EMV®

Payment Tokenisation

A Guide to Use Cases

Version 1.0

June 2019

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 1.0

This is the first version of this document.

Contents

1 Introduction 7

1.1 Scope 7

1.2 Overview 7

1.3 Audience 8

1.4 References 8

1.4.1 Published EMVCo Documents 8

1.5 Definitions 9

1.6 Notational Conventions 9

1.6.1 Abbreviations 9

1.6.2 Terminology and Conventions 9

1.7 Further Information 10

2 Token Programme Participants 11

2.1 Card Issuers 11

2.2 Token Service Providers 11

2.3 Token Requestors 12

3 Relationship Model Descriptions 14

3.1 Relationship Model Diagram 14

3.2 Understanding the Relationship Model Diagram 16

4 Token Issuance and Token Provisioning 17

4.1 Token Issuance and Token Provisioning Relationships and Functions 17

4.1.1 A. Cardholder – Authorised Entity 18

4.1.2 A. Cardholder – Merchant 18

4.1.3 A. Token User – Token Requestor 18

4.1.4 A. Token Service Provider – Token Requestor 18

4.1.5 A. Card Issuer – Token Service Provider 18

4.1.6 A. Card Issuer – Cardholder 19

4.1.7 B. Token Service Provider – Token Requestor 19

4.1.8 B. Cardholder – Token Requestor 19

4.1.9 Variations to Relationships 19

4.2 Token Issuance Characteristics 19

4.3 Token Provisioning Characteristics 20

5 Token Presentment 21

5.1 Token Presentment Relationships and Functions 21

5.1.1 C. Consumer – Merchant 22
5.1.2 C. Cardholder – Authorised Entity 22
5.1.3 C. Token User – Token Requestor 22
5.1.4 Variations to Relationships 22
5.2 Token Presentment Characteristics 22
6 Token Processing 24
6.1 Token Processing Relationships and Functions 24
6.1.1 D. Merchant – Existing Payment Ecosystem Entities 25
6.1.2 D. Authorised Entity – Existing Payment Ecosystem Entities 25
6.2 Token Processing Characteristics 25
7 Payment Token Characteristics 26
8 Use Case Examples 28
8.1 Use Case 1: Proximity at Point of Sale 29
8.1.1 Use Case Relationships and Functions 29
8.1.2 Use Case Characteristics 32
8.1.3 Payment Token Characteristics 33
8.2 Use Case 2: Shared Payment Token 34
8.2.1 Use Case Relationships and Functions: Digital Wallet 34
8.2.2 Use Case Characteristics: Digital Wallet 37
8.2.3 Payment Token Characteristics: Digital Wallet 38
8.2.4 Use Case Relationships and Functions: Third Party Service Provider 38
8.2.5 Use Case Characteristics: Third Party Service Provider 42
8.2.6 Payment Token Characteristics: Third Party Service Provider 43
8.3 Use Case 3: In-Application using a Consumer Device 44
8.3.1 Use Case Relationships and Functions 44
8.3.2 Use Case Characteristics 46
8.3.3 Payment Token Characteristics 47
8.4 Use Case 4: Card-On-File E-Commerce 48
8.4.1 Use Case Relationships and Functions 48
8.4.2 Use Case Characteristics 51
8.4.3 Payment Token Characteristics 52
8.5 Use Case 5: Limited Use Payment Token 52
8.5.1 Use Case Relationships and Functions 53
8.5.2 Use Case Characteristics 55
8.5.3 Payment Token Characteristics 56

Figures

Figure 2-1: Token Service Providers 12
Figure 2-2: Token Requestors........ 13
Figure 3-1: Payment Token ecosystem relationship models........ 15
Figure 3-2: Example Roles........ 16
Figure 3-3: Example Relationships........ 16
Figure 4-1: Token Issuance (A) and Token Provisioning (B) Relationships 17
Figure 5-1: Token Presentment Relationships........ 21
Figure 6-1: Token Processing Relationships 24
Figure 8-1: Use Case 1 Relationships........ 30
Figure 8-2: Use Case 2 (Digital Wallet) Relationships 35
Figure 8-3: Use Case 2 (Third Party Service Provider) Relationships 40
Figure 8-4: Use Case 3 Relationships........ 45
Figure 8-5: Use Case 4 Relationships........ 49
Figure 8-6: Use Case 5 Relationships........ 54

Tables

Table 1-1: EMVCo References ... 8
Table 1-2: Abbreviations ... 9
Table 4-1: Token Issuance Characteristics ... 20
Table 4-2: Token Provisioning Characteristics ... 20
Table 5-1: Token Presentment Characteristics ... 23
Table 6-1: Token Processing Characteristics ... 25
Table 7-1: Payment Token Characteristics ... 26
Table 8-1: Use Case 1 Token Issuance Characteristics ... 32
Table 8-2: Use Case 1 Token Provisioning Characteristics ... 32
Table 8-3: Use Case 1 Token Presentment Characteristics ... 32
Table 8-4: Use Case 1 Token Processing Characteristics ... 33
Table 8-5: Use Case 1 Payment Token Characteristics ... 33
Table 8-6: Use Case 2 Token Presentment Characteristics ... 46
Table 8-7: Use Case 2 Token Processing Characteristics ... 47
Table 8-8: Use Case 2 Payment Token Characteristics ... 47
Table 8-9: Use Case 3 Token Issuance Characteristics ... 51
Table 8-10: Use Case 3 Token Provisioning Characteristics ... 51
Table 8-11: Use Case 3 Token Presentment Characteristics ... 51
Table 8-12: Use Case 3 Token Processing Characteristics ... 51
Table 8-13: Use Case 3 Payment Token Characteristics ... 52
Table 8-14: Use Case 4 (Digital Wallet) Token Issuance Characteristics ... 37
Table 8-15: Use Case 4 (Digital Wallet) Token Provisioning Characteristics ... 37
Table 8-16: Use Case 4 (Digital Wallet) Token Presentment Characteristics ... 37
Table 8-17: Use Case 4 (Digital Wallet) Token Processing Characteristics ... 37
Table 8-18: Use Case 4 (Digital Wallet) Payment Token Characteristics ... 38
Table 8-19: Use Case 4 (Third Party Service Provider) Token Issuance Characteristics ... 42
Table 8-20: Use Case 4 (Third Party Service Provider) Token Provisioning Characteristics ... 42
Table 8-21: Use Case 4 (Third Party Service Provider) Token Presentment Characteristics ... 43
Table 8-22: Use Case 4 (Third Party Service Provider) Token Processing Characteristics ... 43
Table 8-23: Use Case 4 (Third Party Service Provider) Payment Token Characteristics ... 43
Table 8-24: Use Case 5 Token Issuance Characteristics ... 55
Table 8-25: Use Case 5 Token Provisioning Characteristics ... 56
Table 8-26: Use Case 5 Token Presentment Characteristics ... 56
Table 8-27: Use Case 5 Token Processing Characteristics ... 56
Table 8-28: Use Case 5 Payment Token Characteristics ... 57

1 Introduction

This document, Payment Tokenisation – A Guide to Use Cases, is an informational supplement to the EMVCo Payment Tokenisation Specification – Technical Framework, (referred to in this document 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 describe 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

This document describes a limited number of use case examples, some of which are based on established EMV defined-technology:

- Use Case 1: Proximity at Point of Sale (Section 8.1)
- Use Case 2: Shared Payment Token (Section 8.2)
- Use Case 3: In-Application using a Consumer Device (Section 8.3)
- Use Case 4: Card-On-File E-Commerce (Section 8.4)
- Use Case 5: Limited Use Payment Token (Section 8.5)

These are not intended to be exhaustive or represent of all possible usage scenarios supported by the Technical Framework.

A number of use cases described in this document may vary by payment industry implementation and as a result cannot be fully described. These examples exist to show the extent and flexibility of the Technical Framework.

1.2 Overview

This document introduces relationship models which describe potential relationships between the Payment Tokenisation roles and common use case examples. The relationship models and use case examples presented are intended to provide guidance for Payment Tokenisation within existing payment ecosystem and the considerations associated with various usage scenarios. The relationship models and use case examples provided in this document are neither definitive nor exhaustive since the associated usage scenarios may require additional considerations not provided in this document. The guidance provided in this document does not supersede the Technical Framework or policies and processes defined by a Token Programme.

The relationship models are introduced in the following sections of this document.

- 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
- Section 8 Use Case Examples takes the detailed relationship models from Sections 4, 5 and 6 and applies them to specific use cases

1.3 Audience

This document 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

1.4.1 Published EMVCo Documents

Table 1-1: EMVCo References

Publication Date	Version	Publication Name
May 2019	Version 2.1	EMV® Payment Tokenisation Specification – Technical Framework

For further information, including registration procedures and Payment Tokenisation FAQs, please refer to www.emvco.com.

1.5 Definitions

For a list of defined terms used in this document, 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 this document.

Table 1-2: Abbreviations

Abbreviation	Description
MST	Magnetic Secure Transmission
NFC	Near Field Communication
PAN	Primary Account Number
POS	Point Of Sale
QR	Quick Response
TRID	Token Requestor ID

1.6.2 Terminology and Conventions

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

Usage Scenario

A specific instance of Technical Framework usage that has common, distinct characteristics such as technologies used, channel 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.

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 use cases, as well as supporting use cases not contained within the document.

2.1 Card Issuers

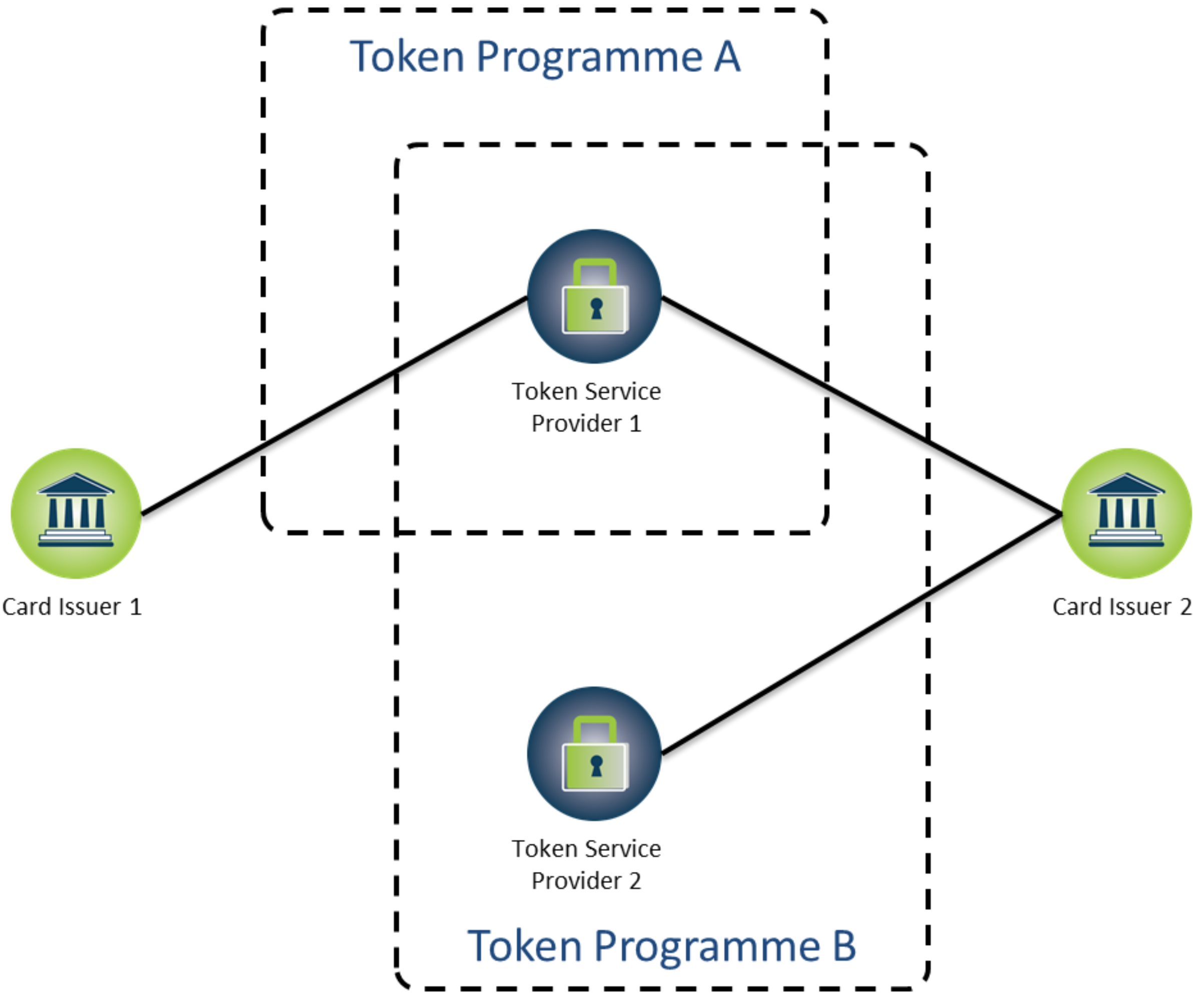
A Token Programme includes participation of one or more Card Issuers. A Card Issuer that supports multiple Payment Systems may participate in multiple Token Programmes. Card Issuers that participate in multiple Token Programmes for a given use case will support the policies, processes and registration programmes of each Token Programme for that use case.

2.2 Token Service Providers

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

Figure 2-1 shows an example of Token Service Providers participating in one or more Token Programmes and supporting one or more Card Issuers.

Figure 2-1: Token Service Providers



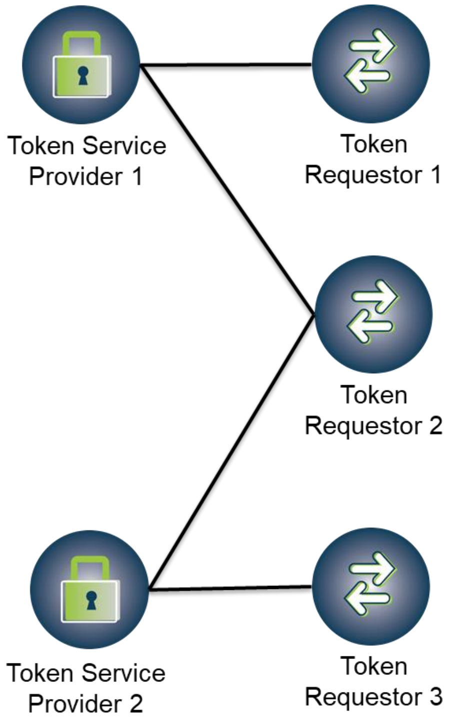
2.3 Token Requestors

Token Requestors may support a wide variety of use cases. It is responsibility of the Token Programme to provide the policies, processes and registration programmes under which Token Service Providers register Token Requestors by identifying a specific use case and Token Requestor Type.

Token Requestors 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.

An example of the possible relationships between Token Service Providers and Token Requestors is shown in Figure 2-2. For purposes of simplicity, the Token Programmes and Card Issuers shown in Figure 2-1 have not been overlaid/included in Figure 2-2.

Figure 2-2: Token Requestors



Token Requestor Type is included in the Technical Framework to ensure that in complex payment ecosystems the Token Programme and Token Service Providers can consistently characterise a Token Requestor and aids consistent registration from one Token Programme to another.

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.

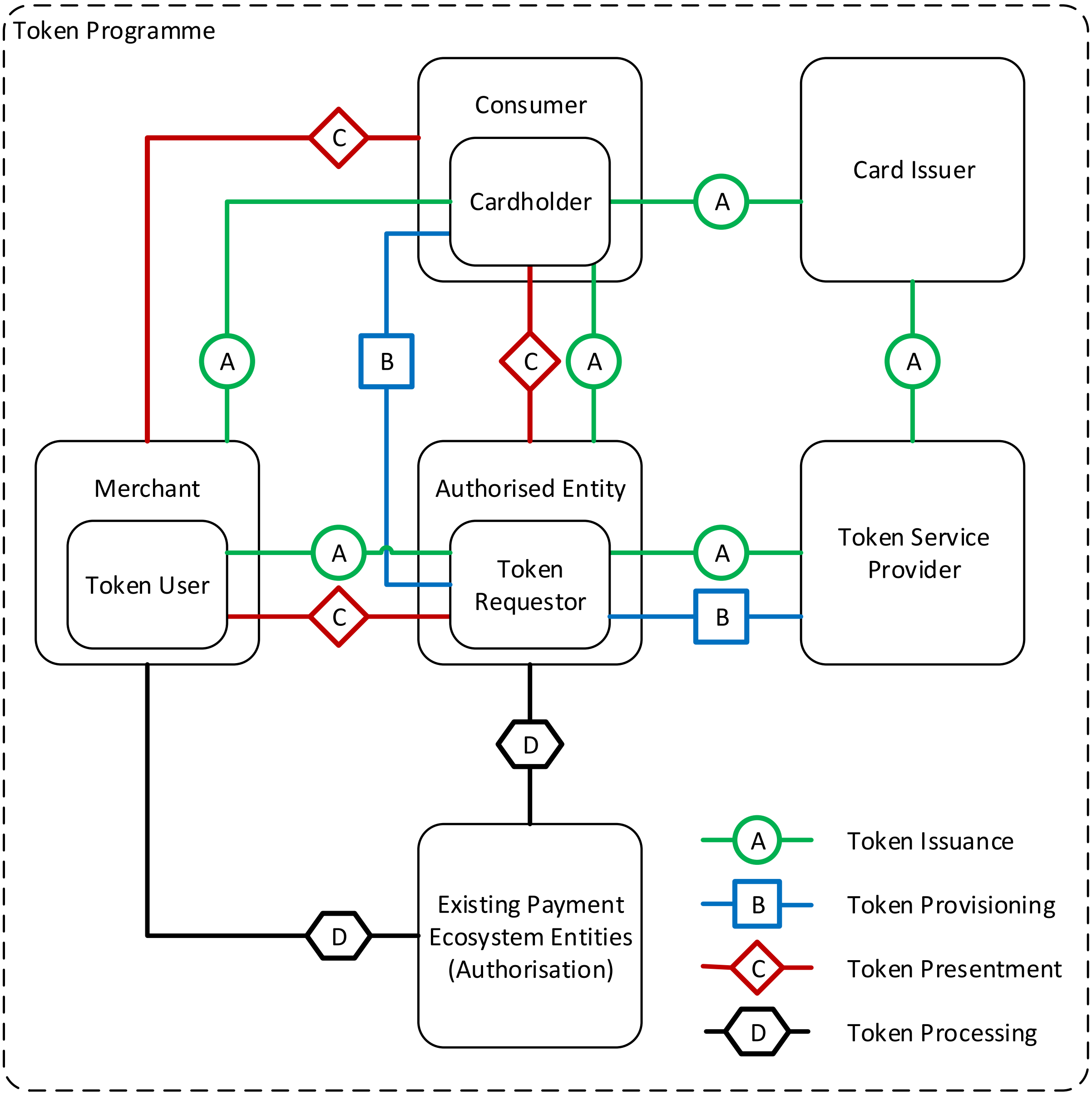
This document introduces a number of examples showing models demonstrating relationships between roles associated with Payment Tokenisation that represent the potential processes and functions performed. Some existing relationships are utilised by Payment Tokenisation, while others are specific to Payment Tokenisation. Each relationship is governed by the policies, processes and registration programmes of a specific Token Programme. Each example relationship model has a number of characteristics which have specific values 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 models



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

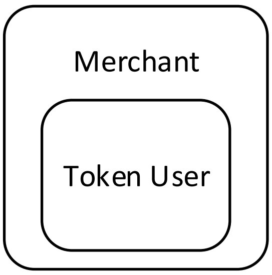
- Section 4 Token Issuance and Token Provisioning
- Section 5 Token Presentment
- Section 6 Token Processing

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.

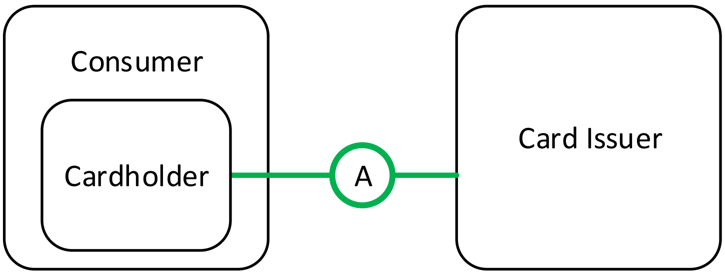
Where applicable, known entities that commonly perform the Payment Tokenisation role are included. Sometimes an additional, inner box is present within a larger, outer box. This occurs when an entity performs a specific role at some point during the process. For example, Figure 3-2 shows the Merchant / Token User. This is an example of a Merchant (shown by the outer box) fulfilling the Payment Tokenisation role of Token User (shown by the inner box).

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



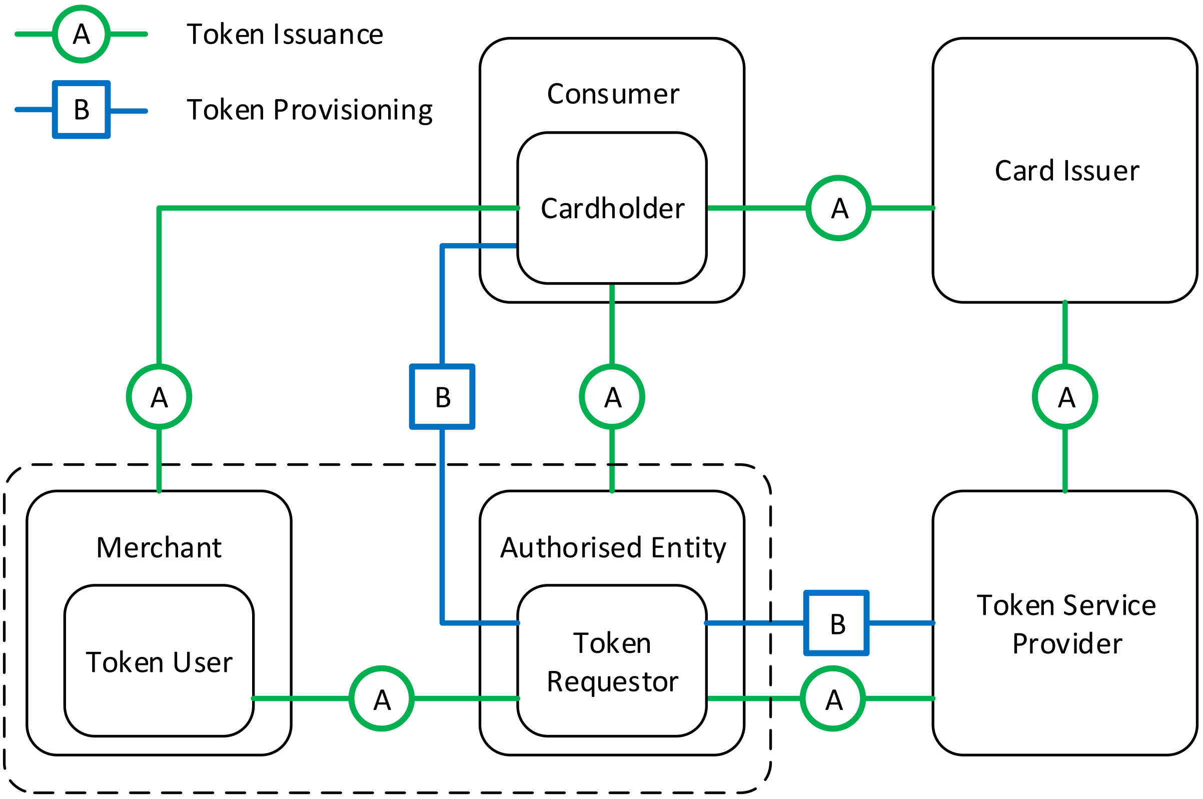
4 Token Issuance and Token Provisioning

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. 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



4.1.1 A. Cardholder – Authorised Entity

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

Function: The authorised Token Requestor initiates a Token Request to replace a PAN with a Payment Token. As part of this Token Request, The Token Requestor may involve the active participation of the Cardholder in Token Assurance as described in the Technical Framework, Section 6 Token Assurance Method.

4.1.2 A. Cardholder – Merchant

Relationship: The Cardholder may have an existing relationship with the Merchant, which is performing the role of Token User, which can be utilised for Payment Tokenisation. This relationship only applies to certain Shared Payment Token Use Cases (see Section 8.2 Use Case 2: Shared Payment Token).

Function: The Token User supplies a PAN to an authorised entity acting as a Token Requestor, which initiates a Token Request to replace the PAN with a Shared Payment Token.

4.1.3 A. Token User – Token Requestor

Relationship: The Merchant, which performs the role of Token User, has an existing relationship with the authorised entity performing the role of Token Requestor, which can be utilised for Payment Tokenisation. This relationship only applies to certain Shared Payment Token Use Cases (see Section 8.2 Use Case 2: Shared Payment Token).

Function: The authorised Token Requestor initiates a Token Request to replace a PAN (provided by the Token User) with a Shared Payment Token.

4.1.4 A. Token Service Provider – Token Requestor

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

Function: The Token Requestor initiates a Token Request with their assigned TRID. In response, the Token Service Provider evaluates the Token Request, determines the Token Domain Restriction Controls, sets the Token Assurance Method and, for successful Token Requests, issues the Payment Token in preparation for Token Provisioning.

4.1.5 A. Card Issuer – Token Service Provider

Relationship: The Card Issuer uses the Token Service Provider to provide Token Issuance and Token Provisioning services to Token Requestors for each individual Token Request as defined in the Technical Framework, Section 5.1.3 Issuance of Payment Tokens.

Function: The Token Service Provider may involve the Card Issuer in Token Assurance as described in the Technical Framework, Section 6 Token Assurance Method.

4.1.6 A. Card Issuer – Cardholder

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 as described in the Technical Framework, Section 6 Token Assurance Method.

4.1.7 B. Token Service Provider – Token Requestor

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

Function: After Token Issuance, the Payment Token and related data is delivered to the corresponding Token Location.

4.1.8 B. Cardholder – Token Requestor

Relationship: The Token Requestor extends Token Provisioning services to the Cardholder (for example to a Token Location on a Consumer Device).

Function: After Token Issuance, the Payment Token and related data is delivered to the corresponding Token Location.

4.1.9 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 Shared Payment Token Use Cases (see, for example, Section 8.2 Use Case 2: Shared Payment Token and Section 8.3 Use Case 3: In-Application using a Consumer Device). For variations where there is no Token User role, see, for example, Figure 8-1 (Section 8.1 Use Case 1: Proximity at Point of Sale) and Figure 8-5 (Section 8.4 Use Case 4: 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 identification and consideration of the technology of 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.	• Token Location

5 Token Presentment

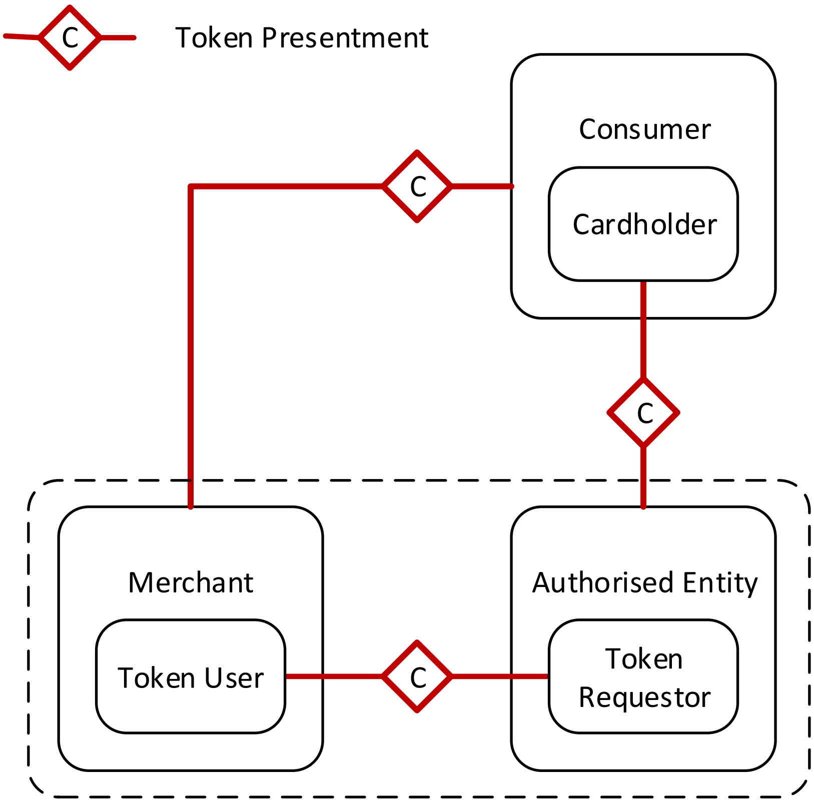
Token Presentment is the process of the Payment Token being presented or made available to the Merchant to start the Token Processing flow. Token Presentment occurs prior to Token Processing as shown in Figure 3.2 of the Technical Framework and follows existing PAN presentment modes for Cardholder-Initiated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

Merchant-Initiated Transactions do not have Token Presentment as a component of a use case since 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. 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 C. Consumer – Merchant

Relationship: The existing Consumer – Merchant relationship is utilised for Cardholder-Initiated Transactions with a Payment Token. The Consumer relationship with the Merchant may persist beyond the specific Cardholder-Initiated Transaction as a Merchant-managed Consumer account.

Function: The Consumer chooses a PAN (with corresponding Payment Token) which leads to a Cardholder-Initiated Transaction. This results in a Payment Token being received by the Merchant or a Third Party Service Provider acting on behalf of the Merchant. How this is achieved is use-case dependent.

5.1.2 C. Cardholder – Authorised Entity

Relationship: The Cardholder may have an existing relationship with the authorised entity performing the role of 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: Use-case dependent.

5.1.3 C. Token User – Token Requestor

Relationship: The Token User – Token Requestor relationship, if any, is dependent on the specific use case. In some use cases, the Merchant itself may be the Token Requestor.

Function: The Merchant receives the Payment Token from the Token Requestor.

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 Shared Payment Token Use Cases (see, for example, Section 8.2 Use Case 2: Shared Payment Token and Section 8.3 Use Case 3: In-Application using a Consumer Device). For variations where there is no Token User role, see, for example, Figure 8-1 (Section 8.1 Use Case 1: Proximity at Point of Sale) and Figure 8-5 (Section 8.4 Use Case 4: 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
Payment Method Access	How the Consumer accesses to the payment method.	• Device-based • Non Device-based

6 Token Processing

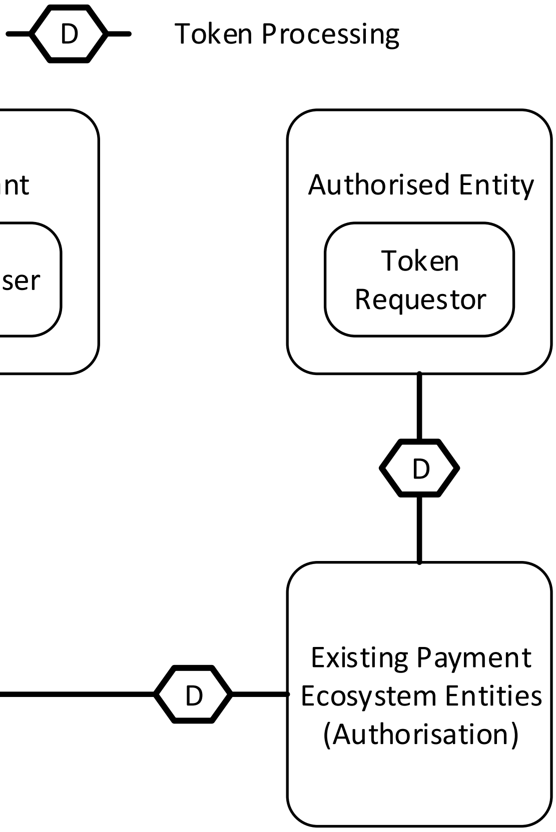
Token Processing occurs when the Payment Token and related data is processed to obtain an authorisation decision for a transaction as described in Section 10 of the Technical Framework.

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. 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 D. Merchant – Existing Payment Ecosystem Entities and 6.1.2 D. Authorised Entity – Existing Payment Ecosystem Entities. In any given use case, only one of these relationships can exist.

6.1.1 D. Merchant – Existing Payment Ecosystem Entities

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

Function: A Token Payment Request is submitted using the Payment Token and related data.

6.1.2 D. Authorised Entity – Existing Payment Ecosystem Entities

Relationship: The authorised entity fulfilling the role of the Token Requestor utilises existing relationships to initiate Token Processing on behalf of the Merchant.

Function: A Token Payment Request is submitted 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	• Merchant • Third Party
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

A Token Programme considers the participants performing Payment Tokenisation roles and associated technology enabling each use case to ensure the integrity of a Payment Token. Payment Token integrity is achieved by considering the relationship model characteristics of each use case and establishing 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 (Use Case 1) and used in another transaction as a Shared Payment Token (Use Case 2).

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
Token Assurance Method	Token Assurance will be determined based on the characteristics of the specific use case.	• Token Assurance Method Categories
Payment Token Type	Options for the type of Payment Token based on considerations of Token Location and Token Domain Restriction Controls. Limited Use Payment Tokens are for use in a single Cardholder-Initiated Transaction (and any subsequent Merchant-Initiated Transactions). Shared Payment Tokens can be used by one or more Token Users for one or more transactions.	• Default • Limited Use • Shared
Token Domain Restriction Controls	Common Token Domain Restriction Control categories available for specific use cases.	• Channel(s) • Device

Characteristic	Description	Typical Outcomes
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. Can be either Cardholder-Initiated or Merchant-Initiated.	• Cardholder-Initiated Transaction • Merchant-Initiated Transaction

8 Use Case Examples

This section describes use case examples in terms of the relationship models and their characteristics introduced in this document (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.

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

- Card-present transactions, where the Cardholder physically interacts with the Merchant's acceptance environment (e.g. presenting a Consumer Device at a Point of Sale terminal)
- Card-not-present transactions, where 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)

Within each category, there are multiple potential use cases. This document presents a limited number of use case examples which illustrate these categories as follows:

Card-present transactions:

- Use Case 1: Proximity at Point of Sale (Section 8.1)

Card-not-present transactions:

- Use Case 2: Shared Payment Token (Section 8.2)
- Use Case 3: In-Application using a Consumer Device (Section 8.3)
- Use Case 4: Card-On-File E-Commerce (Section 8.4)
- Use Case 5: Limited Use Payment Token (Section 8.5)

8.1 Use Case 1: Proximity at Point of Sale

This is an example of a card-present transaction. The use case example outlines using a suitably-enabled Consumer Device at a proximity acceptance environment (e.g. existing contactless Point of Sale technologies). Payment related communication is achieved using a variety of proximity technologies including NFC, QR Code, MST and others. Cardholder experience may differ based on Consumer Device type, capabilities and the acceptance technology available.

An example of Use Case 1: Proximity at Point of Sale is a Consumer making a face-to-face purchase from a Merchant. The Consumer presents a Consumer Device which transfers a Payment Token to the Merchant's acceptance environment (C1, Token Presentment in Figure 8-1).

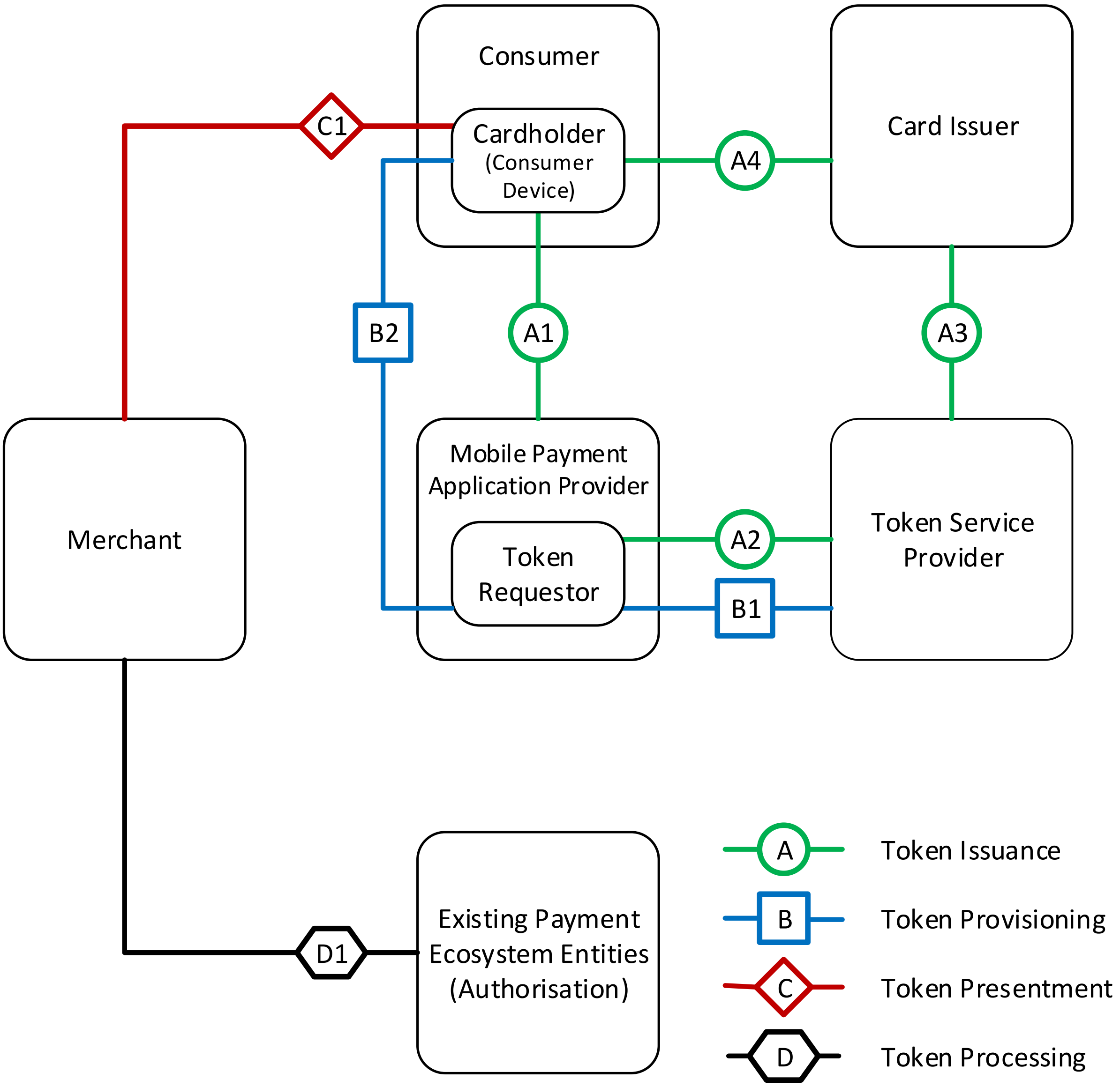
8.1.1 Use Case Relationships and Functions

The relationships for Use Case 1 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

When the relationships in this use case differ from those described in the models in Sections 4.1, 5.1 and 6.1, this is noted in the text following the figure.

Figure 8-1: Use Case 1 Relationships



Token Issuance and Token Provisioning

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

The Cardholder (through its Consumer Device) has a relationship with the mobile payment application provider, which performs the role of Token Requestor. The Cardholder adds an existing PAN and related data to the Consumer Device which triggers the Token Issuance process for this use case.

See Section 4.1.1 A. Cardholder – Authorised Entity.

A2. Token Service Provider – Token Requestor

The Cardholder adds a PAN and related data, triggering the Token Requestor to make a Token Request to the Token Service Provider.

See Section 4.1.4 A. Token Service Provider – Token Requestor.

A3. Card Issuer – Token Service Provider

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

There is no variation from the default relationship model given in Section 4.1.5 A. Card Issuer – Token Service Provider.

A4. Card Issuer – Cardholder (Consumer Device)

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

There is no variation from the default relationship model given in Section 4.1.6 A. Card Issuer – Cardholder.

B1. Token Service Provider – Token Requestor

The Token Service Provider delivers the Payment Token and related data to the Token Requestor.

See Section 4.1.7 B. Token Service Provider – Token Requestor.

B2. Cardholder (Consumer Device) – Token Requestor

The 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.

See Section 4.1.8 B. Cardholder – Token Requestor.

Token Presentment

C1. Cardholder (Consumer Device) – Merchant

The Cardholder may interact with the mobile payment application on the Consumer Device to select the payment method (with corresponding Payment Token). The Cardholder's Consumer Device interacts with the Merchant's acceptance environment. The Merchant's acceptance environment receives the Payment Token and related data from the Consumer Device.

See Section 5.1.1 C. Consumer – Merchant.

Token Processing

D1. Merchant / Existing Payment Ecosystem Entities

The Merchant utilises existing relationships to initiate Token Processing.

There is no variation from the default relationship model given in Section 6.1.1 D. 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.

8.1.2 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: Use Case 1 Token Issuance Characteristics

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

Table 8-2: Use Case 1 Token Provisioning Characteristics

Characteristic	Notes	Typical Outcomes
Token Location	See Table 5.1 of the Technical Framework for defined Token Locations.	• 02, 03, 04

Table 8-3: Use Case 1 Token Presentment Characteristics

Characteristic	Notes	Typical Outcomes
Token Presentment	The Consumer Device, using NFC, QR code, MST or other technologies, interacts with the Merchant acceptance environment.	• Proximity
Acceptance Environment	The acceptance environment, using contactless (for NFC), QR scanner (for QR Code), magnetic stripe reader (for MST) or other technologies, receives a Payment Token and related data.	• Physical
Payment Method Access	Consumer access to the Payment Token is controlled by the Consumer Device.	• Device-based

Table 8-4: Use Case 1 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 restrict the Payment Token to a specific Consumer Device and specific channel(s).	• POS Entry Mode • Token Cryptogram

8.1.3 Payment Token Characteristics

The Payment Token characteristics are shown in Table 8-5.

Table 8-5: Use Case 1 Payment Token Characteristics

Characteristic	Notes	Typical Outcomes
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
Payment Token Type	The Payment Token is associated with the Consumer Device.	• Default
Token Domain Restriction Controls	The Payment Token is restricted for use on a specific Consumer Device and specific channel(s).	• Channel(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 with a Merchant.	• Cardholder-Initiated Transaction

8.2 Use Case 2: Shared Payment Token

This is an example of a card-not-present transaction. The use case example outlines a Token Requestor sharing a Payment Token between multiple Merchants (Token Users). A Payment Token or Token Reference ID is stored by the Token Requestor and made available to a Token User during Token Presentment. The Token Requestor enables controls over which Merchants (Token Users) that it supports will have access to the Shared Payment Token. In this use case, a Payment Token or Token Reference ID is stored by the Token Requestor.

There are several potential variants of the Shared Payment Token use case. These variants depend on the authorised entity fulfilling the role of Token Requestor and its relationship with the Merchant (Token User). Two example variants are presented here:

- Digital Wallet as a Token Requestor (Sections 8.2.1 to 8.2.3)
- Third Party Service Provider as a Token Requestor (8.2.4 to 8.2.6)

8.2.1 Use Case Relationships and Functions: Digital Wallet

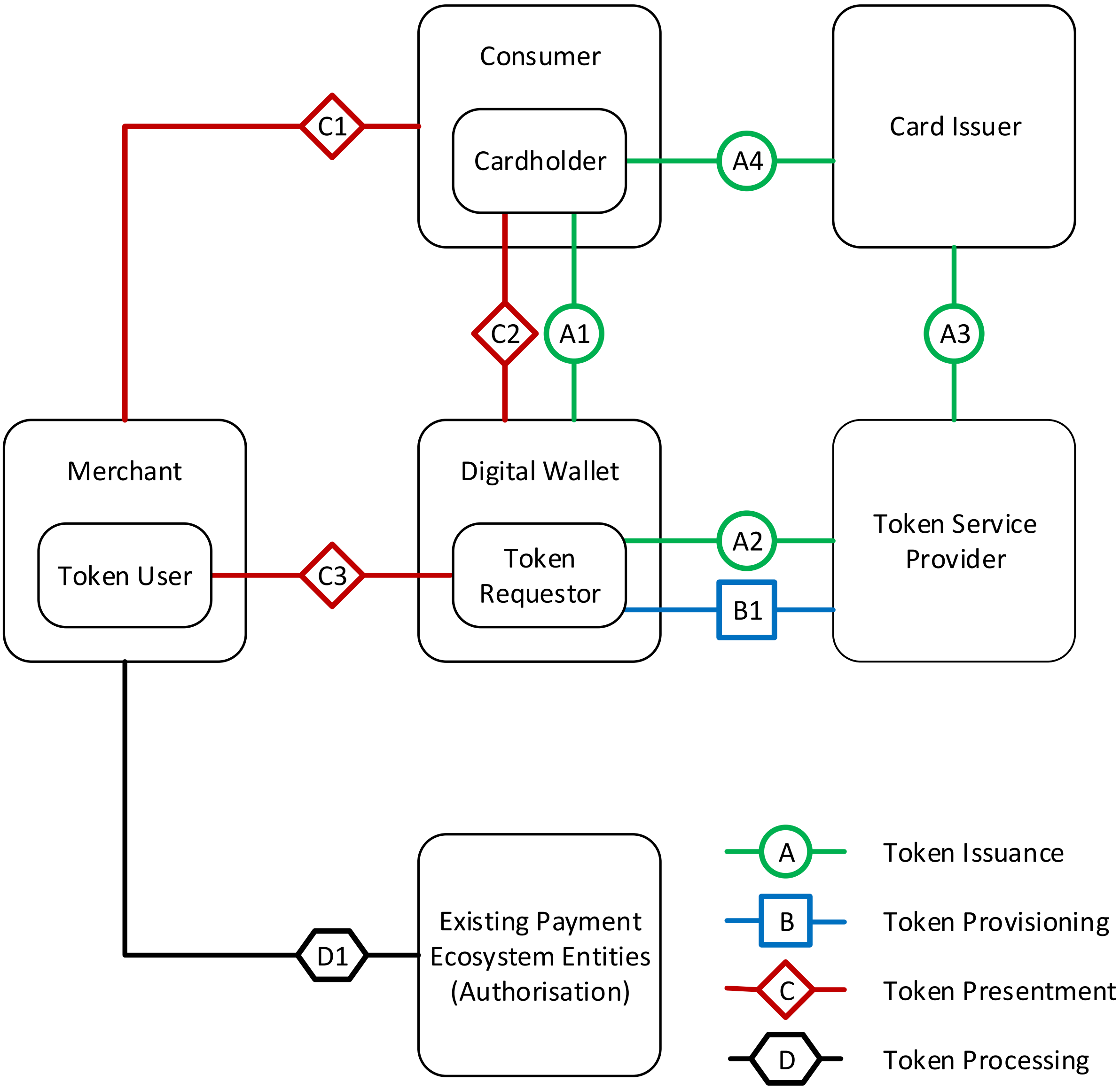
An example of Use Case 2: Shared Payment Token (Digital Wallet) is a Consumer making an e-commerce purchase from a Merchant using a digital wallet for payment. The Consumer selects a payment method from the digital wallet, which is associated with a Shared Payment Token. The digital wallet transfers the Payment Token or Token Reference ID to the Merchant (Token Presentment in Figure 8-2).

The relationships when the Token Requestor is a digital wallet are shown in Figure 8-2. 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

When the relationships in this use case differ from those described in the models in Sections 4.1, 5.1 and 6.1, this is noted in the text following the figure.

Figure 8-2: Use Case 2 (Digital Wallet) Relationships



Token Issuance and Token Provisioning

A1. Cardholder – Digital Wallet

The Cardholder has a relationship with a digital wallet, which performs the role of Token Requestor. The Cardholder adds an existing PAN and related data to the wallet which triggers the Token Issuance process for this use case.

See Section 4.1.1 A. Cardholder – Authorised Entity

A2. Token Service Provider – Token Requestor

The Cardholder adds a PAN and related data to the digital wallet, triggering the Token Requestor to make a Token Request to the Token Service Provider.

See Section 4.1.4 A. Token Service Provider – Token Requestor.

A3. Card Issuer – Token Service Provider

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

There is no variation from the default relationship model given in Section 4.1.5 A. Card Issuer – Token Service Provider.

A4. Card Issuer – Cardholder

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

There is no variation from the default relationship model given in Section 4.1.6 A. Card Issuer – Cardholder.

B1. Token Service Provider – Token Requestor

The Token Service Provider delivers the Shared Payment Token to the Token Requestor. The Token Requestor delivers the Payment Token to the Token Location of the digital wallet.

See Section 4.1.7 B. Token Service Provider – Token Requestor.

Token Presentment

C1 Consumer – Merchant

The Consumer chooses to use the digital wallet that has been previously been integrated with the Merchant for checkout.

See Section 5.1.1 C. Consumer – Merchant.

C2 Consumer – Digit Wallet

Cardholder interacts with the digital wallet to select payment method (with corresponding Shared Payment Token).

See Section 5.1.2 C. Cardholder – Authorised Entity.

C3 Token User – Token Requestor

The Merchant, which performs the role of Token User, receives the Shared Payment Token and related data from the Token Requestor.

See Section 5.1.3 C. Token User – Token Requestor.

Token Processing

D1. Merchant – Existing Payment Ecosystem Entities

The Merchant utilises existing relationships to initiate Token Processing.

There is no variation from the default relationship model given in Section 6.1.1 D. Merchant – Existing Payment Ecosystem Entities.

8.2.2 Use Case Characteristics: Digital Wallet

The use case characteristics are shown in Table 8-6, Table 8-7, Table 8-8 and Table 8-9.

Table 8-6: Use Case 2 (Digital Wallet) Token Issuance Characteristics

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

Table 8-7: Use Case 2 (Digital 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: Use Case 2 (Digital Wallet) Token Presentment Characteristics

Characteristic	Notes	Typical Outcomes
Token Presentment	The Shared Payment Token is presented to the Token User by the Token Requestor. The methods and processes associated with the presentation are implementation specific and depend on the Token User's relationship with the Token Requestor.	• Non-proximity
Acceptance Environment	Shared Payment Tokens are associated with a non-physical acceptance environment.	• Non-physical
Payment Method Access	Consumer access to the Payment Token is not device-based and will require Consumer credentials.	• Non Device-based

Table 8-9: Use Case 2 (Digital Wallet) 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	Merchant Identifiers may be used to restrict the Payment Token to a specific Token User at the time of a given transaction.	• POS Entry Mode • Merchant Identifiers • Token Cryptogram

8.2.3 Payment Token Characteristics: Digital Wallet

The Payment Token characteristics are shown in Table 8-10.

Table 8-10: Use Case 2 (Digital Wallet) Payment Token Characteristics

Characteristic	Notes	Typical Outcomes
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
Payment Token Type	Shared Payment Tokens can be used by one or more Token Users.	• Shared
Token Domain Restriction Controls	The use of the Shared Payment Token is limited to a specific Token User at the time of the transaction.	• Channel(s) • Device
Token Cryptogram	A Token Cryptogram is used to ensure the integrity of the transaction-specific data.	• Used • Not Used
Type of Transaction Initiation	Typically, the Cardholder uses a Merchant application to initiate a transaction that may drive subsequent Merchant-Initiated Transactions.	• Cardholder-Initiated Transaction • Merchant-Initiated Transaction

8.2.4 Use Case Relationships and Functions: Third Party Service Provider

An example of Use Case 2: Shared Payment Token (Third Party Service Provider) is a Consumer making an e-commerce purchase from a Merchant, which uses a Third Party Service Provider to manage payments. The Consumer selects a stored payment method from

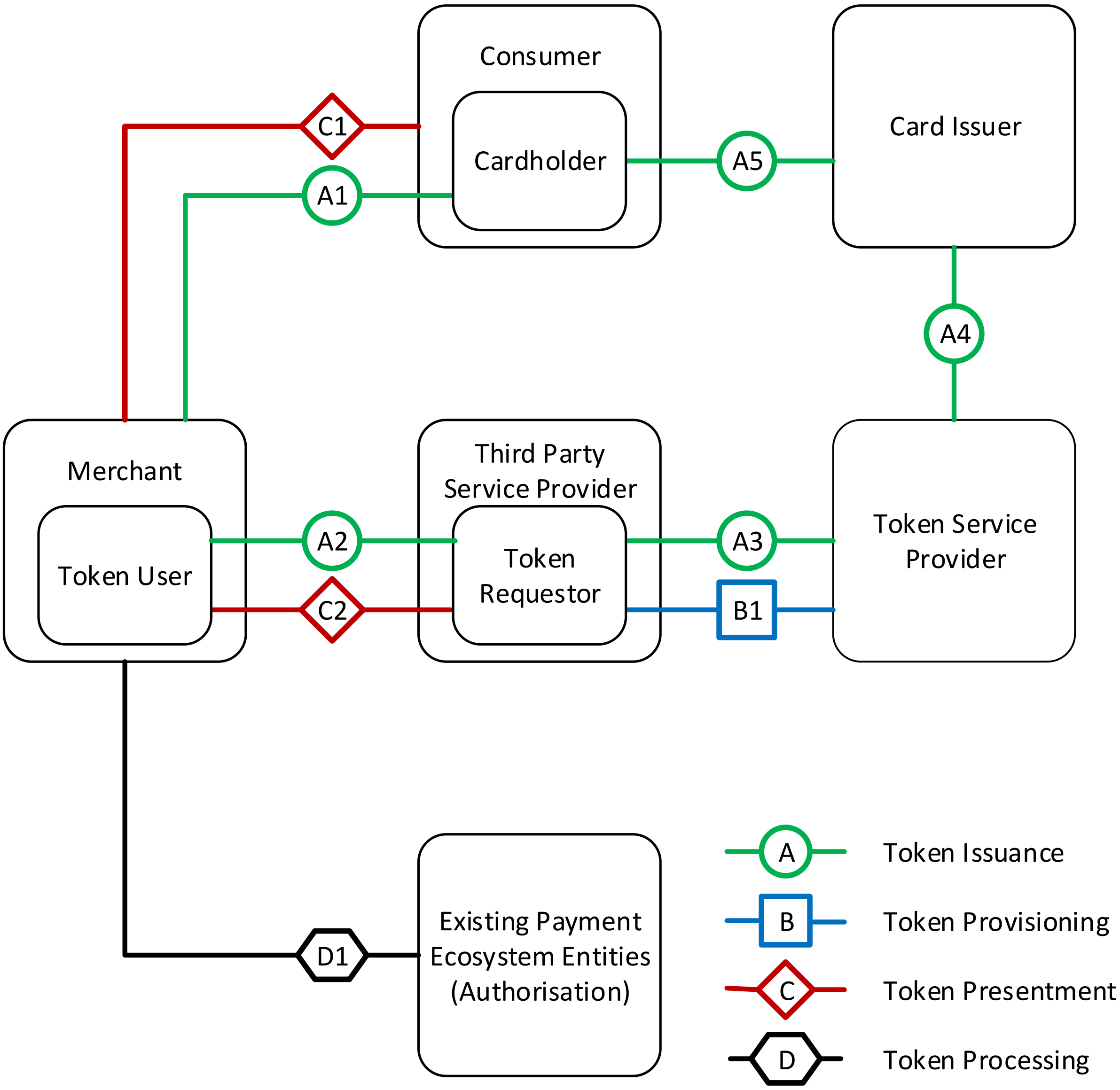
Merchant's acceptance environment, which is associated with a Shared Payment Token, managed by the Third Party Service Provider. The Third Party Service Provider then transfers a Payment Token or Token Reference ID to the Merchant (Token Presentment in Figure 8-3).

The relationships when the Token Requestor is a Third Party Service Provider are shown in Figure 8-3. 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

When the relationships in this use case differ from those described in the models in Sections 4.1, 5.1 and 6.1, this is noted in the text following the figure.

Figure 8-3: Use Case 2 (Third Party Service Provider) Relationships



Token Issuance and Token Provisioning

A1. Cardholder – Merchant

The Consumer / Cardholder has a relationship with the Merchant, which performs the role of Token User. The Cardholder adds a PAN and related data to the Merchant application (mobile or web based). In this use case, this PAN has not previously been Tokenised by the Merchant application, which triggers the Token Issuance process.

See Section 4.1.2 A. Cardholder – Merchant.

A2. Token User – Token Requestor

The Merchant, which performs the role of Token User, has an existing relationship with a Third Party Service Provider, which performs the role of Token Requestor.

The Merchant provides the PAN to the Token Requestor, initialising the Token Issuance process.

See Section 4.1.3 A. Token User – Token Requestor.

A3. Token Service Provider – Token Requestor

The Token User provides a PAN to the Token Requestor, triggering the Token Requestor to make a Token Request to the Token Service Provider.

See Section 4.1.4 A. Token Service Provider – Token Requestor.

A4. Card Issuer – Token Service Provider

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

There is no variation from the default relationship model given in Section 4.1.5 A. Card Issuer – Token Service Provider.

A5. Card Issuer – Cardholder

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

There is no variation from the default relationship model given in Section 4.1.6 A. Card Issuer – Cardholder.

B1. Token Service Provider – Token Requestor

The Token Service Provider delivers the Shared Payment Token to the Token Requestor. In this use case, the Token Requestor stores the Shared Payment Token until it is required for Token Processing.

See Section 4.1.7 B. Token Service Provider – Token Requestor.

Token Presentment

C1 Consumer – Merchant

The Consumer chooses to use the Merchant application for checkout and interacts with it to select the payment method (with corresponding Shared Payment Token). In this use case, the Merchant is the Token User.

See Section 5.1.1 C. Consumer – Merchant.

C2 Token User – Token Requestor

The Merchant, which performs the role of Token User, receives the Shared Payment Token and related data from the Token Requestor in preparation for Token Processing.

See Section 5.1.3 C. Token User – Token Requestor.

Token Processing

D1. Merchant – Existing Payment Ecosystem Entities

The Merchant utilises existing relationships to initiate Token Processing.

There is no variation from the default relationship model given in Section 6.1.1 D. Merchant – Existing Payment Ecosystem Entities.

Variations to Relationships

D1. Third Party Service Party – Existing Payment Ecosystem Entities

Figure 8-3 shows Relationship D1 between the Merchant and the existing payment ecosystem entities. However, there is an alternative, where the Token Processing relationship exists between the Third Party Service Party and the existing payment ecosystem entities.

In this case, the authorised entity fulfilling the role of the Token Requestor utilises existing relationships to initiate Token Processing on behalf of the Merchant.

There is no variation from the default relationship model given in Section 6.1.2 D. Authorised Entity – Existing Payment Ecosystem Entities.

8.2.5 Use Case Characteristics: Third Party Service Provider

The use case characteristics are shown in Table 8-11, Table 8-12, Table 8-13 and Table 8-14.

Table 8-11: Use Case 2 (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 8-12: Use Case 2 (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.	• 01 • 06 • 07

Table 8-13: Use Case 2 (Third Party Service Provider) Token Presentment Characteristics

Characteristic	Notes	Typical Outcomes
Token Presentment	The Shared Payment Token is presented to the Token User by the Token Requestor. The methods and processes associated with the presentation are implementation specific and depend on the Token User's relationship with the Token Requestor.	• Non-proximity
Acceptance Environment	Shared Payment Tokens are associated with a non-physical acceptance environment.	• Non-physical
Payment Method Access	Consumer access to the Payment Token is not device-based and will require Consumer credentials.	• Non Device-based

Table 8-14: Use Case 2 (Third Party Service Provider) 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	Merchant Identifiers may be used to restrict the Payment Token to a specific Token User at the time of a given transaction.	• POS Entry Mode • Merchant Identifiers • Token Cryptogram

8.2.6 Payment Token Characteristics: Third Party Service Provider

The Payment Token characteristics are shown in Table 8-15.

Table 8-15: Use Case 2 (Third Party Service Provider) Payment Token Characteristics

Characteristic	Notes	Typical Outcomes
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

Characteristic	Notes	Typical Outcomes
Payment Token Type	Shared Payment Tokens can be used by one or more Token Users.	• Shared
Token Domain Restriction Controls	The use of the Shared Payment Token is limited to a specific Token User at the time of the transaction.	• Channel(s)
Token Cryptogram	A Token Cryptogram is used to ensure the integrity of the transaction-specific data.	• Used • Not Used
Type of Transaction Initiation	Typically, the Cardholder uses a Merchant application to initiate a transaction that may drive subsequent Merchant-Initiated Transactions.	• Cardholder-Initiated Transaction • Merchant-Initiated Transaction

8.3 Use Case 3: In-Application using a Consumer Device

This is an example of a card-not-present transaction. The use case example outlines using a Consumer Device which is integrated into a Merchant application. The Cardholder experience involves a direct interaction with the Merchant application.

An example of Use Case 3: In-Application using a Consumer Device is a Consumer making an e-commerce purchase from the Consumer Device containing a Payment Token where the Merchant application is also located. The Consumer selects a stored payment method (represented by the Payment Token) from the Consumer Device. The Consumer Device transfers the Payment Token to the Merchant's acceptance environment (C1, C2, Token Presentment in Figure 8-4).

8.3.1 Use Case Relationships and Functions

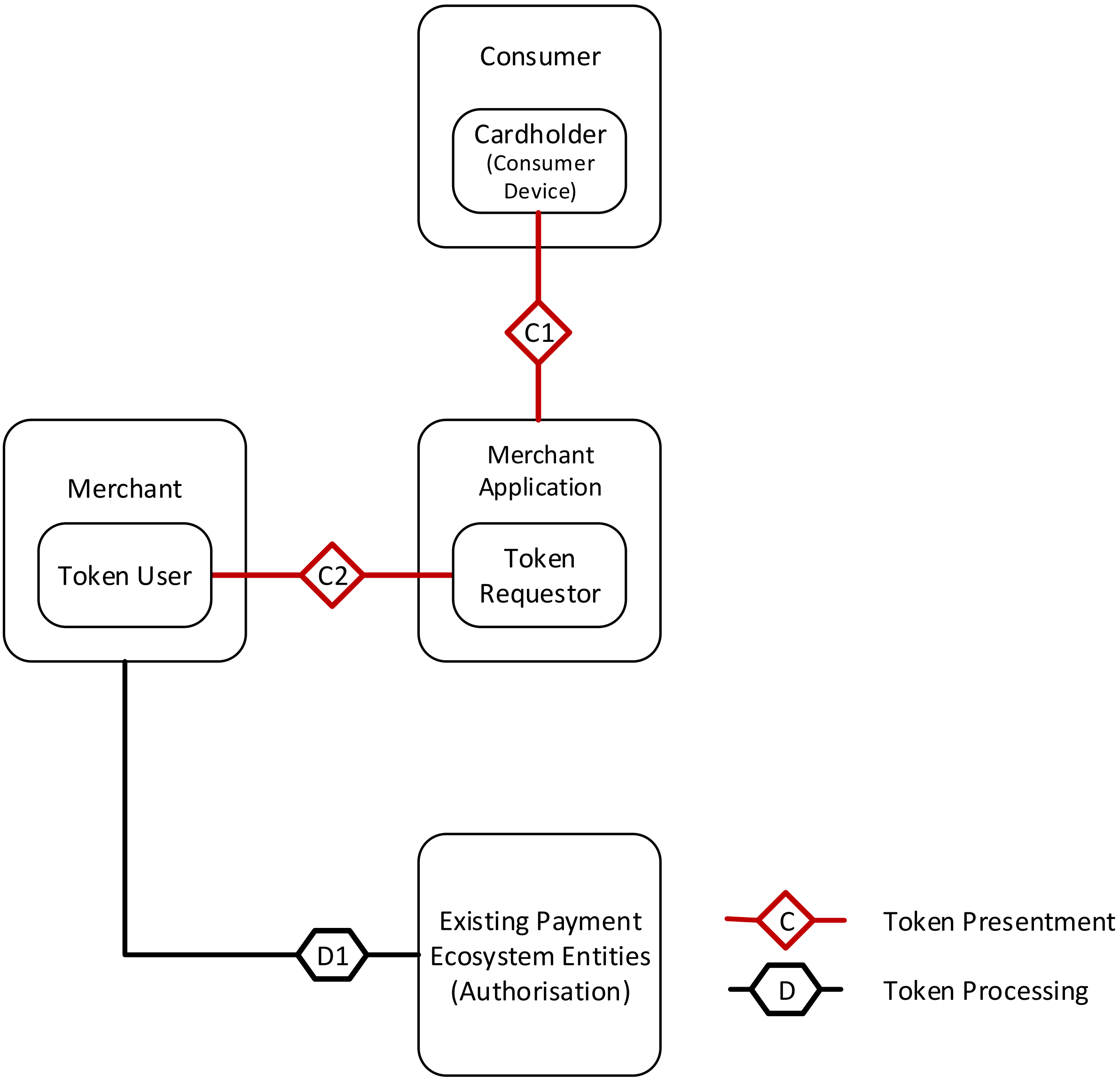
The relationships for Use Case 3 are shown in Figure 8-4. For a description of the baseline relationships and their functions, refer to the models given in Sections:

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

When the relationships in this use case differ from those described in the models in Sections 5.1 and 6.1, this is noted in the text following the figure.

Note that this use case is transactional, and presupposes that a Payment Token has been provisioned to either a proximity-enabled Consumer Device (Section 8.1 Use Case 1: Proximity at Point of Sale) or a digital wallet (Sections 8.2.1 Use Case Relationships and Functions: Digital Wallet to 8.2.3 Payment Token Characteristics: Digital Wallet). Therefore, Token Issuance relationships and Token Provisioning relationships are not shown in Figure 8-4. The Token Issuance and Token Provisioning characteristics are not given in Section 8.3.2.

Figure 8-4: Use Case 3 Relationships



Token Presentment

C1 Cardholder (Consumer Device) – Merchant Application

> The Cardholder may interact with the Merchant application integrated on the Consumer Device to select the payment method (represented by the Payment Token).

See Section 5.1.2 C. Cardholder – Authorised Entity.

C2 Token User – Token Requestor

The Merchant's acceptance environment, which performs the role of Token User, receives the Payment Token and related data from the Token Requestor via the Merchant application. Depending on the use case, this is either a Payment Token issued to the Consumer Device (Use Case 1: Proximity at Point of Sale) or a Shared Payment Token issued by the Token Requestor for use by the Merchant (Use Case 2: Shared Payment Token).

See Section 5.1.3 C. Token User – Token Requestor.

Token Processing

D1. Merchant – Existing Payment Ecosystem Entities

The Merchant utilises existing relationships to initiate Token Processing.

There is no variation from the default relationship model given in Section 6.1.1 D. Merchant – Existing Payment Ecosystem Entities.

8.3.2 Use Case Characteristics

The use case characteristics are given in Table 8-16 and Table 8-17. For the Token Issuance and Token Provisioning characteristics, see either Use Case 1: Proximity at Point of Sale (Section 8.1) or Use Case 2: Shared Payment Token (Section 8.2).

Table 8-16: Use Case 3 Token Presentment Characteristics

Characteristic	Notes	Typical Outcomes
Token Presentment	The Merchant application interacts with Token Requestor to present the Payment Token to the Merchant acceptance environment.	• Non-proximity
Acceptance Environment	The acceptance environment is a Merchant application. Physical terminals are not used.	• Non-physical
Payment Method Access	Consumer access to the Payment Token is controlled either by the Consumer Device or Merchant application (digital wallet).	• Device-based • Non Device-based

Table 8-17: Use Case 3 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	Fields in transaction messages that are typically used to restrict the Payment Token to the appropriate Token Domains.	• POS Entry Mode • Token Cryptogram

8.3.3 Payment Token Characteristics

The Payment Token characteristics are shown in Table 8-18.

Table 8-18: Use Case 3 Payment Token Characteristics

Characteristic	Notes	Typical Outcomes
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
Payment Token Type	A single Payment Token is shared among multiple Merchants / Token Users.	• Shared
Token Domain Restriction Controls	The Payment Token is restricted to the Consumer Device.	• Channel(s) • Device
Token Cryptogram	A Token Cryptogram is used to ensure the integrity of the transaction-specific data.	• Used • Not Used
Type of Transaction Initiation	The Cardholder initiates a transaction that may drive subsequent Merchant-Initiated Transactions.	• Cardholder-Initiated Transaction • Merchant-Initiated Transaction

8.4 Use Case 4: Card-On-File E-Commerce

This is an example of a card-not-present transaction. The use case example outlines a Token Requestor using a Payment Token for a specifically authorised entity. A Payment Token is stored by the Token Requestor (the authorised entity) and made available during Token Presentment.

In this specific example, the Token Requestor is the Merchant.

An example of Use Case 4: Card-On-File E-Commerce is a Consumer making an e-commerce purchase from a Merchant using the Merchant application/website. The Consumer enters a PAN and related data into the Merchant application/website. The Merchant then makes a Token Request, using the resulting Payment Token to initiate Token Processing (Token Issuance and Provisioning in Figure 8-5). The Payment Token is then stored by the Merchant and the PAN (represented by the Payment Token) can be selected by the Consumer during future purchases (Token Presentment in Figure 8-5).

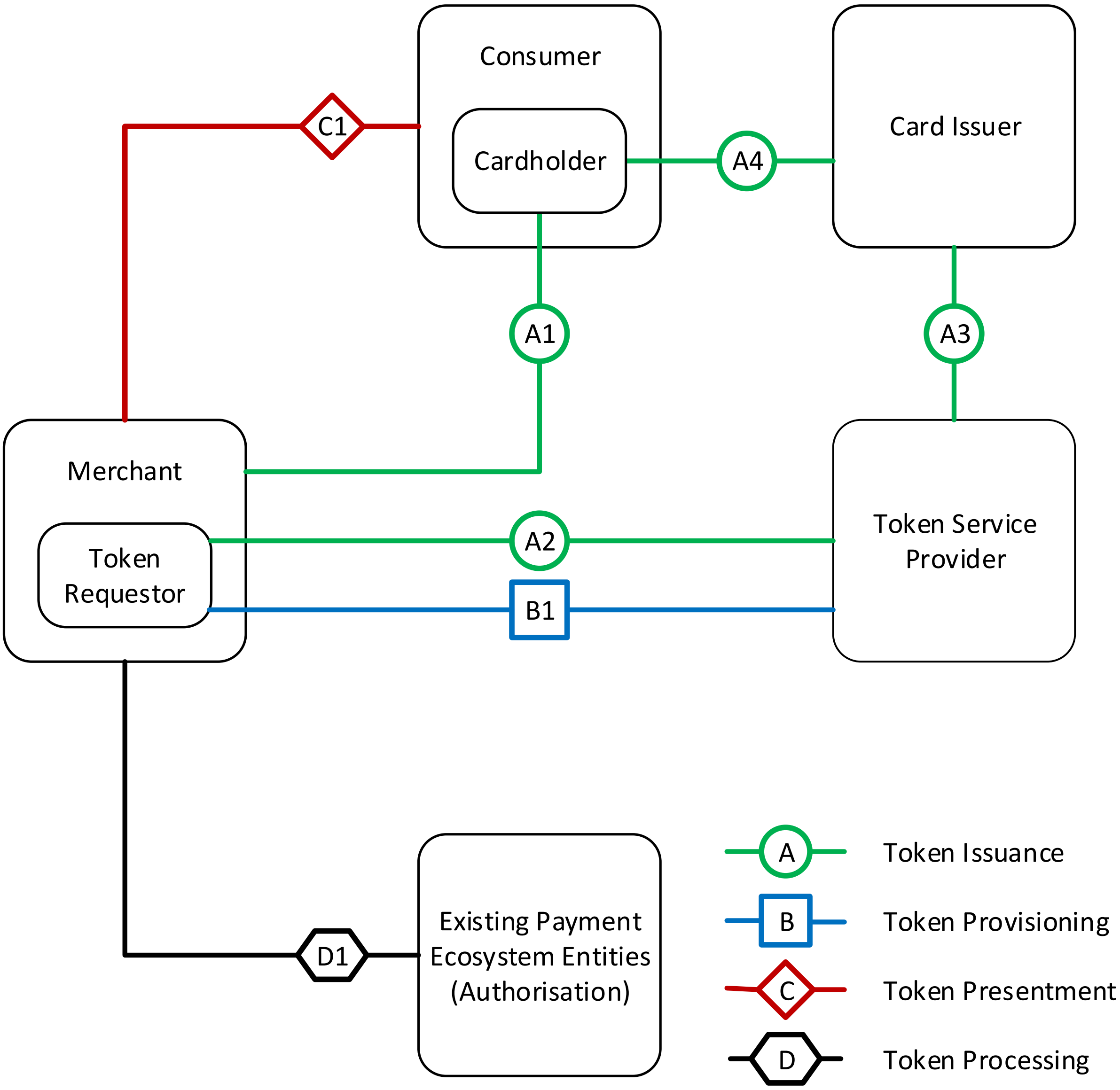
8.4.1 Use Case Relationships and Functions

The relationships for Use Case 4 are shown in Figure 8-5. 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

When the relationships in this use case differ from those described in the models in Sections 4.1, 5.1 and 6.1, this is noted in the text following the figure.

Figure 8-5: Use Case 4 Relationships



Token Issuance and Token Provisioning

A1. Cardholder – Merchant

The Cardholder has a relationship with Merchant, which performs the role of Token Requestor. The Cardholder adds an existing PAN and related data to the Merchant application (mobile or web based) which triggers the Token Issuance process for this use case.

See Section 4.1.1 A. Cardholder – Authorised Entity.

A2. Token Service Provider – Token Requestor

The Cardholder adds a PAN and related data to the Merchant application, triggering the Token Requestor to make a Token Request to the Token Service Provider.

See Section 4.1.4 A. Token Service Provider – Token Requestor.

A3. Card Issuer – Token Service Provider

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

There is no variation from the default relationship model given in Section 4.1.5 A. Card Issuer – Token Service Provider.

A4. Card Issuer – Cardholder

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

There is no variation from the default relationship model given in Section 4.1.6 A. Card Issuer – Cardholder.

B1. Token Service Provider – Token Requestor

The Token Service Provider delivers the Payment Token to the Token Requestor. The Token Requestor delivers the Payment Token to the Token Location of the Merchant application.

See Section 4.1.7 B. Token Service Provider – Token Requestor.

Token Presentment

C1 Consumer – Merchant

The Consumer chooses to use the Merchant application for checkout and interacts with it to select the payment method (represented by the Payment Token). In this use case, the Merchant is the Token Requestor.

See Section 5.1.1 C. Consumer – Merchant.

Token Processing

D1. Merchant – Existing Payment Ecosystem Entities

The Merchant utilises existing relationships to initiate Token Processing.

There is no variation from the default relationship model given in Section 6.1.1 D. 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 8-5.

8.4.2 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: Use Case 4 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: Use Case 4 Token Provisioning Characteristics

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

Table 8-21: Use Case 4 Token Presentment Characteristics

Characteristic	Notes	Typical Outcomes
Token Presentment	The Payment Token is presented by the Token Requestor.	• Non-proximity
Acceptance Environment	The Payment Token is associated with a Merchant application.	• Non-physical
Payment Method Access	Consumer access to the Payment Token is not device-based and will require Consumer credentials.	• Non Device-based

Table 8-22: Use Case 4 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	Token Control Fields used to restrict the Payment Token to a specific Merchant and a specific channel.	• POS Entry Mode • Merchant Identifiers • Token Cryptogram

8.4.3 Payment Token Characteristics

The Payment Token characteristics are shown in Table 8-23.

Table 8-23: Use Case 4 Payment Token Characteristics

Characteristic	Note	Typical Outcomes
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
Payment Token Type	The Payment Token is for use by a specific Merchant.	• Default
Token Domain Restriction Controls	The Payment Token is restricted to a specific Merchant.	• Channel(s)
Token Cryptogram	A Token Cryptogram can be used to ensure the integrity of the transaction-specific data.	• Used • Not Used
Type of Transaction Initiation	Typically, the Cardholder uses a Merchant application to initiate a transaction that may drive subsequent Merchant-Initiated Transactions.	• Cardholder-Initiated Transaction • Merchant-Initiated Transaction

8.5 Use Case 5: Limited Use Payment Token

This is an example of a card-not-present transaction. The use case is transactional, presupposing that the Token Requestor does not store the Payment Token. Each transaction event initiates a unique Token Request, with the resulting Limited Use Payment Token used for Token Processing. The use case shares the same relationships and characteristics as Card-On-File E-Commerce (Use Case 4: Card-On-File E-Commerce). However, the Token Domain Restriction Controls prevent repeated transaction use.

An example of Use Case 5: Limited Use Payment Token is a Consumer making an e-commerce purchase from a Merchant using a guest checkout. The Consumer enters a PAN and related data into the Merchant's acceptance environment and the Merchant generates a Token Request (Token Issuance and Provisioning in Figure 8-6).

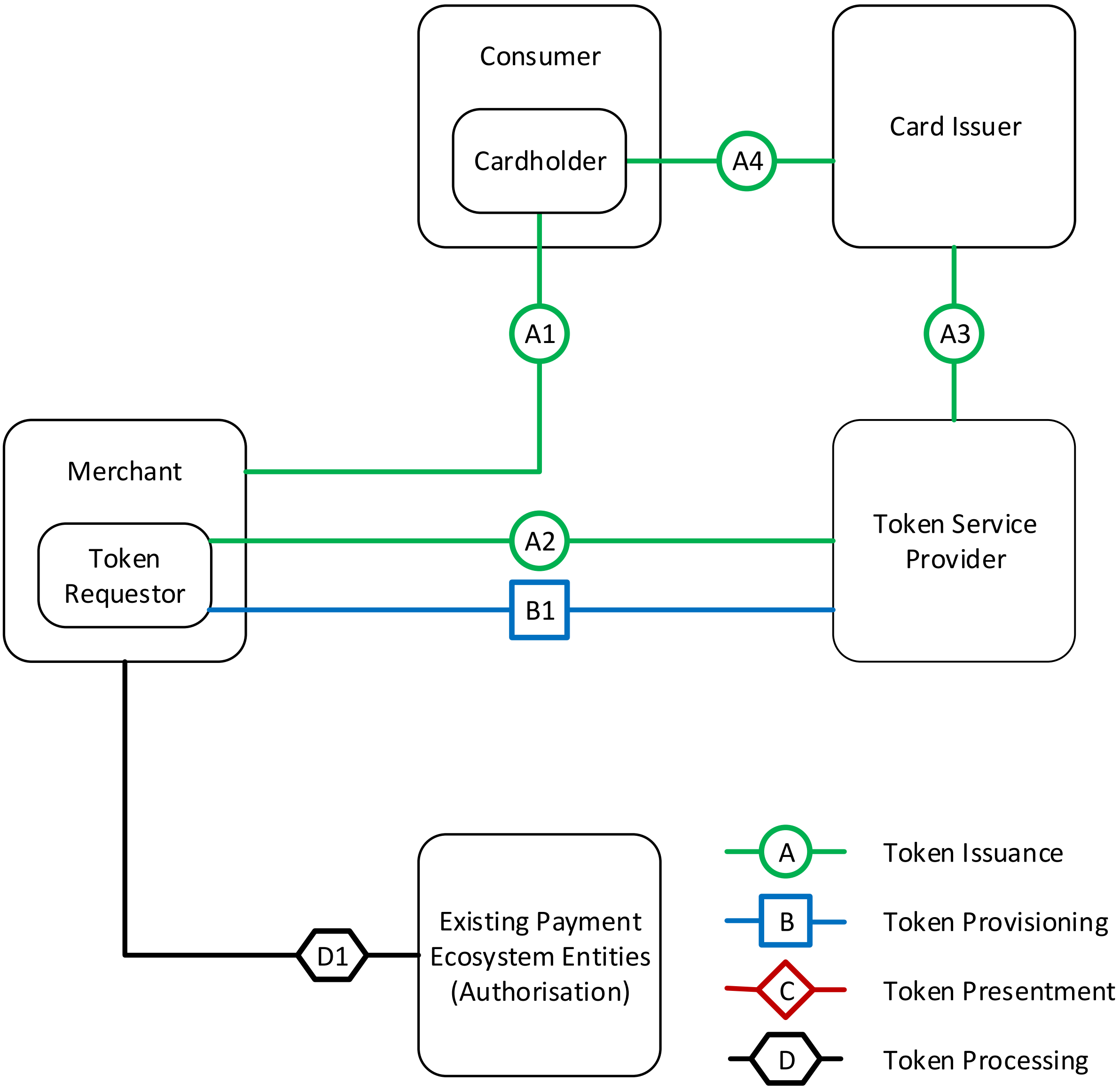
8.5.1 Use Case Relationships and Functions

The relationships for Use Case 5 are shown in Figure 8-6. 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

When the relationships in this use case differ from those described in the models in Sections 4.1, 5.1 and 6.1, this is noted in the text following the figure.

Figure 8-6: Use Case 5 Relationships



Token Issuance and Token Provisioning

A1. Cardholder – Merchant

The Cardholder has a relationship with Merchant, which performs the role of Token Requestor.

The Cardholder presents a PAN and related data to the Merchant application (mobile or web based) which triggers the Token Issuance process for this use case.

See Section 4.1.1 A. Cardholder – Authorised Entity

A2. Token Service Provider – Token Requestor

The Cardholder presents a PAN and related data to the Merchant application, triggering the Token Requestor to make a Token Request to the Token Service Provider.

See Section 4.1.4 A. Token Service Provider – Token Requestor.

A3. Card Issuer – Token Service Provider

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

There is no variation from the default relationship model given in Section 4.1.5 A. Card Issuer – Token Service Provider.

A4. Card Issuer – Cardholder

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

There is no variation from the default relationship model given in Section 4.1.6 A. Card Issuer – Cardholder.

B1. Token Service Provider – Token Requestor

The Token Service Provider delivers the Payment Token to the Token Requestor. The Token Requestor delivers the Payment Token to the Token Location of the Merchant application.

See Section 4.1.7 B. Token Service Provider – Token Requestor.

Token Processing

D1. Merchant – Existing Payment Ecosystem Entities

The Merchant utilises existing relationships to initiate Token Processing.

There is no variation from the default relationship model given in Section 6.1.1 D. 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 facilitates Token Presentment on behalf of the Cardholder.

8.5.2 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: Use Case 5 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: Use Case 5 Token Provisioning Characteristics

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

Table 8-26: Use Case 5 Token Presentment Characteristics

Characteristic	Notes	Typical Outcomes
Token Presentment	The Payment Token is presented by the Token Requestor.	• Non-proximity
Acceptance Environment	Limited Use Payment Tokens are associated with a Merchant application.	• Non-physical
Payment Method Access	Consumer access to the Payment Token is not device-based and will require Consumer credentials.	• Non Device-based

Table 8-27: Use Case 5 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	Fields in transaction messages that are typically used to restrict Payment Token use to the appropriate Merchant and to limit 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

8.5.3 Payment Token Characteristics

The Payment Token characteristics are shown in Table 8-28.

Table 8-28: Use Case 5 Payment Token Characteristics

Characteristic	Note	Typical Outcomes
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
Payment Token Type	The Payment Token is limited for use in a single Cardholder-Initiated Transaction and any subsequent Merchant-Initiated Transactions.	• Limited Use
Token Domain Restriction Controls	The Payment Token is limited to a specific Merchant.	• Channel(s)
Token Cryptogram	A Token Cryptogram can be used to ensure the integrity of the transaction-specific data.	• Used • Not Used
Type of Transaction Initiation	Typically, the Cardholder uses a Merchant application to initiate a transaction that may drive subsequent Merchant Initiated Transactions.	• Cardholder-Initiated Transaction • Merchant Initiated Transaction

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