Service Provider – Token Presentment Characteristics

Characteristic	Notes	Typical Outcomes
Token Presentment	The Merchant (Token User) presents the Payment Token.	• Non-proximity
Acceptance Environment	The acceptance environment is a Merchant e-commerce environment.	• Non-physical

Table 8.27: Third Party Service Provider – Token Processing Characteristics

Characteristic	Notes	Typical Outcomes
Token Payment Request	The Merchant (Token User) submits the Token Payment Request to obtain a PAN authorisation.	• Merchant

Characteristic	Notes	Typical Outcomes
Token Control Fields	Used to constrain the Payment Token to a specific Merchant (Token User) and specific Token Presentment Mode at the time of a given transaction.	• POS Entry Mode • Merchant Identifiers • Token Cryptogram

8.7.4 Payment Token Characteristics

The Payment Token characteristics are shown in Table 8.28.

Table 8.28: Third Party Service Provider – Payment Token Characteristics

Characteristic	Notes	Typical Outcomes
Payment Token Usage	The Payment Token can be used by a Merchant (Token User) that is not the Token Requestor.	• Token User
Token Assurance Method	Token Assurance is Token Programme specific and determined based on the detailed characteristics of this use case.	• Spaces / 00 • 01 – 19 • 20 – 89
Token Domain Restriction Controls	The Payment Token is constrained to specific Merchants (Token Users) and a specific Token Presentment Mode.	• Merchant(s) • Token Presentment Mode
Token Cryptogram	A Token Cryptogram is used to ensure the integrity of the transaction-specific data.	• Used
Type of Transaction Initiation	Typically, the Cardholder uses a Merchant e-commerce environment to initiate a transaction.	• Cardholder-Initiated Transaction

8.7.5 Issuance Flow

The following preconditions and assumptions apply to this specific flow.

Issuance Flow Preconditions

- The Third Party Service Provider (Token Requestor) has registered with a Token Service Provider and has received a Token Requestor ID
- The Merchant (Token User) has registered with the Third Party Service Provider

- The Merchant operates an e-commerce environment which can either be web-based or application-based
- The Consumer does not have an account with the Merchant and needs to create one before a payment credential can be added
- The PAN that the Cardholder adds to the account via the Merchant e-commerce environment is eligible for Tokenisation

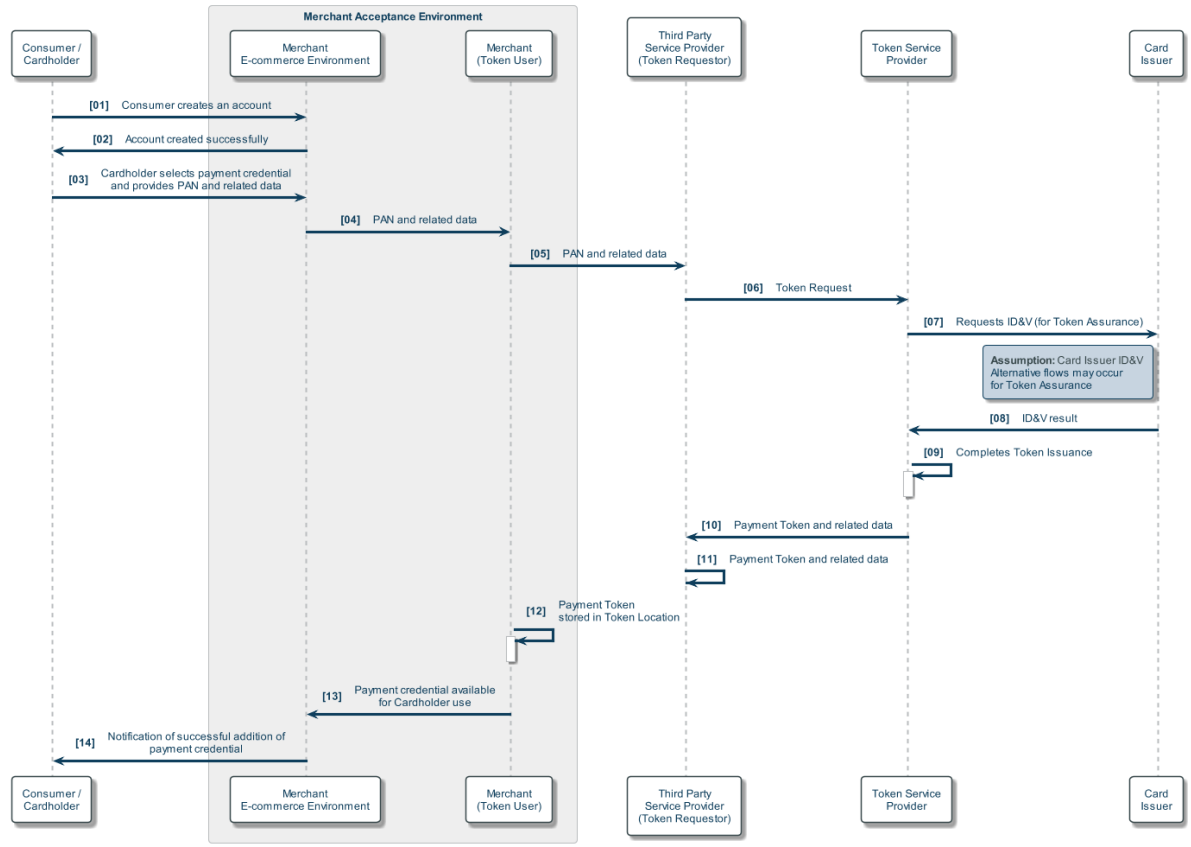
Issuance Flow Assumptions

- A Payment Token is requested by the Merchant (Token User) from the Third Party Service Provider (Token Requestor)
- The Token Request is initiated by the Third Party Service Provider (Token Requestor)
- Token Assurance and the related ID&V is performed by the Card Issuer resulting in the Token Assurance Method value being set to one of the Card Issuer Token Assurance Method Categories
- The designated Token Location is 06 Shared storage

Example Issuance Flow

Figure 8.16 shows an example issuance flow, with numbered steps which are explained following the figure.

Figure 8.16: Third Party Service Provider – Example Issuance Flow



01. The Consumer creates an account with the Merchant via its e-commerce environment
02. The Merchant e-commerce environment confirms that the account has been created
03. The Cardholder selects a payment credential to be added to the account and provides the PAN and related data as required by the Merchant e-commerce environment.
04. The Merchant e-commerce environment provides the PAN and related data to the Merchant
05. The Merchant (Token User) chooses not to store the PAN and related data and provides it to the Third Party Service Provider (Token Requestor) for Tokenisation
06. The Third Party Service Provider (Token Requestor) initiates a Token Request for a Payment Token to the Token Service Provider (using its Token Requestor ID)
07. The Token Service Provider carries out Token Assurance and requests that the Card Issuer undertakes ID&V
08. The Card Issuer responds to the Token Service Provider with its ID&V result
09. The Token Service Provider completes Token Issuance (this is on the assumption that the ID&V result indicates Card Issuer approval)

10. The Token Service Provider delivers a Payment Token and related data to the Third Party Service Provider (Token Requestor) as part of Token Provisioning
11. The Party Service Provider delivers the Payment Token and related data to the Merchant (Token User)
12. The Payment Token and its related data are stored in the designated Token Location by the Merchant (Token User) to complete Token Provisioning
13. The Merchant notifies the Merchant e-commerce environment that the payment credential is now available for the Cardholder's future use
14. The Cardholder is notified of the successful addition of the payment credential. The Cardholder may not be aware of the Tokenisation process

8.7.6 Transaction Flow

The following preconditions and assumptions apply to this specific flow.

Transaction Flow Preconditions

There are no additional preconditions that apply to this specific flow.

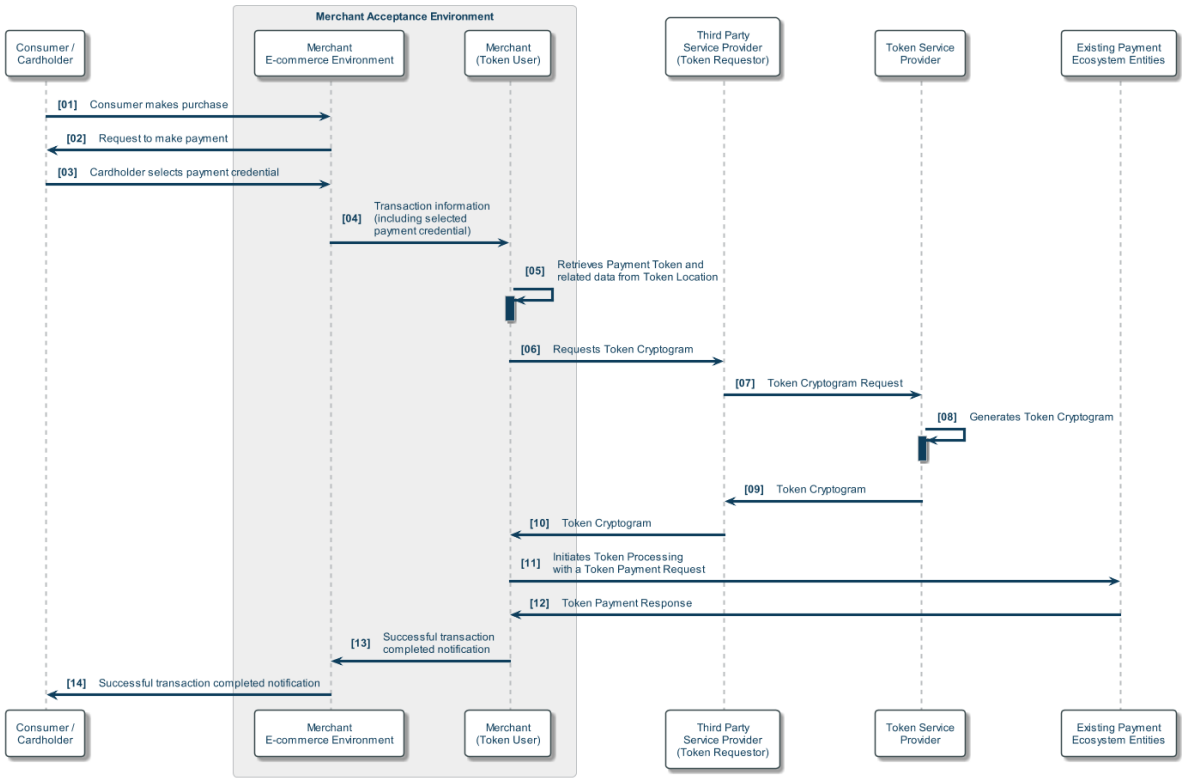
Transaction Flow Assumptions

- The Payment Token is stored by the Merchant (Token User) and is identified in the Merchant e-commerce environment by the last four digits of the underlying PAN and digital card art
- The Consumer has accessed the account via the Merchant e-commerce environment
- The Consumer selects a payment credential stored in the account which has an affiliated Payment Token
- The Token Service Provider generates a Token Cryptogram
- The Merchant (Token User) initiates Token Processing using the Payment Token and related data (along with the provided Token Cryptogram) via existing relationships with the existing Payment Ecosystem Entities

Example Transaction Flow

Figure 8.17 shows an example transaction flow, with numbered steps which are explained following the figure.

Figure 8.17: Third Party Service Provider – Example Transaction Flow



01. The Consumer makes a purchase from the Merchant e-commerce environment and initiates the checkout process
02. The Merchant e-commerce environment initiates the request for a payment credential to be selected
03. The Cardholder selects a previously stored payment credential from the account via the Merchant e-commerce environment
04. The Merchant e-commerce environment provides transaction information, including the selected payment credential, to the Merchant
05. The Merchant (Token User) retrieves the Payment Token and related data from the Token Location
06. The Merchant (Token User) uses the Payment Token and relevant transaction information to request a Token Cryptogram from the Third Party Service Provider (Token Requestor)
07. The Third Party Service Provider (Token Requestor) uses the information received from the Merchant (Token User) to initiate a Token Cryptogram Request to the Token Service Provider
08. The Token Service Provider processes the Token Cryptogram Request and generates a Token Cryptogram

09. The Third Party Service Provider (Token Requestor) receives the Token Cryptogram from the Token Service Provider
10. The Third Party Service Provider (Token Requestor) delivers the Token Cryptogram to the Merchant (Token User)
11. The Merchant (Token User) initiates Token Processing by sending a Token Payment Request
12. The Merchant (Token User) receives a Token Payment Response as a result of successful PAN Authorisation by the Card Issuer
13. The Merchant provides the results to the Merchant e-commerce environment
14. The Cardholder receives confirmation from the Merchant e-commerce environment that the transaction was successful

Token Processing Considerations

Table 8.27 (Token Processing Characteristics) and Table 8.28 (Payment Token Characteristics) show the typical Token Control Fields (Table 8.27) which are used as part of the Token Domain Restriction Controls (Table 8.28). In these specific use case flows, the following Token Control Fields are used:

- POS Entry Mode: has an expected value that indicates an e-commerce transaction, used to constrain the Payment Token to a specific Token Presentment Mode
- Merchant Identifier(s): represents the specific Merchant (Token User) using the Payment Token, used to constrain the Payment Token to this specific Merchant (Token User)
- Token Cryptogram: valid only for this transaction to prevent payment transactional data from being reused in another transaction

As well as the methods described in Section 8.1.3 Payment Account Reference Data (PAR Field and PAR Enquiry), PAR Data may be available to the Merchant:

- As part of the Payment Token Provisioning process

8.7.7 Variations of User Experience

Minor variations may occur for this use case due to possible differences related to whether the Consumer is interacting with a website or Merchant application, which will be Merchant and / or implementation specific.

8.8 Merchant-Initiated Transaction

There are several usage scenarios which may result in one or more Merchant-Initiated Transactions following on from a Cardholder-Initiated Transaction. Common examples include

the split shipment of goods from an e-commerce order, a delayed incidental charge related to a hotel stay or recurring charges related to a subscription service. Further information is provided by EMVCo in the Transaction Types document (EMV® Best Practices Document – Recommendations for EMV® Processing for Industry-Specific Transaction Types).

This use case example illustrates the use of Payment Tokens within a Merchant-Initiated Transaction for a subscription service. This is a popular business model used by many e-commerce Merchants, especially streaming services. To optimise the Consumer experience, these Merchants may offer to store the Consumer's payment credentials in conjunction with other data in an account in order to make regular payments to cover subscription fees, meaning that the Consumer does not need to manually initiate payment when the subscription service is about to expire if an additional subscription payment is not made.

These regular payments are an example of Merchant-Initiated Transactions. A Cardholder-Initiated Transaction is one where the Cardholder actively participates in the transaction. A Merchant-Initiated Transaction is one that relates to a previous Cardholder-Initiated Transaction but is conducted without the active participation of the Cardholder.

This use case example covers:

- Token Processing

8.8.1 Use Case Overview – Problems Addressed & User Experience

This Use Case assumes that the Consumer is purchasing a continuous subscription service from a Merchant. After a successful payment to cover the initial subscription fee (a Cardholder-Initiated Transaction), the Cardholder authorises the Merchant to make regular payments on behalf of the Cardholder (Merchant-Initiated Transactions) to continue the subscription service, using the stored payment credential represented by a Payment Token.

8.8.2 Use Case Relationships and Functions

The relationships for this use case example are shown in Figure 8.18. For a description of the baseline relationships and their functions, refer to the models given in Section:

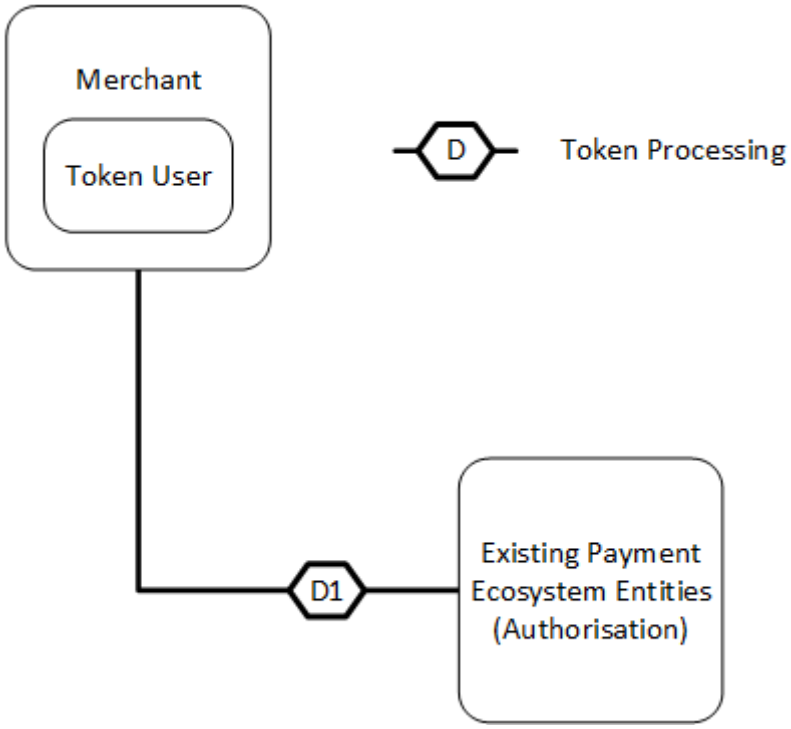
- 6.1 Token Processing Relationships and Functions

For each relationship shown in Figure 8.18, the specific nature of the relationship and its function is given in the text following the figure, along with a reference to the baseline relationship and function.

Note that this use case is transactional and it is a precondition that a Payment Token has been provisioned to the Merchant. The manner in which the Payment Token has been provisioned will depend on the initial Cardholder-Initiated Transaction. Any use case where there is a Cardholder-Initiated Transaction has the potential for subsequent Merchant-Initiated Transactions.

Furthermore, since there is no Cardholder interaction during the Merchant-Initiated Transaction, there is no Token Presentment stage. Therefore, Token Issuance, Token Provisioning and Token Presentment relationships are not shown in Figure 8.18. The Token Issuance, Token Provisioning and Token Presentment characteristics are not given in Section 8.8.3.

Figure 8.18: Merchant-Initiated Transaction – Use Case Relationships



Token Processing

D1. Merchant (Token User) – Existing Payment Ecosystem Entities

Relationship: The Merchant (Token User) utilises existing relationships to initiate Token Processing.

Function: The Merchant submits a Token Payment Request using the Payment Token and related data.

Note: This relationship does not vary by use case.

Reference: Section 6.1.1 D1. Merchant – Existing Payment Ecosystem Entities.

8.8.3 Use Case Characteristics

The use case characteristics are shown in Table 8.29.

Table 8.29: Merchant-Initiated Transaction – Token Processing Characteristics

Characteristic	Notes	Typical Outcomes
Token Payment Request	The Merchant submits the Token Payment Request to obtain a PAN authorisation.	• Merchant
Token Control Fields	Used to constrain the Payment Token to a specific Token Presentment Mode and a specific Cardholder-Initiated Transaction, as well as a specific Merchant-Initiated Transaction.	• POS Entry Mode • Token Cryptogram • Original Transaction Reference • Merchant-Initiated Transaction Identifier

8.8.4 Payment Token Characteristics

The Payment Token characteristics are shown in Table 8.30.

Table 8.30: Merchant-Initiated Transaction – Payment Token Characteristics

Characteristic	Notes	Typical Outcomes
Payment Token Usage	Same as the Payment Token Usage of the initial Cardholder-Initiated Transaction.	• Device Specific • Merchant Specific • Guest Checkout • Token User
Token Assurance Method	Same as the Token Assurance Method of the initial Cardholder-Initiated Transaction.	• Spaces / 00 • 01 – 19 • 20 – 89
Token Domain Restriction Controls	Same as the Token Domain Restriction Controls of the initial Cardholder-Initiated Transaction	• Token Presentment Mode(s) • Device • Merchant(s)

Characteristic	Notes	Typical Outcomes
Token Cryptogram	When used as a Token Domain Restriction Control, the Token Cryptogram must be unique for each Merchant-Initiated Transaction.	• Used • Not Used
Type of Transaction Initiation	The Merchant initiates a transaction following the initial Cardholder-Initiated Transaction.	• Merchant-Initiated Transaction

8.8.5 Issuance Flow

Since any use case where there is a Cardholder-Initiated Transaction has the potential for subsequent Merchant-Initiated Transactions, the flow for the Issuance of the Payment Token will follow the Issuance Flow in the corresponding use case where the initial Cardholder-Initiated Transaction took place.

8.8.6 Transaction Flow

The following preconditions and assumptions apply to this specific flow.

Transaction Flow Preconditions

- The Consumer has made a successful Cardholder-Initiated Transaction at the Merchant for the payment of the initial subscription fee
- The Consumer has authorised the Merchant to store a payment credential represented by a Payment Token in order to use it to cover future fees for the continuation of subscription service

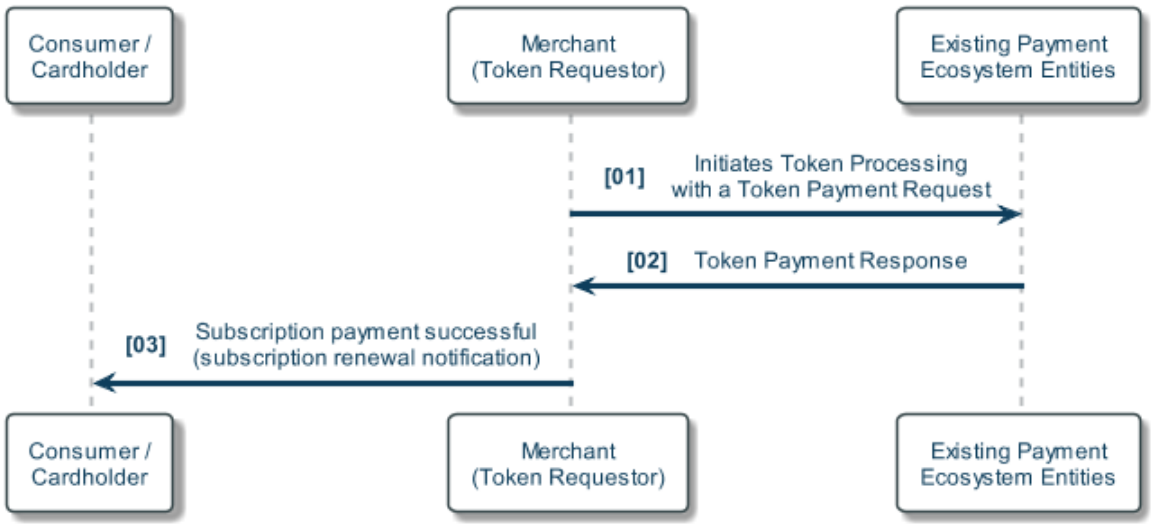
Transaction Flow Assumptions

- A Token Cryptogram is not used

Example Transaction Flow

Figure 8.19 shows an example transaction flow, with numbered steps which are explained following the figure.

Figure 8.19: Merchant-Initiated Transaction – Example Transaction Flow



01. The Merchant (Token Requestor) initiates Token Processing by sending a Token Payment Request using the Payment Token and relevant transaction information
02. The Merchant (Token Requestor) receives a Token Payment Response as a result of successful PAN Authorisation by the Card Issuer
03. The Cardholder receives confirmation from the Merchant that the subscription payment was successful and that the subscription has been renewed

Token Processing Considerations

Table 8.29 (Token Processing Characteristics) and Table 8.30 (Payment Token Characteristics) show the typical Token Control Fields (Table 8.29) which are used as part of the Token Domain Restriction Controls (Table 8.30). In this specific use case flow, the following Token Control Fields are used:

- POS Entry Mode: has a value depending on the specific Token Processing requirements for the Token Programme
- Original Transaction Reference: the value is used to refer this Merchant-Initiated Transaction to the original Cardholder-Initiated Transaction
- Merchant-Initiated Transaction Identifier: identifies this specific transaction as a Merchant-Initiated Transaction

As well as the methods described in Section 8.1.3 Payment Account Reference Data (PAR Field and PAR Enquiry), PAR Data may be available to the Merchant:

- In the PAR Field at the conclusion of Token Processing for the original Cardholder-Initiated Transaction

8.8.7 Variations of User Experience

There are not expected to be any significant variations for this use case since there is no Cardholder interaction.

9 Use Case Variations

This Section addresses potential variations to the use cases defined in Section 8 Use Case Examples. The variations are:

- Payment Tokenisation Aggregator (Section 9.1)
- Bulk Token Request (Section 9.2)
- Token Reference IDs (Section 9.3)
- Token Service Provider in the Issuer Domain (Section 9.4)

9.1 Payment Tokenisation Aggregator

Payment Tokenisation Aggregator is a category of roles within the Payment Tokenisation ecosystem as defined by the Technical Framework. The Technical Framework specifically identifies Token Requestor Aggregators and Card Issuer Aggregators without precluding other types of aggregators.

When a Payment Tokenisation Aggregator is used, the use cases described in Section 8 Use Case Examples will vary slightly. This Section describes these variations, which are potentially applicable to any use cases.

9.1.1 Token Requestor Aggregator

Merchants may outsource the technical implementation aspects of being a Token Requestor by using a Token Requestor Aggregator.

The Token Requestor Aggregator is an authorised entity, authorised within a Token Programme to integrate with a Token Service Provider to perform Payment Token related activities on behalf of one or more Merchants (Token Requestors). The Token Requestor Aggregator may also facilitate the registration of the Merchant (Token Requestor) with the Token Service Provider.

Both the Merchant (Token Requestor) and the Token Requestor Aggregator have specific relationships with the Token Service Provider which are defined within the Token Programme.

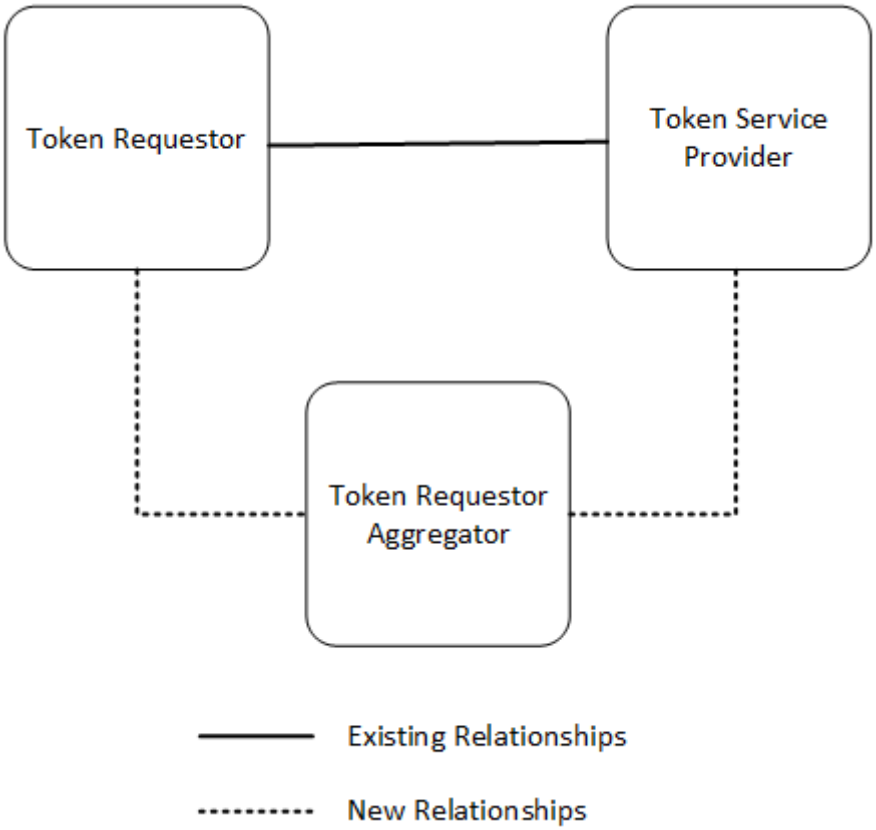
Variations of Relationships

The existing relationships that are described in each use case are essentially unchanged. There are incremental relationships between:

- Merchant (Token Requestor) and Token Requestor Aggregator
- Token Service Provider and Token Requestor Aggregator.

Figure 9.1 shows the incremental relationships involving a Token Requestor Aggregator. This can be applied to any of the relationship diagrams in Section 8 Use Case Examples.

Figure 9.1: Token Requestor Aggregator – Incremental Relationships



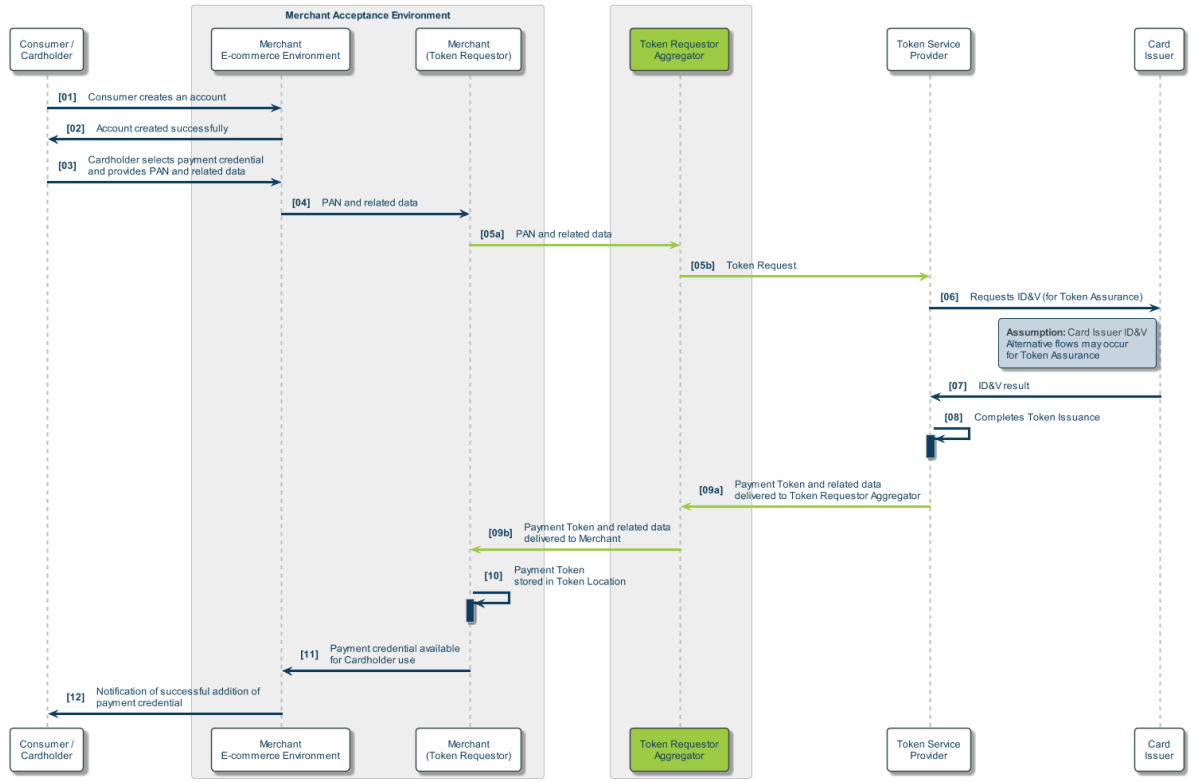
Changes to Token Issuance and Token Provisioning will vary by implementation and the services being provided by the Token Requestor Aggregator.

Variations to Issuance Flow

The Merchant (Token Requestor) still initiates the Token Request, but does so via the Token Requestor Aggregator, which performs the necessary Token Request activities on the Merchant's behalf, using the Merchant's Token Requestor ID. Following the successful completion of Token Issuance, the Token Requestor Aggregator receives the Payment Token from the Token Service Provider and delivers it to the Merchant.

Figure 9.2 illustrates this for the Card-On-File E-Commerce use case (Section 8.5, Figure 8.10), but this applies to all use cases where a Token Requestor Aggregator is used.

Figure 9.2: Token Requestor Aggregator – Example Issuance Flow



The additional actor (the Token Request Aggregator) is shown in green and enclosed in the shaded box in the flow diagram while the additional steps are shown by the green arrows. These additional steps replace the steps of the same number in Figure 8.10 (that is, steps [05a] and [05b] replace step [05], while steps [09a] and [09b] replace step [09]):

05a. The Merchant (Token Requestor) chooses not to store the PAN and related data, providing it to the Token Requestor Aggregator

05b. The Token Requestor Aggregator uses the PAN and related data to initiate a Token Request to the Token Service Provider (using the Merchant's Token Requestor ID)

…….

09a. The Token Service Provider delivers a Payment Token and related data to the Token Requestor Aggregator as part of Token Provisioning

09b. The Token Requestor Aggregator delivers the Payment Token and its related data to the Merchant (Token Requestor) as part of Token Provisioning

9.1.2 Card Issuer Aggregator

Issuers may outsource implementation of interfaces with Token Service Providers for some or all of the Payment Tokenisation activities by using a Card Issuer Aggregator.

The Card Issuer Aggregator is an authorised entity, authorised within the Token Programme to integrate with a Token Service Provider to perform Payment Token related activities on behalf of one or more Card Issuers.

Both the Card Issuer and the Card Issuer Aggregator have specific relationships with the Token Service Provider which are defined within the Token Programme.

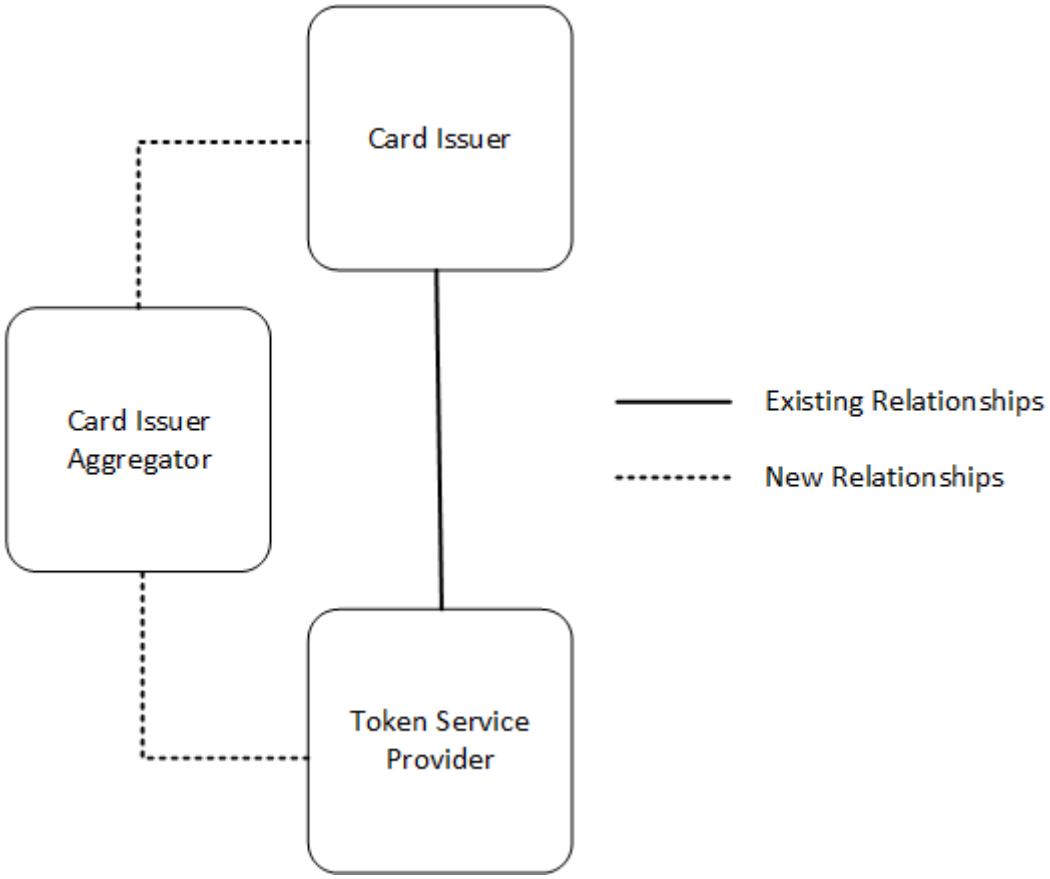
Variations of Relationships

The existing relationships that are described in each use case are essentially unchanged. There are incremental relationships between:

- Card Issuer and Card Issuer Aggregator
- Token Service Provider and Card Issuer Aggregator

Figure 9.3 shows the incremental relationships involving the Card Issuer Aggregator. This can be applied to any of the relationship diagrams in Section 8 Use Case Examples.

Figure 9.3: Card Issuer Aggregator – Incremental Relationships



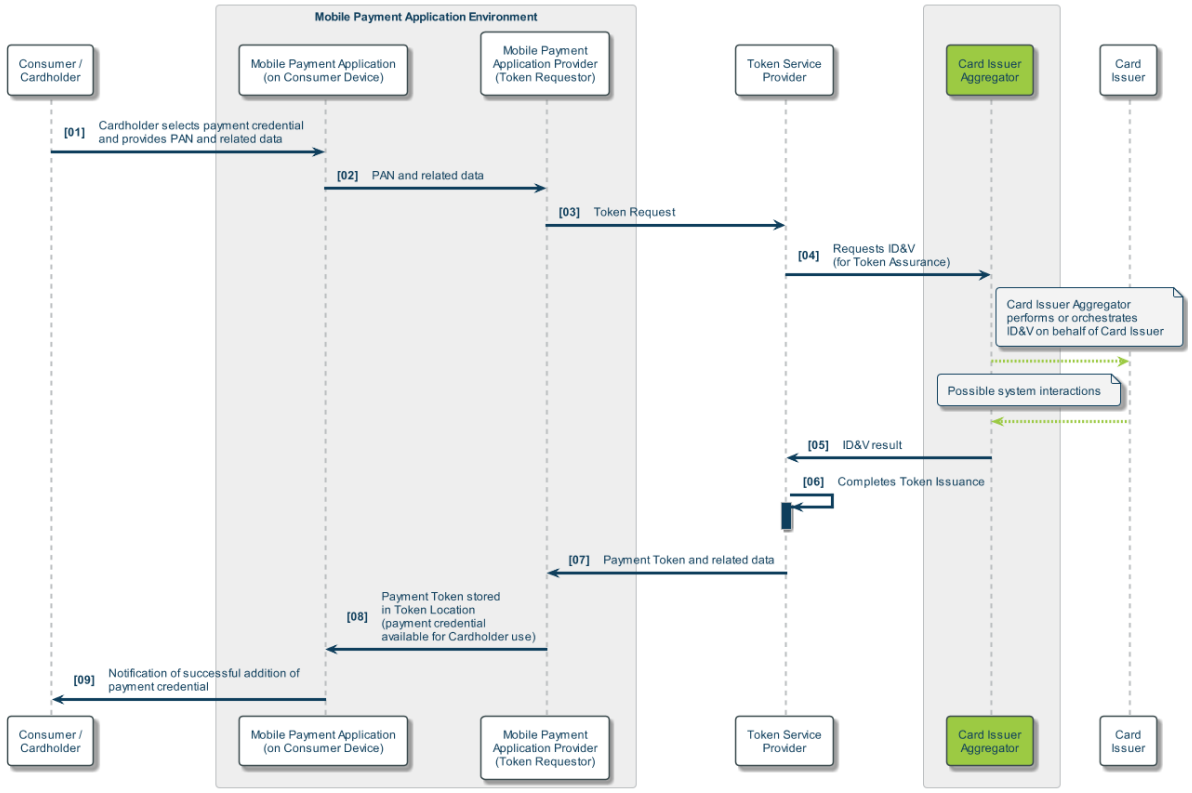
Changes to Token Issuance and Token Provisioning will vary by implementation and the services being provided by the Card Issuer Aggregator.

Variations to Issuance Flow

The Card Issuer Aggregator can either perform or orchestrate the necessary ID&V activities on behalf of the Card Issuer, delivering the ID&V response to the Token Service Provider using any necessary identifiers of the Card Issuer.

Figure 9.4 illustrates this for the Proximity at Point of Sale use case (Section 8.2). This is a single example, but applies to all use cases where a Card Issuer Aggregator is used.

Figure 9.4: Card Issuer Aggregator – Example Issuance Flow



The additional actor (the Card Issuer Aggregator) is shown in green and enclosed in the shaded box in the flow diagram. There are no additional numbered steps since if there is any interaction between the Card Issuer Aggregator and Card Issuer, it will be implementation specific. This is shown by the dotted green lines in the flow diagram.

9.2 Bulk Token Request

The Technical Framework defines a Token Request interface in which a registered Token Requestor requests a single Payment Token from the Token Service Provider. However, Token Service Providers may implement a bulk Token Request through a secure interface file where multiple Payment Tokens and Token Expiry Dates are generated and returned to the Token Requestor.

Bulk Token Requests may be used in a variety of use cases. Its usage is illustrated by a variation to the Card-On-File E-Commerce use case (Section 8.5). This use case variation assumes that a Merchant with an existing PAN-based Card-On-File database wishes to replace the PANs with Payment Tokens using Bulk Token Request(s).

Cardholders have previously provided the Merchant with details of payment credentials (PANs and related data) which the Merchant has stored. The Merchant (Token Requestor) uses the stored PANs to obtain Payment Tokens using a bulk Token Request process. The Payment Tokens are then stored by the Merchant (Token Requestor) to be used in future transactions. When a Cardholder selects a payment credential, the Merchant uses the affiliated Payment Token for Token Processing.

Based on the PANs which the Merchant has stored, requesting Payment Tokens for all eligible PANs may require participating in multiple Token Programmes and interacting with multiple Token Service Providers and multiple Card Issuers working within such Token Programmes.

This use case variation covers:

- Token Issuance and Token Provisioning (Section 9.2.5)

Since this use case variation is based on the Card-On-File E-Commerce use case (Section 8.5), both use cases have the same:

- Use Case Relationships and Functions (Section 9.2.2)
- Use Case Characteristics (Section 9.2.3)
- Payment Token Characteristics (Section 9.2.4)
- Transaction Flows (Section 9.2.6)
- Variations of User Experience (Section 9.2.7)

While bulk Token Requests are discussed and illustrated within the context of this Card-On-File E-Commerce use case, bulk Token Requests may be relevant and applicable as an enablement model within other use cases and its relevance is not limited to this use case example / variation.

9.2.1 Use Case Overview – Problems Addressed & User Experience

This use case provides the same benefits as the Card-On-File E-Commerce use case (see Section 8.5.1). In addition, the bulk Token Request process allows a Merchant (Token Requestor) to initiate a single request for a large number of PANs to be processed for Payment Tokenisation without Cardholder involvement. This enables all eligible PANs to be Tokenised, and the Merchant (Token Requestor) can initiate the process with the Token Service Provider(s) subject to any quantity/capacity constraints that may be in place to control and manage volumes on the respective participant's systems and interfaces (for example, quantity of requests in a single bulk file or number of requests in a period of time for an API approach).

9.2.2 Use Case Relationships and Functions

The relationships are the same as the Card-On-File E-Commerce use case (see Section 8.5.2).

9.2.3 Use Case Characteristics

The Use Case Characteristics are the same as the Card-On-File E-Commerce use case (see Section 8.5.3).

9.2.4 Payment Token Characteristics

The Payment Token Characteristics are the same as the Card-On-File E-Commerce use case (Section 8.5.4).

9.2.5 Issuance Flow

The bulk Token Request process has a different issuance flow, which is illustrated by the following example flow.

The following preconditions and assumptions apply to this specific flow.

Issuance Flow Preconditions

- The Merchant (Token Requestor) has registered with one or more Token Service Providers and has received a Token Requestor ID from each
- Each Token Service Provider supports bulk Token Request functionality
- The Merchant has stored PANs provided by Cardholders in prior interactions

Issuance Flow Assumptions

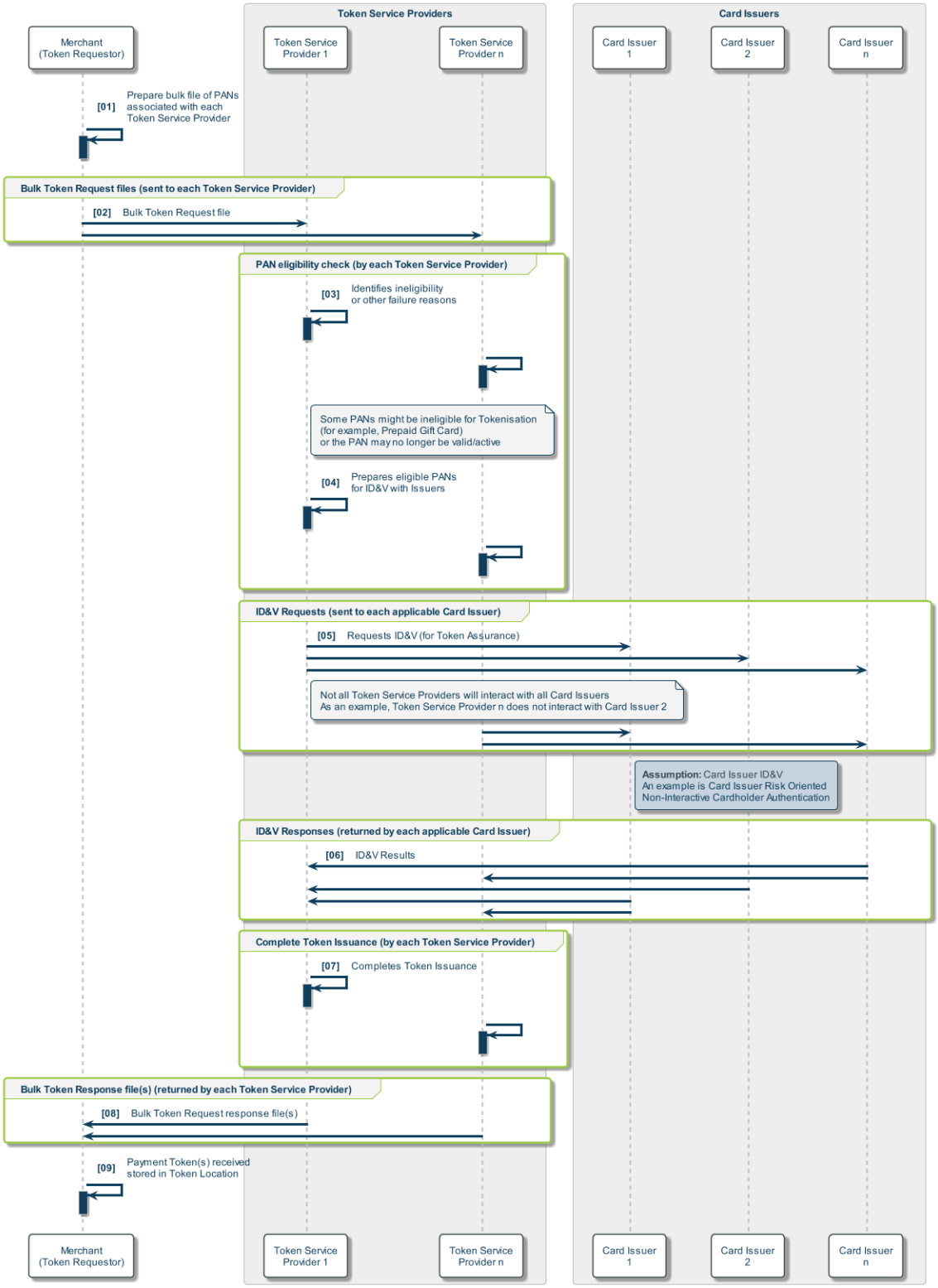
- There is no Consumer / Cardholder interaction since the Merchant (Token Requestor) already has the PAN(s) stored for the Cardholder
- The Bulk Token Request is initiated by the Merchant (Token Requestor) and uses a separate file / bulk file method to transfer data to and to receive responses from each Token Service Provider
- Each Token Service Provider has capacity management processes on the Merchant (Token Requestor) / Token Service Provider interface and on the Token Service Provider / Card Issuer interface
- Each Token Service Provider will review the PANs in the Bulk Token Request to determine which are eligible for Tokenisation
- Not all Card Issuers will be interacting with all Token Service Providers. This has been illustrated in the second example flow by Token Service Provider n not having any Token Requests related to Card Issuer 2. This could be the case for any number of Card Issuers

- Token Assurance and the related ID&V is performed by the Card Issuer resulting in the Token Assurance Method value being set to one of the Card Issuer Token Assurance Method Categories
- Although a specific flow is shown, the exact order and sequence of the steps will vary by implementation and Token Programme policies and processes, so does not dictate the sequence of all steps in the flow
- The designated Token Location is 01 Remote storage

Example Issuance Flow

Figure 9.5 shows an example issuance flow, with numbered steps which are explained following the figure. Note that where steps are repeated across multiple entities, these are not individually numbered.

Figure 9.5: Bulk Token Request – Example Issuance Flow



01. The Merchant (Token Requestor) creates a file of the PANs and related data associated with each Token Service Provider to be sent in the Bulk Token Request

02. The Merchant (Token Requestor) initiates the Bulk Token Request to each Token Service Provider for the PANs and related data associated with that Token Service Provider
03. Each Token Service Provider identifies any PANs that are ineligible for Tokenisation and remove them from further Bulk Token Request processing
04. Each Token Service Provider prepares all eligible PANs and related data to allow the ID&V process to proceed with the respective Card Issuers
05. Each Token Service Provider requests ID&V for each PAN to the appropriate Card Issuer in accordance with the appropriate Token Programme.
06. Card Issuers return the ID&V result(s) to the Token Service Provider
07. Each Token Service Provider completes the Issuance of the Payment Tokens
08. Each Token Service Provider returns one or more files to the Merchant (Token Requestor). These contain Payment Token(s) and related data for PANs which were successfully Tokenised and failure responses and reason codes for PANs that were unable to be Tokenised
09. The Merchant (Token Requestor) receives the Payment Tokens and related data in the Bulk Token Request response file from each Token Service Provider and stores them in the Token Location. Management of PANs that failed Tokenisation are out of the scope of the Technical Framework

Since each PAN will be unique to a Card Issuer, there are no interactions between Token Service Provider n and Card Issuer 2 in Figure 9.5. This illustrates that the Merchant may not have PANs from all Card Issuers supported by a Token Service Provider and demonstrates the potential mixture of PANs which the Merchant has stored.

9.2.6 Transaction Flow

The transaction flow is the same as for the Card-On-File E-Commerce use case (see Section 8.5.6).

9.2.7 Variations of User Experience

The variations of user experience are the same as for the Card-On-File E-Commerce use case (Section 8.5.7).

9.3 Token Reference IDs

The Technical Framework defines a Token Reference ID as a substitute for the Payment Token that does not expose information about the Payment Token or the underlying PAN. It allows an entity to store the Token Reference ID and to use it when needed to identify the Payment Token with which the Token Reference ID is affiliated.

Token Reference IDs may be used in a variety of use cases. Its usage is illustrated by a variation to the Third Party Service Provider use case (Section 8.7) This use case variation assumes that:

- A Merchant (Token User) is provided with a Token Reference ID instead of a Payment Token during Token Provisioning, which is then used during Token Presentment to identify the Payment Token to be used during Token Processing
- The Third Party Service Provider (Token Requestor) generates the Token Payment Request on behalf of the Merchant (Token User), using the Payment Token with which the Token Reference ID is affiliated

Note that the variation where the Third Party Service Provider (Token Requestor) generates the Token Payment Request can also occur when a Payment Token is being used and is not exclusive to the Token Reference ID use case variation.

This use case variation covers:

- Token Issuance and Token Provisioning
- Token Presentment and Token Processing

9.3.1 Use Case Overview – Problems Addressed & User Experience

This use case variation provides the same benefits as the Third Party Service Provider use case (Section 8.7.1). In addition, by receiving and storing a Token Reference ID rather than a Payment Token, the Merchant (Token User) has the following benefits:

- Minimise systems impacts by potentially re-using existing interfaces and processes with the Third Party Service Provider to store only references to payment credentials
- Minimise systems impacts if alternative tokenisation solutions are already in place in the Token User's environments or between the Third Party Service Provider and the Token User
- By not storing the Payment Token, the Token User's environment(s) will not contain values that might resemble a PAN even if they are in fact Payment Tokens, as part of overall PCI scope management and reduction efforts

By using the Third Party Service Provider (Token Requestor) to initiate Token Payment Requests, the Merchant (Token User) has the following benefits:

- Where a Token User currently uses a Third Party Service Provider for PAN Authorisation services and the Token User stores a reference ID for a payment credential, Token User processes can remain unchanged
- Where additional steps are required to use a Payment Token, such as a Token Cryptogram, these can be managed by the Third Party Service Provider

The Consumer experience is unchanged.

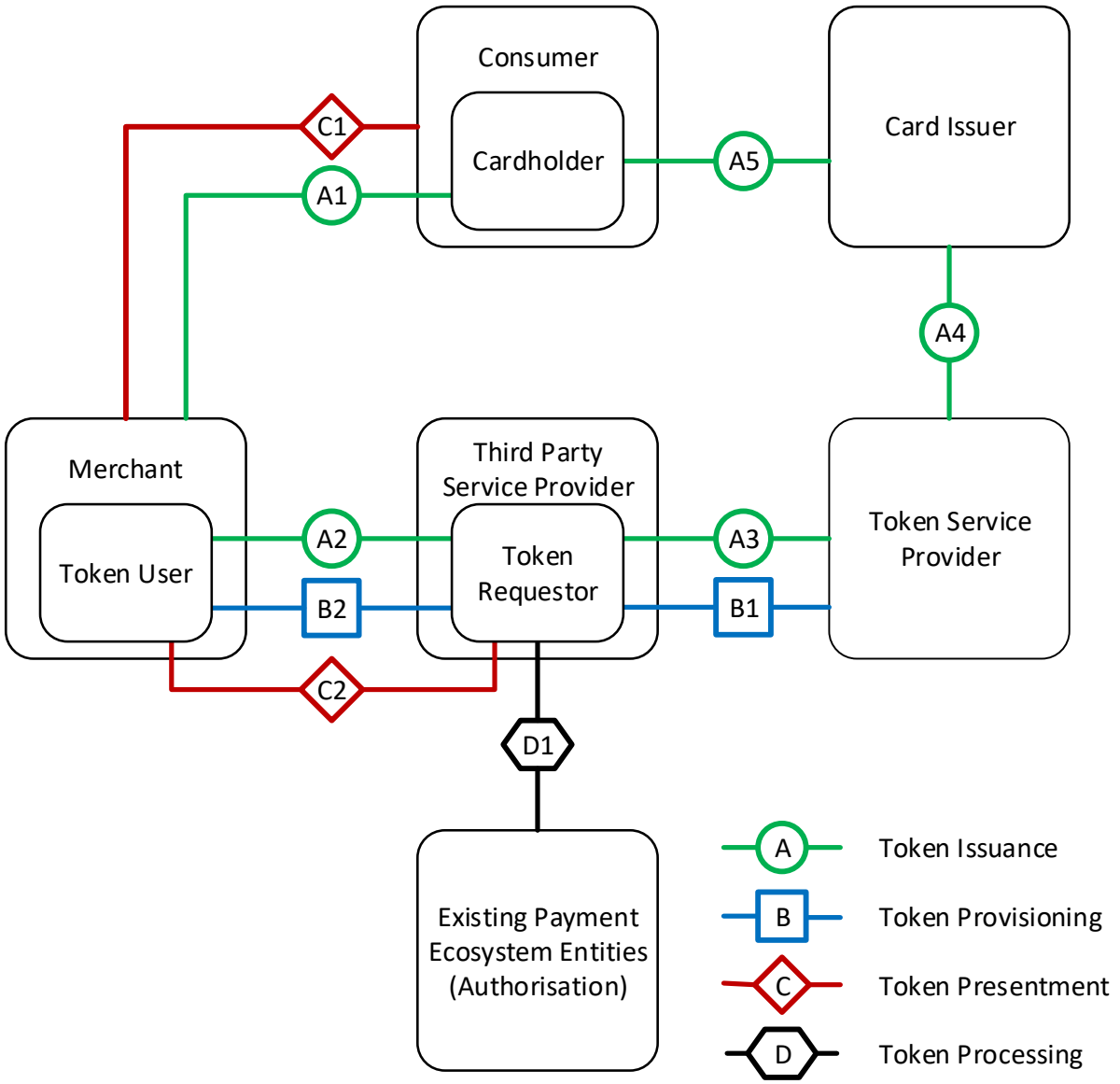
9.3.2 Use Case Relationships and Functions

For this use case variation, the Third Party Service Provider is performing the role of the authorised entity described in Sections 4.1, 5.1 and 6.1. The relationships shown in Figure 9.6 are the same as the Third Party Service Provider use case (see Section 8.7.2), except that:

- The function of the Token Presentment relationship (C2) reflects the Merchant (Token User) receiving a Token Reference ID rather than a Payment Token
- The Token Processing relationship between the Merchant (Token User) and the Existing Payment Ecosystem Entities has been replaced with a Token Processing relationship (D1) between the Third Party Service Provider (Token Requestor) and the Existing Payment Ecosystem Entities

For these two relationships, the specific nature of the relationship and its function is given in the text following the figure, along with a reference to the baseline relationship and function.

Figure 9.6: Token Reference IDs – Use Case Relationships



Token Presentment

C2 Merchant (Token User) – Third Party Service Provider (Token Requestor)

Relationship: The Merchant (Token User) has an existing relationship with the Third Party Service Provider (Token Requestor) to provide Payment Tokenisation services.

Function: The Merchant (Token User) has previously been supplied with the Token Reference ID by the Third Party Service Provider (Token Requestor) during Token Provisioning (see B2). The Merchant (Token User) provides the Token Reference ID to the Third Party Service Provider (Token Requestor) to identify the Payment Token to be used in Token Processing.

Reference: Section 5.1.3 C3. Merchant (Token User) – Authorised Entity (Token Requestor).

Token Processing

D1. Third Party Service Provider (Token Requestor) – Existing Payment Ecosystem Entities

Relationship: The Third Party Service Provider (Token Requestor) utilises existing relationships to initiate Token Processing on behalf of the Merchant (Token User).

Function: The Third Party Service Provider (Token Requestor) submits a Token Payment Request using the Payment Token and related data, retrieved using the Token Reference ID provided by the Merchant (Token User) during Token Presentment (see C2).

Reference: Section 6.1.2 D2. Authorised Entity (Token Requestor) – Existing Payment Ecosystem Entities.

9.3.3 Use Case Characteristics

The use case characteristics are the same as the Third Party Service Provider use case (Section 8.7.3) with the following exceptions, which are shown in Table 9.1 and Table 9.2.

Table 9.1: Token Reference IDs – Token Presentment Characteristics

Characteristic	Notes	Typical Outcomes
Token Presentment	The Merchant (Token User) presents the Token Reference ID to the Third Party Service Provider (Token Requestor).	• Non-proximity

Table 9.2: Token Reference IDs – Token Processing Characteristics

Characteristic	Notes	Typical Outcomes
Token Payment Request	The Third Party Service Provider (Token Requestor) submits the Token Payment Request to obtain a PAN authorisation.	• Third Party Service Provider

9.3.4 Payment Token Characteristics

The Payment Token Characteristics are the same as the Third Party Service Provider use case (Section 8.7.4).

9.3.5 Issuance Flow

The issuance flow is the same as the Third Party Service Provider use case (Section 8.7.5) with minor variations related to the use of the Token Reference ID. Where variations occur, they are identified in the specific numbered steps, which are shown after the diagram.

The following preconditions and assumptions apply to this specific flow in addition to those that apply to the Third Party Service Provider use case (Section 8.7.5).

Issuance Flow Preconditions

There are no additional preconditions that apply to this specific flow.

Issuance Flow Assumptions

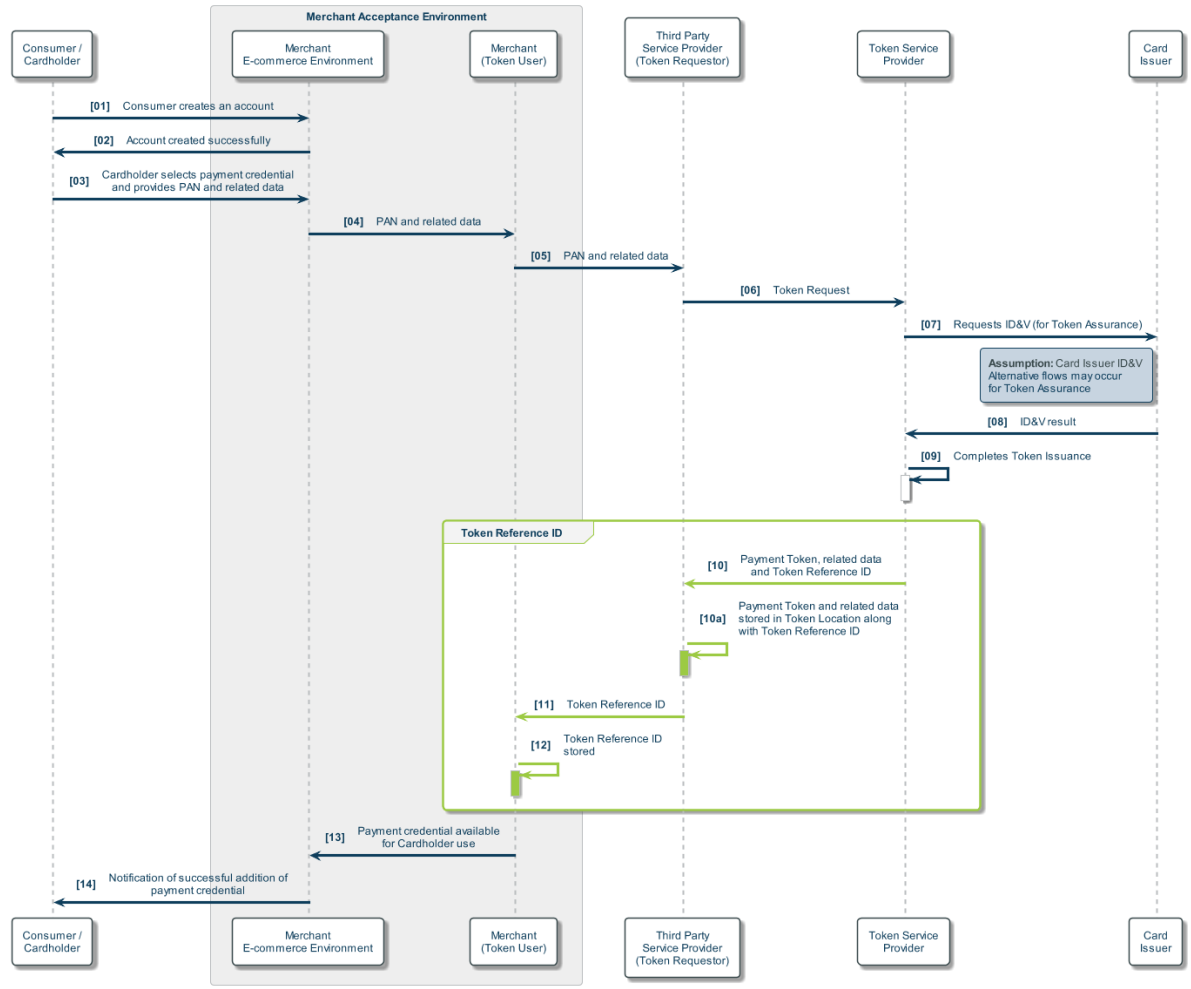
- The Token Service Provider creates the Token Reference ID and delivers it to the Third Party Service Provider (Token Requester) along with the Payment Token and its related data as part of Token Provisioning

There are no additional assumptions that apply to this specific flow.

Example Issuance Flow

Figure 9.7 shows an example issuance flow. The numbered steps which differ from the example issuance flow in the Third Party Service Provider use case (Section 8.7.5) are shown in green and highlighted in the box marked “Token Reference ID”. Only these steps are explained in the text following the figure.

Figure 9.7: Token Reference IDs – Example Issuance Flow



10. In addition to a Payment Token and its related data, the Token Service Provider delivers a Token Reference ID to the Third Party Service Provider (Token Requestor) as part of Token Provisioning

10a. The Third Party Service Provider (Token Requestor) stores the Payment Token and related data in the Token Location as well as storing the Token Reference ID

11. The Third Party Service Provider delivers the Token Reference ID to the Merchant (Token User)

12. The Merchant (Token User) stores the Token Reference ID to complete Token Provisioning

9.3.6 Transaction Flow

The following preconditions and assumptions apply to this specific flow.

Transaction Flow Preconditions

- The Token Reference ID stored by the Merchant (Token User) is affiliated with a Payment Token, stored by the Third Party Service Provider

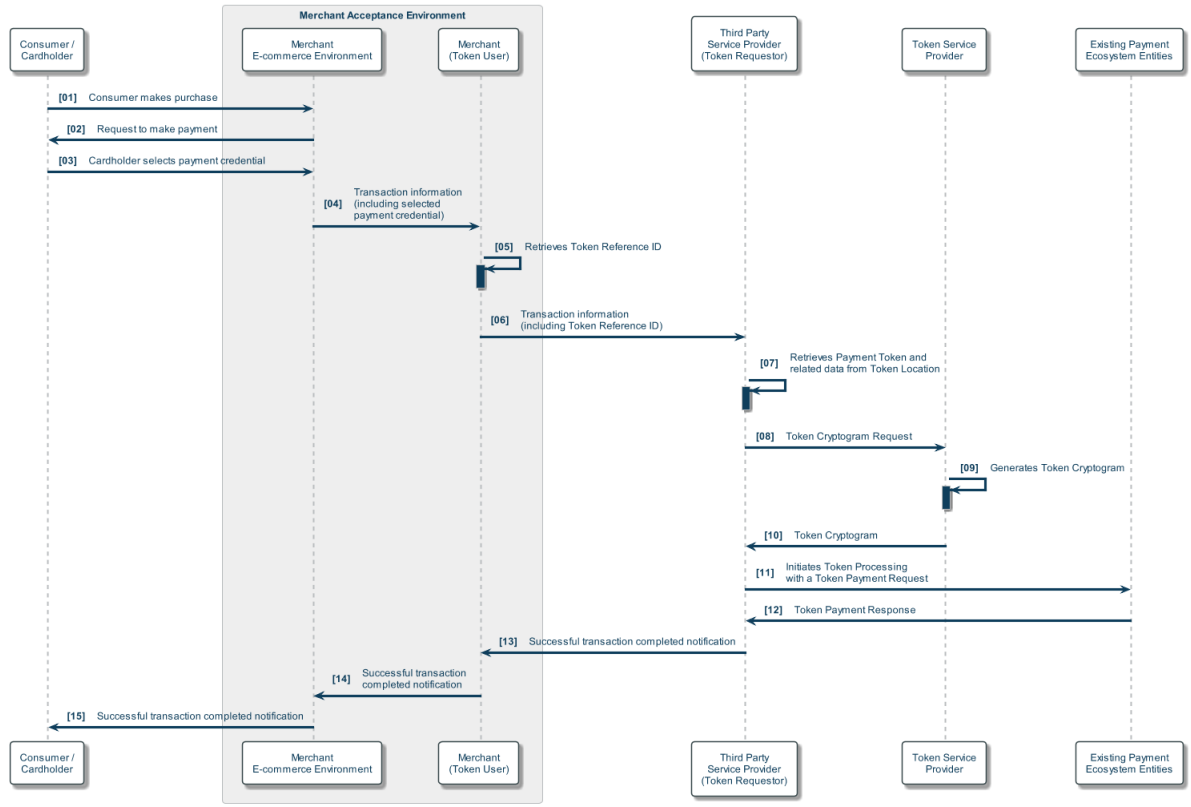
Transaction Flow Assumptions

- The Consumer has accessed the account via the Merchant e-commerce environment
- The Token Reference ID stored by the Merchant (Token User) is identified by the Last 4 Digits of PAN and digital card art
- The Consumer selects a payment credential stored in the account that is affiliated with a stored Token Reference ID
- The Merchant (Token User) presents the Token Reference ID and related data to the Third Party Service Provider as part of Token Presentment
- The Third Party Service Provider uses the Token Reference ID to retrieve the Payment Token
- The Token Service Provider generates a Token Cryptogram, which is sourced by the Third Party Service Provider
- The Third Party Service Provider initiates Token Processing using the Payment Token (along with the provided Token Cryptogram and other related data) via existing relationships with the existing Payment Ecosystem Entities

Example Transaction Flow

Figure 9.8 shows an example transaction flow, with numbered steps which are explained following the figure.

Figure 9.8: Token Reference IDs – Example Transaction Flow



01. The Consumer makes a purchase from the Merchant e-commerce environment and initiates the checkout process
02. The Merchant e-commerce environment initiates the request for a payment credential to be selected
03. The Cardholder selects a previously stored payment credential from the account via the Merchant e-commerce environment
04. The Merchant e-commerce environment provides transaction information, including the selected payment credential, to the Merchant
05. The Merchant (Token User) retrieves the Token Reference ID
06. The Merchant (Token User) provides the relevant transaction information, including the Token Reference ID to the Third Party Service Provider (Token Requestor)
07. The Third Party Service Provider (Token Requestor) uses the Token Reference ID to retrieve the Payment Token and related data from the Token Location
08. The Third Party Service Provider (Token Requestor) uses the information received from the Merchant (Token User) and the retrieved Payment Token to initiate a Token Cryptogram Request to the Token Service Provider

09. The Token Service Provider processes the Token Cryptogram Request and generates a Token Cryptogram
10. The Third Party Service Provider (Token Requestor) receives the Token Cryptogram from the Token Service Provider
11. The Third Party Service Provider initiates Token Processing by sending a Token Payment Request
12. The Third Party Service Provider receives a Token Payment Response as a result of successful PAN Authorisation by the Card Issuer
13. The Third Party Service Provider provides the results to the Merchant (Token User)
14. The Merchant provides the results to the Merchant e-commerce environment
15. The Cardholder receives confirmation from the Merchant e-commerce environment that the transaction was successful

Token Processing Considerations

The Token Processing considerations are the same as the Third Party Service Provider use case (Section 8.8.6).

9.3.7 Variations of User Experience

The variations of user experience are the same as for the Third Party Service Provider use case (Section 8.7.7).

9.4 Token Service Provider in the Issuer Domain

The Technical Framework supports a variety of implementation models and does not place any restrictions on the entities that may perform the Payment Tokenisation specific roles. The role of the Token Service Provider can be performed by any appropriate entity that meets the requirements of the Token Programme and follows the requirements defined within the Technical Framework.

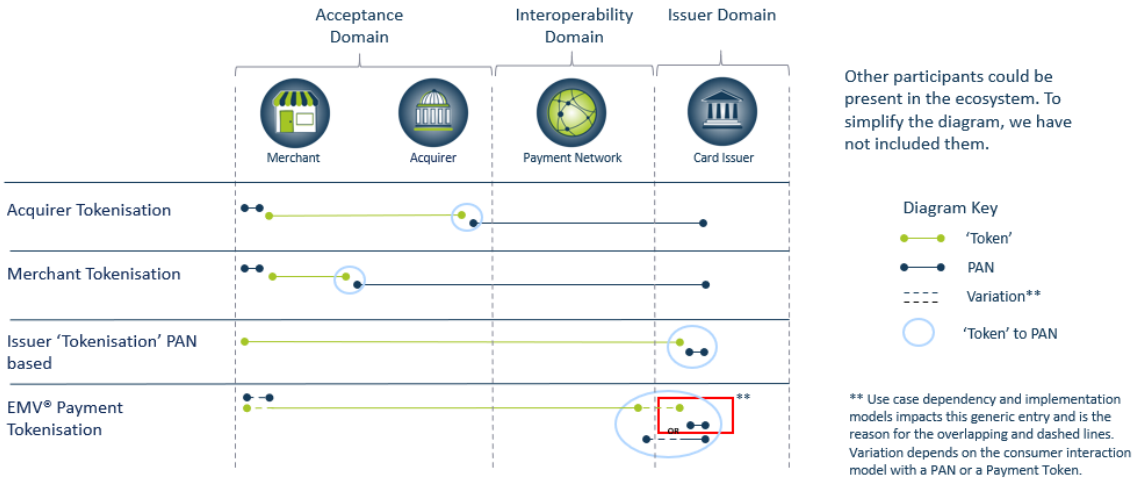
Whilst each Token Programme must have at least one Token Service Provider, multiple Token Service Providers within a Token Programme are fully supported (see Figure 2.3 in Section 2.2 Token Service Providers).

This use case variation applies to a variety of use cases. Its usage is illustrated by a variation to the Card-On-File E-Commerce use case (Section 8.5). This use case variation provides more detailed Issuance and Transaction Flows that may occur when the role of the Token Service Provider is performed in the issuer domain. This will be an implementation decision.

Figure 9.9 explains how Payment Tokens differ from other forms of tokenisation and highlights the potential for the De-Tokenisation of the Payment Token to the underlying PAN to occur in

the issuer domain, which is shown by the red box. This may have a dependency on the use case and the implementation models defined within the Token Programme. For additional detail, please refer to the EMV® Payment Tokenisation FAQs.

Figure 9.9: Tokenisation Domains



This variation uses the example of a Card Issuer which either performs the Token Service Provider role itself or has outsourced the Token Service Provider function to a Third Party Service Provider.

This use case variation covers:

- Token Issuance and Token Provisioning (Section 9.4.5)
- Transaction Flows (Section 9.4.6)

Since this use case variation is based on the Card-On-File E-Commerce use case (Section 8.5), both use cases have the same:

- Use Case Relationships and Functions (Section 9.4.2)
- Use Case Characteristics (Section 9.4.3)
- Payment Token Characteristics (Section 9.4.4)
- Variations of User Experience (Section 9.4.7)

9.4.1 Use Case Overview – Problems Addressed & User Experience

This use case provides the same benefits as the Card-On-File E-Commerce use case (see Section 8.5.1) with the same user experience.

9.4.2 Use Case Relationships and Functions

The relationships are the same as the Card-On-File E-Commerce use case (see Section 8.5.2.)

9.4.3 Use Case Characteristics

The Use Case Characteristics are the same as the Card-On-File E-Commerce use case (see Section 8.5.3).

9.4.4 Payment Token Characteristics

The Payment Token Characteristics are the same as the Card-On-File E-Commerce use case (Section 8.5.4).

9.4.5 Issuance Flow

The issuance flow is the same as the Card-On-File E-Commerce use case (see Section 8.4.5) with additional detail related to the this use case variation.

The following preconditions and assumption apply to this specific flow in addition to those that apply to the Card-On-File E-Commerce use case (see Section 8.4.5).

Issuance Flow Preconditions

- The Token Programme policies and processes support this implementation approach

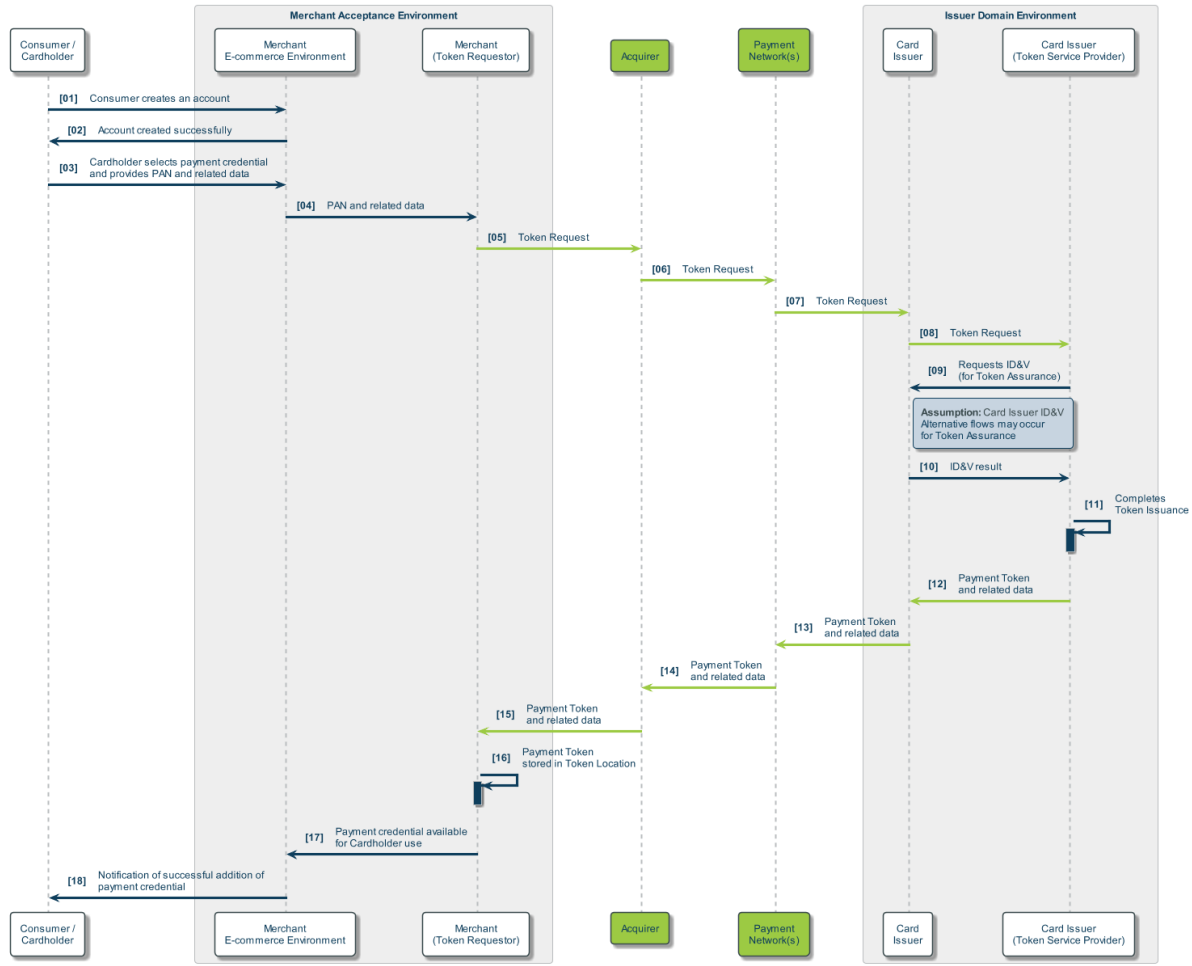
Issuance Flow Assumptions

- The Token Request uses existing authorisation interfaces that have been repurposed for use as a Token Request and include the appropriate indicator to reflect this
- The Card Issuer is performing the role of Token Service Provider using an in-house capability

Example Issuance Flow

Figure 9.10 shows an example issuance flow, with numbered steps which are explained following the figure. The actors and steps shown in green in the flow diagram have been explicitly included in this use case variation. Note that where steps are repeated across multiple entities, these are not individually numbered.

Figure 9.10: Token Service Provider in the Issuer Domain – Example Issuance Flow



01. The Consumer creates an account with the Merchant via its e-commerce environment
02. The Merchant e-commerce environment confirms that the account has been created
03. The Cardholder selects a payment credential to be added to the account and provides the PAN and related data as required by the Merchant e-commerce environment
04. The Merchant e-commerce environment provides the PAN and related data to the Merchant
05. The Merchant (Token Requestor) chooses not to store the PAN and related data and uses it to initiate a Token Request to the Token Service Provider (using its Token Requestor ID). This Token Request is routed, via an Acquirer, over an existing authorisation interface which supports Token Requests for the relevant Token Programme and Token Service Provider
06. The Acquirer routes the Token Request to a Payment Network that can support this request and pass it to the Card Issuer
07. The Payment Network routes the Token Request to the Card Issuer

08. The Card Issuer routes the Token Request to its internal Token Service Provider systems
09. The Card Issuer's Token Service Provider systems carries out Token Assurance and requests the Card Issuer systems undertakes ID&V
10. The Card Issuer systems respond to the Card Issuer's Token Service Provider systems with the ID&V result
11. The Card Issuer's Token Service Provider systems completes Token Issuance (this is on the assumption that the ID&V result indicates Card Issuer approval)
12. The Card Issuer's Token Service Provider systems delivers a Payment Token and its related data to the Card Issuer systems
13. The Card Issuer returns the Payment Token and its related data to the Payment Network using the appropriate response message
14. The Payment Network routes the Token Request response message from the Card Issuer (which contains a Payment Token and its related data) to the Acquirer
15. The Acquirer returns the response to the Merchant (Token Requestor)
16. The Payment Token and related data is stored in the designated Token Location by the Merchant (Token Requestor) to complete Token Provisioning
17. The Merchant notifies the Merchant e-commerce environment that the payment credential is now available for the Cardholder's future use
18. The Cardholder is notified of the successful addition of the payment credential by the Merchant e-commerce environment. The Cardholder may not be aware of the Tokenisation process

9.4.6 Transaction Flow

The transaction flow is the same as the Card-On-File E-Commerce use case (see Section 8.4.6) with additional detail related to the this use case variation.

The following preconditions and assumption apply to this specific flow in addition to those that apply to the Card-On-File E-Commerce use case (see Section 8.4.6).

Transaction Flow Preconditions

- The Token Programme policies and processes support this implementation approach

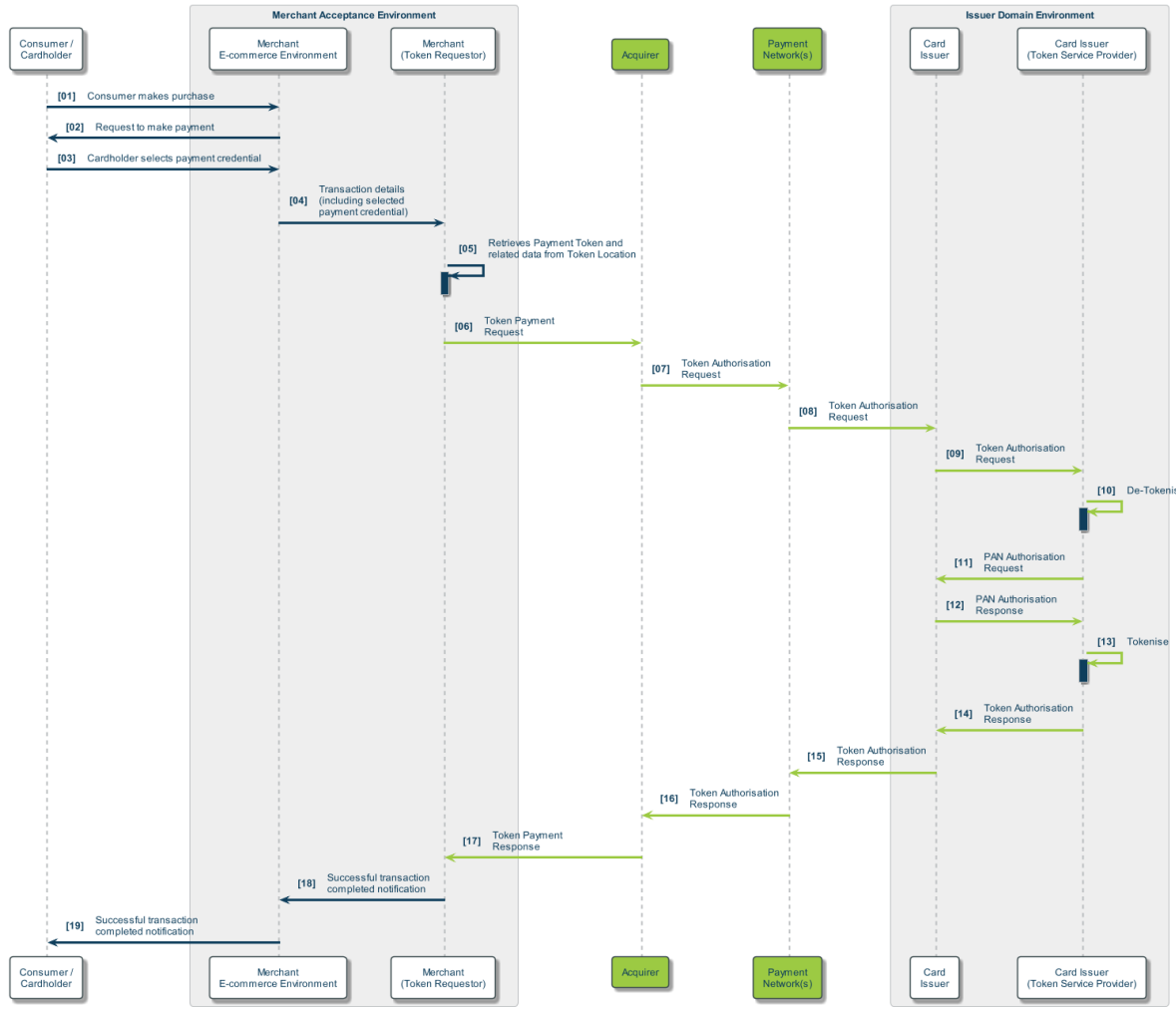
Transaction Flow Assumptions

- The Card Issuer is performing the role of Token Service Provider using an in-house capability
- The Token Service Provider applies Token Domain Restriction Controls and these pass successfully to facilitate the PAN authorisation being sent to the Card Issuer

Example Transaction Flow

Figure 9.11 shows an example transaction flow, with numbered steps which are explained following the figure. The actors and steps shown in green in the flow diagram have been explicitly included in this use case variation. Note that where steps are repeated across multiple entities, these are not individually numbered.

Figure 9.11: Token Service Provider in the Issuer Domain – Example Transaction Flow



01. The Consumer makes a purchase from the Merchant e-commerce environment and initiates the checkout process
02. The Merchant e-commerce environment initiates the request for a payment credential to be selected
03. The Cardholder selects a previously stored payment credential from the account via the Merchant e-commerce environment
04. The Merchant e-commerce environment provides details of the transaction, including the selected payment credential, to the Merchant

05. The Merchant (Token Requestor) retrieves the Payment Token and related data from the Token Location
06. The Merchant initiates Token Processing by sending a Token Payment Request to the Acquirer
07. The Acquirer routes the Token Authorisation Request to an appropriate Payment Network
08. The Payment Network uses appropriate routing information to send the Token Authorisation Request to the Card Issuer
09. The Card Issuer identifies the message as a Token Authorisation Request that requires De-Tokenisation and routes the Token Authorisation Request to its internal Token Service Provider systems
10. The Card Issuer's Token Service Provider systems perform De-Tokenisation and applies the Token Domain Restriction Controls
11. The Card Issuer's Token Service Provider systems sends the PAN Authorisation to the Card Issuer's systems
12. The Card Issuer's systems process the PAN Authorisation and returns a PAN Authorisation Response to the Card Issuer's Token Service Provider systems
13. The Card Issuer's Token Service Provider systems replaces the PAN in the PAN Authorisation Response with the original Payment Token and generates the Token Authorisation Response
14. The Card Issuer's Token Service Provider systems returns the Token Authorisation Response to the Card Issuer's systems
15. The Card Issuer returns the Token Authorisation Response to the Payment Network
16. The Payment Network routes the Token Authorisation Response to the Acquirer
17. The Acquirer returns the Token Authorisation Response to the Merchant and the Merchant receives a Token Authorisation Response as a result of successful PAN Authorisation by the Card Issuer
18. The Merchant provides the results to the Merchant e-commerce environment
19. The Cardholder receives confirmation from the Merchant e-commerce environment that the transaction was successful

Token Processing Considerations

The Token Processing considerations are the same as the Card-On-File E-Commerce use case (Section 8.4.6).

9.4.7 Variations of User Experience

The variations of user experience are the same as for the Card-On-File E-Commerce use case (Section 8.5.7).

10 Payment Tokenisation Lifecycle Management

The creation of a Payment Token and its affiliation with an underlying PAN results in a need for ongoing lifecycle management which is crucial to ensuring the integrity and security of Payment Tokens. Lifecycle management events either:

- Impact the affiliation of the Payment Token to the underlying PAN (PAN lifecycle management events)
- Affect the function of the Payment Token (Payment Token lifecycle management events)

Each Token Programme has policies and processes relating to the maintenance of the Token Vault for managing the implications of PAN and Payment Token lifecycle management events.

This Section describes the following lifecycle management use case examples:

- Merchant Deletion of Payment Credential (Section 10.5)
- Lost / Stolen Consumer Device (Section 10.6)
- PAN Replacement (Section 10.7)

10.1 PAN Lifecycle Management Events

Card Issuers continue to manage PAN lifecycle management events. When there is an affiliated Payment Token, the Card Issuer interacts with the Token Service Provider to ensure accurate content in the Token Vault. Triggering of the event may be as the result of actions by the Cardholder (e.g. reporting a PAN lost or stolen) or by the Card Issuer (e.g. renewal of the PAN on expiry). These events may result in the issuance of a new PAN and PAN Expiry Date or other changes which are needed for maintenance and accuracy in the Token Vault.

Card Issuer Aggregators performing Payment Token related activities may include support for PAN lifecycle management events on behalf of the Card Issuer.

PAN lifecycle management events include, but are not limited to changes:

- To the PAN, e.g. lost, stolen or no longer valid
- To the PAN Expiry Date, e.g. renewal
- To the status of the Payment Account with the Card Issuer represented by the PAN e.g. authorisation prohibited, delinquency, fraud alert on PAN
- Associated with PAR data

10.2 Payment Token Lifecycle Management Events

Payment Token lifecycle management events occur between either Token Service Providers and Token Requestors or Token Service Providers and Card Issuers and in both scenarios can be initiated by either entity.

Token Requestor Aggregators performing Payment Token related activities may include support for Payment Token lifecycle management events on behalf of the Token Requestor.

Card Issuer Aggregators performing Payment Token related activities may include support for Payment Token lifecycle management events on behalf of the Card Issuer.

Payment Token lifecycle management events include, but are not limited to:

- Activate Payment Token
- Suspend Payment Token
- Unlink Payment Token
- Update Payment Token Attributes

10.3 Lifecycle Management Relationships

The introduction of Payment Tokenisation into an existing payment ecosystem requires consideration of lifecycle management usage scenarios. Within each Token Programme, many functions may be common across the lifecycle management usage scenarios as they are achieving similar objectives. These common lifecycle management functions are associated with processes that are grouped as follows:

- PAN lifecycle
- Payment Token lifecycle

Each process is comprised of functions performed in lifecycle management usage scenarios that may be applied as guidelines for the lifecycle management use case examples (for a definition of usage scenarios and use cases, see Section 1.6.2 Terminology and Conventions).

The Technical Framework identifies a number of roles within the Payment Tokenisation ecosystem that carry out these functions and processes. These are the same roles that are identified in Section 3.1 Relationship Model Diagram and the relationships between them are essentially unchanged for lifecycle management.

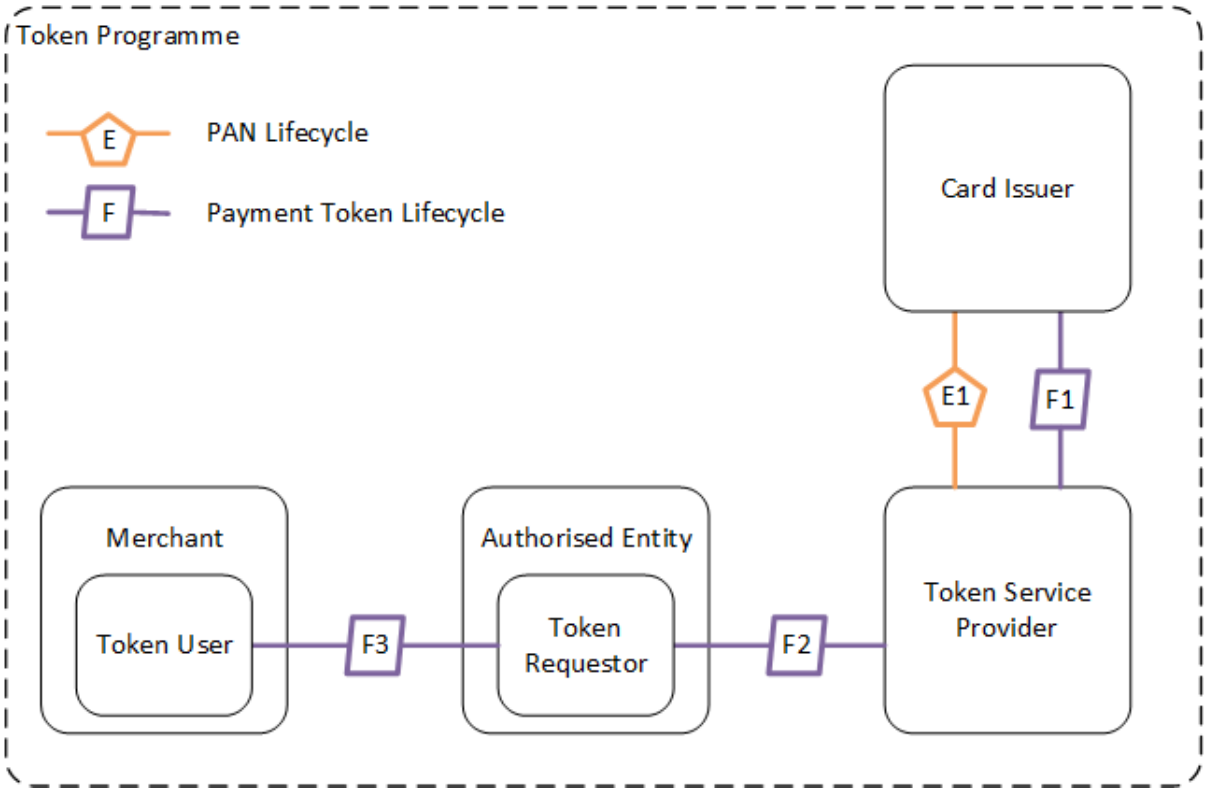
10.3.1 Lifecycle Relationship Model Diagram

Figure 10.1 displays all lifecycle management relationship models in a single diagram (for a definition of relationship model, see Section 1.6.2 Terminology and Conventions). These represent the various processes, showing the potential placement of the various Payment

Tokenisation roles within the Payment Tokenisation ecosystem. This diagram represents a common configuration for Payment Tokenisation roles and their relationships by identifying the roles as boxes and relationships as lines.

Note that the relationships in the figure do not imply flows between the entities shown and the numbers do not represent any specific order. Not all roles, relationships and processes may be present in any given lifecycle management usage scenario or lifecycle management use case example.

Figure 10.1: Lifecycle Management Relationship Models



This diagram establishes a baseline representation which is the basis for the more detailed relationship model diagrams introduced in the following sections:

- Section 10.3.2 PAN Lifecycle Relationships and Functions
- Section 10.3.3 Payment Token Lifecycle Relationships and Functions

Note that the relationships do not vary by lifecycle management use case (although they are not necessarily present in all lifecycle management use cases). However, when a relationship is present, the functions may vary or may not apply, which is noted in the individual lifecycle management use cases.

10.3.2 PAN Lifecycle Relationships and Functions

E1. Card Issuer – Token Service Provider

Relationship: The Card Issuer has a relationship with the Token Service Provider to provide Payment Tokenisation services which is used for PAN lifecycle management.

Function: The Token Service Provider uses PAN lifecycle management updates provided by the Card Issuer to maintain the PAN and affiliated Payment Token information and all related data in the Token Vault.

10.3.3 Payment Token Lifecycle Relationships and Functions

F1. Card Issuer – Token Service Provider

Relationship: The Card Issuer has a relationship with the Token Service Provider to provide Payment Tokenisation services which is used for Payment Token lifecycle management.

Function: The Card Issuer provides the Token Service Provider with Payment Token lifecycle management updates that impact the Payment Token and / or Payment Token related data enabling maintenance of the Token Vault.

Function: The Token Service Provider provides the Card Issuer with Payment Token lifecycle management notifications performed as part of maintenance of the Token Vault to ensure that the Card Issuer has current information available for all affiliated Payment Tokens.

F2. Token Service Provider – Authorised Entity (Token Requestor)

Relationship: The Token Service Provider provides Payment Token lifecycle management services to the authorised entity (Token Requestor).

Function: The Token Service Provider provides the authorised entity (Token Requestor) with Payment Token lifecycle management notifications for the Payment Token and / or Payment Token related data.

Function: The authorised entity (Token Requestor) provides the Token Service Provider with Payment Token lifecycle management updates that impact the Payment Token and / or Payment Token related data enabling maintenance of the Token Vault.

F3. Merchant (Token User) – Authorised Entity (Token Requestor)

Relationship: The Merchant (Token User) has an existing relationship with the authorised entity (Token Requestor) which can be utilised for Payment Token lifecycle management.

Function: The authorised entity (Token Requestor) provides the Merchant (Token User) with Payment Token lifecycle management notifications for the Payment Token and / or Payment Token related data.

Function: The Merchant (Token User) provides the authorised entity (Token Requestor) with Payment Token lifecycle management updates that impact the Payment Token and / or Payment Token related data.

10.4 Lifecycle Management Events

Some PAN lifecycle management events trigger Payment Token lifecycle management event(s), while other PAN lifecycle management events have no effect on Payment Token lifecycle management. Currently there is no identified use case where a Payment Token lifecycle management event triggers a PAN lifecycle management event.

PAN lifecycle management and Payment Token lifecycle management events have two components which are illustrated in Table 10.1.

Table 10.1: Lifecycle Management Components

Component	Description
Object	The area of lifecycle management event (e.g. PAN or Payment Token)
Function	The type of the lifecycle management event (e.g. Update or Notification)

This enables flexibility and expansion beyond the examples provided, while supporting a consistent definition for use in the lifecycle management use cases defined in this document. The concept is demonstrated in Table 10.2.

Table 10.2: Lifecycle Management Events

Event	Description	Examples
PAN Update	Object: PAN Function: Update Card Issuer provides the Token Service Provider with updated PAN and related information for management of the Token Vault.	• Change to PAN (e.g. lost, stolen or no longer valid) • Change to PAN Expiry Date (e.g. renewal) • Changes to the status of the Payment Account with the Card Issuer represented by the PAN (e.g. authorisation prohibited, delinquency, fraud alert on PAN) • Changes associated with PAR (e.g. BIN Controller governance determines if a new PAR value is required)
Payment Token Update	Object: Payment Token Function: Update Token Requestor (on its own behalf or on behalf of a Token User), or Card Issuer requests that the Token Service Provider updates the Token Vault, or the Token Service Provider self-maintains the Token Vault.	• Change to Payment Token related data (e.g. Expiry Date, Token Assurance Method, Last 4 Digits of PAN) • Change to the status of the Payment Token (e.g. activated or suspended)
Payment Token Notification	Object: Payment Token Function: Notification Token Service Provider notifies Token Requestor or Card Issuer of modifications to the Token Vault. Payment Token notification is usually triggered by other lifecycle management events.	• Notify Card Issuer of a change to the status of the Payment Token (e.g. deleted) • Notify Token Requestor of a change to the Payment Token's related data (e.g. new Last 4 Digits of PAN) • Token Requestors may pass on notifications of any relevant changes to Token Users

10.5 Merchant Deletion of Payment Credential

This use case example describes the lifecycle management that may occur when a Merchant (Token Requestor) deletes a stored payment credential which is represented by a Payment Token. This use case example is illustrated by a Cardholder successfully closing an account with a Merchant which was providing ongoing services (e.g. a subscription service).

The Cardholder had provided a payment credential, represented by a PAN, to the Merchant (Token Requestor), which the Merchant used in a Token Request to obtain and store a Payment Token. The Merchant made recurring subscription charges to the Cardholder via regular Token Payment Requests according to the subscription plan, which were performed as Merchant-Initiated Transactions as described in the Technical Framework and Transaction Types document (for further details, see Section 8.8 Merchant-Initiated Transaction).

10.5.1 Use Case Overview

This use case only covers the Payment Token lifecycle management events that may occur once the Cardholder has successfully closed the account with the Merchant, which means that there is no reason to retain the Payment Token.

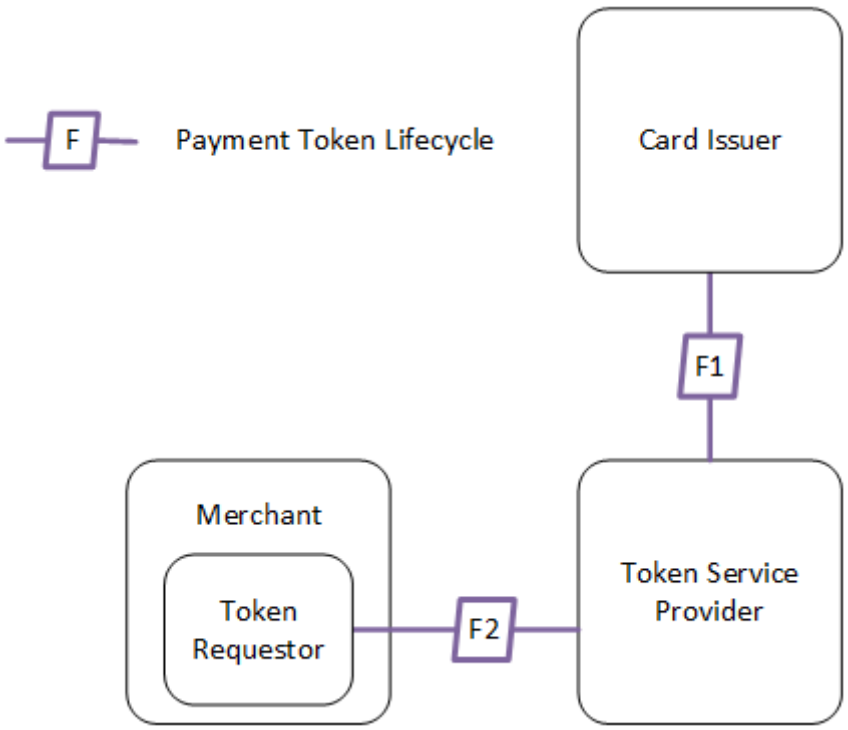
From a Cardholder perspective there is no difference in user experience whether a Payment Token or PAN has been stored by the Merchant.

10.5.2 Use Case Lifecycle Management Relationships and Functions

The relationships for this use case are shown in Figure 10.2. For a description of the baseline relationships and their functions, refer to the model described in Section 10.3 Lifecycle Management Relationships.

For each relationship shown in Figure 10.2, the specific nature of the relationship and its function or functions are given in the text following the figure, along with a reference to the baseline relationship and functions.

Figure 10.2: Merchant Deletion of Payment Credential – Use Case Relationships



F1. Card Issuer – Token Service Provider

Relationship: The Card Issuer has a relationship with the Token Service Provider to provide Payment Tokenisation services which is used for Payment Token lifecycle management.

Function: The Token Service Provider provides the Card Issuer with Payment Token lifecycle management notifications performed as part of maintenance of the Token Vault to ensure that the Card Issuer has current information available for all affiliated Payment Tokens.

Note: This relationship does not vary by use case.

Reference: Section 10.3.3 Payment Token Lifecycle Relationships and Functions.

F2. Token Service Provider – Merchant (Token Requestor)

Relationship: The Token Service Provider provides Payment Token lifecycle management services to the Merchant (Token Requestor).

Function: The Merchant (Token Requestor) provides the Token Service Provider with Payment Token lifecycle management updates that impact the Payment Token and / or Payment Token related data enabling maintenance of the Token Vault.

Note: This relationship does not vary by use case.

Reference: Section 10.3.3 Payment Token Lifecycle Relationships and Functions.

10.5.3 Lifecycle Management Flow

The following preconditions and assumptions apply to this specific flow.

Lifecycle Management Preconditions

- The Cardholder has an account for an on-going service with the Merchant
- The Merchant (Token Requestor) has obtained a Payment Token for the Cardholder's PAN, which was used in recurring payments for the service
- The Payment Token is stored by the Merchant (Token Requestor) in the designated Token Location

Lifecycle Management Assumptions

- The Merchant is the Token Requestor
- The Cardholder has successfully closed the account and the Merchant has no reason to retain the Payment Token for any additional services or transactions
- The Merchant (Token Requestor) provides the Payment Token lifecycle management update to the Token Service Provider, resulting in the Merchant (Token Requestor) subsequently deleting the Payment Token from the Token Location

Lifecycle Management Events

The lifecycle management events in this use case are shown in Table 10.3.

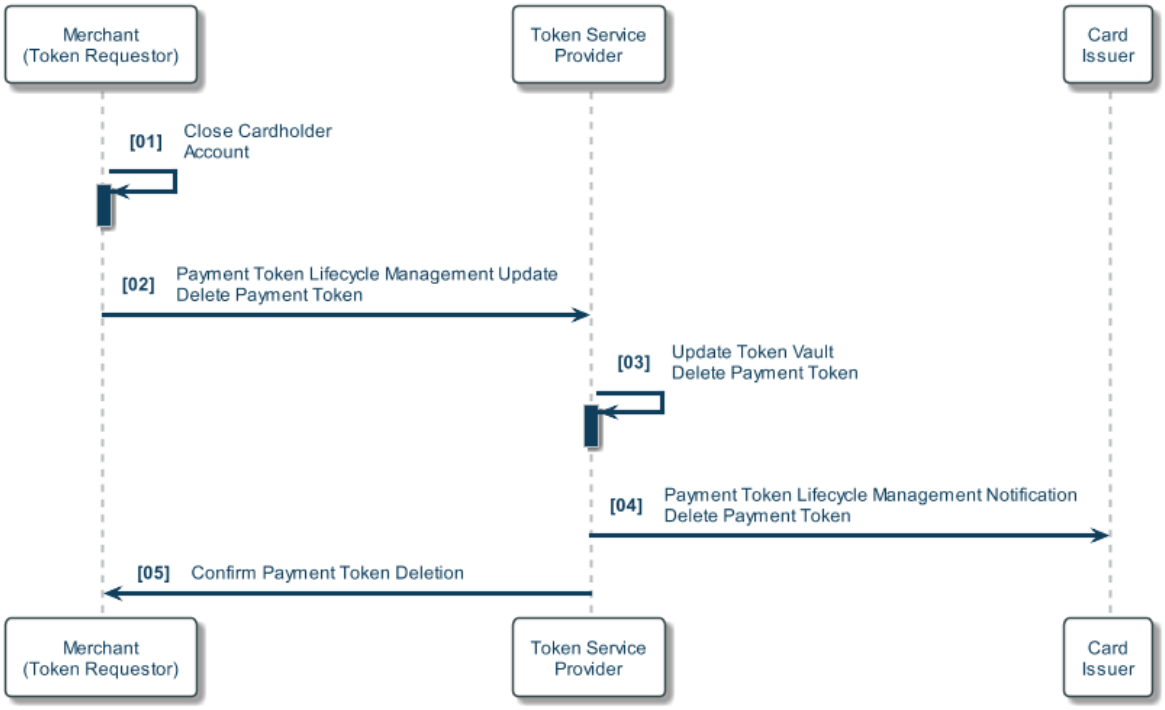
Table 10.3: Merchant Deletion of Payment Credential – Lifecycle Management Events

Event	Components	Description
Payment Token Update	Object: Payment Token Function: Update	The Merchant (Token Requestor) requests that the Token Service Provider deletes the specified Payment Token.
Payment Token Notification	Object: Payment Token Function: Notification	The Token Service Provider notifies the Card Issuer that the Payment Token has been deleted.

Example Lifecycle Management Flow

Figure 10.3 shows an example lifecycle management flow, with numbered steps which are explained following the figure.

Figure 10.3: Merchant Deletion of Payment Credential – Example Lifecycle Management Flow



01. The Merchant closes the Cardholder account
02. The Merchant (Token Requestor) sends a Payment Token lifecycle management update to the Token Service Provider, requesting the deletion of a Payment Token
03. The Token Service Provider deletes the Payment Token from the Token Vault
04. The Token Service Provider sends a Payment Token lifecycle management notification to the Card Issuer, indicating that the Payment Token issued to the Merchant (Token Requestor) has been deleted
05. The Token Service Provider confirms to the Merchant (Token Requestor) that the Payment Token has been successfully deleted

10.6 Lost / Stolen Consumer Device

This use case example describes the lifecycle management that may occur when a Consumer Device is reported as lost and / or stolen.

A Payment Token has been issued to a mobile payment application installed on the Consumer Device (as described in Section 8.2 Proximity at Point of Sale). In the first instance the Payment Token is suspended following notification by the Card Issuer of a lost / stolen Consumer Device. It is subsequently deleted from the mobile payment application once it becomes clear that the Consumer Device will not be recovered.

10.6.1 Use Case Overview

Although the Consumer Device and mobile payment application may have various access controls (PIN, password, pattern, biometrics etc.) to aid with prevention of unauthorised use, the loss or theft of the Consumer Device will require that the Payment Token is appropriately managed.

This use case describes the Payment Token lifecycle management updates originated by the Card Issuer that may occur:

- In the first instance, once the Cardholder has reported the loss of the Consumer Device to the Card Issuer
- In the second instance, once the Consumer Device is considered unrecoverable by the Cardholder

Since a Payment Token had been issued to a mobile payment application, there is no impact on the associated Payment Account. In addition, there is no requirement to replace the PAN and the associated payment card due to the Consumer Device being unrecoverable.

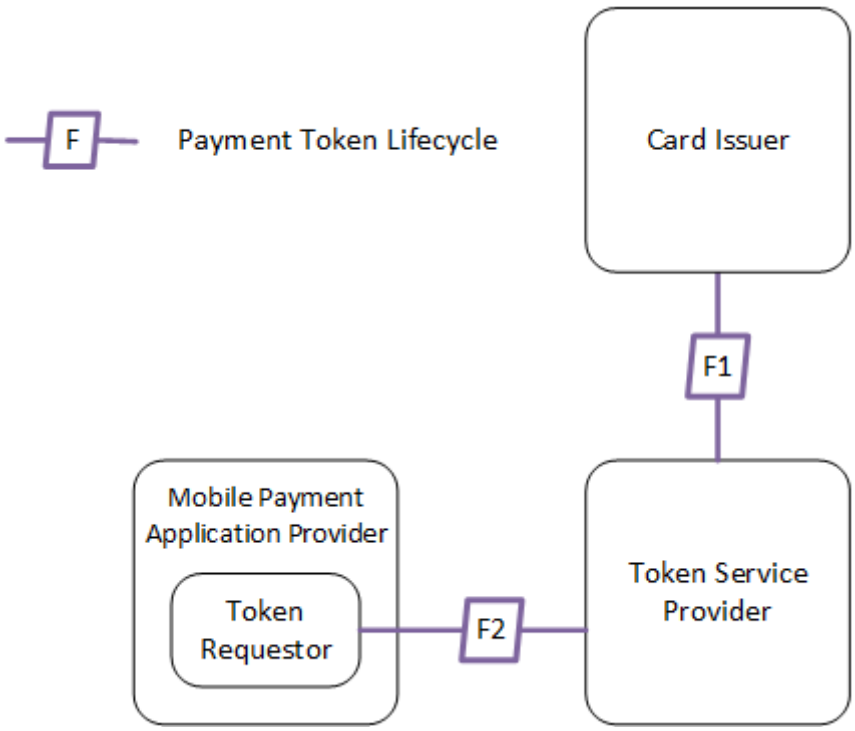
If the Cardholder obtains a replacement Consumer Device, the Issuance Flow described in Section 8.2 Proximity at Point of Sale would need to be performed.

10.6.2 Use Case Lifecycle Management Relationships and Functions

The relationships for this use case are shown in Figure 10.4. For a description of the baseline relationships and their functions, refer to the model described in Section 10.3 Lifecycle Management Relationships.

For each relationship shown in Figure 10.4, the specific nature of the relationship and its function or functions are given in the text following the figure, along with a reference to the baseline relationship and functions.

Figure 10.4: Lost / Stolen Consumer Device – Use Case Relationships



F1. Card Issuer – Token Service Provider

Relationship: The Card Issuer has a relationship with the Token Service Provider to provide Payment Tokenisation services which is used for Payment Token lifecycle management.

Function: The Card Issuer provides the Token Service Provider with Payment Token lifecycle management updates that impact the Payment Token, enabling maintenance of the Token Vault.

Note: This relationship does not vary by use case.

Reference: Section 10.3.3 Payment Token Lifecycle Relationships and Functions.

F2. Token Service Provider – Merchant (Token Requestor)

Relationship: The Token Service Provider provides Payment Token lifecycle management services to the Merchant (Token Requestor).

Function: The Token Service Provider provides the Merchant (Token Requestor) with Payment Token lifecycle management notifications for the Payment Token.

Note: This relationship does not vary by use case.

Reference: Section 10.3.3 Payment Token Lifecycle Relationships and Functions.

10.6.3 Lifecycle Management Flow

The following preconditions and assumptions apply to this specific flow.

Lifecycle Management Preconditions

- The Cardholder has added a PAN to the mobile payment application which the mobile payment application provider (Token Requestor) has successfully used to obtain a Payment Token

Lifecycle Management Assumptions

- The mobile payment application provider is the Token Requestor
- The Consumer Device can receive and send communications over a network while lost or stolen (e.g. the Consumer Device is a smartphone with mobile data and / or Wifi connection)
- In the first instance, the Card Issuer requests that the Payment Token is suspended
- In the second instance, the Card Issuer requests that the Payment Token is deleted from the mobile payment application

Lifecycle Management Events

The lifecycle management events in this use case are shown in Table 10.4.

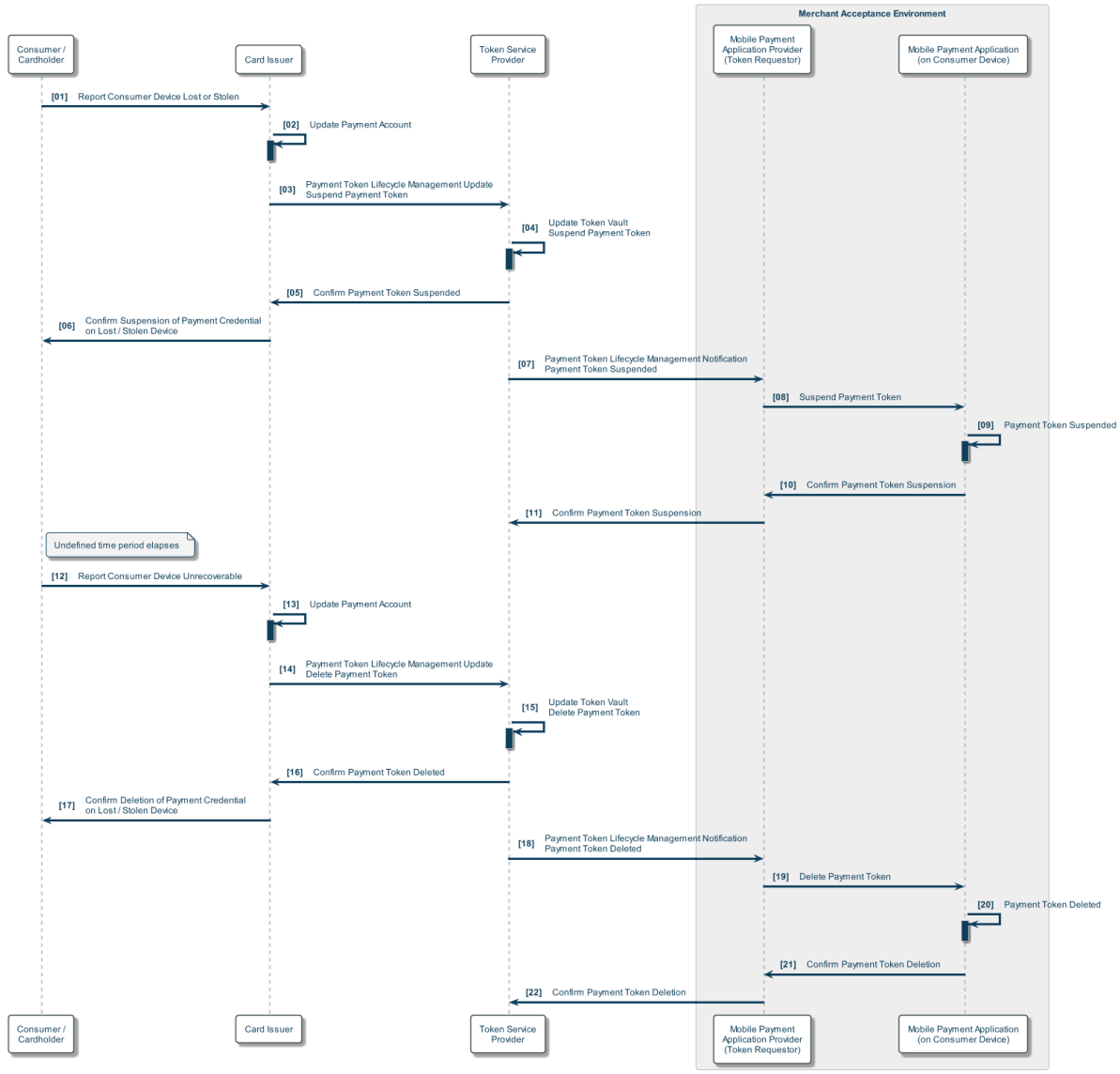
Table 10.4: Lost / Stolen Consumer Device – Lifecycle Management Events

Event	Components	Description
Payment Token Update	Object: Payment Token Function: Update	The Card Issuer requests that the Token Service Provider suspends the specified Payment Token.
Payment Token Notification	Object: Payment Token Function: Notification	The Token Service Provider notifies the mobile payment application provider (Token Requestor) that the Payment Token has been suspended.
Payment Token Update	Object: Payment Token Function: Update	The Card Issuer requests that the Token Service Provider deletes the specified Payment Token.
Payment Token Notification	Object: Payment Token Function: Notification	The Token Service Provider notifies the mobile payment application provider (Token Requestor) that the Payment Token has been deleted.

Example Lifecycle Management Flow

Figure 10.5 shows an example issuance flow, with numbered steps which are explained following the figure.

Figure 10.5: Lost / Stolen Consumer Device – Example Lifecyle Management Flow



01. The Cardholder contacts the Card Issuer to advise that the Consumer Device is currently lost or possibly stolen, but the Cardholder believes there is still a possibility for the Consumer Device to be recovered

02. The Card Issuer updates the Payment Account status.

03. The Card Issuer sends a Payment Token lifecycle management update to the Token Service Provider, requesting the suspension of the Payment Token

04. The Token Service Provider updates the Token Vault to reflect the suspension of the Payment Token
05. The Token Service Provider confirms the suspension of the Payment Token to the Card Issuer
06. The Card Issuer informs the Cardholder of the suspension of the payment credential stored in the mobile payment application on the reported Consumer Device
07. The Token Service Provider sends a Payment Token lifecycle management notification to the mobile payment application provider (Token Requestor), indicating that the Payment Token on the mobile payment application has been suspended
08. The mobile payment application provider (Token Requestor) instructs the mobile payment application on the Consumer Device to suspend the Payment Token
09. The mobile payment application receives the instruction and suspends the Payment Token
10. The mobile payment application confirms the Payment Token suspension to the mobile payment application provider (Token Requestor)
11. The mobile payment application provider (Token Requestor) confirms to the Token Service Provider that the Payment Token has been successfully suspended in the mobile payment application
12. After an unspecified period of time, the Cardholder contacts the Card Issuer to advise that the Consumer Device is unrecoverable
13. The Card Issuer updates the Payment Account status
14. The Card Issuer sends a Payment Token lifecycle management update to the Token Service Provider, requesting the deletion of the Payment Token
15. The Token Service Provider updates the Token Vault to reflect the deletion of the Payment Token
16. The Token Service Provider confirms the deletion of the Payment Token to the Card Issuer
17. The Card Issuer informs the Cardholder of the deletion of the payment credential stored in the mobile payment application on the unrecoverable Consumer Device
18. The Token Service Provider sends a Payment Token lifecycle management notification to the mobile payment application provider (Token Requestor), indicating that the Payment Token on the mobile payment application has been deleted
19. The mobile payment application provider (Token Requestor) instructs the mobile payment application on the Consumer Device to delete the Payment Token
20. The mobile payment application receives the instruction and deletes the Payment Token
21. The mobile payment application confirms the Payment Token deletion to the mobile payment application provider (Token Requestor)

22. The mobile payment application provider (Token Requestor) confirms to the Token Service Provider that the Payment Token has been successfully deleted from the mobile payment application

10.7 PAN Replacement

This use case example describes the lifecycle management that may occur following the replacement of a PAN which has one or more affiliated Payment Tokens. When the Token Service Provider is informed of the replacement of the PAN, it updates the Token Vault by removing the affiliation between the Payment Tokens and the original PAN, instead affiliating the Payment Tokens with the replacement PAN.

This use case example uses suspected fraudulent activity on the Payment Account associated with the PAN as a trigger for the PAN replacement. When a Cardholder reports suspected fraudulent activity on the Payment Account to the Card Issuer, a business-as-usual process will change the affected PAN assigned to the Payment Account and issue a replacement payment card with the new PAN which is sent to the Cardholder. Where the affected PAN has affiliated Payment Tokens, the Card Issuer provides the Token Service Provider with PAN lifecycle management updates.

This use case example covers the PAN lifecycle management updates which then trigger additional Payment Token lifecycle management notifications.

This specific use case example is illustrated by a Merchant (Token Requestor) which is storing the Payment Token in a Card-On-File usage scenario (see Section 8.5 Card-On-File E-Commerce). However, PAN replacement and the corresponding lifecycle management activity applies to all Payment Tokenisation usage scenarios. For example, if the card was lost, stolen or is just being replaced with a new PAN for any reason, the same PAN lifecycle management updates and subsequent Payment Token lifecycle management notifications would occur.

10.7.1 Use Case Overview

This use case example assumes that a Payment Token was issued for the original PAN and is stored by a Merchant (Token Requestor) as defined in Section 8.5 Card-On-File E-Commerce.

From a Cardholder perspective there is no expectation that they will understand that a Payment Token is involved. The Merchant receives a Payment Token lifecycle management notification containing the Last 4 Digits of PAN for the replacement PAN (alongside any other related data). The Merchant can then display the new last four digits to the Cardholder, so that the Cardholder has clarity for which payment credential is being selected. Since this update is automatic, without any involvement from the Cardholder, it should provide a positive Cardholder user experience with the Merchant (Token Requester) and Card Issuer.

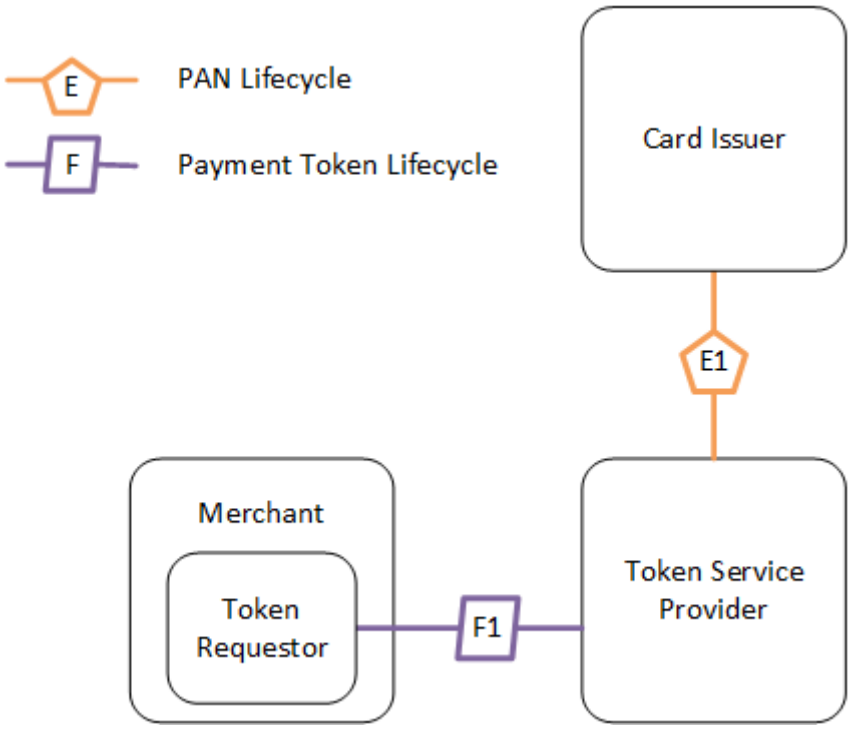
An additional benefit to the Merchant is that the replacement of the underlying PAN has no impact on any affiliated Payment Token(s), so the Payment Token can continue to transact uninterrupted.

10.7.2 Use Case Lifecycle Management Relationships and Functions

The relationships for this use case are shown in Figure 10.6. For a description of the baseline relationships and their functions, refer to the model described in Section 10.3 Lifecycle Management Relationships.

For each relationship shown in Figure 10.4, the specific nature of the relationship and its function or functions are given in the text following the figure, along with a reference to the baseline relationship and functions.

Figure 10.6: Replacement PAN – Use Case Relationships



E1. Card Issuer – Token Service Provider

Relationship: The Card Issuer has a relationship with the Token Service Provider to provide Payment Tokenisation services which is used for PAN lifecycle management.

Function: The Token Service Provider uses PAN lifecycle management updates provided by the Card Issuer to maintain the PAN and affiliated Payment Token information and all related data in the Token Vault.

Note: This relationship does not vary by use case.

Reference: Section 10.3.2 PAN Lifecycle Relationships and Functions.

F1. Token Service Provider – Merchant (Token Requestor)

Relationship: The Token Service Provider provides Payment Token lifecycle management services to the Merchant (Token Requestor).

Function: The Token Service Provider provides the Merchant (Token Requestor) with Payment Token lifecycle management notifications for the Payment Token related data.

Note: This relationship does not vary by use case.

Reference: Section 10.3.3 Payment Token Lifecycle Relationships and Functions.

10.7.3 Lifecycle Management Flow

The following preconditions and assumptions apply to this specific flow.

Lifecycle Management Preconditions

- The Merchant operates an e-commerce environment which can either be web-based or application-based
- The Consumer has an account with the Merchant
- The Cardholder has added a payment credential, represented by a PAN, to the account which the Merchant (Token Requestor) has used to request a Payment Token
- The Payment Token is stored by the Merchant (Token Requestor) and is identified in the Merchant e-commerce environment by the last four digits of the underlying PAN

Lifecycle Management Assumptions

- The PAN has a single affiliated Payment Token
- PAR has been implemented and is based on specific BIN Controller governance policies. This results in the PAR value which was assigned to the original PAN being transferred to the replacement PAN to maintain continuity for transaction linkage purposes

Lifecycle Management Events

The lifecycle management events in this use case are shown in Table 10.5.

Table 10.5: PAN Replacement – Lifecycle Management Events

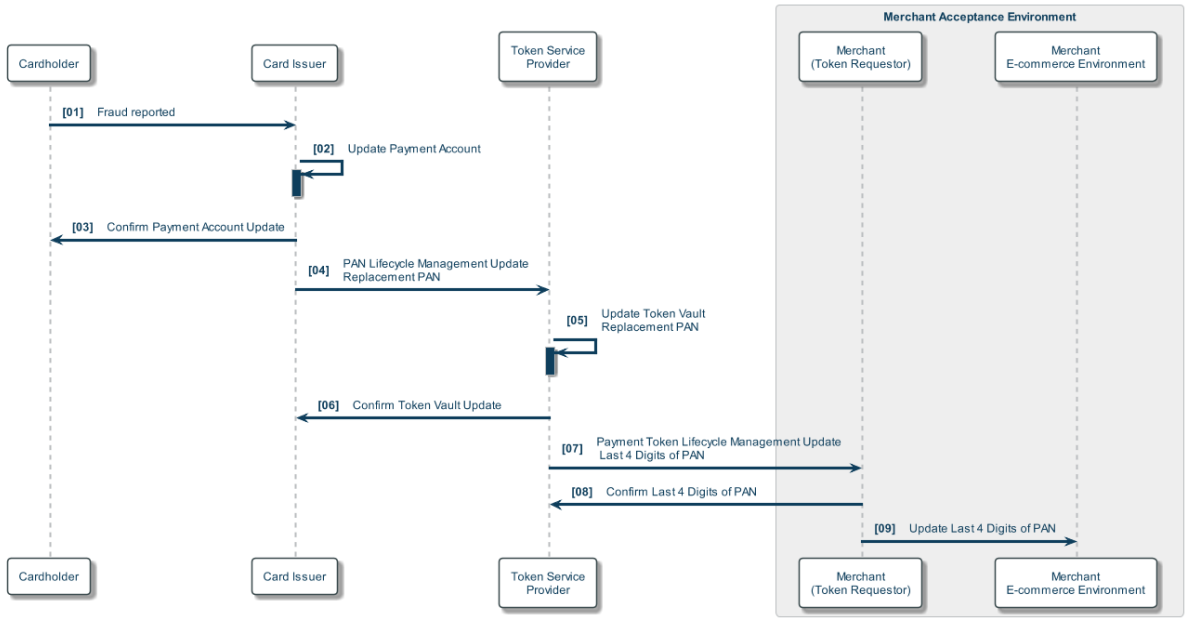
Event	Component	Description
PAN Update	Object: PAN Function: Update	The Card Issuer provides the Token Service Provider with the replacement PAN and related information for management of the Token Vault.

Event	Component	Description
Payment Token Notification	Object: Payment Token Function: Notification	The Token Service Provider notifies the Merchant (Token Requestor) of the Last 4 Digits of PAN for the replacement PAN which is used to identify the affiliated Payment Token.

Example Lifecycle Management Flow

Figure 10.7 shows an example lifecycle management flow, with numbered steps which are explained following the figure.

Figure 10.7: PAN Replacement – Example Lifecycle Management Flow



01. The Cardholder reports suspected fraudulent activity on the Payment Account to the Card Issuer
02. The Card Issuer updates the Payment Account status, blocks the original PAN and assigns a replacement PAN for the Payment Account that will be used on a replacement payment card sent to the Cardholder
03. The Card Issuer confirms to the Cardholder that the Payment Account has been updated
04. The Card Issuer sends a PAN lifecycle management update to the Token Service Provider
05. The Token Service Provider updates the Token Vault, removing the affiliation between the Payment Token and the original PAN, instead affiliating the Payment Token with the replacement PAN

06. The Token Service Provider confirms to the Card Issuer that the Token Vault has been successfully updated
07. The Token Service Provider sends a Payment Token lifecycle management notification to the Merchant (Token Requestor) to provide the Last 4 Digits of PAN for the replacement PAN and any other related data that needs to be updated
08. The Merchant (Token Requestor) confirms to the Token Service Provider that the Last 4 Digits of PAN and any other related data has been received
09. The Merchant (Token Requestor) updates the Merchant e-commerce environment with the Last 4 Digits of PAN for the replacement PAN, which it uses to identify the Payment Token

11 Payment Tokenisation and Other EMV Technologies

EMVCo supports a number of technologies which, while capable of operating independently of each other, are designed to be interoperable. This is particularly true of Payment Tokenisation, which can be used in combination with other EMV technologies such as Secure Remote Commerce (SRC) and EMV® 3-D Secure.

This Section provides specific use case examples where the Technical Framework and other EMV Specifications work together to support a specific use case. Since A Guide to Use Cases is a Payment Tokenisation document, the use case examples are focused on Payment Tokenisation, with the other EMV technologies covered to a basic level of detail for overall understanding. For further details of other EMV technologies involved in any use case example, please refer to the relevant EMV Specification(s).

11.1 Secure Remote Commerce

Secure Remote Commerce (SRC) enables a common Consumer e-checkout that promotes simplicity, familiarity, interoperability, convenience and trust. Consumer-facing solutions and programmes based on the SRC specifications can be described as Click to Pay. This universal description enables ease of recognition for Consumers, and signals that a Consumer can confidently transact through a consistent e-checkout, regardless of the Payment Card, digital channel or device used.

As with all EMV Specifications, SRC is designed to enable card-based payment products to work together seamlessly and securely worldwide. SRC implementations support transactions based on PAN, but may additionally integrate Payment Tokenisation, so that both Payment Tokenisation and SRC are used to support a single use case.

The following use case examples show a combination of Payment Tokenisation and SRC:

- SRC E-Commerce Transaction (Section 11.2)
- SRC Guest Checkout (Section 11.3)

In all SRC use case examples, the Cardholder interacts with both Payment Tokenisation and SRC Participants to complete an e-commerce transaction. The overlap between Payment Tokenisation and SRC environments are represented in these use case examples and provide a limited set of examples.

The SRC specifications provide details on communication between participants using specified application programming interfaces (API) as well as JavaScript Software Development Kit (SDK). These use case examples simplify the interactions between participants using API or SDK messages to highlight the intersection between SRC and

Payment Tokenisation. For additional details on Secure Remote Commerce, including defined terms used within SRC, please refer to the relevant SRC specifications.

11.2 SRC E-Commerce Transaction

This use case example describes an SRC checkout using an SRC Trigger represented by the Click to Pay icon. This is a checkout model where a Merchant has registered with an SRC Initiator that provides the Consumer with a complete checkout experience (in conjunction with an SRC System) and where the SRC Initiator performs Token Processing on behalf of the Merchant.

When a Consumer chooses Click to Pay for payment, the SRC Initiator interacts with the Merchant e-commerce environment to trigger an SRC checkout resulting in the delivery of a Payment Token.

The Cardholder may be required to perform a variety of other actions within the SRC checkout which are out of scope for the description of this use case example.

This use case example covers:

- Token Issuance and Token Provisioning
- Token Presentment and Token Processing

11.2.1 Use Case Overview – Problems Addressed & User Experience

SRC enables the delivery of a Payment Token to an SRC Initiator as a result of a successful SRC checkout. The characteristics of the Payment Token may be defined at the time the Merchant registers within an SRC Programme. Alternatively, the SRC Programme enables participants to determine the Payment Token characteristics at the time of the transaction based on underlying properties of the SRC checkout. The Payment Token characteristics may change based on the Consumer and Cardholder authentication performed as part of the SRC checkout.

This use case example assumes the Payment Token is issued and provisioned to an SRC System and is then delivered to the Merchant e-commerce environment for subsequent transactions. As the Token Requestor, the SRC System may request a Token Cryptogram for each transaction to ensure transaction integrity. Additionally, the SRC System may enable additional security options described in the SRC specifications (e.g. SRC Dynamic Data).

11.2.2 Use Case Relationships and Functions

Entities that participate in Payment Tokenisation and SRC may perform functions associated with roles described in each specification to enable a variety of use cases. Table 11.1 describes the relationships between the Payment Tokenisation and SRC entities and the functions that they carry out for this use case example.

Table 11.1: SRC E-Commerce Transaction – Relationships

Tokenisation	SRC	Function (SRC / Token)
Token Service Provider	N/A	• As defined in the Technical Framework
Token Requestor	SRC System	• Register for Token Requestor ID (Token) • Request Payment Token (Token) • Facilitate delivery of Payment Token and other related data (Token)
Authorised Entity	SRC Initiator	• Facilitate SRC checkout (SRC) • Initiate Token Processing (Token)
Merchant (Token User)	Digital Payment Application	• Register with Token Requestor (Token) • Provide Click to Pay option within e-commerce checkout (SRC)

11.2.3 Use Case Characteristics

The use case characteristics are shown in Table 11.2, Table 11.3, Table 11.4 and Table 11.11.

Table 11.2: SRC E-Commerce Transaction – Token Issuance Characteristics

Characteristic	Notes	Typical Outcomes
Cardholder Availability	Payment Tokens can be issued when the Cardholder is not available.	• Not Required

Table 11.3: SRC E-Commerce Transaction – Token Provisioning Characteristics

Characteristic	Notes	Typical Outcomes
Token Location	See Table 5.1 of the Technical Framework for defined Token Locations.	• 06

Table 11.4: SRC E-Commerce Transaction – Token Presentment Characteristics

Characteristic	Notes	Typical Outcomes
Token Presentment	The SRC System (Token Requestor) presents the Payment Token to the SRC Initiator (Authorised Entity)	• Non-proximity
Acceptance Environment	The acceptance environment is a Merchant e-commerce environment.	• Non-physical

Table 11.5: SRC E-Commerce Transaction – Token Processing Characteristics

Characteristic	Notes	Typical Outcomes
Token Payment Request	The SRC Initiator (Authorised Entity) submits the Token Payment Request to obtain a PAN authorisation.	• Third Party Service Provider
Token Control Fields	Used to constrain the Payment Token to a specific Merchant (Token User) and specific Token Presentment Mode at the time of a given transaction.	• POS Entry Mode • Merchant Identifiers • Token Cryptogram

11.2.4 Payment Token Characteristics

The Payment Token characteristics are shown in Table 11.6.

Table 11.6: SRC E-Commerce Transaction – Payment Token Characteristics

Characteristic	Notes	Typical Outcomes
Payment Token Usage	The Payment Token is for use by a specific Merchant (Token User).	• Token User
Token Assurance Method	Token Assurance is Token Programme specific and determined by a combination of the Token Programme and the SRC Programme policies and processes based on the detailed characteristics of this use case.	• 10 – 19 • 20 – 89

Characteristic	Notes	Typical Outcomes
Token Domain Restriction Controls	The Payment Token is constrained to specific Merchants (Token Users) and a specific Token Presentment Mode.	• Merchant • Token Presentment Mode
Token Cryptogram	A Token Cryptogram is used to ensure the integrity of the transaction-specific data.	• Used
Type of Transaction Initiation	Typically, the Cardholder uses a Merchant e-commerce environment / Digital Payment Application to initiate a transaction.	• Cardholder-Initiated Transaction

11.2.5 Issuance Flow

The following preconditions and assumptions apply to this specific flow.

Issuance Flow Preconditions

- The SRC System (Token Requestor) has registered with the Token Service Provider and has received a Token Requestor ID
- The PAN that the Cardholder enrols with the SRC System is eligible for Payment Tokenisation

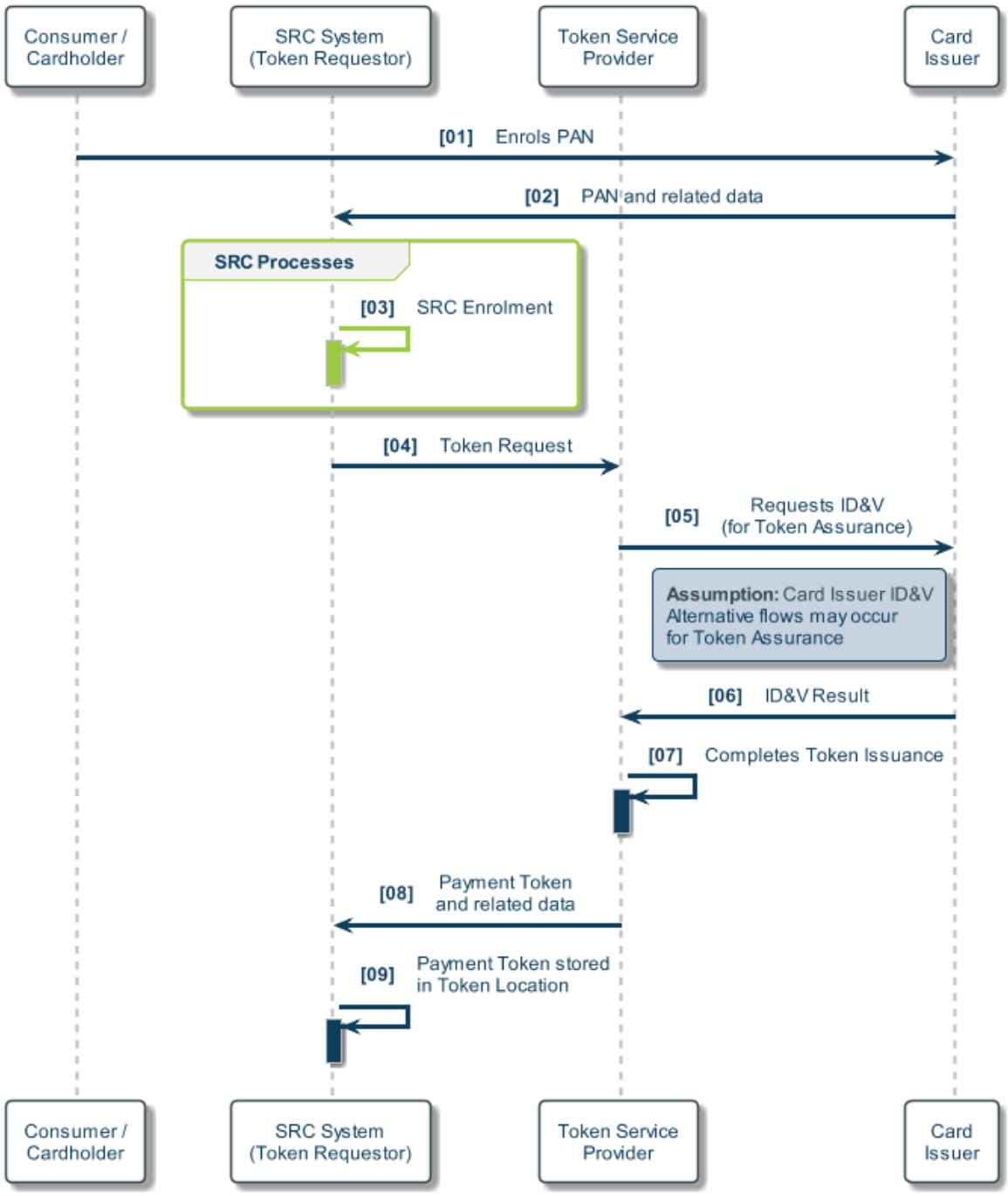
Issuance Flow Assumptions

- The Token Request is initiated by the SRC System (Token Requestor) based on an interaction between the Card Issuer and Cardholder
- Token Assurance and the related ID&V is performed by the Card Issuer, resulting in the Token Assurance Method value being set to one of the Card Issuer Token Assurance Method Categories
- The SRC System, in coordination with the Card Issuer, performs Cardholder assurance
- The designated Token Location is 06 Shared Storage

Example Issuance Flow

Figure 11.1 shows an example issuance flow, with numbered steps which are explained following the figure. Note that the SRC-specific functions (e.g. enrolling the PAN) are not shown as individual steps.

Figure 11.1: SRC E-Commerce Transaction – Example Issuance Flow



01. The Cardholder signs into the Card Issuer application to enrol a PAN into the SRC System
02. The Card Issuer provides the PAN and related data to the SRC System for enrolment
03. The SRC System undertakes a variety of SRC-specific actions to enrol the PAN
04. The SRC System (Token Requestor) initiates a Token Request for a Payment Token to the Token Service Provider (using its Token Requestor ID)

05. The Token Service Provider carries out Token Assurance and requests that the Card Issuer undertakes ID&V
06. The Card Issuer responds to the Token Service Provider with its ID&V result
07. The Token Service Provider completes Token Issuance (this is on the assumption that the ID&V result indicates Card Issuer approval)
08. Token Service Provider delivers a Payment Token and related data to the SRC System (Token Requestor) as part of Token Provisioning
09. The Payment Token and its related data are stored in the designated Token Location by the SRC System (Token Requestor) to complete Token Provisioning

11.2.6 Transaction Flow

The following preconditions and assumptions apply to this specific flow.

Transaction Flow Preconditions

- The Merchant has enabled an SRC Initiator (Authorised Entity) within its e-commerce environment to facilitate SRC checkout from the Merchant's Digital Payment Application and to perform Token Processing on the Merchant's behalf
- The Cardholder has successfully enrolled a PAN into the SRC System which is represented by a Digital Card and which has an associated Payment Token

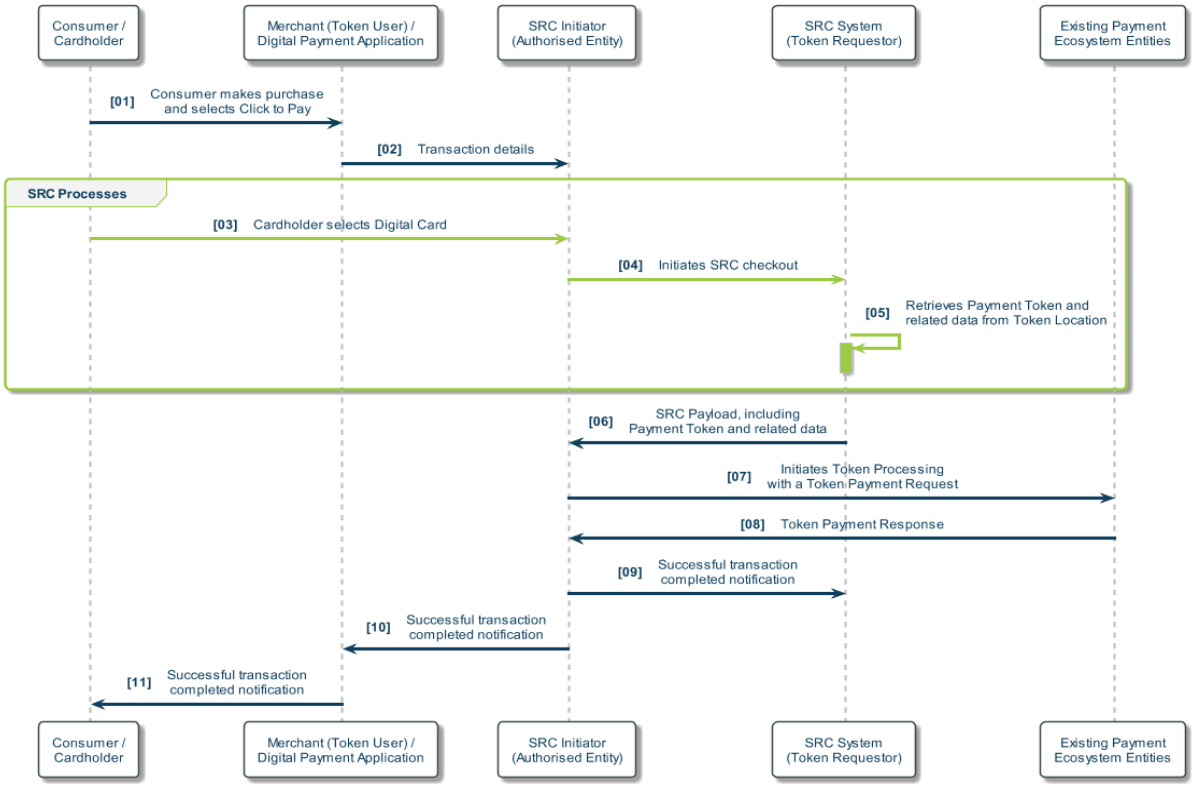
Transaction Flow Assumptions

- The Cardholder accesses a Digital Card that is associated with a stored Payment Token
- The Digital Card / Payment Token is stored by the SRC System and is identified during SRC checkout by the last four digits of the underlying PAN and digital card art
- A Token Cryptogram as well as Dynamic Data from an SRC System is used
- The SRC Initiator (Authorised Entity) initiates Token Processing using the Payment Token and related data via existing relationships with the existing payment ecosystem entities

Example Transaction Flow

Figure 11.2 shows an example transaction flow, with numbered steps which are explained following the figure. Note that the SRC-specific functions (e.g. presenting the list of Digital Cards) are not shown as individual steps.

Figure 11.2: SRC E-Commerce Transaction – Example Transaction Flow



01. The Consumer makes a purchase from the Merchant e-commerce environment / Digital Payment Application and initiates the SRC checkout process by selecting Click to Pay
02. The Digital Payment Application provides details of the transaction to the SRC Initiator
03. The Cardholder selects a previously stored Digital Card from a list presented by the SRC Initiator
04. The SRC Initiator initiates SRC checkout with the SRC System by providing details of the transaction and the selected Digital Card
05. The SRC System (Token Requestor) retrieves the Payment Token as part of processing the SRC checkout
06. The SRC System responds to the SRC checkout by returning an SRC Payload (which includes the Payment Token and related data) to the SRC Initiator
07. The SRC Initiator (Authorised Entity) initiates Token Processing by sending a Token Payment Request
08. The SRC Initiator (Authorised Entity) receives a Token Payment Response as a result of successful PAN Authorisation by the Card Issuer
09. The SRC Initiator provides the results to the SRC System

10. The SRC Initiator (Authorised Entity) provides the results to the Merchant e-commerce environment / Digital Payment Application
11. The Cardholder receives confirmation from the Merchant e-commerce environment / Digital Payment Application that the transaction was successful

Token Processing Considerations

Table 8.9 (Token Processing Characteristics) and Table 8.10 (Payment Token Characteristics) show the typical Token Control Fields (Table 8.9) which are used as part of the Token Domain Restriction Controls (Table 8.10). In these specific use case flows, the following Token Control Fields are used:

- Token Cryptogram: SRC System will provide the SRC Initiator (Authorised Entity) a Payment Token and Token Cryptogram, including Dynamic Data

As well as the methods described in Section 8.1.3 Payment Account Reference Data (PAR Field and PAR Enquiry), PAR Data may be available to the Merchant:

- As part of the related data provided by the SRC System with the Payment Token via the SRC Initiator (Authorised Entity)

11.2.7 Variations of User Experience

Minor variations may occur for this use case due to possible differences related to whether the Consumer is interacting with a website or Merchant application, which will be Merchant and / or implementation specific.

11.3 SRC Guest Checkout

This use case example describes an SRC guest checkout using an SRC Trigger represented by the Click to Pay icon. This is a checkout model where the details of the Consumer's payment credential are used by the Merchant for this specific purchase only.

When the Consumer chooses Click to Pay for payment, the SRC Initiator interacts with the Merchant e-commerce environment to trigger an SRC checkout resulting in the delivery of a Payment Token to the Merchant (Token User) which uses it for Token Processing.

The Cardholder may be required to perform a variety of other actions within the SRC checkout which are out of scope for the description of this use case example.

This use case example covers:

- Token Issuance and Token Provisioning
- Token Presentment and Token Processing

11.3.1 Use Case Overview – Problems Addressed & User Experience

SRC enables the delivery of a Payment Token to a Merchant at the time of the checkout. The characteristics of the Payment Token are determined at the time of the transaction, based on underlying properties of the SRC checkout. The SRC Programme enables participants to evaluate the Payment Token characteristics at the time of the transaction rather than at the time of Token Issuance.

The Consumer will see typical SRC checkout experience regardless of the characteristics of the Payment Tokenisation.

11.3.2 Use Case Relationships and Functions

Entities that participate in Payment Tokenisation and SRC may perform functions associated with roles described in each specification to enable a variety of uses cases. Table 11.7 describes the relationships between the Payment Tokenisation and SRC entities and the functions that they carry out for this use case example.

Table 11.7: SRC Guest Checkout – Relationships

Tokenisation	SRC	Function (SRC / Token)
Token Service Provider	N/A	• As defined in the Technical Framework
Merchant	Digital Payment Application	• Provide Click to Pay option within e-commerce checkout (SRC)
Merchant (Token User)	SRC Initiator	• Register with Token Requestor (Token) • Facilitate SRC checkout (SRC) • Initiate Token Processing (Token)
Token Requestor	SRC System	• Register with Token Service Provider for Token Requestor ID (Token) • Facilitate Payment Token Request (Token) • Facilitate delivery of Payment Token and other related data (Token)
N/A	Digital Card Facilitator	• As defined in the SRC specifications

11.3.3 Use Case Characteristics

The use case characteristics are shown in Table 11.8, Table 11.9, Table 11.10 and Table 11.11.

Table 11.8: SRC Guest Checkout – Token Issuance Characteristics

Characteristic	Notes	Typical Outcomes
Cardholder Availability	Payment Tokens can be issued when the Cardholder is not available.	• Not Required

Table 11.9: SRC Guest Checkout – Token Provisioning Characteristics

Characteristic	Notes	Typical Outcomes
Token Location	See Table 5.1 of the Technical Framework for defined Token Locations.	• 06, 07

Table 11.10: SRC Guest Checkout – Token Presentment Characteristics

Characteristic	Notes	Typical Outcomes
Token Presentment	The SRC System (Token Requestor) presents the Payment Token to the Merchant (Token User) / SRC Initiator.	• Non-proximity
Acceptance Environment	The acceptance environment is a Merchant e-commerce environment.	• Non-physical

Table 11.11: SRC Guest Checkout – Token Processing Characteristics

Characteristic	Notes	Typical Outcomes
Token Payment Request	The Merchant (Token User) / SRC Initiator submits the Token Payment Request to obtain a PAN authorisation.	• Merchant
Token Control Fields	Used to constrain the Payment Token to a specific Merchant (Token User) and specific Token Presentment Mode at the time of a given transaction.	• POS Entry Mode • Merchant Identifiers • Token Cryptogram

11.3.4 Payment Token Characteristics

The Payment Token characteristics are shown in Table 11.12.

Table 11.12: SRC Guest Checkout – Payment Token Characteristics

Characteristic	Notes	Typical Outcomes
Payment Token Usage	The Payment Token can be used by a Merchant (Token User) that is not the Token Requestor and is constrained for use in a single Cardholder-Initiated Transaction and any subsequent Merchant-Initiated Transactions.	• Guest Checkout • Token User
Token Assurance Method	Token Assurance is Token Programme specific and determined by a combination of the Token Programme and the SRC Programme policies and processes based on the detailed characteristics of this use case.	• 01 – 19 • 20 – 89
Token Domain Restriction Controls	The Payment Token is constrained to a specific Merchant (Token User) and a specific Token Presentment Mode.	• Merchant • Token Presentment Mode
Token Cryptogram	When a Token Cryptogram is used, it ensures the integrity of the transaction-specific data.	• Used • Not Used
Type of Transaction Initiation	Typically, the Cardholder uses a Merchant e-commerce environment / Digital Payment Application to initiate a transaction.	• Cardholder-Initiated Transaction

11.3.5 Issuance Flow

The following preconditions and assumptions apply to this specific flow.

Issuance Flow Preconditions

- The SRC System (Token Requestor) has registered with the Token Service Provider and has received a Token Requestor ID
- The Merchant (Token User) has registered with the SRC System (Token Requestor)
- The Merchant provides both the Digital Payment Application and SRC Initiator in its e-commerce environment, which can either be web-based or application-based
- The PAN that the Cardholder uses for the SRC guest checkout is eligible for Tokenisation

Issuance Flow Assumptions

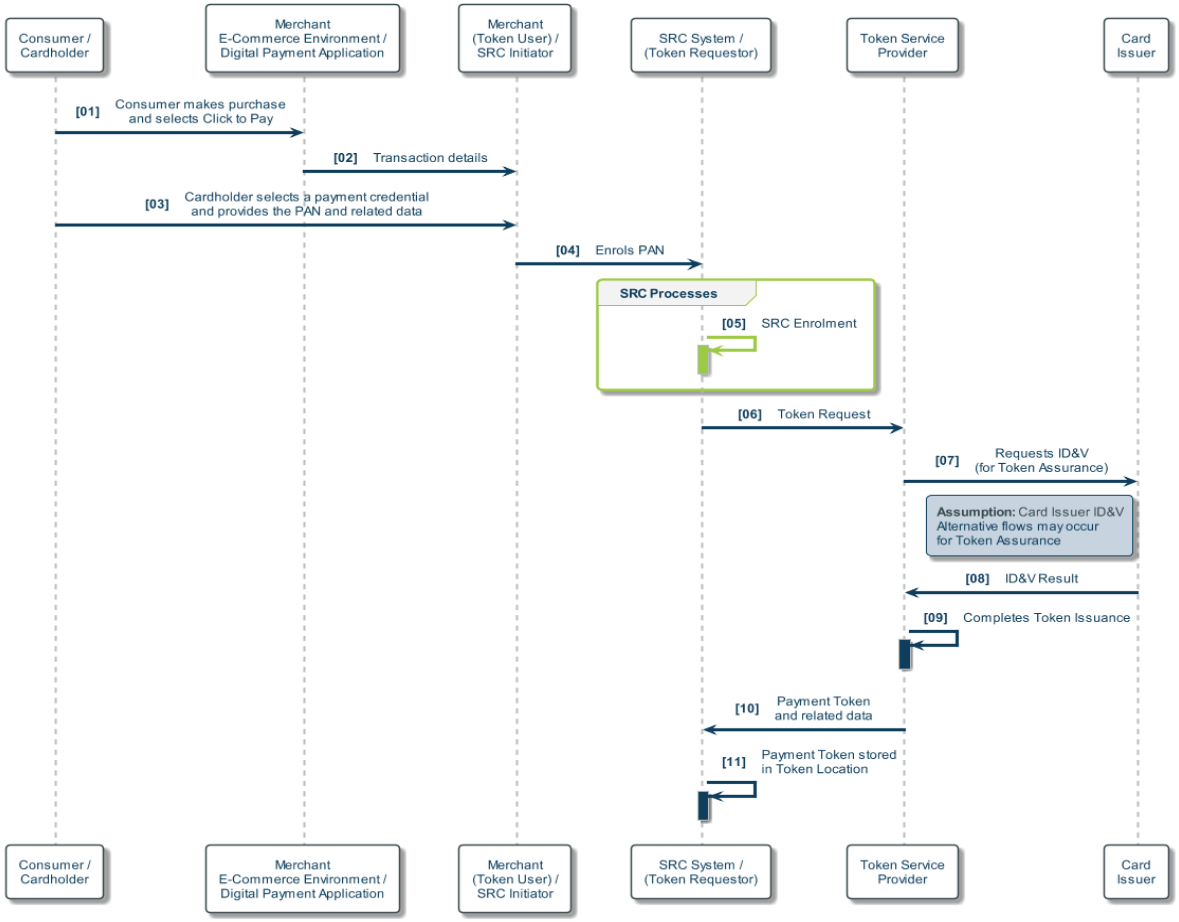
- The Token Request is initiated by the SRC System (Token Requestor) based on a request from the Merchant (Token User) / SRC Initiator

- Token Assurance and the related ID&V is performed by the Card Issuer, resulting in the Token Assurance Method value being set to one of the Card Issuer Token Assurance Method Categories
- The designated Token Location is 07 Temporary storage

Example Issuance Flow

Figure 11.3 shows an example transaction flow, with numbered steps which are explained following the figure. Note that the SRC-specific functions (e.g. enrolling the PAN) are not shown as individual steps.

Figure 11.3: SRC Guest Checkout – Example Issuance Flow



01. The Consumer makes a purchase from the Merchant e-commerce environment / Digital Payment Application and initiates the SRC checkout process by selecting Click to Pay
02. The Digital Payment Application provides details of the transaction to the SRC Initiator
03. The Cardholder selects a payment credential and provides the PAN and related data as required by the SRC Initiator
04. The SRC Initiator enrols the PAN in the SRC System

05. The SRC System undertakes a variety of SRC-specific actions to enrol the PAN
06. The SRC System (Token Requestor) uses the enrolled PAN and related data to initiate a Token Request to the Token Service Provider, using its Token Requestor ID
07. The Token Service Provider carries out Token Assurance and requests that the Card Issuer undertakes ID&V
08. The Card Issuer responds to the Token Service Provider with its ID&V result
09. The Token Service Provider completes Token Issuance (this is on the assumption that the ID&V result indicates Card Issuer approval)
10. The Token Service Provider delivers a Payment Token and related data to the SRC System (Token Requestor) as part of Token Provisioning
11. The SRC System (Token Requestor) stores the Payment Token and its related data in the designated Token Location

11.3.6 Transaction Flow

The following preconditions and assumptions apply to this specific flow.

Transaction Flow Preconditions

There are no additional preconditions that apply to this specific flow.

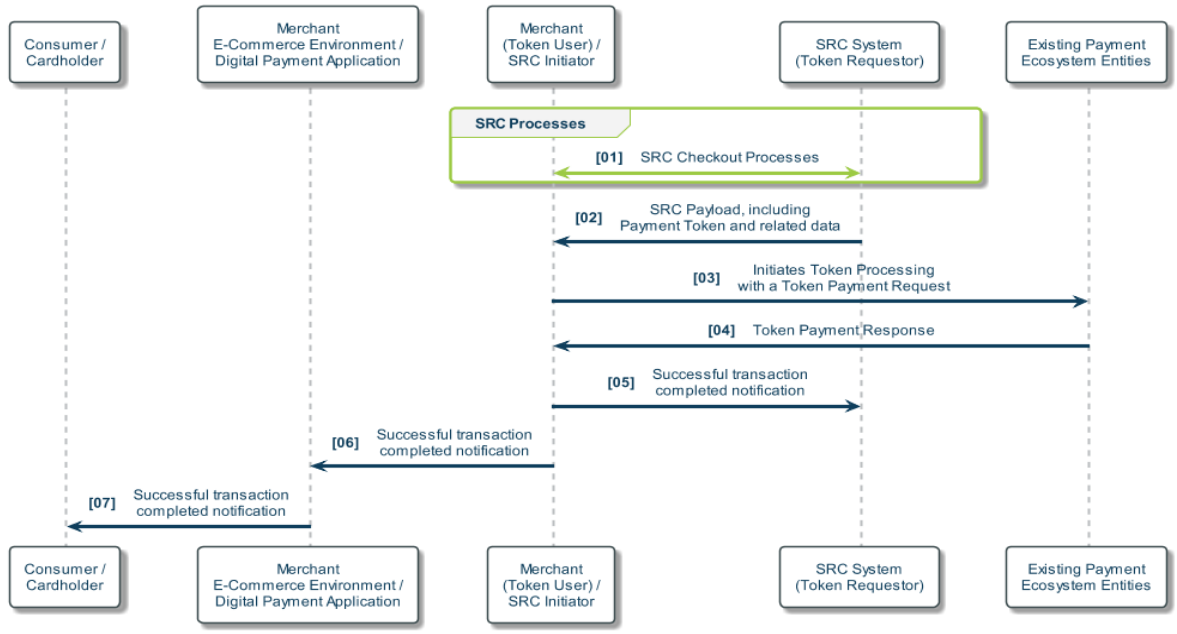
Transaction Flow Assumptions

- Dynamic Data, provided by the SRC System, is used
- The Merchant (Token User) / SRC Initiator initiates Token Processing using the Payment Token and related data (which includes the provided Dynamic Data) via existing relationships with the existing payment ecosystem entities

Example Transaction Flow

Figure 11.4 shows an example transaction flow, with numbered steps which are explained following the figure. Note that the SRC-specific functions (e.g. presenting the Digital Card for confirmation) are not shown as individual steps.

Figure 11.4: SRC Guest Checkout – Example Transaction Flow



01. The SRC System undertakes a variety of SRC-specific actions related to SRC checkout and SRC Payload creation.
02. SRC System (Token Requestor) returns an SRC Payload (which includes the Payment Token and related data) to the Merchant (Token User) / SRC Initiator
03. The Merchant (Token User) / SRC Initiator initiates Token Processing by sending a Token Payment Request
04. The Merchant (Token User) / SRC Initiator receives a Token Payment Response as a result of successful PAN Authorisation by the Card Issuer
05. The SRC Initiator provides the results to the SRC System
06. The Merchant (Token User) / SRC Initiator provides the results to the Merchant e-commerce environment / Digital Payment Application
07. The Cardholder receives confirmation from the Merchant e-commerce environment / Digital Payment Application that the transaction was successful

Token Processing Considerations

Table 11.10 (Token Processing Characteristics) and Table 11.11 (Payment Token Characteristics) show the typical Token Control Fields (Table 11.10) which are used as part of the Token Domain Restriction Controls (Table 11.11). In these specific use case flows, the following Token Control Fields are used:

- POS Entry Mode: has an expected value that indicates an e-commerce transaction, used to constrain the Payment Token to a specific Token Presentment Mode

- Merchant identifier(s): represents the specific Merchant using the Payment Token for this transaction, used to constrain the Payment Token to this specific Merchant
- Dynamic Data: secures this transaction

As well as the methods described in Section 8.1.3 Payment Account Reference Data (PAR Field and PAR Enquiry), PAR Data may be available to the Merchant:

- As part of the related data provided by the SRC System with the Payment Token

11.3.7 Variations of User Experience

Minor variations may occur for this use case due to possible differences related to whether the Consumer is interacting with a website or Merchant application, which will be Merchant and / or implementation specific.

11.4 EMV® 3-D Secure

EMV® 3-D Secure (EMV 3DS) is a messaging protocol that promotes frictionless Consumer authentication and enables Consumers to authenticate themselves with their Card Issuers when making card-not-present e-commerce purchases. The additional security layer helps prevent unauthorised card-not-present transactions and helps protect the Merchant from exposure to card-not-present fraud.

The three domains consist of the Merchant / Acquirer domain, Issuer domain, and the interoperability domain (e.g. payment systems). EMVCo has created, owns and manages the EMV® 3-D Secure – Protocol and Core Functions Specification and related industry materials. For additional details on EMV 3DS please refer to the relevant EMV 3DS specifications.

As with all EMV Specifications, EMV 3DS is designed to enable card-based payment products to work together seamlessly and securely worldwide. EMV 3DS implementations support transactions based on PAN, but may additionally integrate with payments ecosystems that have implemented Payment Tokenisation, so that both Payment Tokenisation and EMV 3DS are used to support a single use case.

The following use case example shows a combination of Payment Tokenisation and EMV 3DS:

- Card-On-File E-Commerce with EMV 3DS Payment Authentication

In this use case example, the Cardholder interacts with both Payment Tokenisation participants and EMV 3DS components, to complete an e-commerce transaction. The combination of Payment Tokenisation and EMV 3DS components provide an example of how to support the use case.

The EMV 3DS specifications provide details on communication between EMV 3DS components. These are simplified in this use case example in order to highlight the intersection between EMV 3DS and Payment Tokenisation.

11.5 Card-On-File E-Commerce with EMV 3DS Payment Authentication

This use case provides details for a Card-On-File E-Commerce transaction, as described in the Card-On-File E-Commerce use case (see Section 8.5) with the addition of a browser- or app based EMV 3DS Payment Authentication flow being performed to verify that the person performing the transaction is the valid Cardholder. The Merchant will determine when to use the EMV 3DS Payment Authentication flow based on payment ecosystem or regulatory requirements.

Additional information can be provided to the Access Control Server using additional Payment Token data elements. These are available when using either EMV 3DS v2.1 or v2.2 with the EMV® 3-D Secure Payment Token Message Extension, or when using EMV 3DS v2.3 or above. This additional information about the Payment Token and other Payment Tokenisation related data can assist with the Cardholder Payment Authentication process.

This use case example covers:

- Token Presentment and Token Processing preceded by an EMV 3DS Payment Authentication

11.5.1 Use Case Overview – Problems Addressed & User Experience

This is essentially the same use case as Card-on-File E-Commerce section 8.5 but expanded to include the use of EMV 3DS to demonstrate the capabilities of the combination of the two EMV technologies.

The use of EMV 3DS addresses the need (or possible requirement) to authenticate that the person conducting the transaction via the Merchant's e-commerce environment, is the Cardholder for the selected payment credential. This uses Payment Authentication which EMV 3DS supports within the EMV 3DS core specification.

When the additional Payment Token data elements are provided, the Access Control Server can better evaluate the risk of the transaction by linking the Merchant, the PAN and Cardholder information. The additional information may avoid the need for a Cardholder Challenge or "step-up authentication" process, which adds friction into the overall process. Enabling the best possible risk decisions supports the Card Issuer, Merchant and Cardholder.

The additional information may help confirm that the Payment Token was issued specifically for the Merchant at which the transaction is taking place and for the specific Cardholder's use at that Merchant. This may be combined with other data, such as the identity of a Consumer

Device being used for the transaction, which the Card Issuer can link to the Cardholder. Such a combination of data could result in an increase in the Card Issuer's confidence in the authentication of the Cardholder.

11.5.2 Use Case Relationships and Functions

Entities that participate in Payment Tokenisation and EMV 3DS may perform functions associated with roles described in each specification to enable a variety of use cases. Table 11.13 describes the relationships between the Payment Tokenisation roles and EMV 3DS components and the functions that they carry out for this use case example.

Table 11.13: Card-On-File E-Commerce with EMV 3DS Payment Authentication – Relationships

Tokenisation Role	EMV 3DS Component	Function (Token / EMV 3DS)
Merchant (Token Requestor)	3DS Requestor	• Register for Token Requestor ID (Token) • Request Payment Token (Token) • Provide e-commerce checkout (EMV 3DS) • Submit transaction details to 3DS Server (EMV 3DS)
N/A	3DS Server	• As defined in the EMV 3DS specifications
N/A	Directory Server	• As defined in the EMV 3DS specifications
Card Issuer	Access Control Server	• Risk decisioning via Access Control Server (EMV 3DS)
Token Service Provider	N/A	• As defined in the Technical Framework

11.5.3 Use Case Characteristics

These are unchanged from Card-On-File E-Commerce use case (see Section 8.5.3).

11.5.4 Payment Token Characteristics

These are unchanged from Card-On-File E-Commerce use case (see Section 8.5.4).

11.5.5 Issuance Flow

This is unchanged from Card-On-File E-Commerce use case (see Section 8.5.5).

11.5.6 Transaction Flow

The following preconditions and assumptions apply to this specific flow.

Transaction Flow Preconditions

The Payment Token preconditions that apply to this specific flow follow on from the Issuance flow in the Card-On-File E-Commerce use case (see Section 8.5.5):

- The Merchant operates an e-commerce environment which can either be web-based or application-based
- The Consumer has an account with the Merchant
- The Cardholder added a PAN to the account with the Merchant
- The Merchant (Token Requestor) was issued with a Payment Token for the PAN

Transaction Flow Assumptions

- The Payment Token is stored by the Merchant (Token Requestor) and is identified in the Merchant e-commerce environment by the last four digits of the underlying PAN and digital card art
- The Consumer has accessed the account via the Merchant e-commerce environment
- The Consumer selects a payment credential stored in the account which has an affiliated Payment Token
- A Token Cryptogram is used and it is sourced by the Merchant (Token Requestor) from the Token Service Provider

Payment Authentication Flow Preconditions

- The additional Payment Token data elements are available.

Payment Authentication Flow Assumptions

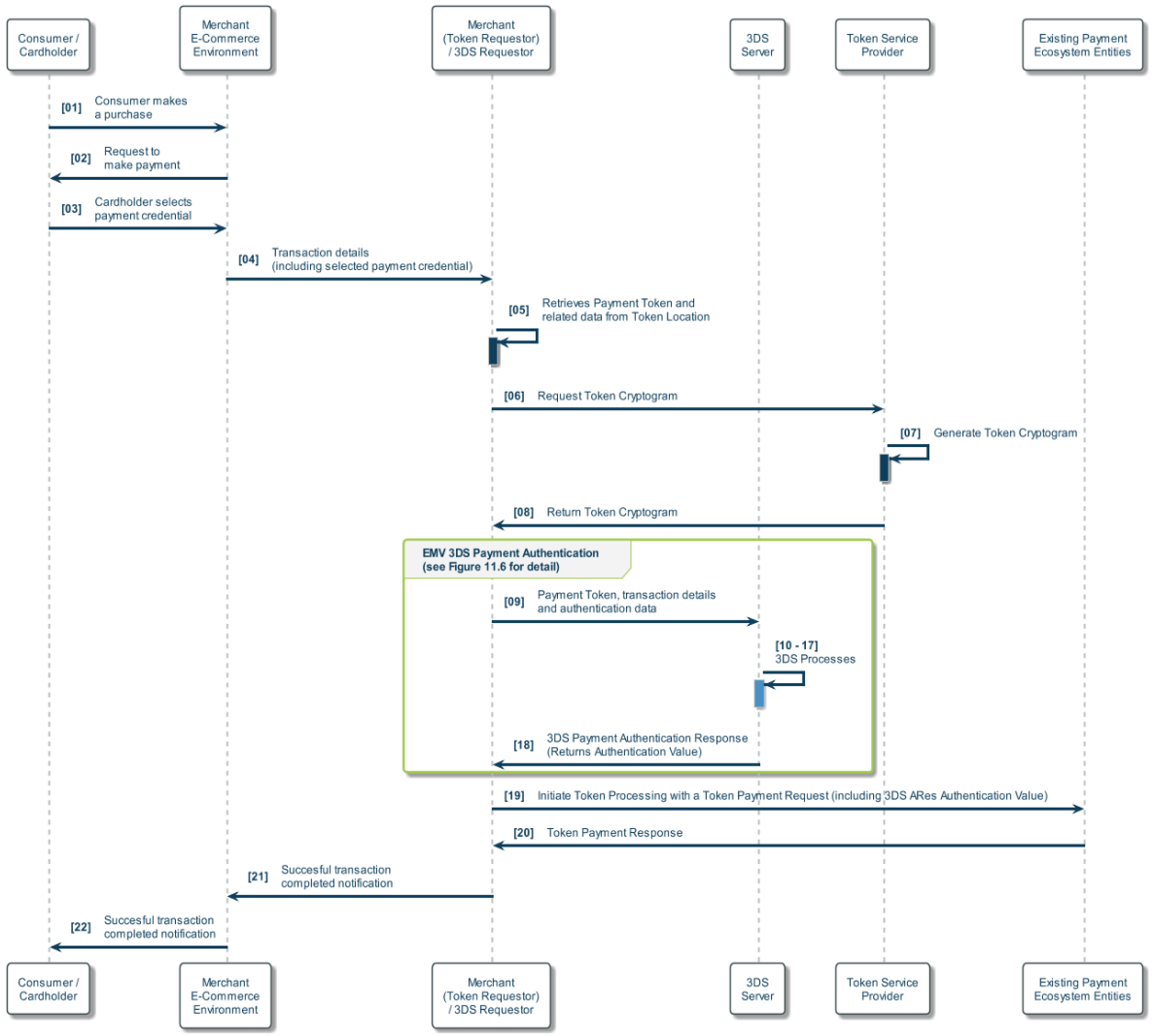
- The Token Service Provider is able to provide the additional Payment Token data elements
- Token Assurance Method is Category 12 Card Issuer Interactive Cardholder Authentication - 2 Factor
- The Token Requestor ID is recognised and identifies the Merchant for whom the Payment Authentication request (AReq) is being made as the same entity as the Merchant (Token Requestor)
- The Token Service Provider responds with confirming that the Token Cryptogram is valid / verified

- The Directory Server populates the Token Cryptogram Validity Indicator with a value of 01 – Verified, based on the response received from the Token Service Provider
- The Token Service Provider responds with the Token Status Indicator value that confirms the Payment Token is valid / active
- The Access Control Server recognises the Consumer Device ID from which the e-commerce transaction is being made as a Consumer Device linked to the Cardholder.

Example Transaction Flow

Figure 11.5 shows an example transaction flow, with numbered steps which are explained following the figure. The specific EMV 3DS Payment Authentication steps summarised in the box in Figure 11.5 are shown in Figure 11.6.

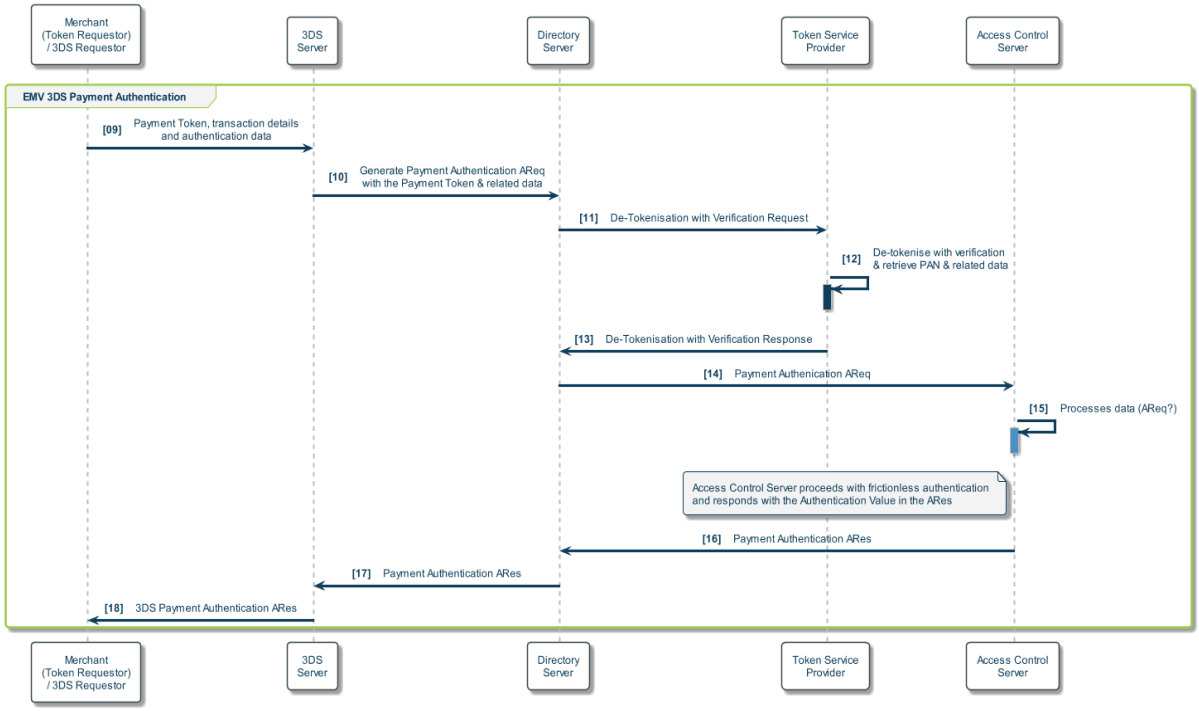
Figure 11.5: Card-On-File E-Commerce with EMV 3DS Payment Authentication – Example Transaction Flow



01. The Consumer makes a purchase from the Merchant e-commerce environment and initiates the checkout process
02. The Merchant e-commerce environment initiates the request for a payment credential to be selected
03. The Cardholder selects a previously stored payment credential from the account via the Merchant e-commerce environment
04. The Merchant e-commerce environment provides details of the transaction, including the selected payment credential, to the Merchant
05. The Merchant (Token Requestor) retrieves the Payment Token and related data from the Token Location
06. The Merchant (Token Requestor) uses the Payment Token and relevant transaction information to request a Token Cryptogram from the Token Service Provider
07. The Token Service Provider processes the request and generates a Token Cryptogram
08. The Token Service Provider delivers the Token Cryptogram to the Merchant (Token Requestor)
09. The Merchant (Token Requestor) / 3DS Requestor sends the Payment Token, its related data (including the Token Cryptogram) and all relevant transaction data to the 3DS Server for the generation of a Payment Authentication AReq message
10. Steps 10 – 17 are explained in Figure 11.6.
18. The 3DS Server returns the ARes including the Authentication Value to the Merchant (Token Requestor) / 3DS Requestor
19. The Merchant initiates Token Processing by sending a Token Payment Request and includes the Authentication Value received from the EMV 3DS Payment Authentication process outcome
20. The Merchant receives a Token Payment Response as a result of successful PAN Authorisation by the Card Issuer
21. The Merchant provides the results to the Merchant e-commerce environment
22. The Cardholder receives confirmation from the Merchant e-commerce environment that the transaction was successful

Figure 11.6 shows the specific EMV 3DS Payment Authentication steps which were summarised in the box in Figure 11.5, with the numbered steps explained following the figure.

Figure 11.6: Card-On-File E-Commerce with EMV 3DS Payment Authentication – Additional 3DS Steps



01. Steps 01 – 08 are shown in Figure 11.5.

09. The Merchant (Token Requestor) / 3DS Requestor sends the Payment Token, its related data (including the Token Cryptogram) and all relevant transaction data to the 3DS Server

10. The 3DS Server uses the relevant data to generate the Payment Authentication AReq message and sends it to the appropriate Directory Server

11. The Directory Server processes the AReq and sends a De-tokenisation with Verification request to the Token Service Provider, including the Payment Token, its related data and the additional Payment Token data elements

12. The Token Service Provider processes the De-tokenisation with Verification request, using the information contained in the additional Payment Token data elements, such as TAM, TRID, Token Status and Token Cryptogram verification outcome

13. The Token Service Provider provides a De-tokenisation with Verification response to the Directory Server, including the PAN, the additional Payment Token data elements (such as Token Cryptogram verification outcome, TAM, TRID, Token Status) and any other relevant data

14. The Directory Server sends the Payment Authentication AReq to the Access Control Server, including all the relevant data received from the Token Service Provider

15. The Access Control Server processes the Payment Authentication AReq using all the data available, including the additional Payment Token related data elements, determining that

the Cardholder can be positively authenticated, no Challenge is required and an Authentication Value can be generated

16. The Access Control Server returns an ARes message to the Directory Server, confirming successful authentication and including the Authentication Value
17. The Directory Server returns the ARes, including the Authentication Value, to the 3DS Server
18. The 3DS Server returns the ARes, including the Authentication Value, to the Merchant (Token Requestor) / 3DS Requestor

Variations of User Experience

The Cardholder may experience fewer Payment Authentication Challenge requests.

12 Payment Account Reference

Payment Account Reference (PAR) is defined in Section 7 of the Technical Framework with additional information given in the PAR White Paper. In addition to the use of PAR with Payment Tokenisation, the PAR Field and PAR Data may also be included in PAN-based transactions in which Payment Token(s) have been previously generated for the PAN. Feedback suggests there is also inherent value in propagating PAR Data for PANs in situations where Payment Tokens have not yet been generated for such PANs. This enables the support of multiple use cases in advance of the implementation of Payment Tokenisation and avoids the need to develop redundant / non-interoperable solutions to address the same problem.

The use case examples presented in A Guide to Use Cases (see Section 8 Use Case Examples) define the relationships between the roles within the Payment Tokenisation ecosystem and provide issuance and transaction flows for specific scenarios. In contrast, this Section highlights the possible uses of PAR, showing how PAR Data can be used as a linkage mechanism to simplify activities when the transaction mix changes from PAN-only based transactions to a transaction mix that includes both PAN-based and Payment Token-based transactions. This is possible since, as defined in Section 7 of the Technical Framework, PAR Data is the same for a PAN and all affiliated Payment Tokens.

Two PAR use case examples are presented to illustrate the use of PAR as a linkage mechanism:

- Transit Open Loop Payments (Section 12.1)
- Merchant Loyalty Schemes (Section 12.2)

12.1 Transit Open Loop Payments

For the purposes of this use case example, an “open loop” payment is one made using a payment credential from a Card Issuer using a Payments System and Payment Network(s) that is designed to work at all Merchants which support that Payment System. This is in contrast to a “closed loop” payment where a Merchant has a payment solution which only works within the Merchant’s own system.

The use of open loop payments for transit has advantages but also introduces the need for adjustments to operating processes and systems for Merchants which are transit operators. This use case example illustrates how PAR Data can be used as a linkage mechanism by transit operators to manage a number of potential situations that arise as a result of allowing open loop payments (for example, calculating the correct fare in a “pay as you go” scenario).

The following preconditions apply:

- A transit rider enters the transit system using an open loop payment credential
- On exiting the transit system, the transit rider uses the same open loop payment credential, but presented in different manner
- Entry and exit are at contactless-enabled entry / exit points

On many existing transit systems using open loop payments, the scenario described above will result in the transit operator treating the entry and exit as two separate journeys, unaware that they have been made by the same transit rider using different payment credentials.

This use case example uses example entry and exit transaction flows to illustrate how PAR Data can be used to link the entry and exit to the same transit rider / journey. Two sequences of entry and exit flows are given:

- Entry / Exit with PAN And Payment Token (Section 12.1.1)
- Entry / Exit with Different Payment Tokens (Section 12.1.2)

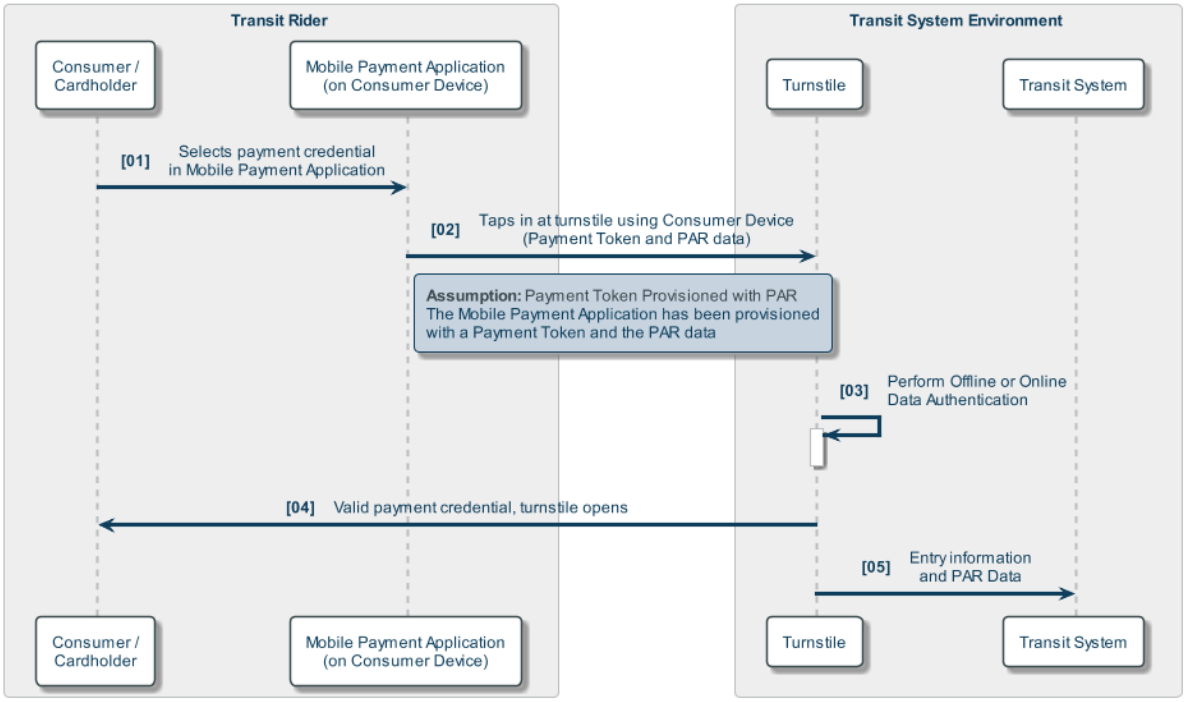
12.1.1 Entry / Exit with PAN And Payment Token

The following assumptions apply to these entry / exit flows:

- The open loop payment credential used to enter and exit the transit system is represented by both a:
  - Contactless-enabled payment card which presents a PAN to the transit system
  - Consumer Device with a mobile payment application provisioned with a Payment Token (where the underlying PAN is the same as the contactless-enabled payment card) which is presented to the transit system (see Proximity at Point of Sale use case example, Section 8.2)
- Both the contactless card and Consumer Device / mobile payment application have been personalised with PAR Data such that it is provided in Tag 9F24 data exchanges with contactless-enabled entry / exit points

The entry flow is illustrated in Figure 12.1 with numbered steps which are explained following the figure.

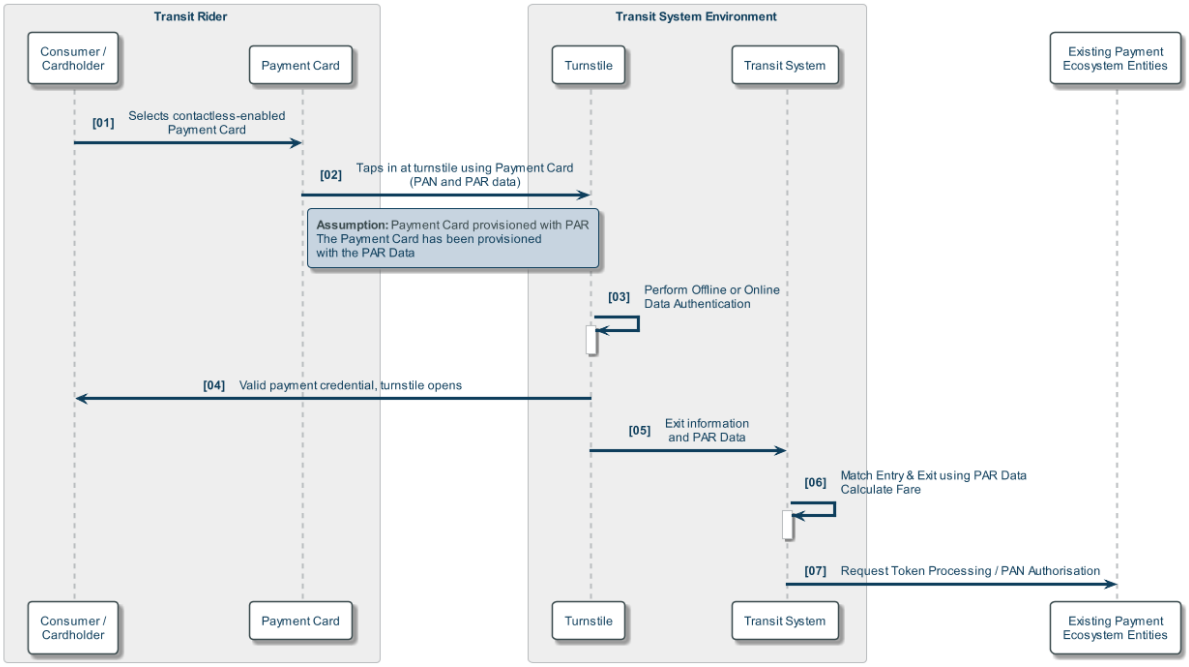
Figure 12.1: Example Entry Flow with PAR Data Transfer



01. The transit rider selects a payment credential from the Mobile Payment Application on the transit rider's Consumer Device
02. The transit rider enters the transit system using the Consumer Device at a contactless-enabled entry point (turnstile), which receives the PAR data in Tag 9F24 as part of the information passed during the contactless tap
03. The turnstile verifies the authenticity of the payment credential typically using Online or Offline Data Authentication (ODA)
04. Following verification, the turnstile opens, allowing the transit rider to enter
05. The turnstile passes the entry information, including the PAR Data, to the transit system

The exit flow is illustrated in Figure 12.2.

Figure 12.2: Example Exit Flow with PAR Data Transfer and Matching



01. The transit rider selects a contactless-enabled Payment Card (for example, the Consumer Device using to enter the transit system ran out of power during the journey, so the transit rider uses the corresponding payment card to exit the transit system)
02. The transit rider exits the transit system, using the Payment Card at another contactless-enabled exit point (turnstile), which receives the PAR data in tag 9F24 as part of the information passed during the contactless tap
03. The turnstile verifies the authenticity of the payment credential typically using Online or Offline Data Authentication (ODA)
04. Following verification, the turnstile opens, allowing the transit rider to exit
05. The turnstile passes the exit information, including the PAR Data, to the transit system
06. Since the PAR Data is the same as that received at the start of the transit rider's journey, the transit system can use it to link the entry and exit as a single journey. With this information, for example, the transit system can correctly calculate the appropriate fare
07. The transit system initiates Token Processing or PAN Authorisation for the correct fare amount.

Without the PAR Data, the transit system would need to utilise other proprietary systems and processes to link the PAN provided at entry to the Payment Token provided at exit. Alternatively, the transit system may be unable to link entry and exit which could lead, for example, to the transit rider being charged twice for the same journey.

12.1.2 Entry / Exit with Different Payment Tokens

The following assumptions apply to these entry / exit flows:

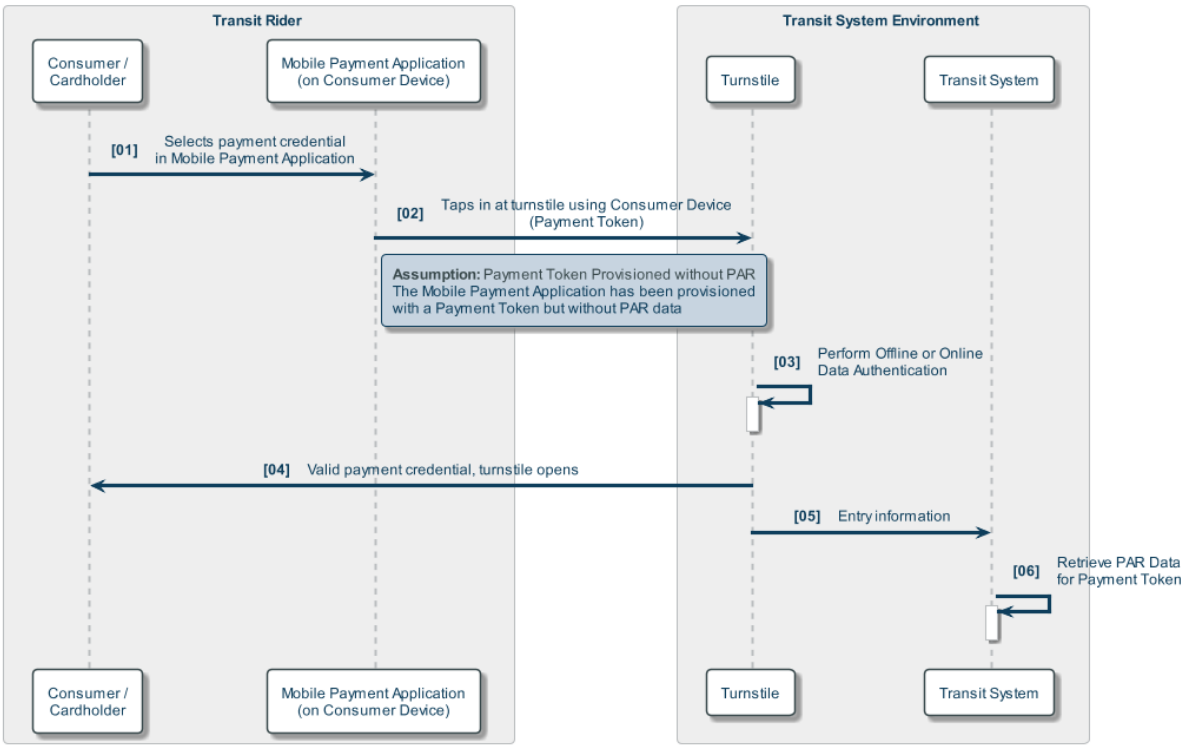
- The transit rider has a:
  - Consumer Device with a mobile payment application, provisioned with a Payment Token (with an underlying PAN from an open loop payment credential) which is presented to the transit system (see Proximity at Point of Sale use case example, Section 8.2)
  - Wearable Consumer Device provisioned with a different Payment Token (with the same underlying PAN)
- Neither the Consumer Device / mobile payment application nor the wearable Consumer Device have been personalised with PAR Data

In this example, since PAR data is not presented to the transit system on entry / exit, the transit system can retrieve the PAR data by:

- Making a PAR Enquiry request, via the Acquirer or other service provider
- Initiating an account status inquiry or other low value Token Payment Request, receiving the PAR data in the Token Payment Response message
- Looking up the PAR data from within its own records if the transit rider has used the same Payment Token before and the transit systems stores Payment Token / PAR data

The entry flow is illustrated in Figure 12.3 with numbered steps which are explained following the figure.

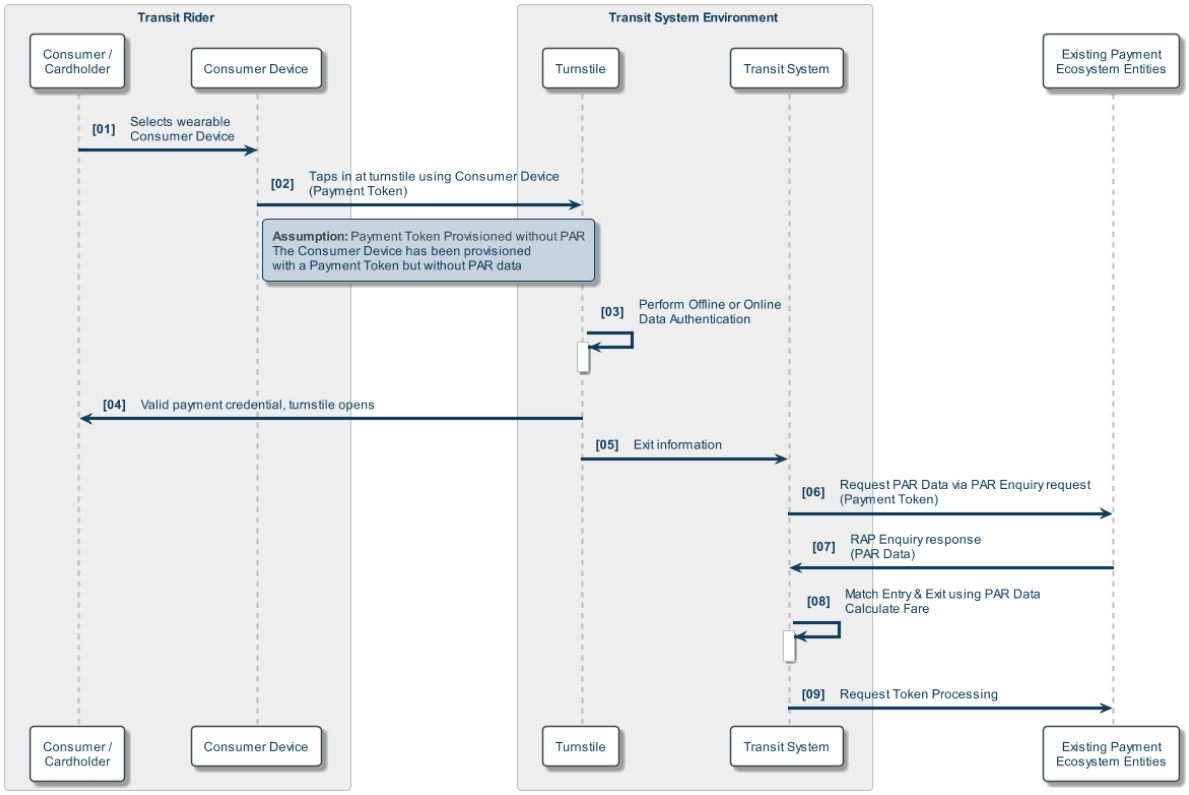
Figure 12.3: Example Entry Flow with PAR Data Retrieval



08. The transit rider selects a payment credential from the Mobile Payment Application on the transit rider's Consumer Device
09. The transit rider enters the transit system using the Consumer Device at a contactless-enabled entry point (turnstile), which receives the Payment Token as part of the information passed during the contactless tap
10. The turnstile verifies the authenticity of the payment credential, typically using Offline or Online Data Authentication (ODA)
11. Following verification, the turnstile opens, allowing the transit rider to enter
12. The turnstile passes the entry information to the transit system
13. The transit system retrieves the PAR Data for the Payment Token (in the example, the transit system has previously received the Payment Token and has already retrieved and stored the PAR Data)

The exit flow is illustrated in Figure 12.4.

Figure 12.4: Example Exit Flow with PAR Data Retrieval and Matching



01. The transit rider selects a wearable Consumer Device which is provisioned with a single Payment Token
02. The transit rider exits the transit system using the wearable Consumer Device with another contactless-enabled exit point (turnstile) which receives the Payment Token as part of the information passed during the contactless tap
03. The turnstile verifies the authenticity of the payment credential typically using Online or Offline Data Authentication (ODA)
04. Following verification, the turnstile opens, allowing the transit rider to exit
05. The turnstile passes the exit information to the transit system
06. The transit system retrieves the PAR Data for the Payment Token, in this example by using the Payment Token to make a PAR Enquiry request to the Acquirer or other service provider
07. The PAR Data is returned in the PAR Enquiry response
08. Since the PAR Data is the same as that received at the start of the transit rider's journey, the transit system can use it to link the entry and exit as a single journey. With this information, for example, the transit system can correctly calculate the appropriate fare
09. The transit system initiates Token Processing for the correct fare amount.

12.2 Merchant Loyalty Schemes

Merchants may implement loyalty schemes to support customer retention and increase ongoing business across a variety of channels (e.g. in-store, e-commerce). Sometimes these are implemented in conjunction with a payment credential or simply managed as part of an account relationship with a Consumer. In either example, the Merchant will typically link payment credential(s) to the loyalty scheme account so that tracking of Consumer / Cardholder spending can be implemented to allow the recognition and crediting of the loyalty scheme benefits to the Consumer.

This use case example illustrates how PAR Data can support a Merchant loyalty scheme when the Consumer uses different payment methods (e.g. payment card, Consumer Device with a mobile payment application) all linked to the same loyalty account. The following assumptions apply:

- The loyalty scheme applies only to transactions occurring at the Merchant which operates the loyalty scheme
- The Consumer / Cardholder has a loyalty account with the Merchant and has registered a payment credential
- The Merchant uses this payment credential to enable tracking of transactions so that the Consumer can receive the loyalty scheme benefits / rewards
- The payment credential is represented by a:
    - Contactless-enabled payment card which presents a PAN
    - Consumer Device with a mobile payment application provisioned with a Payment Token (see Proximity at Point of Sale use case example, Section 8.2)
    - Wearable device provisioned with a different Payment Token (affiliated with the same underlying PAN)
- The Merchant has received and stored the PAR Data for the payment credential
- The stored PAR Data is available to the Merchant's internal systems and loyalty scheme so that where the PAR Data is linked to a transaction, that transaction data can be applied to the specific loyalty scheme account

12.2.1 In-Store Transactions Example

In this example, the transaction occurs in-store as a Proximity at Point of Sale transaction using a Consumer Device (see Proximity at Point of Sale use case example, Section 8.2.6). The Merchant can receive the PAR Data in any of the supported ways described under Token Processing Considerations in Section 8.2.6 and use this to link the transaction to the loyalty account of the Consumer / Cardholder.

Similarly, if the in-store transaction was conducted with a wearable device, although the Merchant will receive a different Payment Token, the PAR Data will be the same, allowing the Merchant to link the transaction to the loyalty account of the Consumer / Cardholder.

Finally, the in-store transaction could be made by the payment card. Although this would present a PAN to the Merchant, the PAR Data will still be the same. It is this consistent PAR Data which provides the linkage that the Merchant needs to link all the transactions to the correct loyalty scheme account.

12.2.2 E-Commerce Transactions Example

In this example, a transaction occurs on the Merchant's e-commerce environment. The following additional assumptions apply:

- The Cardholder has registered the payment credential with the Merchant's e-commerce environment
- The Merchant has chosen not to store PAN in the Card-On-File database and instead has made a Token Request and subsequently stored the Payment Token that was issued in response to the Token Request (see the Card-On-File E-Commerce use case, Section 8.5.5)

The transaction follows the same flows as for the Card-On-File E-Commerce use case, Section 8.5.6. The Merchant may receive the PAR Data in any of the supported ways described under Token Processing Considerations in Section 8.5.6. When the same Consumer / Cardholder uses the Merchant's e-commerce environment and uses the payment credential that was stored and connected with the loyalty scheme account, the PAR Data will enable the appropriate linkage between this e-commerce transaction and the loyalty scheme account of the Consumer / Cardholder.

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