EMV®
Secure Remote Commerce

Use Cases

Version 1.1

March 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 1.1

The following changes have been made to the document since the publication of version 1.0.

- Minor editorial changes
- Section 1.2 Overview has been revised to accommodate the new use cases which have been added in the following Sections:
  - Section 7 SRC Checkout with 3DS “ONBEHALF”
  - Section 8 Management Service
  - Section 9 Authentication Facilitation Services
  - Section 10 Merchant Orchestrated Recognition
  - Section 11 Last Used Card

Contents

Legal Notice ..... **i**

Revision Log – Version 1.1 ..... **ii**

Contents ..... **iii**

Figures ..... **vi**

Tables ..... **vii**

1 Introduction **1**

1.1 Scope 1

1.2 Overview 1

1.2.1 Enrolment 3

1.2.2 Checkout 3

1.2.3 Other Services 4

1.3 Audience 5

1.4 References 5

1.4.1 Published EMVCo Documents 5

1.5 Definitions 6

1.6 Notational Conventions 6

1.6.1 Abbreviations 6

1.6.2 Terminology and Conventions 6

1.7 Further Information 7

2 Enrolment **8**

2.1 Use Case Overview 8

2.2 Preconditions 8

2.3 Assumptions 8

2.4 Sequence Diagrams 8

3 SRC Checkout **11**

3.1 Use Case Overview 11

3.2 Preconditions 11

3.3 Assumptions 12

3.4 Sequence Diagrams 12

4 Merchant Digital Card-On-File Checkout **18**

4.1 Use Case Overview 18

4.2 Preconditions 19

4.3 Assumptions 19
4.4 Sequence Diagrams 20
4.4.1 Pre-Checkout Setup 20
4.4.2 Inline-Checkout / Post-Checkout Setup 22
4.4.3 Merchant Digital Card-On-File Checkout 26
4.4.4 Merchant Digital Card-On-File Merchant-Initiated Transaction 27

5 Merchant Orchestrated Checkout 29

5.1 Use Case Overview 29
5.2 Preconditions 30
5.3 Assumptions 30
5.4 Sequence Diagrams 31
5.4.1 Merchant Orchestrated Checkout (Consumer Recognised) 31
5.4.2 Merchant Orchestrated Checkout (Consumer Credentials Not Recognised / Frictionless) 33
5.4.3 Merchant Orchestrated Checkout (Consumer Credentials Not Recognised / Consumer Identity) 35
5.4.4 Merchant Orchestrated Checkout (Common Flow) 38

6 Merchant Presented QR Code Checkout 41

6.1 Use Case Overview 41
6.2 Preconditions 41
6.3 Assumptions 42
6.4 Sequence Diagrams 42

7 SRC Checkout with 3DS “ONBEHALF” 46

7.1 Use Case Overview 46
7.2 Preconditions 46
7.3 Assumptions 47
7.4 Sequence Diagrams 47

8 Management Service 51

8.1 Use Case Overview 51
8.2 Preconditions 51
8.3 Assumptions 51
8.4 Sequence Diagrams 52
8.4.1 DPA Registration and Maintenance 52

9 Authentication Facilitation Services 54

9.1 Use Case Overview 54

9.2 Preconditions 54
9.3 Assumptions 54
9.4 Sequence Diagrams 55
9.4.1 Authentication Methods Lookup 55
9.4.2 Invocation Model 1 56
9.4.3 Invocation Model 2 58
9.4.4 Invocation Model 3 59
9.4.5 Invocation Model 4 62

10 Merchant Orchestrated Recognition 64

10.1 Use Case Overview 64
10.2 Preconditions 64
10.3 Assumptions 64
10.3.1 Remember 65
10.3.2 Recognition 67
10.3.3 Un-Remember 69

11 Last Used Card 72

11.1 Use Case Overview 72
11.2 Preconditions 72
11.3 Assumptions 73
11.4 Sequence Diagrams 73

Figures

Figure 2.1: Example Enrolment Flow for Enrolment Outside Checkout 9
Figure 3.1: Example SRC Checkout Flow (Recognition) 13
Figure 3.2: Example SRC Checkout Flow (Returning Consumer Not Recognised) . 14
Figure 3.3: Example SRC Checkout Flow (Card Selection and Checkout) 16
Figure 4.1: Example Merchant Digital Card-On-File Checkout Flow (Pre-Checkout Setup)..... 21
Figure 4.2: Example Merchant Digital Card-On-File Checkout Flow (Inline-Checkout Setup)..... 23
Figure 4.3: Example Merchant Digital Card-On-File Checkout Flow (Post-Checkout Setup)..... 25
Figure 4.4: Example Merchant Digital Card-On-File Checkout Flow..... 27
Figure 4.5: Example Merchant Digital Card-On-File Merchant-Initiated Transaction Flow..... 28
Figure 5.1: Example Merchant Orchestrated Checkout (Consumer Recognised).... 32
Figure 5.2: Example Merchant Orchestrated Checkout (Consumer Credentials Not Recognised / Frictionless) Flow..... 34
Figure 5.3: Example Merchant Orchestrated Checkout (Consumer Credentials Not Recognised / Consumer Identity) Flow 36
Figure 5.4: Example Merchant Orchestrated Checkout (Consumer Identity Validation) Flow..... 37
Figure 5.5: Example Merchant Orchestrated Checkout (Common Flow) 39
Figure 6.1: Example Merchant Presented QR Code Checkout Card Selection Flow 43
Figure 6.2: Example Merchant Presented QR Code Checkout Flow 44
Figure 7.1: Example SRC Checkout with 3DS “ONBEHALF” – Initiation 47
Figure 7.2: Example SRC Checkout with 3DS “ONBEHALF” – 3DS Authentication 48
Figure 7.3: Example SRC Checkout with 3DS “ONBEHALF” – Completion 49
Figure 8.1: Example Management Service (DPA Registration and Maintenance) ... 52
Figure 9.1: Example Authentication Methods Lookup Flow 55
Figure 9.2: Example Invocation Model 1 Flow..... 57
Figure 9.3: Example Invocation Model 2 Flow..... 58
Figure 9.4: Example Invocation Model 3 Flow..... 60
Figure 9.5: Example Invocation Model 4 Flow..... 62
Figure 10.1: Example Remember Flow 66
Figure 10.2: Example Recognition Flow..... 68
Figure 10.3: Example Un-Remember Flow 70
Figure 11.1: Last Used Card – Example Identity Validation..... 73
Figure 11.2: Last Used Card – Example Identity Validation..... 74
Figure 11.3: Last Used Card – Example Card Selection 76

Tables

Table 1.1: Functionality by Use Case Examples 2
Table 1.2: EMVCo References..... 5

1 Introduction

This document, EMV® Secure Remote Commerce – Use Cases (referred to as "the Use Cases document"), is an informational supplement to the EMV Secure Remote Commerce (SRC) Specifications (collectively referred to as the "SRC Specifications"). It describes common use case examples and is intended to be read in conjunction with the SRC Specifications.

The SRC Specifications describe a common baseline set of roles and associated functions for SRC that can be adopted to meet the unique payment ecosystem requirements of international, regional, national or local implementations.

1.1 Scope

The Use Cases document describes a limited number of use case examples, including relevant variations, some of which are based on established EMV-defined technology.

These use case examples provide guidance for SRC within existing payment ecosystems and the considerations associated with various usage scenarios. They are neither exhaustive nor representative of all possible usage scenarios supported by the SRC Specifications since the associated usage scenarios may require additional considerations not provided here. Each use case has specific preconditions and assumptions which limit the scope of that use case. The absence of a particular use case does not preclude its use within SRC.

The implementation of any specific use case example contained in the Use Cases document is at the discretion of individual SRC Programmes. Implementation of each use example may vary by SRC Programme. The Use Cases document does not describe the practical implementation of any specific use case example.

Each use case may vary by payment industry implementation and as a result, all possible variations cannot be fully described. These examples exist to illustrate the potential extent and flexibility of the SRC Specifications. The guidance provided in the Use Cases document does not supersede the SRC Specifications or policies and processes defined by an SRC Programme.

1.2 Overview

The use case examples fall into three broad categories:

- Enrolment (Section 2)
- Checkout (Sections 3 to 7)

- SRC Checkout (Section 3)
- Merchant Digital Card-On-File Checkout (Section 4)
- Merchant Orchestrated Checkout (Section 5)
- Merchant Presented QR Code Checkout (Section 6)
- SRC Checkout with 3DS “ONBEHALF” (Section 7)

- Other Services (Sections 8 to 11)
  - Management Service (Section 8)
  - Authentication Facilitation Services (Section 9)
  - Merchant Orchestrated Recognition (Section 10)
  - Last Used Card (Section 11)

Table 1.1 shows the functionality offered by each use case example, along with optional functionality that can be offered to complement the use case.

Table 1.1: Functionality by Use Case Examples

Use Case Example	Enrolment	Checkout	Optional Functionality	Other Services
Enrolment (Section 2)	X			
SRC Checkout (Section 3)		X	X	
Merchant Digital Card-On-File Checkout (Section 4)		X		
Merchant Orchestrated Checkout (Section 5)		X		
Merchant Presented QR Code Checkout (Section 6)		X		
SRC Checkout with 3DS “ONBEHALF” (Section 7)		X	X	
Management Service (Section 8)				X
Authentication Facilitation Services (Section 9)				X

Use Case Example	Enrolment	Checkout	Optional Functionality	Other Services
Merchant Orchestrated Recognition (Section 10)			X	X
Last Used Card (Section 11)			X	X

Optional functionality includes:

- Binding
- Delete card
- Digital Card management / selection
- Management of remembered / unremembered states
- 3DS “ONBEHALF”

Any optional functionality is complementary to primary function of the use case example. It is at the discretion of the SRC System or the merchant or commerce provider offering the checkout as to whether any of these are available to the Consumer. For merchant checkout use cases, it is likely that any additional functionality may require a redirection to a domain separate from the merchant domain (for example, to a separate DCF domain).

1.2.1 Enrolment

Enrolment can occur as a standalone event, or within a checkout. In the current use case examples, Enrolment is shown as a standalone event.

1.2.2 Checkout

Checkout allows a merchant or commerce provider to request permission to use a payment method, represented by a Digital Card, for a Consumer’s purchase of the merchant’s product or service. Checkout may also include:

- SRC Trigger (e.g. Click to Pay trigger)
- Collection of personal information from the Consumer to facilitate payment verification or represent a bill of sale
- Collection or selection of delivery information for the purchased goods or services

Once a Digital Card has been selected for payment, the Consumer reviews and confirms it. The merchant then interacts with its e-commerce environment to process the authorisation using the payload provided by the SRC System.

The SRC Specifications do not provide any requirements for payment authentication nor govern activities within it. However, they offer the Digital Payment Application the choice to conduct payment authentication:

- During a checkout, when it is facilitated by the SRC System
- After a checkout

The SRC Specifications support the option for SRC Participants to implement other EMV technologies during checkout, such as Payment Tokenisation and EMV 3-D Secure. The SRC Participants will conform to requirements defined by Payment Tokenisation and EMV 3-D Secure implementations.

The SRC Specifications offer the flexibility to support a variety of checkout experiences. These differences are influenced by:

- SRC Participants commonly associated with the use case
- Functions performed by each SRC Participant
- SRC Participants that deliver the user experience
- Trigger mechanism presented to initiate a checkout
- Presence or absence of the Consumer and/or Consumer Device

The SRC Specifications support the ability for implementations to provide Cardholder-Initiated and Merchant-Initiated Transactions as defined in EMV® Best Practices Document – Recommendations for EMV Processing for Industry-Specific Transaction Types. These are reliant on unique rules and policies of Payment Systems, along with any required Consumer disclosures.

- Cardholder-Initiated Transactions are invoked through a Digital Payment Application on a Consumer Device by activating an SRC Trigger. The user experience depends on whether it is a merchant checkout or an SRC checkout
- Merchant-Initiated Transactions do not involve the Consumer or the Consumer Device. All Merchant-Initiated Transactions are managed by the merchant or its payment provider, involve industry specific events or standing instructions (such as reauthorisation, split shipment or recurring payments) and follow on from a previously successful Cardholder-Initiated Transaction

1.2.3 Other Services

This is a broad category which covers all other services not directly related to enrolment or checkout. This includes services such as recognition and authentication facilitation, which can be used during checkout.

1.3 Audience

The Use Cases 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

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 1.2 contain provisions that are referenced in this guide and are available from www.emvco.com.

Table 1.2: EMVCo References

Reference	Publication Name
EMV 3-D Secure Specification	EMV® 3-D Secure – Protocol and Core Functions Specification
Payment Tokenisation	EMV® Payment Tokenisation Specification – Technical Framework
SRC Core Specification	EMV® Secure Remote Commerce Specification
SRC Reproduction Requirements	EMV® Secure Remote Commerce (SRC): Click to Pay Icon Reproduction Requirements
SRC UI Guidelines and Requirements	EMV® Secure Remote Commerce Specification – User Interface Guidelines and Requirements
SRC API	EMV® Secure Remote Commerce Specification – API
SRC JavaScript SDK	EMV® Secure Remote Commerce Specification – JavaScript SDK
SRC Version Management	EMV® Secure Remote Commerce Version Management for SRC API and JavaScript SDK Specifications
Transaction Types	EMV® Best Practices Document – Recommendations for EMV Processing for Industry-Specific Transaction Types

Collectively, the term SRC Specifications refers to the following documents, with this version of the Use Cases document compatible with the following versions:

- SRC Core Specification v1.1
- SRC UI Guidelines and Requirements v1.1
- SRC API v1.2
- SRC JavaScript SDK v1.2

For the following documents, please refer to the latest published version:

- SRC Reproduction Requirements
- SRC Version Management

1.5 Definitions

For a list of defined terms used in the Use Cases document, please refer to Table 1.3 in Section 1.8 of the SRC Core Specification.

1.6 Notational Conventions

1.6.1 Abbreviations

For a list of abbreviations used in the Use Cases document, please refer to Table 1.4 in Section 1.9 of the SRC Core Specification.

1.6.2 Terminology and Conventions

The Use Cases document uses the following words which have a specific meaning:

Assumptions

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

Preconditions

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

Usage Scenario

A specific instance of SRC Specifications usage that has common, distinct characteristics such as technologies used, etc. This is usually representing the presentment, acceptance and intended payment offering to Consumers in the ecosystem.

Use Case

A specific example of utilisation of the SRC Specifications within a usage scenario, showing specifics of interactions between SRC roles. It includes an overview of the use case, the preconditions for the use case and specific assumptions that apply to given use case example(s), along with sequence diagrams for those use case example(s).

1.7 Further Information

Additional information about SRC can be found at www.emvco.com.

2 Enrolment

Enrolment is the process of associating a PAN with an existing or new SRC Profile. It can occur as a standalone event, or within a checkout. It is described here as an independent use case, with the specific use case example given representing an enrolment which takes place outside of a checkout.

2.1 Use Case Overview

The Card Enrolment operation either enrols a Consumer and Digital Card (associated with an underlying PAN) to a new SRC Profile, or it adds a Digital Card to an existing SRC Profile.

2.2 Preconditions

The following preconditions apply to this use case:

- The Card Issuer has onboarded with the SRC System
- The Consumer has one or more Payment Cards for that are eligible for Enrolment

2.3 Assumptions

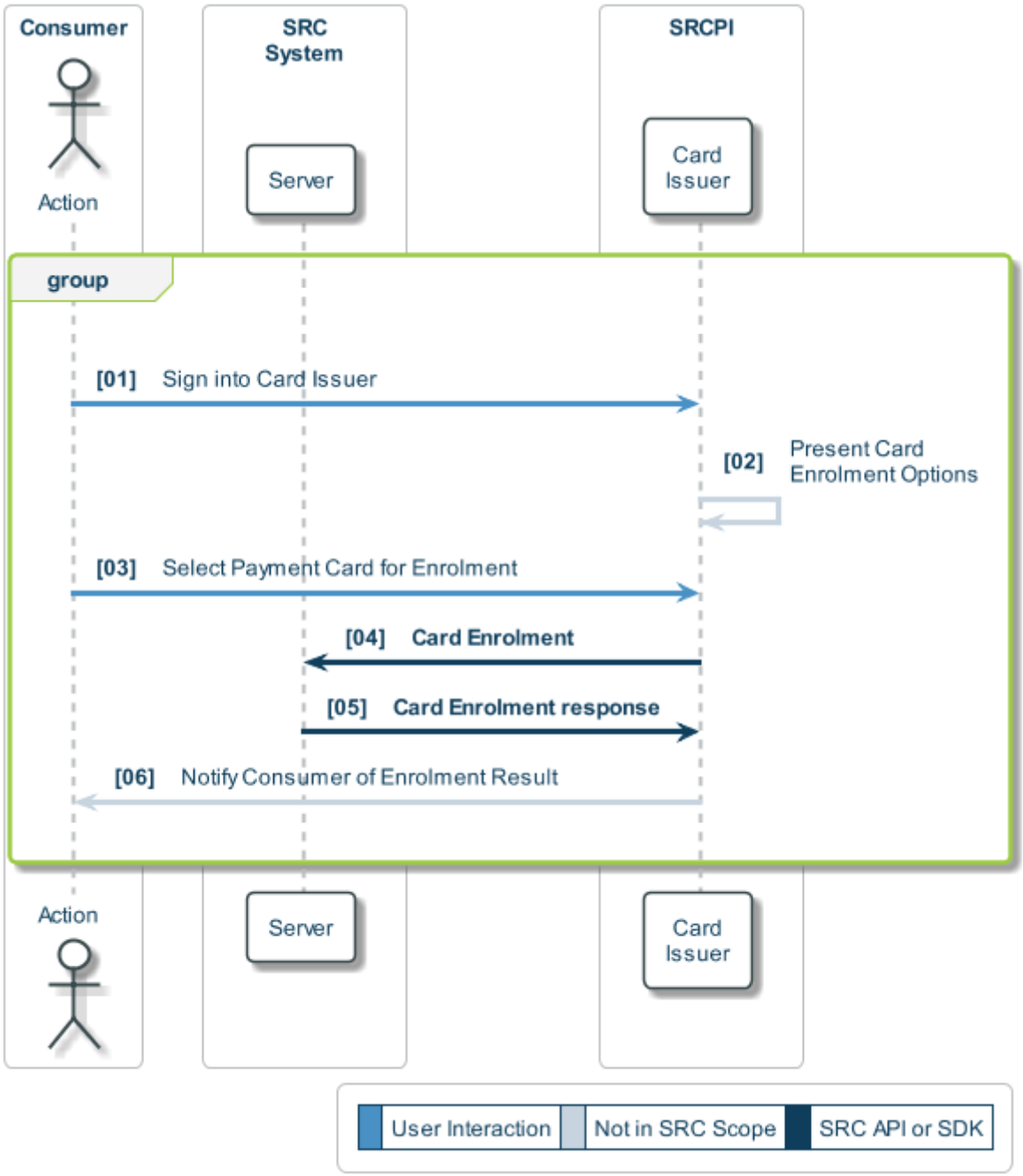
The following assumptions apply to this use case example:

- The Enrolment is initiated by the Card Issuer, based on an interaction between the Card Issuer and Consumer
- Assurance and the related ID&V is performed by the Card Issuer, resulting in the SRC Assurance Method value being set to one of the Card Issuer SRC Assurance Method Categories

2.4 Sequence Diagrams

Figure 2.1 shows an example Enrolment flow, with numbered steps which are explained following the figure. In this specific use case example, the Enrolment takes place outside of a checkout.

Figure 2.1: Example Enrolment Flow for Enrolment Outside Checkout



01. The Consumer signs into the Card Issuer application
02. The Card Issuer application presents the eligible Payment Cards and Enrolment options to the Consumer
03. The Consumer chooses to enrol a Payment Card into an SRC System (Click to Pay)
04. The Card Issuer calls the Card Enrolment operation, sending the PAN and related data associated with the Payment Card to the SRC System

05. The SRC System enrols the Consumer and Payment Card, providing a response to the Card Issuer
06. The Card Issuer notifies the Consumer of the Enrolment results

3 SRC Checkout

SRC checkout is the facilitation of checkout orchestrated by an SRC Initiator integrating the SDKs of one or more SRC System(s) in order to simplify and streamline purchase experiences across multiple Digital Payment Applications. It enables Consumers with at least one SRC Profile to access their Digital Cards across participating Digital Payment Applications for single and repeat uses.

SRC checkout is characterised by the following:

- Presentation of an SRC Trigger that initiates a checkout experience
- SRC Initiator presentation of any Digital Card(s) returned by an SRC System that recognises or can identify the Consumer
- Following selection of a Digital Card for payment, Digital Card Facilitator presentation for review and confirmation of details
- The ability of the Consumer to choose to be remembered or not
- Usage of the payload returned by an SRC System to process the authorisation

3.1 Use Case Overview

The SRC checkout use case consists of the following:

- The Consumer visits a merchant e-commerce environment that includes a Click to Pay trigger (underpinned by an SRC Initiator integrating the SDKs of one or more SRC Systems) at checkout
- The Consumer does not sign in to a merchant account and proceeds as a guest by activating the Click to Pay trigger

There are two variations, depending on whether the Consumer is recognised:

- Returning Consumer (Recognised):
  - A frictionless method of recognition is available (returning recognized consumer)
- Returning Consumer (Not Recognised)
  - The Consumer is prompted to enter a Consumer Identity

3.2 Preconditions

The following preconditions apply to this use case:

- The Consumer has enrolled with one or more SRC System(s)

- The merchant has integrated an SRC Initiator into its e-commerce environment
- The SRC Initiator has onboarded with at least one SRC System where the Consumer has enrolled

3.3 Assumptions

The following assumptions apply to the Returning Consumer (Recognised) use case example:

- The Consumer Device is recognised by at least one SRC System

The following assumptions apply to the Returning Consumer (Not Recognised) use case example:

- The Consumer Device is not recognised by any SRC System, resulting in additional recognition and identity validation steps

3.4 Sequence Diagrams

Two variations to the use case are presented:

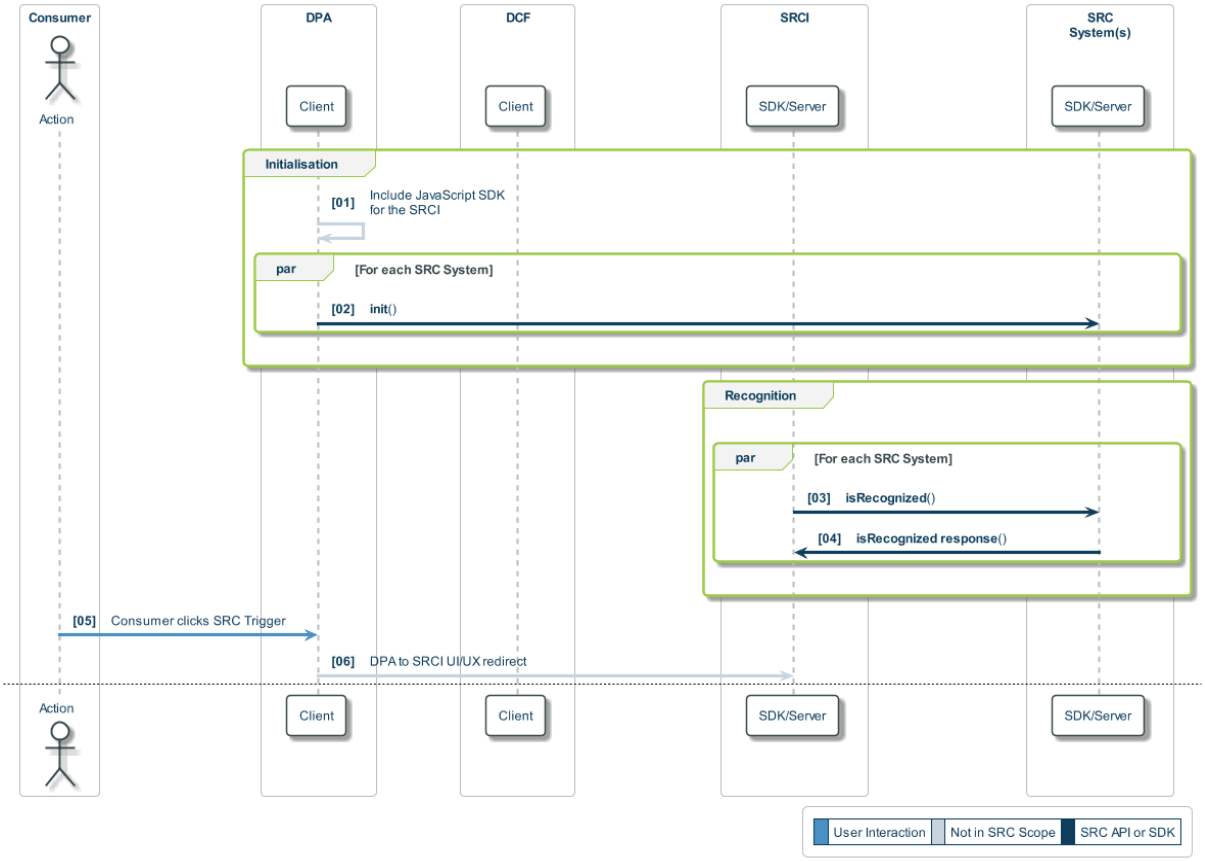
- Returning Consumer (Recognised)
- Returning Consumer (Not Recognised)

Both variations follow the same overall flow, starting with common initialisation and recognition steps. In the case of the Returning Consumer (Not Recognised) variation, additional recognition and additional identity validation steps take place. Both variations then end with common steps to prepare the SRC Profile, allow the Consumer to select a Digital Card and to enable the merchant to complete the transaction.

Note that the sequence diagrams show the flows using SDK methods. However, the same flow can be performed using API operations.

Figure 3.1 shows the start of an example SRC checkout flow, with numbered steps which are explained following the figure. In this figure, if the returning Consumer is not recognised by at least one SRC System, then the additional recognition steps take place.

Figure 3.1: Example SRC Checkout Flow (Recognition)

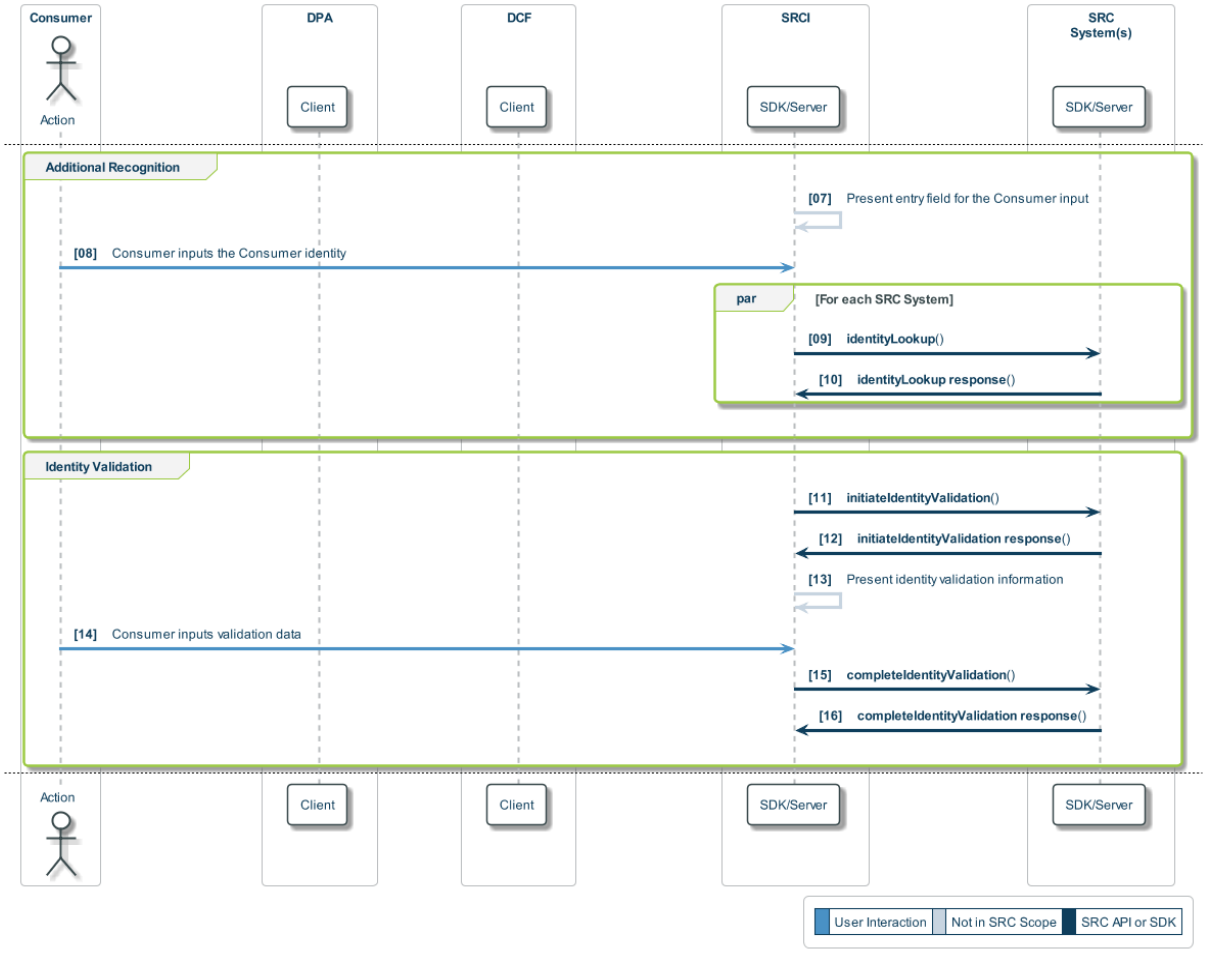


01. On rendering the page containing the Click to Pay trigger, the Digital Payment Application (DPA) includes JavaScript for the SRC Initiator (SRCI)
02. For each SRC System from which the merchant accepts payment, the SRCI calls the init() method of the SRC System's SDK to initialise it
03. For each SRC System, the SRCI calls the isRecognized() method
04. Each SRC System responds indicating whether the Consumer has been recognised:
    - For the Returning Consumer (Recognised) variation, one or more SRC Systems respond, indicating that the Consumer Device / Consumer is recognised and returning a Federated ID Token
    - For the Returning Consumer (Not Recognised) variation, all the SRC Systems respond, indicating that the Consumer has not been recognised
05. The Consumer chooses Click to Pay as the payment method by clicking the SRC Trigger
06. The DPA redirects the UI/UX to the SRCI

For the Returning Consumer (Recognised) variation, the flow continues in Figure 3.3, with the SRCI using the returned Federated ID Token(s) to retrieve one or more SRC Profiles. However, before this can happen in the Returning Consumer (Not Recognised) variation, the

following additional recognition and identity validation flow takes place, which is shown in Figure 3.2.

Figure 3.2: Example SRC Checkout Flow (Returning Consumer Not Recognised)

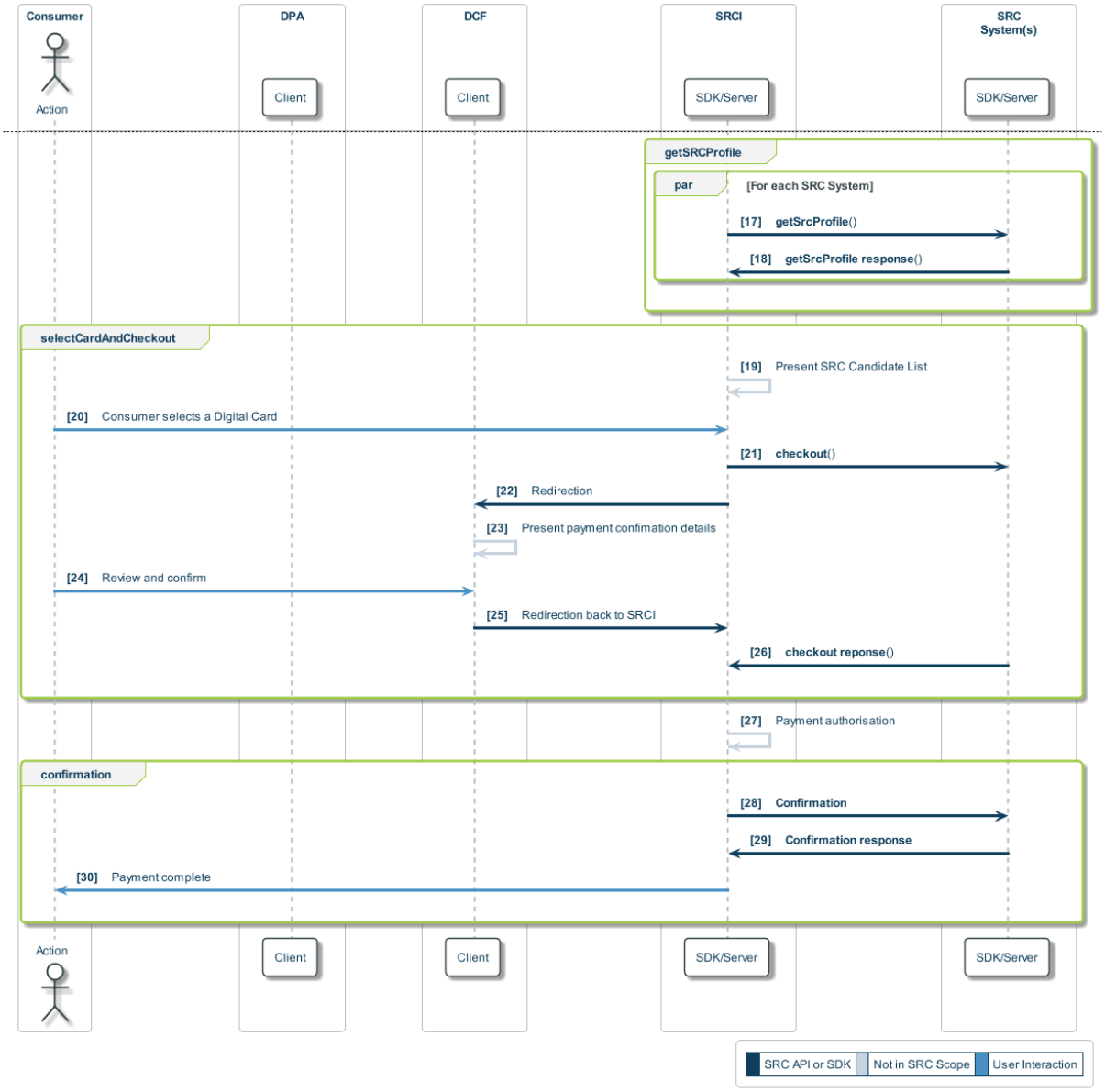


07. The SRCI presents an entry field for the Consumer to input a Consumer Identity (email or phone number)
08. The Consumer inputs a Consumer Identity
09. For each SRC System, the SRCI calls the identityLookup() method using the Consumer Identity provided by the Consumer
10. One or more SRC Systems respond, indicating that the Consumer Device / Consumer is recognised and providing options for validating the Consumer Identity
11. The SRCI calls the initiateIdentityValidation() method for the SRC System which responded (if more than one SRC System responds, the SRCI needs only call one SRC System)
12. The SRC System responds with a message to be presented to the Consumer

13. The SRCI presents any relevant identity validation information to the Consumer and, if necessary, enables the Consumer to provide the required validation data
14. The Consumer inputs the validation data
15. The SRCI calls the completeIdentityValidation() method, providing any relevant validation data
16. The SRC System returns a Federated ID Token

At this point, regardless of the variation, the SRCI has received Federated ID Token(s) from one or more SRC Systems. Both variations continue with the flows shown in Figure 3.3 which cover the card selection and checkout steps of the example SRC checkout flow.

Figure 3.3: Example SRC Checkout Flow (Card Selection and Checkout)



17. For each SRC System, the SRCI calls the getSrcProfile() method using the returned Federated ID Token
18. Each SRC System that is called responds with a list of SRC Profiles
19. The SRCI presents the Consumer with the SRC Candidate List (comprising of the available Digital Cards from each of the Consumer's SRC Profiles)
20. The Consumer selects a Digital Card from the SRC Candidate List
21. The SRCI calls the checkout() method for the corresponding SRC System based on the selected Digital Card

22. The SRCI redirects the UX to the corresponding Digital Card Facilitator (DCF) based on the selected Digital Card
23. The DCF displays the review and confirm information to the Consumer
24. The Consumer reviews the information for correctness and confirms payment
25. The DCF redirects the UX back to SRCI
26. The SRC System responds to the SRCI with checkout related data including the payload
27. The SRCI uses the payload and initiates payment authorisation as defined per agreements with the merchant and the merchant's payment processor. Authorisation occurs after checkout, but can be delayed at the merchant's discretion
28. Following successful payment authorisation, the SRCI calls the Confirmation operation
29. The SRC System responds to the SRCI with the confirmation response
30. The SRCI notifies the Consumer that payment is complete

4 Merchant Digital Card-On-File Checkout

Merchant Digital Card-on-file is a type of merchant checkout that integrates with one or more SRC System(s) to allow the Consumer to designate a Digital Card as a merchant Digital Card-on-file for purchases. This provides the Consumer with simplified, streamlined purchase experiences across the merchant's Digital Payment Applications.

Note that when a Consumer designates a Digital Card as a merchant Digital Card-on-file, this only applies to the specific merchant which is driving the checkout experience.

Merchant Digital Card-on-file is characterised by:

- Presentation of Click to Pay trigger provided by the merchant that:
  - Uses the merchant Digital Card-on-file for the current purchase; *or*
  - If the Consumer has not previously designated a merchant Digital Card-on-file, initiates retrieval of Digital Cards so that the Consumer can designate one as the merchant Digital Card-on-file (Digital Card-on-file setup)
- Merchant can use the merchant Digital Card-on-file for any subsequent Merchant-Initiated Transactions
- Usage of the payload returned by an SRC System to process the authorisation
- Digital Payment Application, and related SRC Initiator and Digital Card Facilitator functionality, all provided by the merchant

Selection of a merchant Digital Card-on-file is described further in Section 4.1 Use Case Overview.

4.1 Use Case Overview

There are two elements to the Merchant Digital Card-on-file Checkout use case:

- Digital Card-on-file setup, which describes how the Consumer designates a merchant Digital Card-on-file and agrees to the merchant's T&Cs for use of a merchant Digital Card-on-file
- Checkout, which describes the use of the merchant Digital Card-on-file during Cardholder-Initiated and Merchant-Initiated Transactions

There are three Merchant Digital Card-on-file setup variants, which depend on when the Consumer designates a merchant Digital Card-on-file / agrees to the merchant's T&Cs:

- Pre-checkout setup
- Inline-checkout setup
- Post-checkout setup

Once a merchant Digital Card-on-file has been designated, any subsequent Cardholder-Initiated Transactions with that merchant will result in the merchant Digital Card-on-file being presented to the Consumer by the merchant during checkout. The trigger, navigation, and confirmation for the merchant Digital Card-on-file is rendered by the merchant. Some form of step-up may be performed by merchant for the use of a merchant Digital Card-on-file.

Additionally, if the merchant has been authorised by the Consumer to make recurring payments using the merchant Digital Card-on-file, this will result in one or more Merchant-Initiated Transactions.

4.2 Preconditions

The following preconditions apply to this use case:

- The merchant:
  - Provides the Digital Payment Application, and related SRC Initiator and Digital Card Facilitator functionality
  - Has onboarded to one or more SRC System(s)
  - Controls the Consumer acceptance of merchant T&Cs for use of a merchant Digital Card-on-file
  - Controls the checkout experience
- The Consumer has enrolled one or more Payment Card(s) with one or more SRC System(s)
- The Consumer has created a Consumer account with the merchant

4.3 Assumptions

The following assumptions apply to all the use case examples except the Merchant-Initiated Transaction use case example:

- The Consumer has signed into the Consumer account at the merchant
- On selecting Click to Pay, the Consumer is recognised by the SRC System and successfully completes any required verification

The following assumption applies to the post-checkout variation:

- The Consumer has successfully completed a purchase and the Consumer decides to designate the card used as the merchant Digital Card-on-file for that merchant

The following assumption applies to the two checkout only use case examples:

- The Consumer has successfully designated a merchant Digital Card-on-file

The following assumptions apply to the Merchant-Initiated Transaction use case example:

- The Consumer has successfully completed a Cardholder-Initiated Transaction at the merchant using the merchant Digital Card-on-file
- The Consumer has agreed to the merchant's T&Cs for a recurring payment to be made using the merchant Digital Card-on-file

4.4 Sequence Diagrams

There are several sequence diagrams, each of which illustrates a specific use case example or variation. The first two sequence diagrams illustrate various Digital Card-on-file setup flows, which depend on when the Consumer designates a merchant Digital Card-on-file:

- Pre-Checkout Setup (Section 4.4.1)
- Inline-Checkout / Post-Checkout Setup (Section 4.4.2)

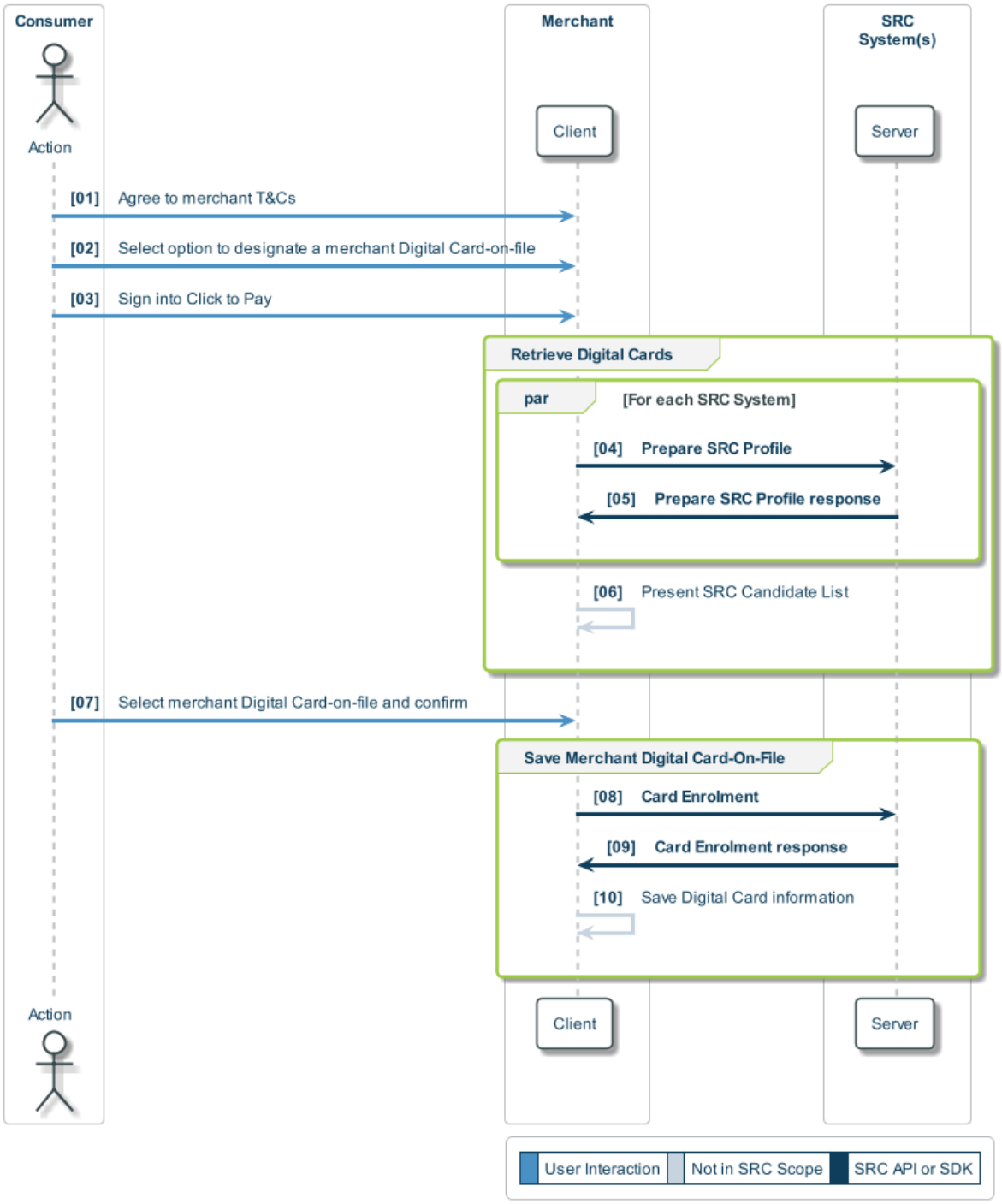
The remaining sequence diagrams illustrate various checkout flows once a merchant Digital Card-on-file has been designated for the Consumer's use at that merchant.

- Merchant Digital Card-On-File Checkout (Section 4.4.3)
- Merchant Digital Card-On-File Merchant-Initiated Transaction (Section 4.4.4)

4.4.1 Pre-Checkout Setup

Figure 4.1 shows an example flow where the Consumer designates a merchant Digital Card-on-file at the merchant prior to a checkout, with numbered steps which are explained following the figure.

Figure 4.1: Example Merchant Digital Card-On-File Checkout Flow (Pre-Checkout Setup)



01. The Consumer agrees to the merchant T&Cs to designate a merchant Digital Card-on-file with Click to Pay
02. The Consumer selects the option to designate a merchant Digital Card-on-file with Click to Pay

03. The Consumer signs into Click to Pay, following standard recognition / identity validation steps which are not shown here (see Section 10 Merchant Orchestrated Recognition)
04. For each SRC System where the Consumer is recognised, the merchant calls the Prepare SRC Profile operation to retrieve the Consumer's SRC Profile
05. The SRC System returns the SRC Profile to the merchant
06. The merchant presents the Consumer with the SRC Candidate List (comprising of the available Digital Cards from each of the Consumer's SRC Profiles)
07. The Consumer selects a Digital Card from the SRC Candidate List to be the merchant Digital Card-on-file at that merchant and confirms the selection
08. The merchant calls the Card Enrolment operation for the selected Digital Card with a unique service identifier to indicate to the SRC System that this is the merchant Digital Card-on-file (for that merchant)
09. The SRC System returns the Digital Card information to the merchant
10. The merchant saves the Digital Card information, which will be used as the merchant Digital Card-on-file for the Consumer at that merchant

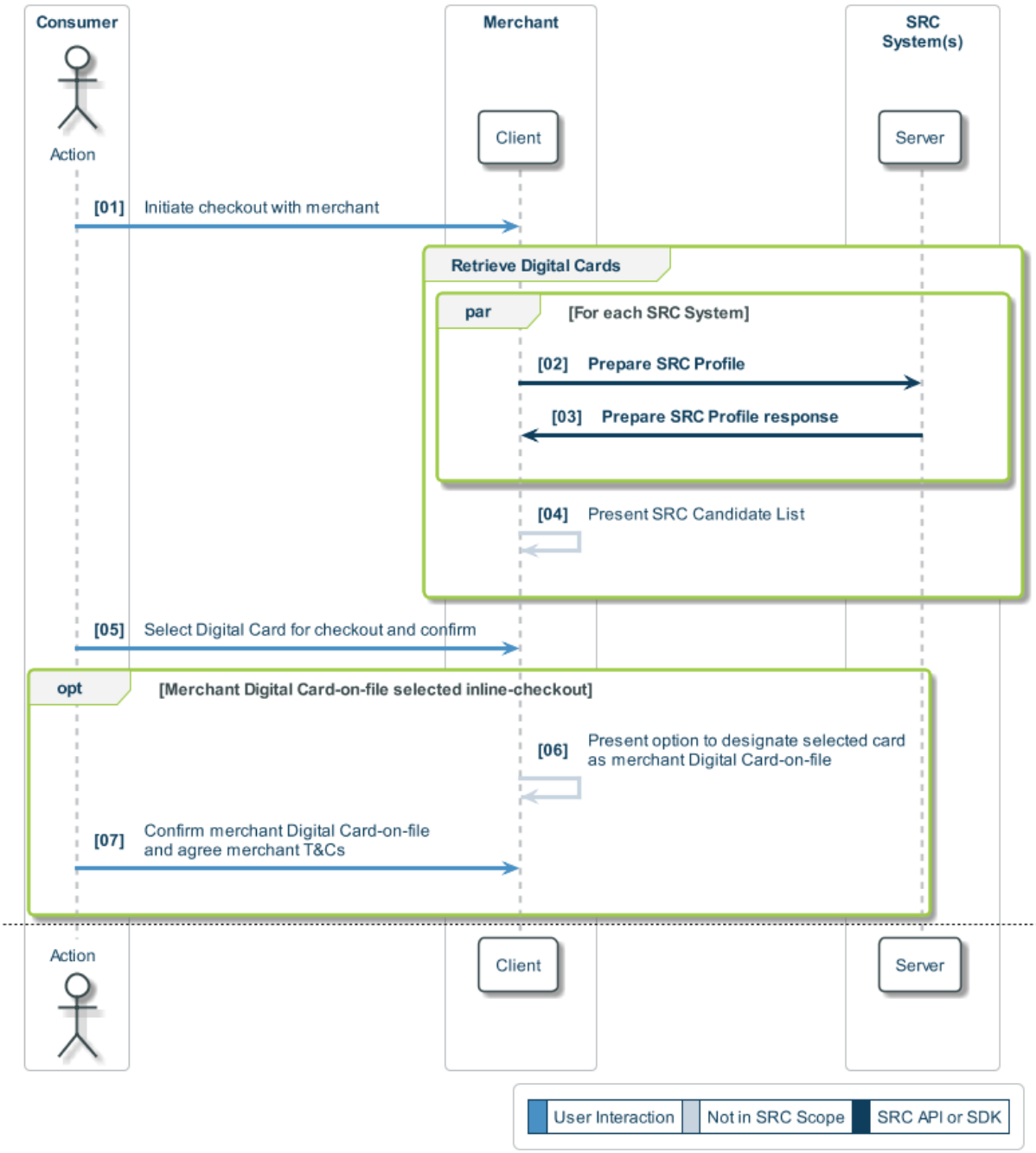
Now that the Consumer has designated a merchant Digital Card-on-file, this will be presented as the default card in any subsequent checkout at that merchant (see Section 4.4.3 Merchant Digital Card-On-File Checkout).

4.4.2 Inline-Checkout / Post-Checkout Setup

Figure 4.2 and Figure 4.3 show an example flow where the Consumer designates a merchant Digital Card-on-file at the merchant either during the checkout (inline-checkout) or once checkout is complete (post-checkout). Both flows have common steps which are explained following the figures, while optional steps are shown for:

- Inline-checkout setup (Figure 4.2)
- Post-checkout setup (Figure 4.3)

Figure 4.2: Example Merchant Digital Card-On-File Checkout Flow (Inline-Checkout Setup)



01. The Consumer initiates checkout with the merchant by selecting Click to Pay as the payment method for checkout and signs into Click to Pay, following standard recognition / identity validation steps which are not shown here (see Section 10 Merchant Orchestrated Recognition)
02. For each SRC System where the Consumer is recognised, the merchant calls the Prepare SRC Profile operation to retrieve the Consumer's SRC Profile

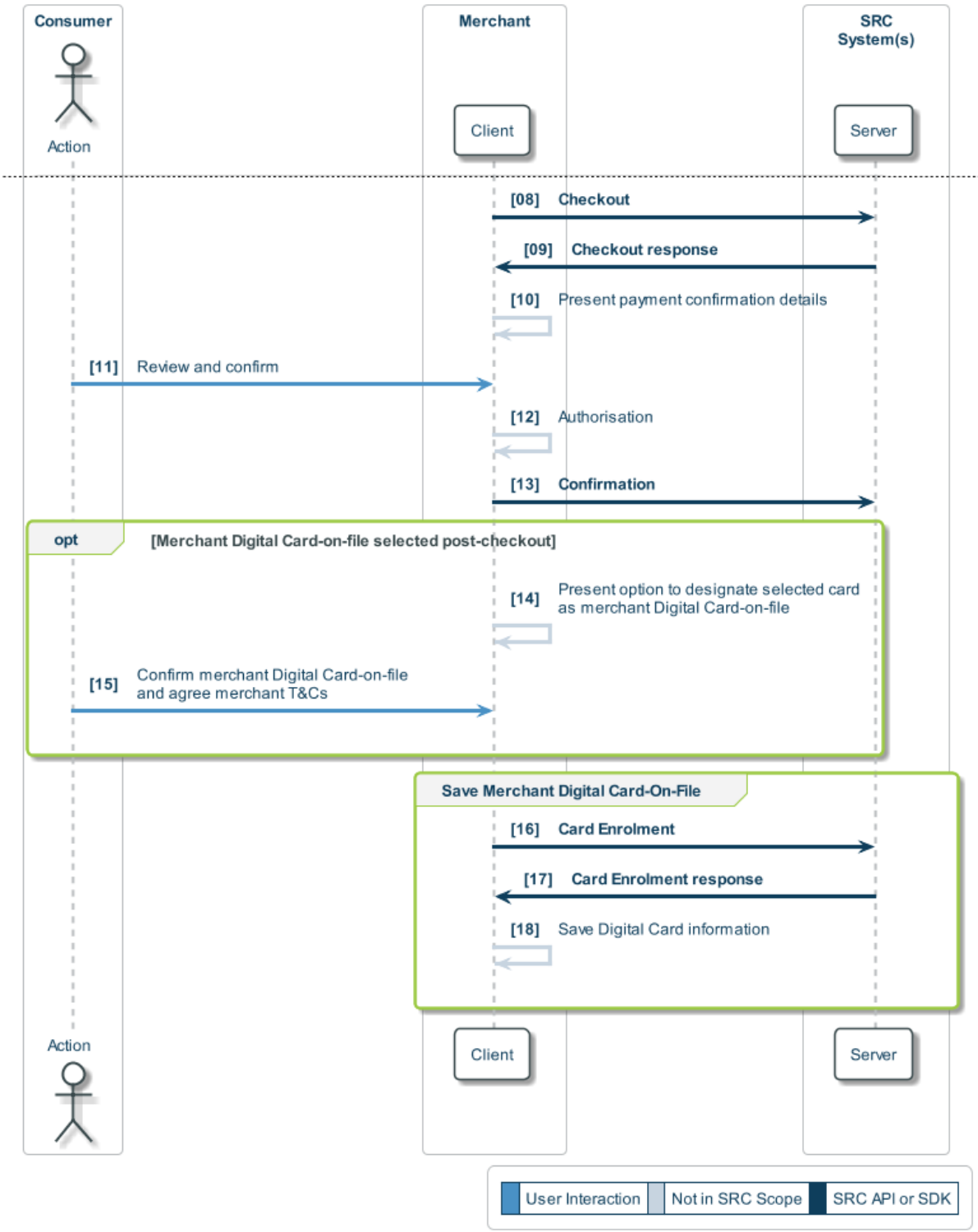
03. The SRC System returns the SRC Profile to the Merchant
04. The Merchant presents the Consumer with the SRC Candidate List (comprising of the available Digital Cards from each of the Consumer's SRC Profiles)
05. The Consumer selects a Digital Card from the SRC Candidate List to be used for checkout and confirms the selection

Steps [06] to [07] only occur during the inline-checkout setup variation.

06. The mechant presents the Consumer with the option to designate the selected Digital Card as the merchant Digital Card-on-file for that merchant
07. The Consumer confirms the merchant Digital Card-on-file and agrees to the merchant's T&Cs

Figure 4.3 shows the remaining steps for the combined flows, including the optional steps for post-checkout setup.

Figure 4.3: Example Merchant Digital Card-On-File Checkout Flow (Post-Checkout Setup)



08. The merchant sends the checkout (including information on the selected Digital Card) to the SRC System for payload retrieval, authorisation and confirmation (Steps [08] to [13], which are not individually described)

Steps [14] to [15] only occur during the post-checkout setup variation.

14. The mechant presents the Consumer with the option to designate the card used during checkout as the merchant Digital Card-on-file for that merchant
15. The Consumer confirms the merchant Digital Card-on-file and agrees to the merchant's T&Cs

Regardless of whether the merchant Digital Card-on-file was designated by the inline-checkout or post-checkout variation, the following common steps conclude the example flow.

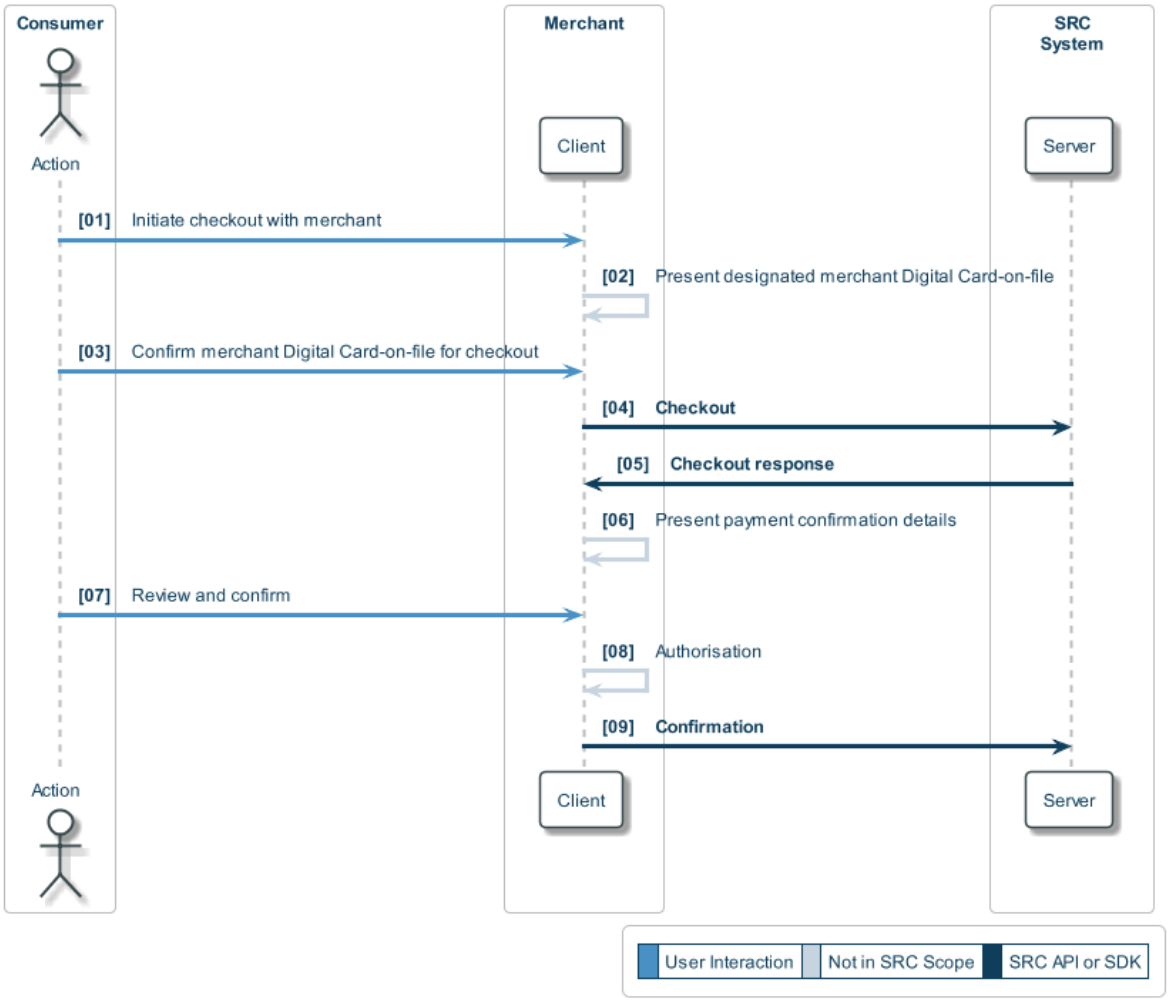
16. The merchant calls the Card Enrolment operation for the selected Digital Card with a unique service identifier to indicate to the SRC System that this is the merchant Digital Card-on-file (for that merchant)
17. The SRC System returns the Digital Card information to the merchant
18. The merchant saves the Digital Card information, which will be used as the merchant Digital Card-on-file for the Consumer at that merchant

Now that the Consumer has designated a merchant Digital Card-on-file, this will be presented as the default card in any subsequent checkout at that merchant (see Section 4.4.3 Merchant Digital Card-On-File Checkout).

4.4.3 Merchant Digital Card-On-File Checkout

Figure 4.4 shows an example flow where the Consumer uses a merchant Digital Card-on-file at the merchant for checkout, with numbered steps which are explained following the figure.

Figure 4.4: Example Merchant Digital Card-On-File Checkout Flow

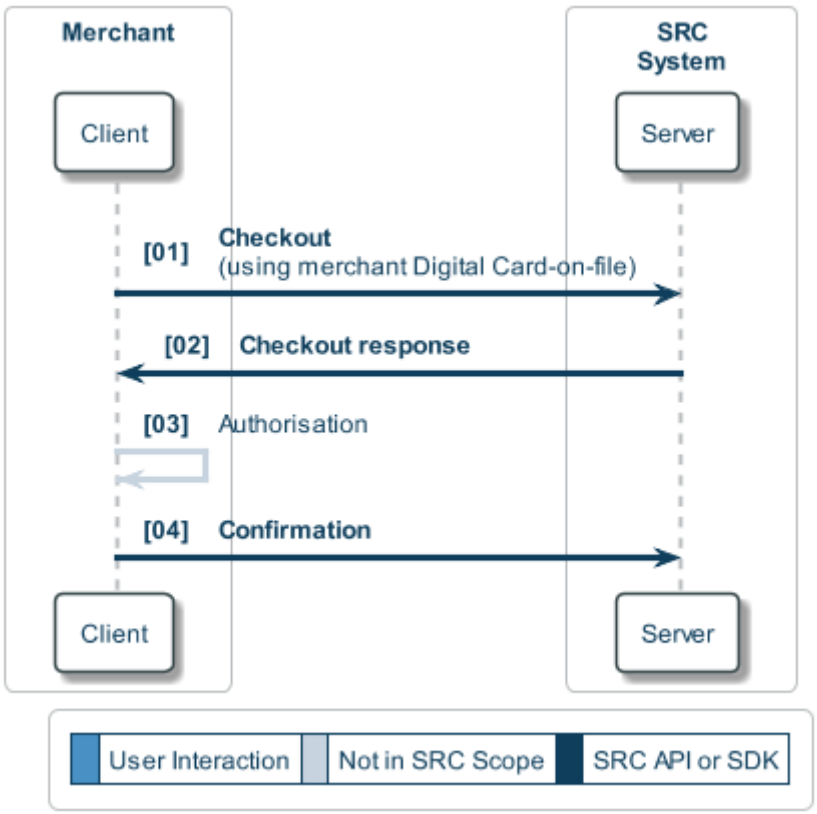


01. The Consumer initiates checkout with the merchant
02. The merchant displays the designated merchant Digital Card-on-file for confirmation by the Consumer
03. The Consumer confirms the merchant Digital Card-on-file for checkout
04. The merchant sends the checkout to the SRC System (including the stored Digital Card information representing the merchant Digital Card-on-file) for payload retrieval, authorisation and confirmation (Steps [04] to [09], which are not individually described)

4.4.4 Merchant Digital Card-On-File Merchant-Initiated Transaction

Figure 4.5 shows an example flow where the Consumer's merchant Digital Card-on-file is used by the merchant for a subsequent Merchant-Initiated Checkout, with numbered steps which are explained following the figure.

Figure 4.5: Example Merchant Digital Card-On-File Merchant-Initiated Transaction Flow



01. The merchant selects the merchant Digital Card-on-file and sends the checkout (including the stored Digital Card information representing the merchant Digital Card-on-file) to the SRC system for payload retrieval, authorisation and confirmation (Steps [01] to [04], which are not individually described)

5 Merchant Orchestrated Checkout

Merchant orchestrated checkout is a type of merchant checkout. It provides a purchase experience which is fully integrated within the merchant's current checkout experience. It enables Consumers with one or more SRC Profile(s) to access to Digital Cards for use within checkout.

For merchant orchestrated checkout, the SRC Trigger is integrated with the merchant's checkout call-to-action and is not a separate Click to Pay call-to-action. If the Consumer needs to enter a Consumer Identity, a step-up is required to verify the Consumer Identity.

Merchant orchestrated checkout is characterised by:

- Presentation of an integrated merchant trigger that initiates a checkout experience and includes the Click to Pay Icon and SRC System operating images in close proximity to the trigger.
- Presentation of any Digital Card(s) returned by an SRC System that recognises or can identify the Consumer
- Following selection of a Digital Card for payment, presentation of review and confirmation details
- Usage of the payload returned by an SRC System to process the authorisation
- The Digital Payment Application, and related SRC Initiator and Digital Card Facilitator functionality, all provided by the merchant

5.1 Use Case Overview

There are several variations to the Integrated Checkout use case, depending on:

- Whether the Consumer is:
  - Signed into a merchant account
  - Checking out as a guest (either does not have an account or has not signed in)
- If the Consumer is signed into a merchant account, whether the Consumer is:
  - Recognised by one or more SRC System(s) using the phone number or email in the Consumer's merchant profile
  - Not recognised by any SRC System
- If the phone number or email in the Consumer's merchant profile are not recognised or the Consumer is a guest, whether:
  - The Consumer is prompted to enter a Consumer Identity

- There is an alternate frictionless method of recognition which does not involve Consumer interaction

These alternatives can be summarised as follows:

- Consumer signs into an account and is recognised:
  - Consumer recognised
- Consumer signs into an account and is not recognised or Consumer checks out as a guest. In both cases, which are equivalent to the Consumer not being recognised, a further recognition step is required, which is either:
  - Frictionless; *or*
  - Consumer Identity

The navigation to the point in checkout where the Digital Cards are presented to the Consumer is rendered by the merchant.

5.2 Preconditions

The following preconditions apply to this use case:

- The merchant:
  - Provides the Digital Payment Application and related SRC Initiator and Digital Card Facilitator functionality
  - Has onboarded to one or more SRC System(s) as an integrated merchant
- The Consumer has enrolled at one or more Payment Card(s) with one or more SRC System(s)

5.3 Assumptions

The following assumptions apply to this use case example when the Consumer has an account:

- The merchant and SRC System have agreed that the merchant's management of Consumer sign-in is an adequate form of Consumer Assurance
- The Consumer is recognised if an email or phone number contained in the Consumer's merchant account is also used as a Consumer Identity in one or more SRC System(s)

5.4 Sequence Diagrams

There are three sequence diagrams, each of which illustrates a specific variation of the use case example. These are:

- Merchant Orchestrated Checkout (Consumer Recognised) (Section 5.4.1)
- Merchant Orchestrated Checkout (Consumer Credentials Not Recognised / Frictionless) (Section 5.4.2)
- Merchant Orchestrated Checkout (Consumer Credentials Not Recognised / Consumer Identity) (Section 5.4.3)

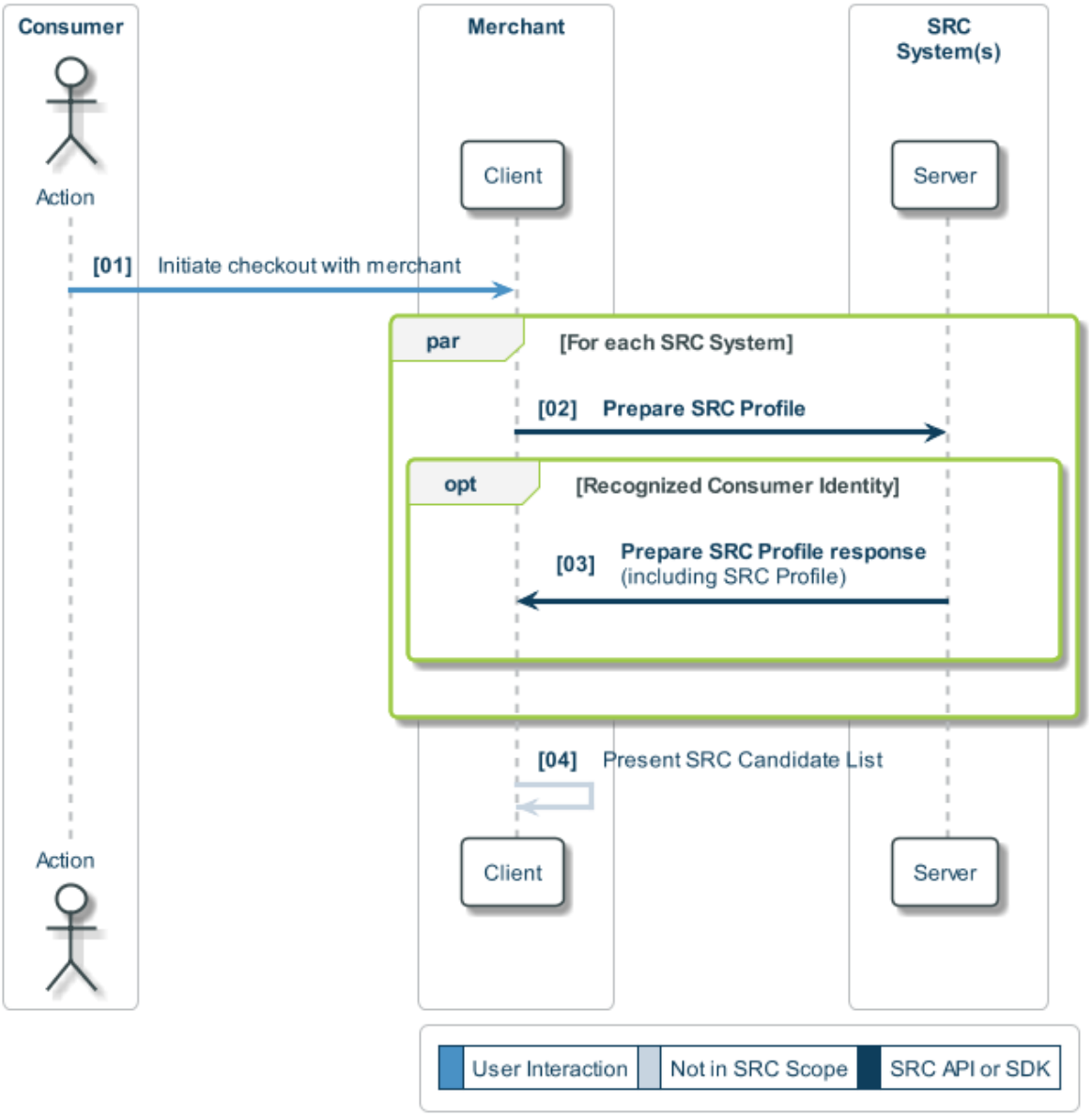
Each of the example flows in the sections above ends with the SRC Candidate List being presented to the Consumer by the merchant, after which all the variations have a common checkout flow, shown in Section 5.4.4 Merchant Orchestrated Checkout (Common Flow).

The Digital Payment Application, SRC Initiator and Digital Card Facilitator functions are all represented by “merchant / client” in the sequence diagrams. The sequence diagrams illustrate the functionality using API operations, although it can also be implemented using SDK methods, which are not shown.

5.4.1 Merchant Orchestrated Checkout (Consumer Recognised)

Figure 5.1 shows an example flow where the Consumer signs into a merchant account and is recognised by the SRC System. After the presentation of the SRC Candidate List, the flow continues as shown in Figure 5.5 with the selection of a Digital Card. The numbered steps are explained following the figure.

Figure 5.1: Example Merchant Orchestrated Checkout (Consumer Recognised)



01. The Consumer initiates checkout with the merchant
02. For each SRC System that the merchant is registered with, the merchant calls the Prepare SRC Profile operation using a Consumer Identity (email or phone number) obtained from the Consumer's account at the Merchant
03. One or more SRC Systems responds with a list of SRC Profiles for the Consumer
04. The merchant presents the Consumer with the SRC Candidate List (comprising of the available Digital Cards from each of the Consumer's SRC Profiles) along with any other payment methods accepted by the merchant

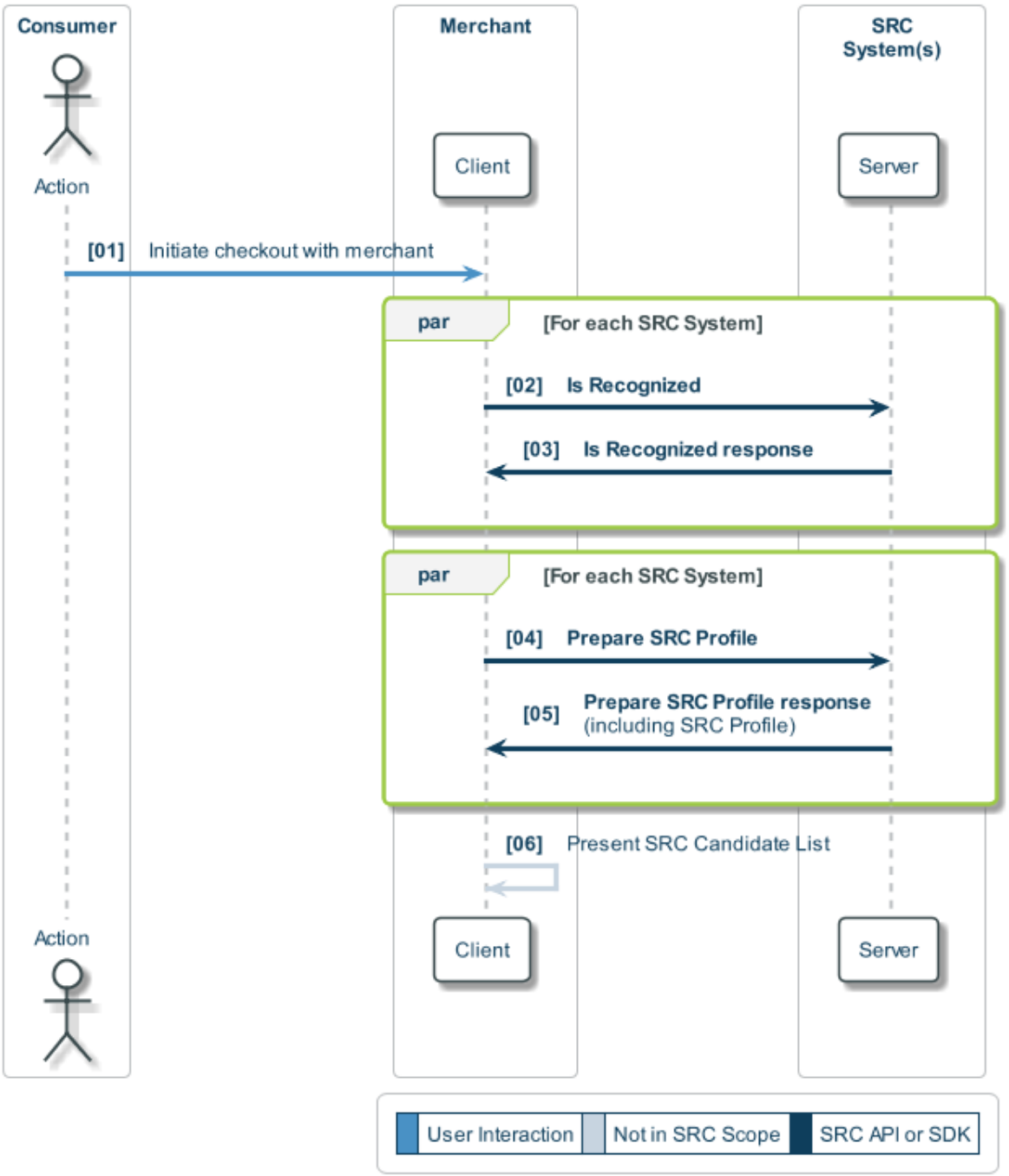
5.4.2 Merchant Orchestrated Checkout (Consumer Credentials Not Recognised / Frictionless)

Figure 5.2 shows an example flow where the Consumer either:

- Signs into a merchant account, but the Consumer's credentials at the merchant are not recognised by the SRC System; *or*
- Checks out as a guest

In both cases, an alternative, frictionless method of recognition (one which does not require Consumer interaction) is available (for example, the SRC System recognises the Consumer Device). After the presentation of the SRC Candidate List, the flow continues as shown in Figure 5.5 with the selection of a Digital Card. The numbered steps are explained following the figure.

Figure 5.2: Example Merchant Orchestrated Checkout (Consumer Credentials Not Recognised / Frictionless) Flow



01. The Consumer initiates checkout with the merchant
02. The merchant does not have access to a Consumer Identity this that is recognised by any SRC Systems, so for each SRC System that the merchant is registered with, the merchant calls the Is Recognized operation. How the SRC System recognises the Consumer Device or Consumer is out of scope (for an example of how recognition can

be achieved using recognition tokens stored on the Consumer Device, see Figure 10.2 in Section 10 Merchant Orchestrated Recognition)

03. One or more SRC Systems respond, indicating that the Consumer Device / Consumer is recognised and returning a Federated ID Token
04. For each SRC System that the merchant is registered with, the merchant calls the Prepare SRC Profile operation using the returned Federated ID Token(s)
05. The SRC System responds with a list of SRC Profiles
06. The merchant presents the Consumer with the SRC Candidate List (comprising of the available Digital Cards from each of the Consumer's SRC Profiles) along with any other payment methods accepted by the merchant

5.4.3 Merchant Orchestrated Checkout (Consumer Credentials Not Recognised / Consumer Identity)

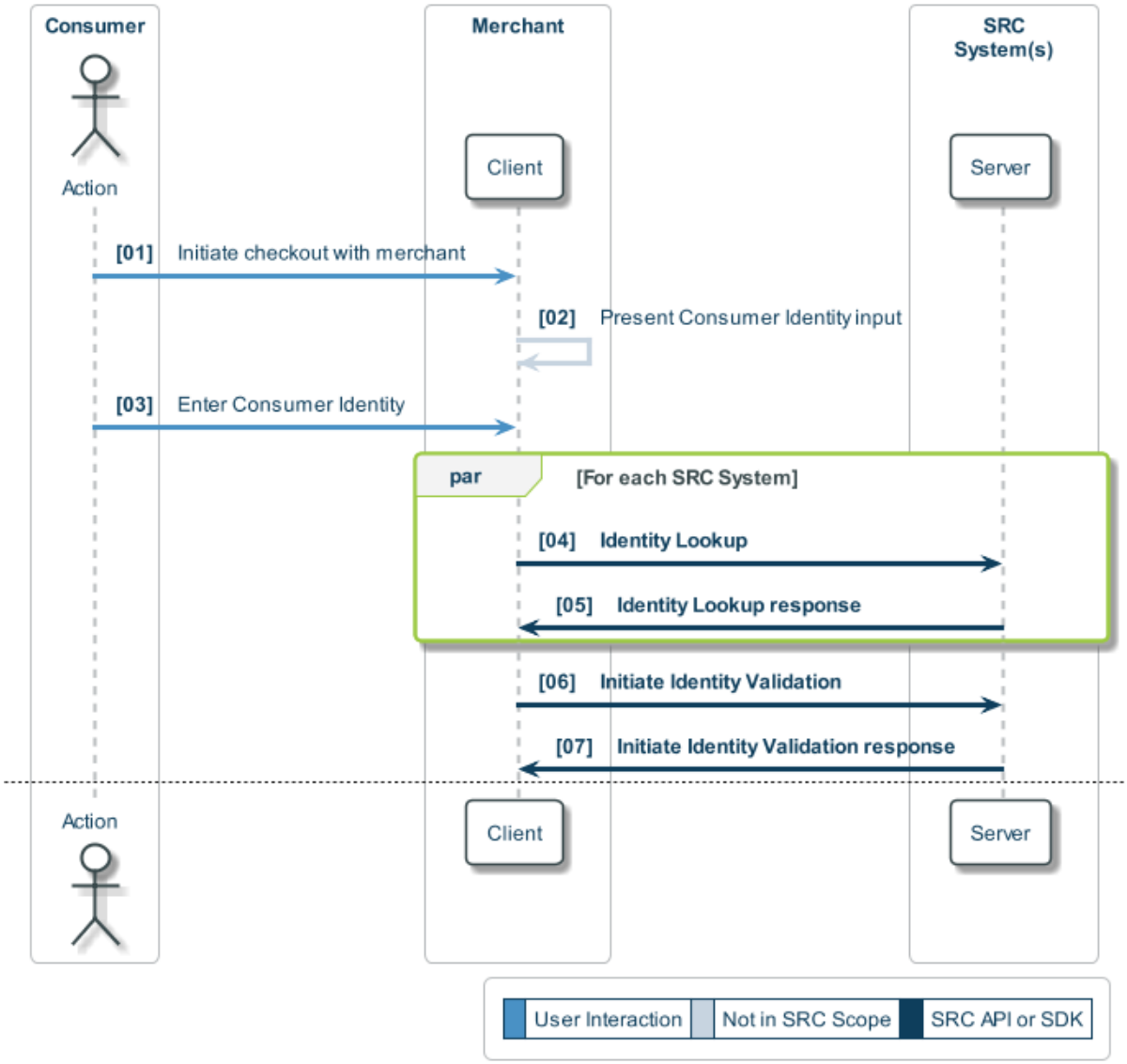
Figure 5.3 and Figure 5.4 show an example flow where the Consumer either:

- Signs into a Merchant account, but the Consumer's credentials at the merchant are not recognised by the SRC System; *or*
- Checks out as a guest

In both cases an alternative, frictionless method of recognition is not available so the Consumer is required to input a Consumer Identity (Figure 5.3), which then requires additional validation (Figure 5.4). The numbered steps are explained following the figure.

After the presentation of the SRC Candidate List at the end of Figure 5.4, the flow continues as shown in Figure 5.5 with the selection of a Digital Card.

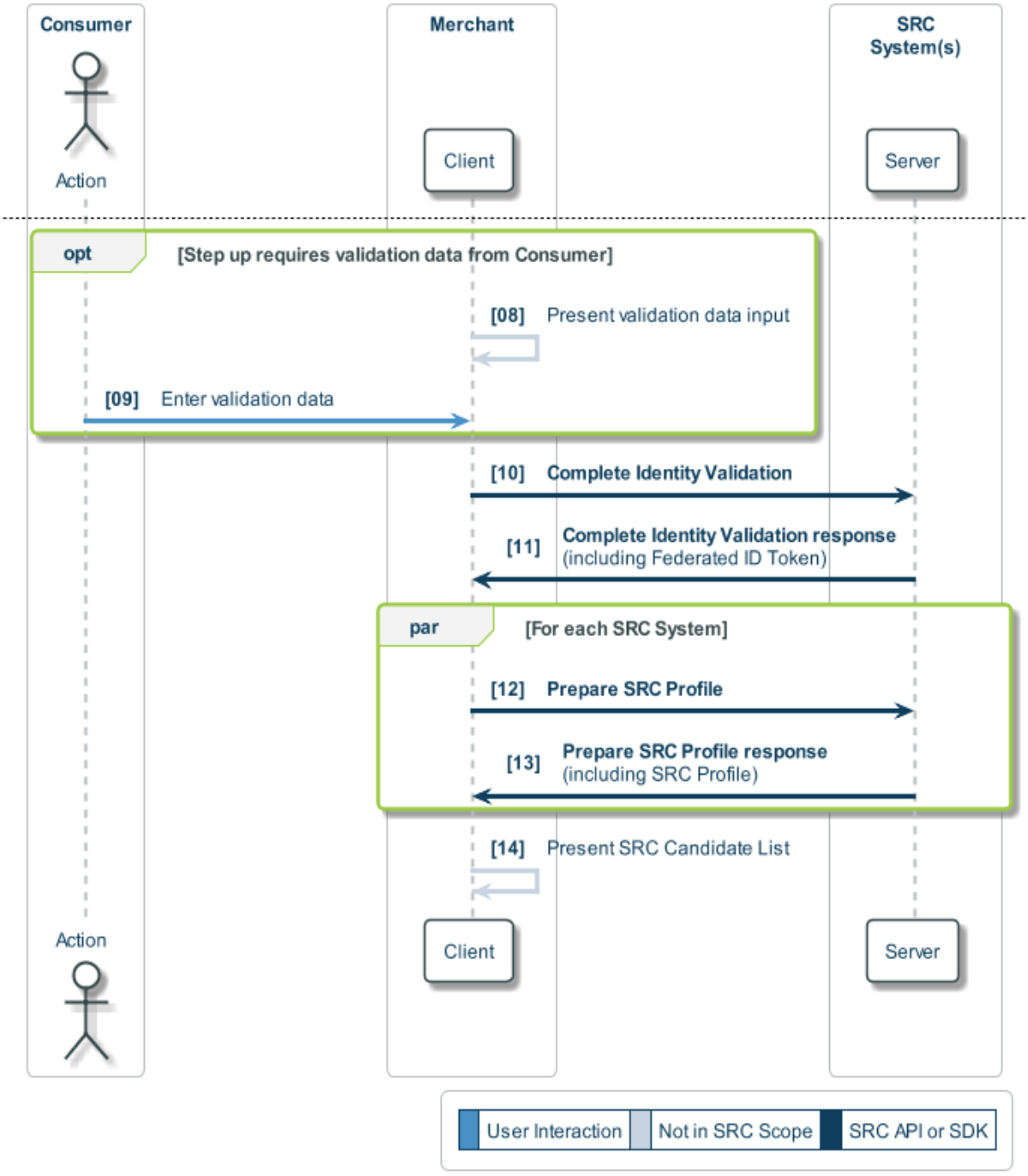
Figure 5.3: Example Merchant Orchestrated Checkout (Consumer Credentials Not Recognised / Consumer Identity) Flow



01. The Consumer initiates checkout with the merchant
02. Since the merchant does not have access to a Consumer Identity recognised by any SRC Systems and there are no other frictionless methods available to recognise the Consumer Device or Consumer, the merchant provides an option for the Consumer to enter a Consumer Identity (email or phone number) along with any other payment methods accepted by the merchant
03. The Consumer provides a Consumer Identity
04. For each SRC System that the merchant is registered with, the merchant calls the Identity Lookup operation

05. One or more SRC Systems respond, indicating that the Consumer Device / Consumer is recognised and providing options for validating the Consumer Identity
06. The merchant calls the Initiate Identity Validation operation
07. The SRC System responds with a message to be presented to the Consumer

Figure 5.4: Example Merchant Orchestrated Checkout (Consumer Identity Validation) Flow

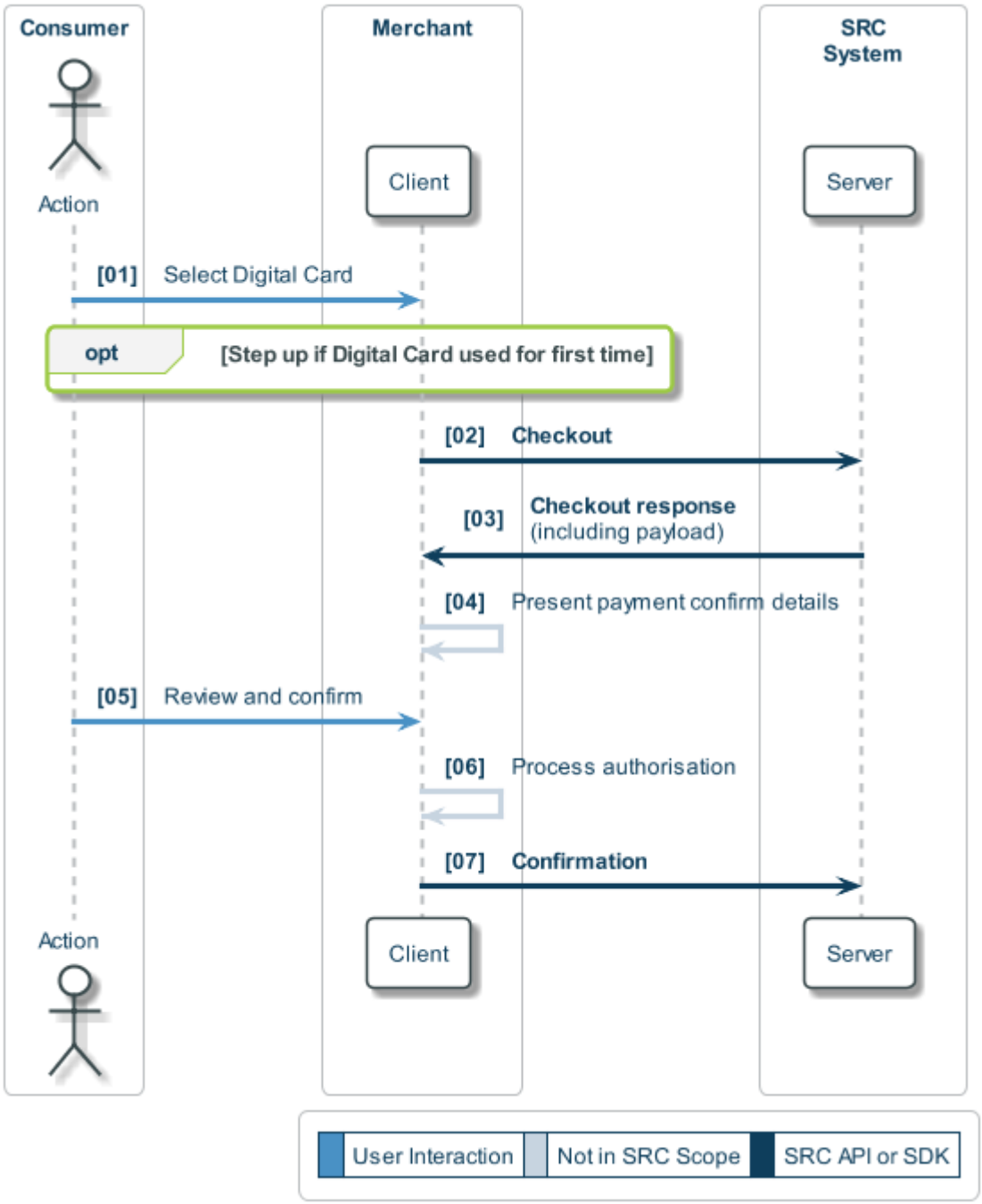


08. The merchant presents any relevant Identity Validation information to the Consumer and if necessary, provides the ability for the Consumer to provide Validation Data
09. The Consumer inputs the Validation data
10. The merchant calls the Complete Identity Validation operation, providing any relevant Validation Data
11. The SRC System returns a Federated ID Token
12. For each SRC System that the merchant is registered with, the merchant calls the Prepare SRC Profile operation using the returned Federated ID Token
13. The SRC System responds with a list of SRC Profiles
14. The merchant presents the Consumer with the SRC Candidate List (comprising of the available Digital Cards from each of the Consumer's SRC Profiles) along with any other payment methods accepted by the merchant

5.4.4 Merchant Orchestrated Checkout (Common Flow)

Figure 5.5 shows an example flow which is common to all Merchant Orchestrated Checkout flows, coming immediately after the presentation of the SRC Candidate List. The numbered steps are explained following the figure.

Figure 5.5: Example Merchant Orchestrated Checkout (Common Flow)



01. The Consumer selects a Digital Card from the SRC Candidate List

Note that an additional step up may be required following the selection of the Digital Card if it has not been previously used at the merchant to ensure that the Consumer is consenting to its use.

02. The merchant calls the Checkout operation for the relevant SRC System based on the selected Digital Card

03. The SRC System responds to the merchant with checkout related data, including the payload
04. The merchant presents the payment confirmation details to the Consumer
05. The Consumer reviews the information for correctness and confirms payment
06. The merchant or the merchant's Payment SRCI processes the payment authorisation
07. On completion of payment authorisation, the merchant calls the Confirmation operation for the relevant SRC System

6 Merchant Presented QR Code Checkout

Merchant Presented QR Code Checkout is a type of merchant checkout. It is orchestrated by a split SRC Initiator model where Payment SRC Initiator related merchant data is populated in a dynamic QR code and consumed by an application on a Consumer Device (a Non-Payment SRC Initiator) to trigger an SRC checkout experience. It enables Consumers with at least one existing SRC Profile to access Digital Cards within a provided application for single use, based on the consumed merchant data.

Merchant Presented Checkout is characterised by the following:

- A Payment SRC Initiator that performs payment related functions on behalf of the merchant based on the payloads provided by SRC Systems
- Correctly formatted merchant data including at a minimum the merchant data needed by an SRC System to identify the Payment SRC Initiator and the transaction amount.
- An entity that provides a Non-Payment SRC Initiator application for a Consumer's Device to facilitate:
  - A recognised returning Consumer and providing an SRC Candidate List
  - Consumption of merchant data
  - The checkout user experience
  - Initiation of the checkout with an SRC System
  - Receipt of a notification of the outcome of the transaction from an SRC System
- Presentation or delivery of merchant data to initiate a checkout experience

6.1 Use Case Overview

The Merchant Presented QR Code Checkout use case consists of a Consumer, with an application on a Consumer Device, scanning a QR code generated in accordance with EMV® QR Code Specification for Payment Systems (EMV QRCPS) – Merchant-Presented Mode (known as an EMV MPQR). The EMV MPQR contains the amount and any other information required to trigger an SRC checkout.

6.2 Preconditions

The following preconditions apply to this use case:

- The Consumer has a Consumer Device with a Non-Payment SRC Initiator application installed which is capable of scanning EMV MPQR

- The merchant has registered with a Payment SRC Initiator which:
  - Has provided the data necessary to enable the display of a dynamic EMV MPQR
  - Enables the authorisation of Payment Cards
- The Payment SRC Initiator and Non-Payment SRC Initiator have
  - Each separately onboarded with one or more SRC Systems
  - At least one SRC System in common
  - The ability to communicate with each other
- Each SRC System enables the delivery of a payload to the Payment SRC Initiator for each checkout facilitated by the Non-Payment SRC Initiator
- The Payment SRC Initiator has registered the merchant as a Digital Payment Application with each SRC Systems
- All SRC System Participants support the Confirmation API
- The Consumer has enrolled one or more Payment Card(s) with one or more of the SRC System(s) which the merchant is registered with

6.3 Assumptions

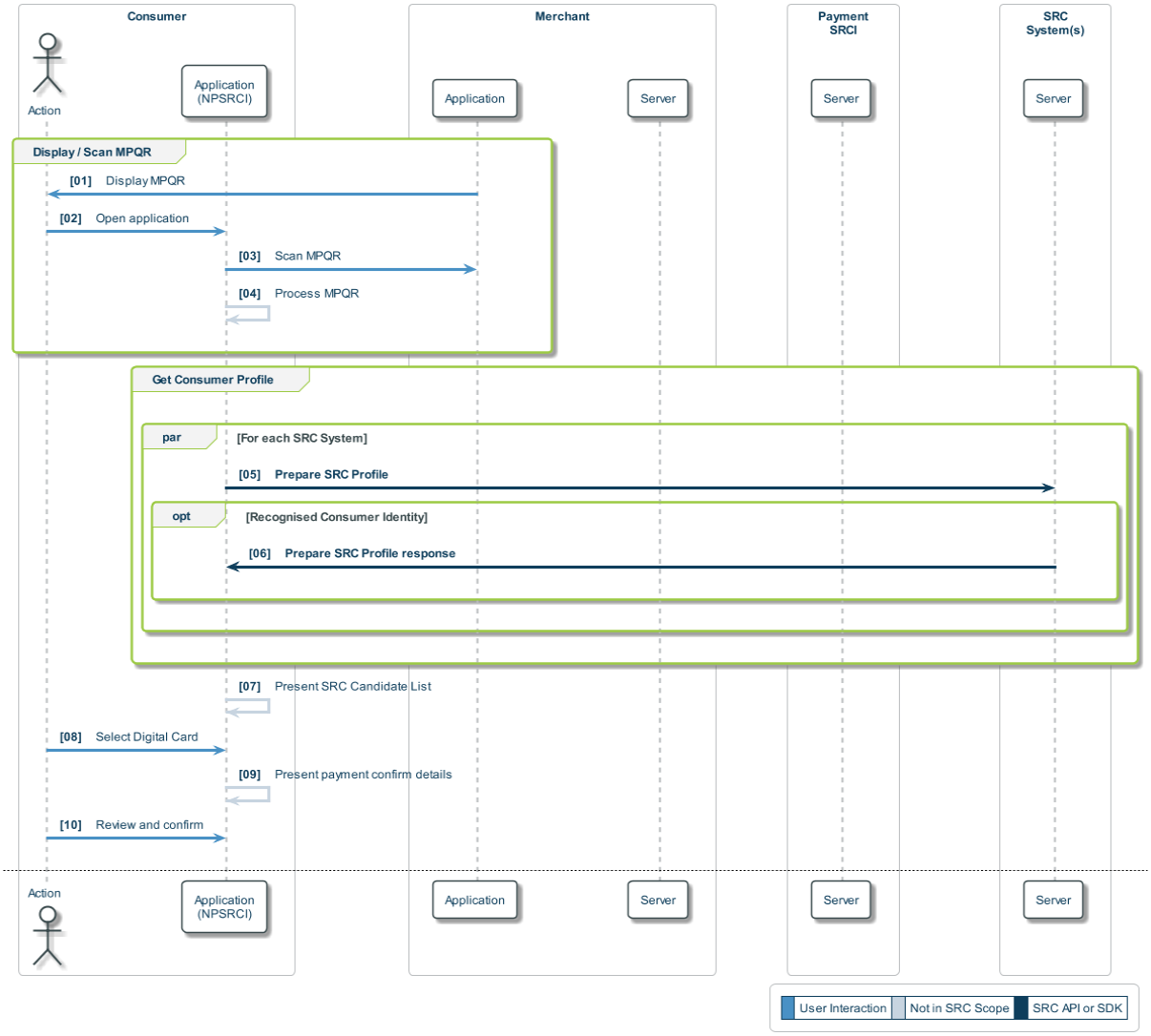
The following assumptions apply to this use case example:

- The Non-Payment SRC Initiator application on the Consumer Device can authenticate the Consumer
- The Consumer has previously retrieved Digital Cards from one or more SRC Systems and agreed to be remembered by the Non-Payment SRC Initiator application
- There is no requirement for the Consumer to enter any data prior to checkout

6.4 Sequence Diagrams

Figure 6.1 and Figure 6.2 show an example flow for the Merchant Presented QR Code Checkout use case, with card selection (Figure 6.1) and checkout (Figure 6.2). The numbered steps are explained following the figure.

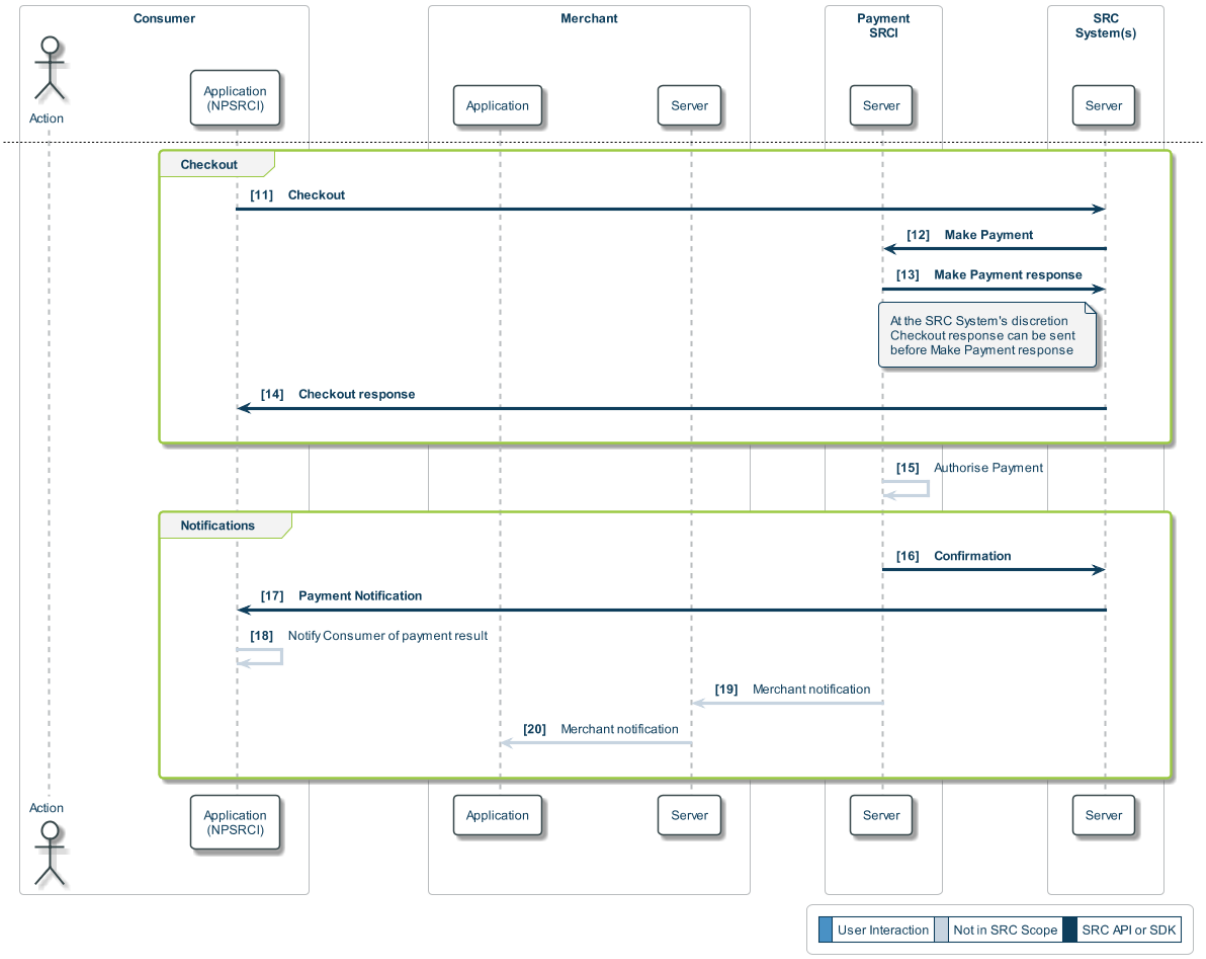
Figure 6.1: Example Merchant Presented QR Code Checkout Card Selection Flow



01. The merchant creates and displays a dynamic MPQR with registered merchant and transaction information
02. The Consumer opens the Non-Payment SRC Initiator application on the Consumer Device (the application) and signs in if needed
03. The Consumer scans the MPQR using the application
04. The application reads the MPQR, maps the data to SRC Data fields and uses the merchant account information from the MPQR to compile a list of SRC Systems where the merchant is registered
05. For each SRC System in the list where the application has previously retrieved Digital Cards, the application calls the Prepare SRC Profile operation
06. One or more SRC Systems respond with a list of SRC Profiles

07. The application presents the Consumer with the SRC Candidate List (comprising of the available Digital Cards from each of the Consumer's SRC Profiles)
08. The Consumer selects one of the Digital Cards from the SRC Candidate List
09. The application presents the payment confirmation information to the Consumer
10. The Consumer reviews the information for correctness and confirms payment

Figure 6.2: Example Merchant Presented QR Code Checkout Flow



11. The application calls the Checkout operation for the relevant SRC System based on the selected Digital Card
12. The SRC System calls the Make Payment operation for the Payment SRCI
13. The Payment SRCI responds to the Make Payment call

Note: The SRC System does not need to wait until it has received the Make Payment response before it sends the Checkout response.

14. The SRC System responds to the application indicating receipt of checkout data

Note: The application should not block or wait after it has received a valid Checkout Response.

15. The Payment SRCI processes the payment authorisation
16. On completion of payment authorisation, the Payment SRCI calls the confirmation operation for the relevant SRC System
17. The SRC System notifies the application of the result of the checkout
18. The application notifies the Consumer of the result of the checkout
19. The Payment SRCI notifies the merchant server the results of the payment authorisation
20. The merchant application is notified of the payment processing results

7 SRC Checkout with 3DS “ONBEHALF”

SRC Checkout with 3DS “ONBEHALF” is the facilitation of checkout orchestrated by an SRC Initiator integrating the SDKs of one or more SRC System(s) that perform 3DS on behalf of the merchant.

SRC Checkout with 3DS “ONBEHALF” is characterised by the following:

- An SRC Checkout where the merchant requests the facilitation of a 3DS Browser-based flow by the SRC System, with the ACS deciding whether a challenge is required and, if it is, what challenge method is used
- Usage of the payload with relevant 3DS output data returned to process the authorisation

7.1 Use Case Overview

The SRC Checkout with 3DS “ONBEHALF” use case consists of the following:

- The Consumer visits a merchant e-commerce environment that presents a Click to Pay trigger (underpinned by an SRC Initiator integrating the SDKs of one or more SRC Systems) at checkout
- 3DS is to be facilitated by the SRC System on behalf of the merchant
- All 3DS functions and processes are performed / facilitated in accordance with EMV 3-D Secure

There are no variations to this use case.

7.2 Preconditions

The following preconditions apply to this use case:

- The Consumer has enrolled with one or more SRC System(s)
- The SRC System SDK is performing the functions of a:
  - 3DS Requestor
- The SRC System is performing the functions of a:
  - 3DS Server (compliant with EMV 3-D Secure)
  - Digital Card Facilitator
- The Issuer is performing functions of an:
  - Access Control Server (ACS)

- SRCPI
- The Directory Server functions are performed as defined by EMV 3-D Secure

7.3 Assumptions

The following assumptions apply to the SRC Checkout with 3DS “ONBEHALF” use case example:

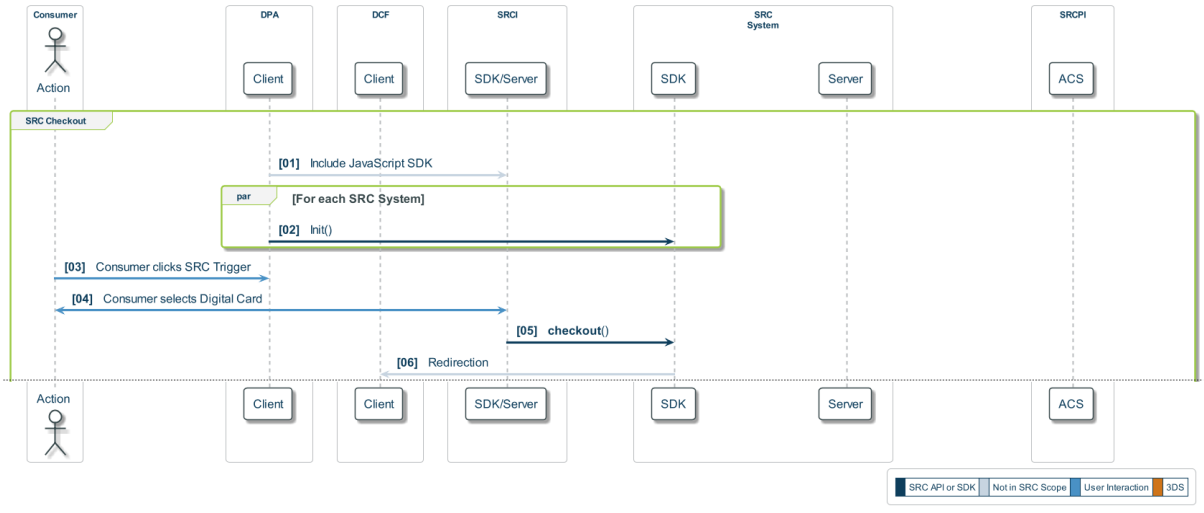
- The `dpaTransactionOptions` data element in `threeDsPreference` is populated as “ONBEHALF” in the Checkout operation
- The SRC System may use the 3DS data element Requestor Authentication Information to provide SRC Assurance Data
- If the ARes results in a transaction with a challenge (Transaction Status = C), a 3DS Challenge Flow will be initiated
- The Cardholder does not wish to change any of the order details after the checkout request

7.4 Sequence Diagrams

The sequence diagrams in Figure 7.1 to Figure 7.3 illustrate the use of EMV 3-D Secure applied to a typical SRC Checkout use case (see Section 3 SRC Checkout).

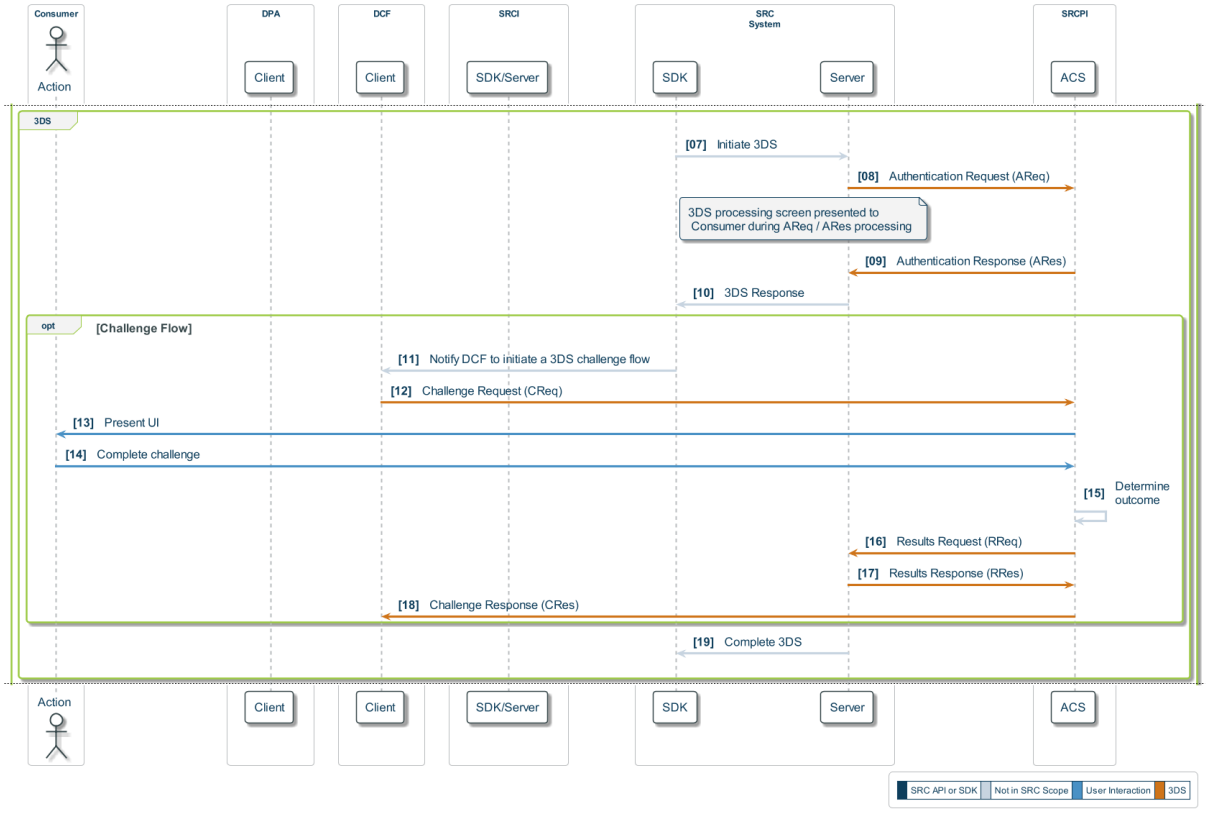
Note: The Issuer, listed as the actor SRCPI, performs the functions of an SRCPI as described in the SRC specifications and enables ACS availability within the SRC ecosystem. The Directory Server is omitted from the sequence diagram for simplicity.

Figure 7.1: Example SRC Checkout with 3DS “ONBEHALF” – Initiation



01. On rendering the page containing the Click to Pay trigger, the Digital Payment Application (DPA) includes JavaScript for the SRC Initiator (SRCI)
02. For each SRC System from which the merchant accepts payment, the SRCI calls the init() method of the SRC System's SDK to initialise it
03. The Consumer chooses Click to Pay as the payment method by clicking the SRC Trigger, following standard recognition / identity validation steps
04. The Consumer selects a Digital Card from the SRC Candidate List
05. The SRCI calls the checkout() method for the corresponding SRC System based on the selected Digital Card. The checkout includes information on the selected Digital Card, `merchantCategoryCode`, `transactionAmount` and `threeDsInputData`
06. The SRC System redirects the Consumer experience to the Digital Card Facilitator (DCF)

Figure 7.2: Example SRC Checkout with 3DS "ONBEHALF" – 3DS Authentication



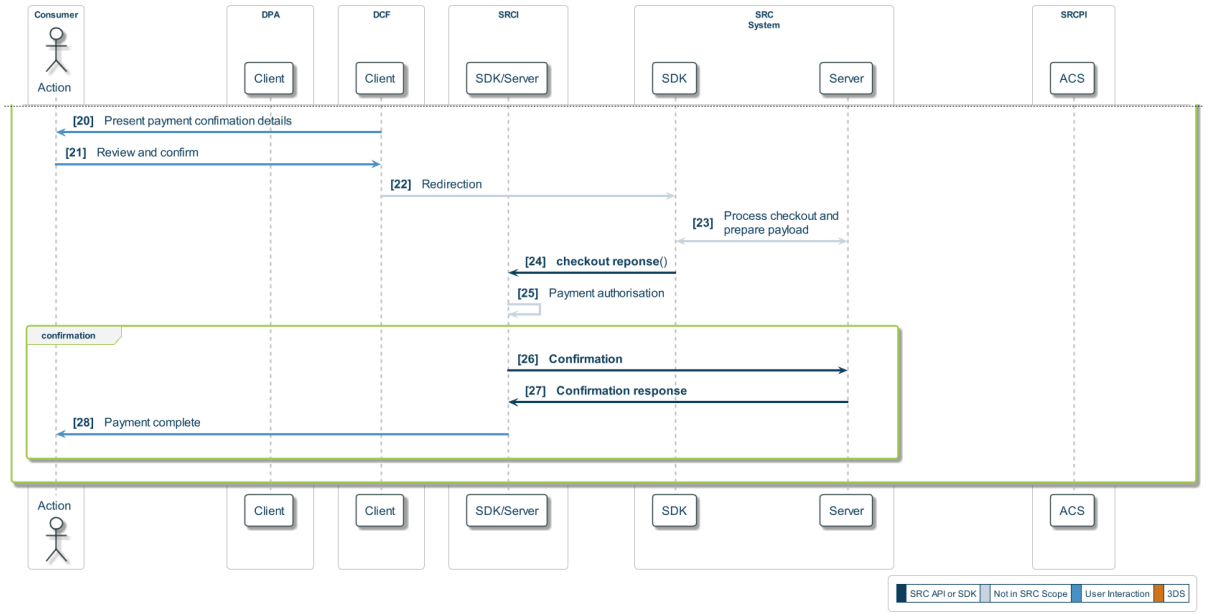
07. The SRC System initiates the EMV 3DS flow
08. The SRC System sends an Authentication Request (AReq)

Note: while the AReq / ARes is processing, the Consumer is presented with a 3DS processing screen (as per EMV 3-D Secure)

09. The ACS sends an Authentication Response (ARes)

10. The SRC System facilitates the requested challenge provided by the ACS and provides the result to the SRC System SDK
11. The SRC System constructs the Challenge Request (CReq) message, which is sent to the DCF Client to notify it to initiate a 3DS challenge flow
12. The DCF sends a Challenge Request (CReq)
13. The ACS presents the UI to the Consumer within the DCF
14. The Consumer completes the challenge as provided by the ACS
15. The ACS determines the outcome by validating the challenge data
16. The ACS sends the Result Request (RReq) to the SRC System
17. The SRC System sends Result Response (RRes) to the ACS
18. The ACS sends the Challenge Response (CRes) to the DCF
19. The SRC System completes the 3DS flow

Figure 7.3: Example SRC Checkout with 3DS "ONBEHALF" – Completion



20. The DCF displays the review and confirm information to the Consumer
21. The Consumer reviews the information for correctness and confirms payment
22. The DCF redirects to SRC System SDK
23. The SRC System processes the checkout and prepares the payload with the relevant 3DS Output Data

24. The SRC System responds to the SRCI with checkout related data, including the payload and `threeDsOutputData`
25. The merchant or the merchant's Payment SRCI processes the payment authorisation
26. Following successful payment authorisation, the SRCI calls the Confirmation operation for the relevant SRC System
27. The SRC System responds to the SRCI with the confirmation response
28. The SRCI notifies the Consumer that payment is complete

8 Management Service

Management Service is the facilitation of DPA Registration and maintenance orchestrated by an SRC Initiator.

Management Service is characterised by the following:

- Registration of a merchant's Digital Payment Application with an SRC System by an SRC Initiator
- On-going management of a registered Digital Payment Application by an SRC Initiator

8.1 Use Case Overview

The Management Service use case consists of the following examples:

- Registration of a Digital Payment Application (DPA Registration)
- Maintenance of a registered Digital Payment Application (DPA Maintenance)

8.2 Preconditions

The following preconditions apply to this use case:

- The SRC System offers Management Services

8.3 Assumptions

The following assumption applies to the Management Service DPA Registration use case example:

- The registration is initiated by the SRC Initiator, based on an interaction between the merchant and the SRC Initiator

The following assumption applies to the Management Service DPA Maintenance use case example:

- A previous DPA registration was successful and resulted in a reference identifier being provided for the DPA

8.4 Sequence Diagrams

A single sequence diagram (shown in Section 8.4.1 DPA Registration and Maintenance) illustrates both Management Service use case examples:

The specific use case example depends on how the data element `action` (passed by the SRC Initiator to the SRC System in Step [02] of Figure 8.1) is set:

- REGISTRATION: DPA Registration
- UPDATE: DPA Maintenance

Other variations to this flow include when `action` is set to:

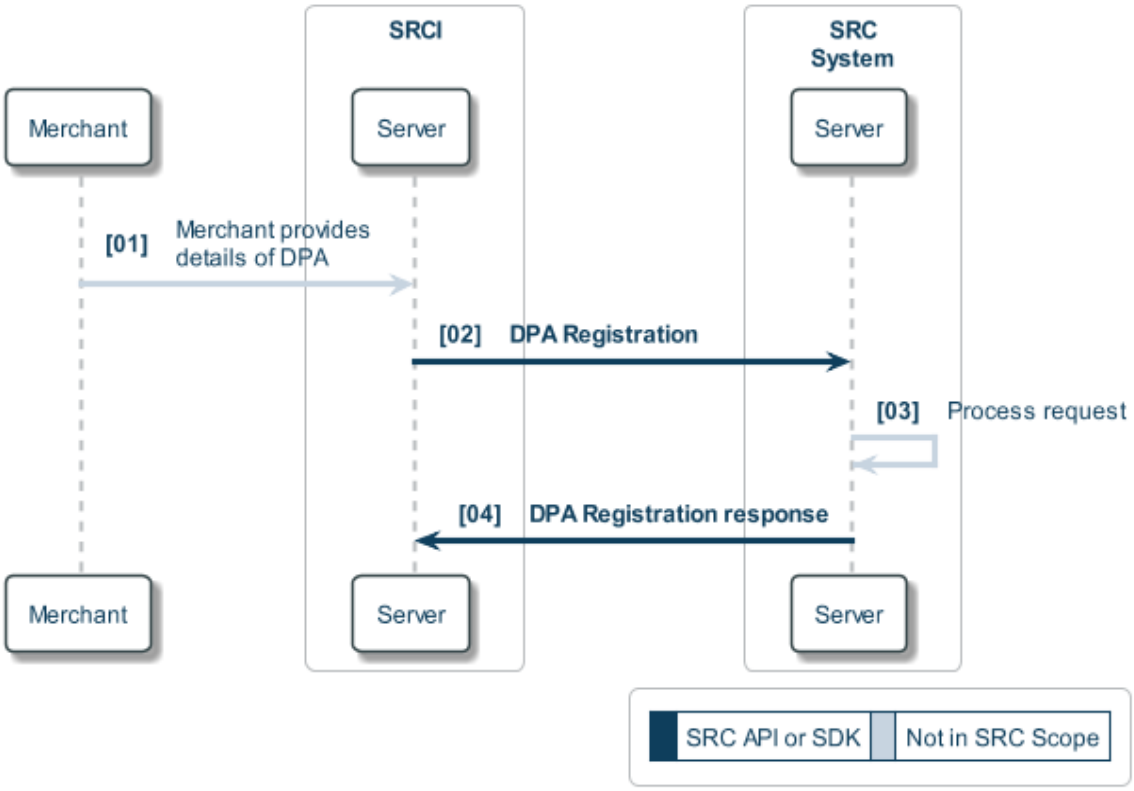
- ACTIVATE
- DEACTIVATE

These will correspondingly change the status of the DPA within the SRC System.

8.4.1 DPA Registration and Maintenance

The sequence diagram for the DPA Registration and Maintenance flow is shown in Figure 8.1.

Figure 8.1: Example Management Service (DPA Registration and Maintenance)



01. Merchant provides the details of the Digital Payment Application (DPA) to the SRC Initiator (SRCI), either for registration with the SRC System (DPA Registration) or to update details already held by the SRC System (DPA Maintenance)
02. The SRCI calls the DPA Registration operation with the data element `action` set to:
    - REGISTRATION to register the DPA with the SRC System
    - UPDATE to update the DPA details held by the SRC System
03. The SRC System processes the request and, for DPA Registration, generates a reference identifier for the DPA
04. The SRC System responds to the SRCI. The response includes the reference identifier in the data element `srcDpaID`

Note: it is up to the SRCI whether it informs the merchant of the outcome of the operation

9 Authentication Facilitation Services

Authentication Facilitation Services supports four invocation models using the Authentication APIs and SDK methods which are listed below:

- Invocation model 1: Authentication is handled by the SRC System SDK by calling the checkout() method
- Invocation model 2: Authentication is handled by the SRC System SDK by calling the Authenticate() method
- Invocation model 3: Authentication is handled by the merchant (through its DPA / SRCI) directly calling the Authentication Facilitation API operations or SDK methods. In addition, the merchant fully controls the authentication UI
- Invocation model 4: Authentication is initiated by the merchant (through its DPA / SRCI) by opening the Authentication URL provided for that authentication method by the SRC System

9.1 Use Case Overview

This Section provides flows illustrating the four invocation models. The intention of this use case is to describe how various authentication methods can be invoked rather than providing details of the specific authentication method. All flows begin with a common initiation flow and then continue with one of the four invocation models.

Note that the example flows use the Merchant Card-On-File checkout (see Section 4 Merchant Digital Card-On-File Checkout) and have the Cardholder as the authentication subject. This does not preclude the authentication facilitation services being used with other checkout use cases and other authentication subjects.

9.2 Preconditions

The following preconditions apply to this use case:

- The Consumer has enrolled into an SRC System and has one or more Merchant Digital Card-on-file cards (see Section 4 Merchant Digital Card-On-File Checkout)

9.3 Assumptions

The following assumptions apply:

- The Consumer has:

- Created and signed into the Consumer account at the merchant
- Successfully undergone merchant ID&V
- Selected a Digital Card for checkout

9.4 Sequence Diagrams

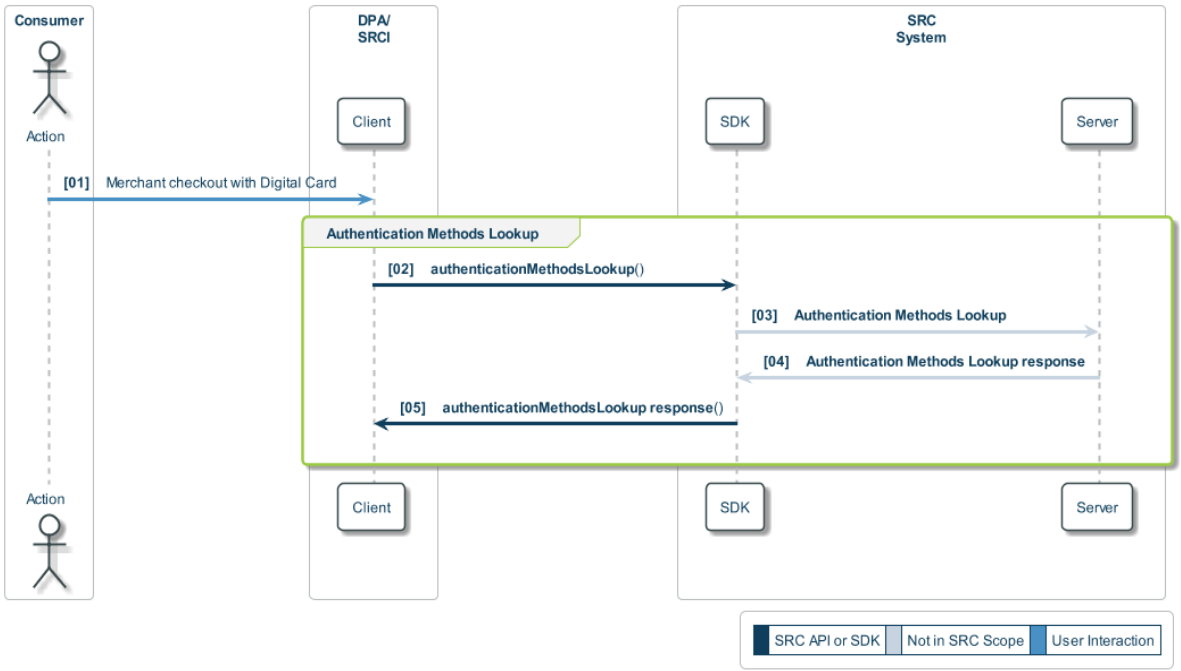
The sequence diagrams in the following Sections shows various authentication flows for the invocation models listed at the start of Section 9. All the flows start with the example flow in Section 9.4.1 Authentication Methods Lookup. The specific flow taken will depend on the invocation model:

- Invocation Model 1 (Section 9.4.2)
- Invocation Model 2 (Section 9.4.3)
- Invocation Model 3 (Section 9.4.4)
- Invocation Model 4 (Section 9.4.5)

9.4.1 Authentication Methods Lookup

The common authentication flow begins with the example Authentication Methods Lookup flow shown in Figure 9.1.

Figure 9.1: Example Authentication Methods Lookup Flow



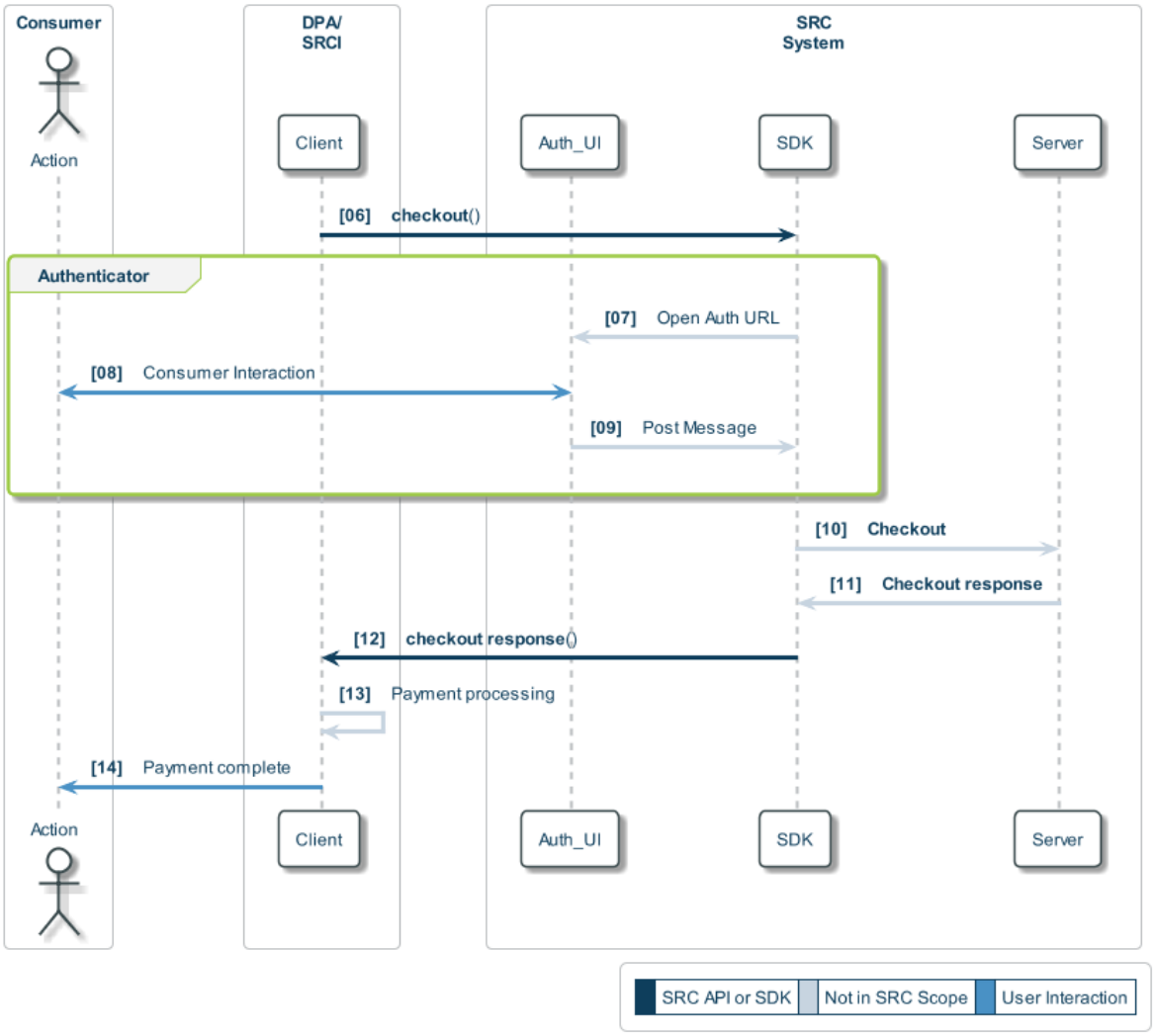
01. The Consumer initiates checkout with the merchant

02. The merchant, through its DPA, calls the authenticationMethodsLookup() method of the SRC System SDK
03. The SRC System SDK calls the Authentication Methods Lookup operation of the SRC System
04. The SRC System responds with list of Authentication Methods supported
05. The SRC System SDK responds to the merchant with the list of Authentication Methods supported. When multiple methods are returned by the SRC System SDK, the merchant chooses one of them to continue with authentication using one of the four invocation models

9.4.2 Invocation Model 1

The example flow for invocation model 1 is shown in Figure 9.2. The SRC System SDK handles the UI and the complexity of the authentication through the checkout() method.

Figure 9.2: Example Invocation Model 1 Flow



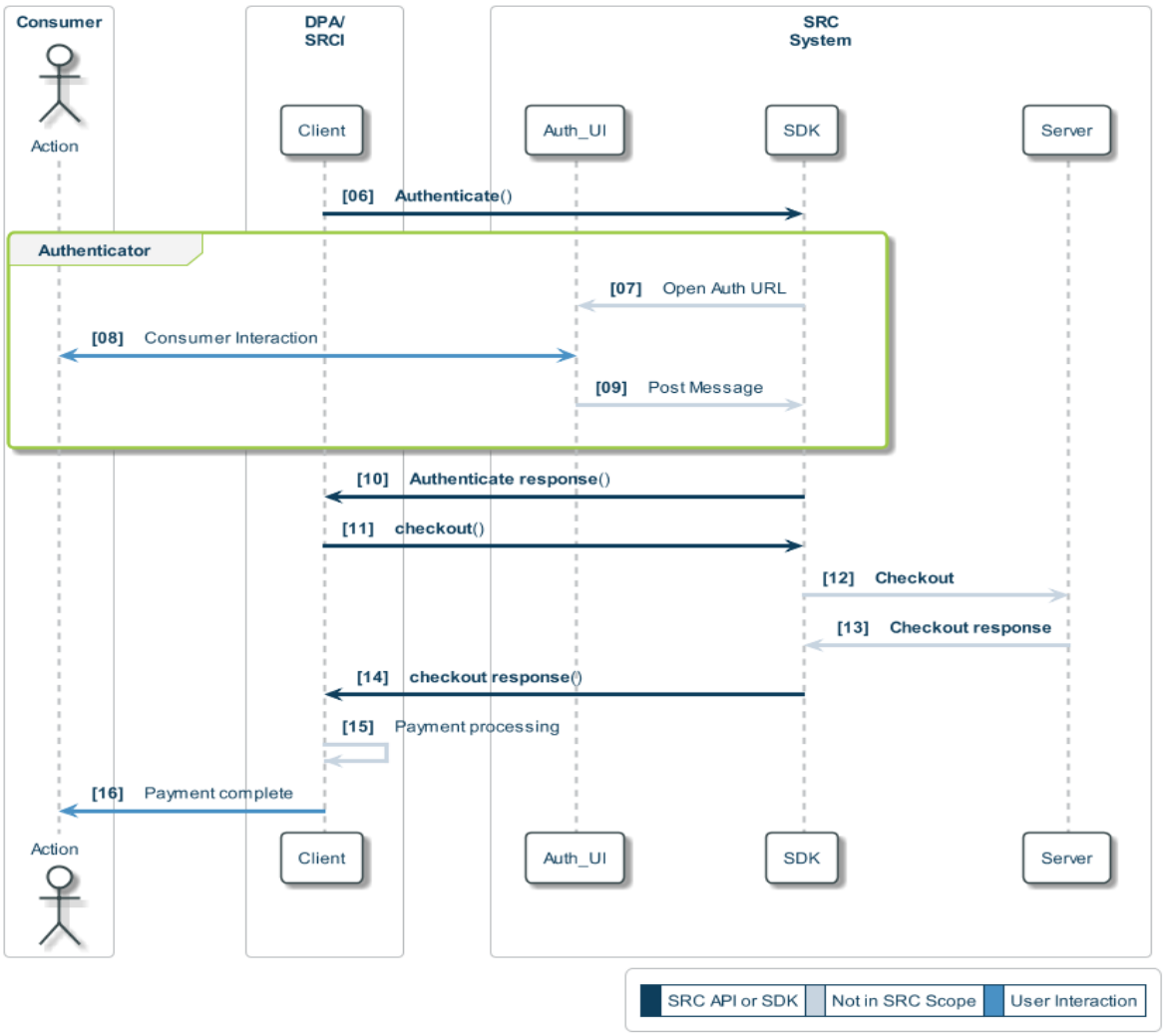
06. The merchant, through its Digital Payment Application (DPA) / SRC Initiator (SRCI), calls the checkout() method with a window reference and the preferred authentication method
07. The SRC System SDK hosts the authenticator by opening the authentication URL
08. The Consumer interacts with the UI of the selected authentication method
09. The Auth_UI sends a post message to the SRC System SDK when authentication is complete
10. The SRC System SDK calls the Checkout operation
11. The SRC System returns the checkout payload in the Checkout response
12. The SRC System SDK returns the checkout payload to the DPA / SRCI in the checkout() response
13. The DPA / SRCI sends the payload for payment processing

14. The DPA / SRCI sends confirmation of payment to the Consumer

9.4.3 Invocation Model 2

The example flow for invocation model 2 is shown in Figure 9.3. The SRC System SDK handles the UI and the complexity of the authentication through the Authenticate() method.

Figure 9.3: Example Invocation Model 2 Flow



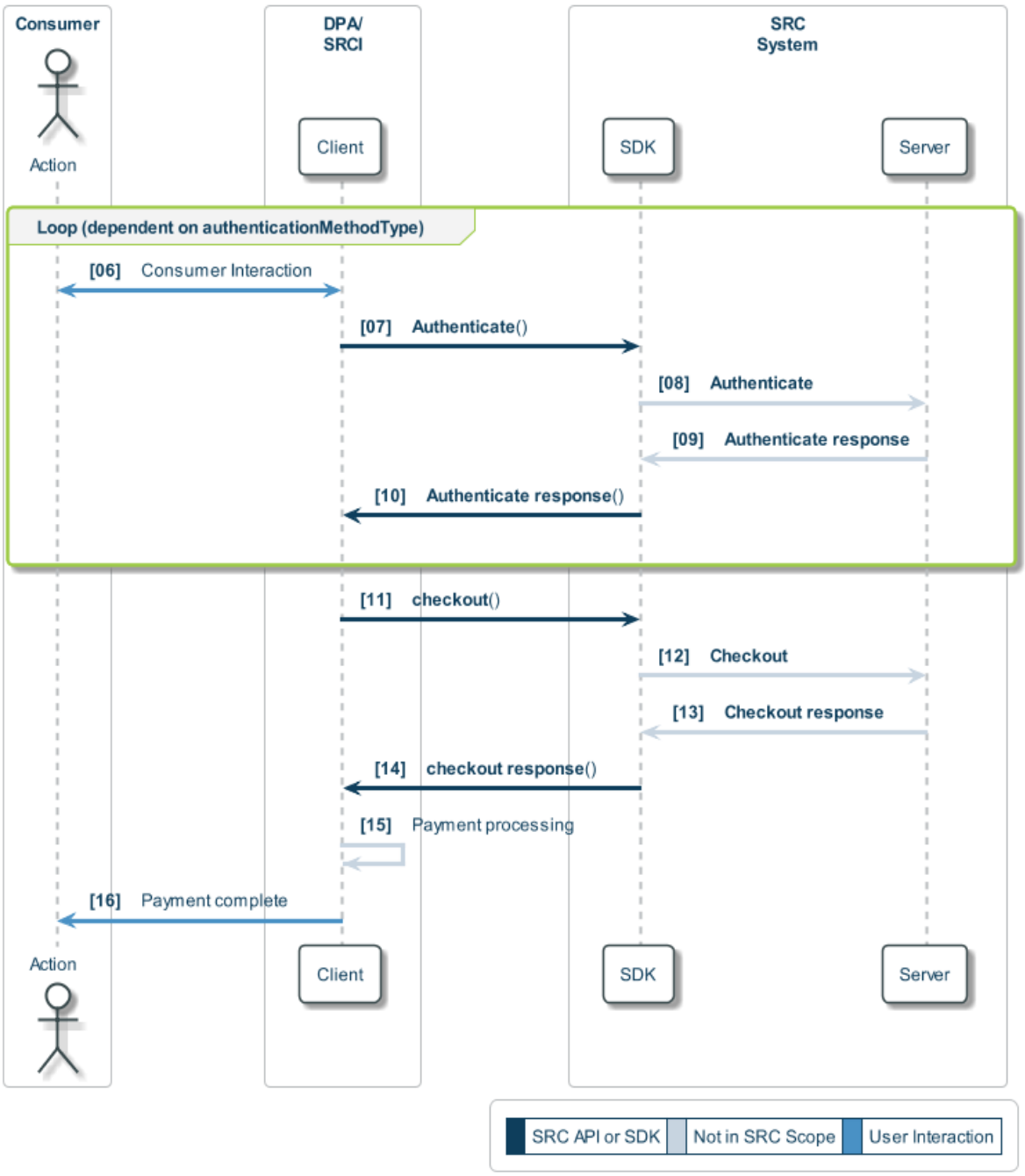
06. The merchant, through its Digital Payment Application (DPA) / SRC Initiator (SRCI), calls the Authenticate() method with a window reference and the preferred authentication method
07. The SRC System SDK hosts the authenticator by opening the authentication URL
08. The Consumer interacts with the UI of the selected authentication method
09. The Auth_UI posts the `assuranceData` to the SRC System SDK when authentication is complete

10. The SRC System SDK returns the `assuranceData` to the DPA / SRCI in the Authenticate() response.
11. The DPA / SRCI calls the checkout() method, which includes the `assuranceData`
12. The SRC System SDK calls the Checkout operation
13. The SRC System returns the checkout payload in the Checkout response
14. The SRC System SDK returns the checkout payload to the DPA / SRCI in checkout() response
15. The DPA / SRCI sends the payload for payment processing
16. The DPA / SRCI sends the confirmation of payment to the Consumer

9.4.4 Invocation Model 3

The example flow for invocation model 3 is shown in Figure 9.4. The merchant controls the authentication experience through its DPA / SRCI, which handles the UI and the complexity of authentication using the Authenticate operation.

Figure 9.4: Example Invocation Model 3 Flow



Steps [06] to [10] begin with an optional Consumer interaction (depending on the selected authentication method) and are repeated until authentication is complete.

06. If required, the merchant renders the appropriate authentication UI and the Consumer interacts with it
07. The merchant, through its Digital Payment Application (DPA) / SRC Initiator (SRCI), calls the Authenticate() method, including any data provided by the Consumer in Step [06]

08. The SRC System SDK calls the Authenticate operation
09. The SRC System returns the Authenticate response (which includes `assuranceData` if authentication is complete)
10. The SRC System SDK returns the Authenticate() response

    Depending on the outcome of the Authenticate() method, the flow continues as follows:

- If `assuranceData` has been received (authentication is complete), the flow continues with Step [11]
- If no `assuranceData` has been received (authentication has not been completed), the flow returns to Step [06]

11. The DPA / SRCI calls the checkout() method, which includes the `assuranceData`
12. The SRC System SDK calls the Checkout operation
13. The SRC System returns the checkout payload in the Checkout response
14. The SRC System SDK returns the checkout payload to the DPA / SRCI in checkout() response
15. The DPA / SRCI sends the payload for payment processing
16. The DPA / SRCI sends the confirmation of payment to the Consumer

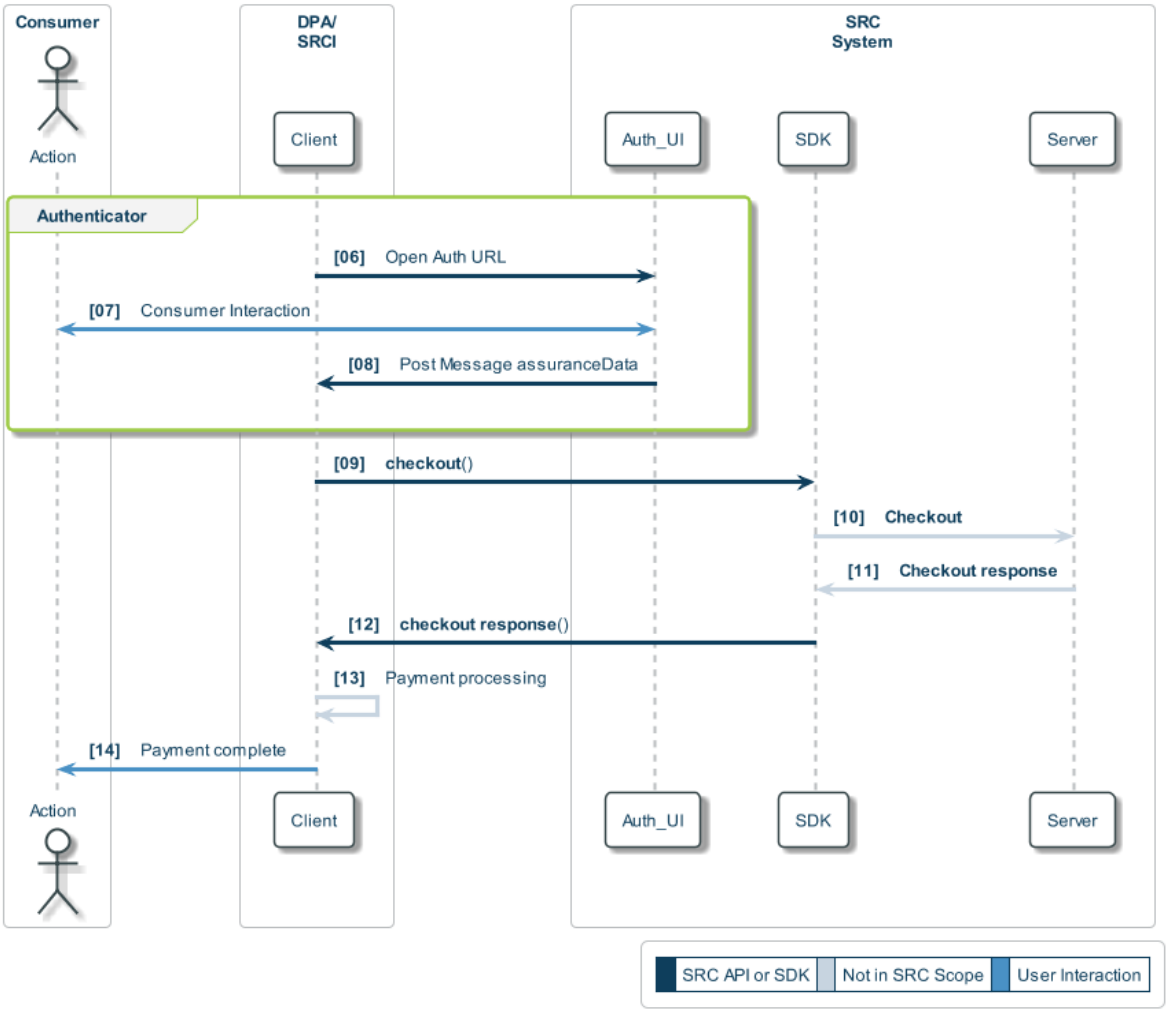
The number of times Steps [06] to [10] are executed depend on the selected authentication method. For example, assuming authentication is completed successfully:

- The steps are executed once if the merchant requested:
  - An authentication method such as CSC_VALIDATION or ADDRESS_VERIFICATION. In this case, Consumer interaction occurs in Step [06]
  - 3DS was requested and completed successfully without step-up. In this case, there is no Consumer interaction
- The steps are executed more than once if the merchant requested:
  - An authentication method such as APP_OTP, SMS_OTP or EMAIL_OTP. In this case, there is no Consumer interaction in the first loop. Consumer interaction occurs at the start of the second loop and the Authenticate() method is used to provide the SRC System with the OTP value (that may be delivered in another channel i.e. via APP, SMS or EMAIL)
  - 3DS, which required step-up. In this case, Consumer interaction occurs at the start of the second loop and the Authenticate() method is used to poll the SRC System for the 3DS results. Steps [07] to [10] are repeated until authentication is completed successfully

9.4.5 Invocation Model 4

The example flow for invocation model 4 is shown in Figure 9.5. The DPA / SRCI opens the authentication method URL which has been provided for that authentication method. The entity controlling the UI and the complexity of authentication depends on the authentication method chosen and the provider of the authentication method.

Figure 9.5: Example Invocation Model 4 Flow



06. The merchant, through its Digital Payment Application (DPA) / SRC Initiator (SRCI), opens the Authentication URL provided for the authentication method, which provides the necessary UI for the authentication
07. The Consumer interacts with the UI of the selected authentication method
08. The Auth_UI posts the `assuranceData` to the DPA / SRCI when authentication is complete
09. The DPA / SRCI calls the checkout() method, which includes the `assuranceData`

10. The SRC System SDK calls the Checkout operation
11. The SRC System returns the checkout payload in the Checkout response
12. The SRC System SDK returns the checkout payload to the DPA / SRCI in checkout() response
13. The DPA / SRCI sends the payload for payment processing
14. The DPA / SRCI sends the confirmation of payment to the Consumer

10 Merchant Orchestrated Recognition

The Recognition, Remember and Un-Remember functionality provides an SRC System with tools for the recognition and management of a Consumer who has enrolled in one or more SRC Systems. The use case examples in this Section illustrate how this functionality is used with the Merchant Orchestrated Checkout use case (see Section 5).

The Recognition, Remember and Un-Remember functionality uses recognition tokens which are generated by SRC Systems. These are stored (Remember), retrieved (Recognition) and managed (Un-Remember) by the merchant and/or its SRC Initiator on the browser of the Consumer Device.

10.1 Use Case Overview

This Section provides the following use case examples for a returning Consumer (i.e. one who has already enrolled with at least one SRC System):

- Remember
- Recognition
- Un-Remember

Rather than present the full use case and example flows (which can be found in Section 5 Merchant Orchestrated Checkout), this Section highlights the additional preconditions, assumptions and steps for each of the three use case examples.

10.2 Preconditions

The following preconditions apply to this use case in addition to those that apply to the Merchant Orchestrated Checkout (see Section 5.2):

- The Consumer has given consent to be remembered by the merchant

10.3 Assumptions

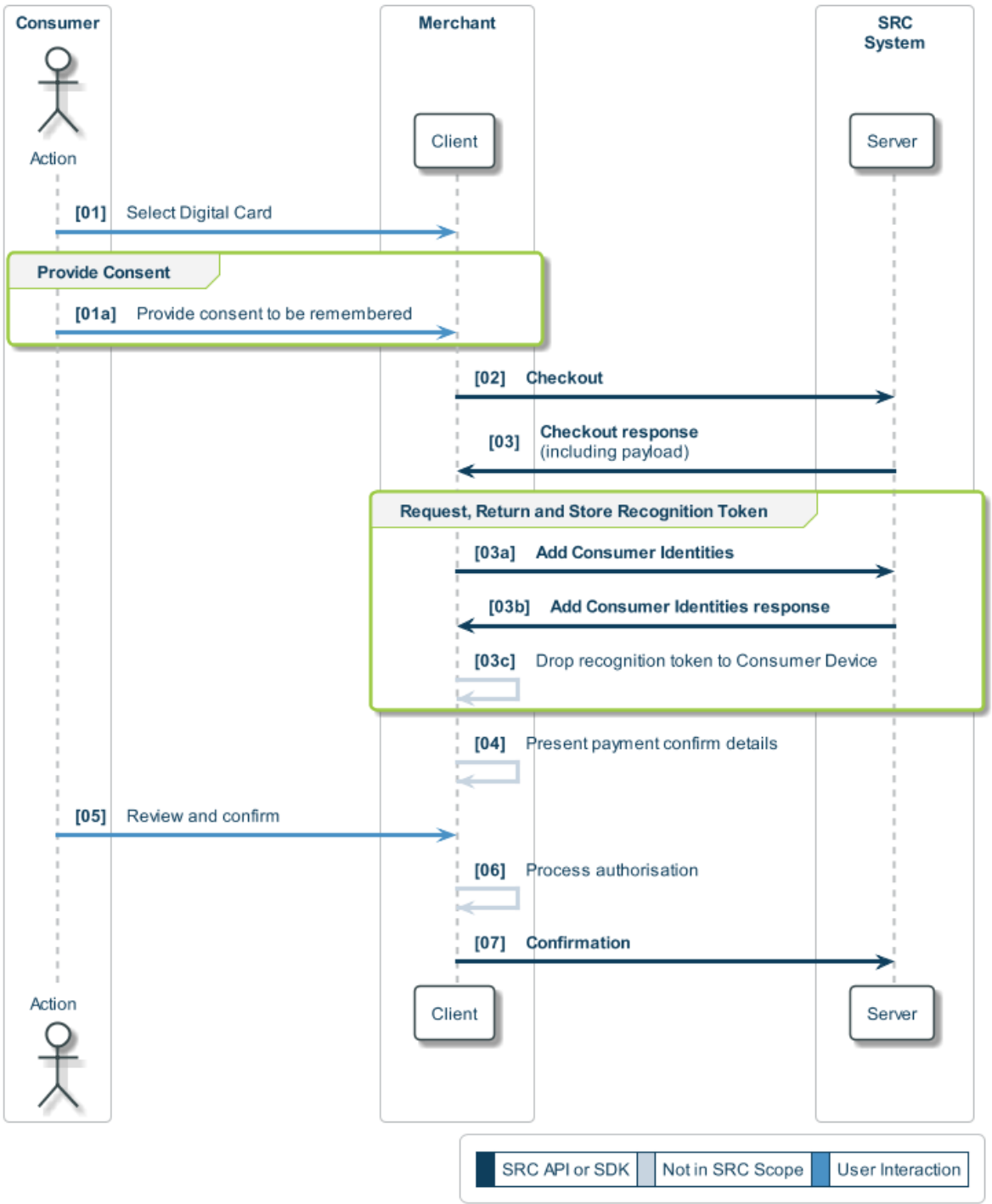
The following assumptions to this use case in addition to those that apply to the Merchant Orchestrated Checkout (see Section 5.3):

- Recognition is performed using a recognition token stored by the merchant on the browser of the Consumer Device

10.3.1 Remember

In this use case example, the Consumer is given the option to be remembered at the merchant during checkout following the selection of a Digital Card from the SRC Candidate List. The flow is shown in Figure 10.1 and is the same as the Merchant Orchestrated Checkout (Common Flow) shown in Figure 5.5 (Section 5.4.4) with the steps which differ highlighted in green boxes. Only these steps are explained in the text following the figure.

Figure 10.1: Example Remember Flow



01a Once the Consumer has selected a Digital Card, the Consumer provides consent to the merchant to be remembered on the Consumer Device

03a The merchant calls the Add Consumer Identities operation

03b The SRC System responds with a recognition token

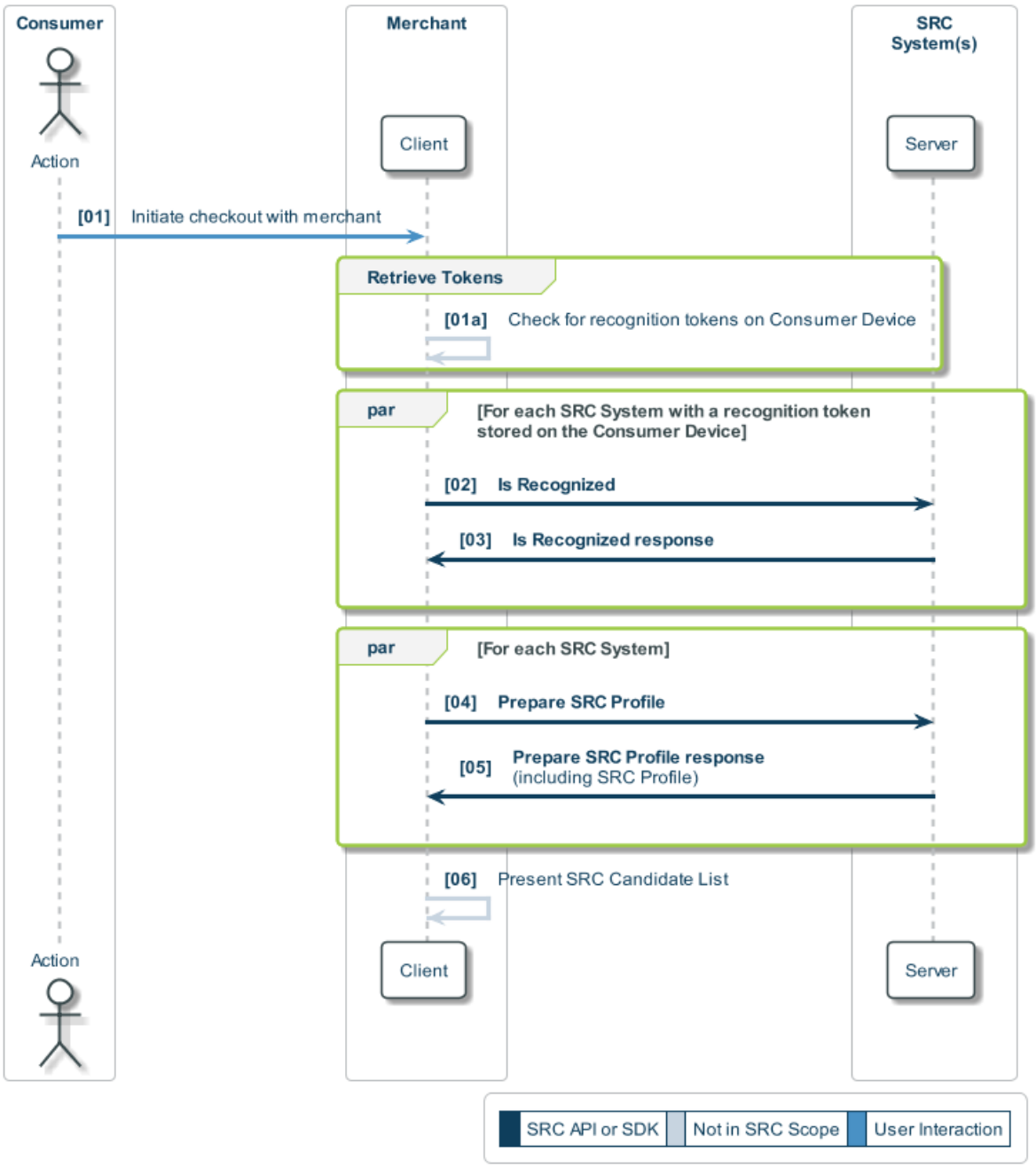
03c The merchant drops the recognition token to the browser on the Consumer Device

The flow then continues through Steps [04] to [07] as described in Section 5.4.4.

10.3.2 Recognition

In this use case example, the Consumer is recognised by the merchant retrieving the stored recognition token from the Consumer Device. The flow is shown in Figure 10.2 and is the same as the Merchant Orchestrated Checkout (Consumer Credentials Not Recognised / Frictionless) shown in Figure 5.2 (Section 5.4.2) with the steps which differ highlighted in green boxes. Only these steps are explained in the text following the figure.

Figure 10.2: Example Recognition Flow



01a Once the Consumer has initiated checkout, the merchant checks for recognition tokens stored in the browser of the Consumer Device

02 For each recognition token retrieved by the merchant in Step [01a], the merchant calls the Is Recognized operation for the SRC System which originally created the token

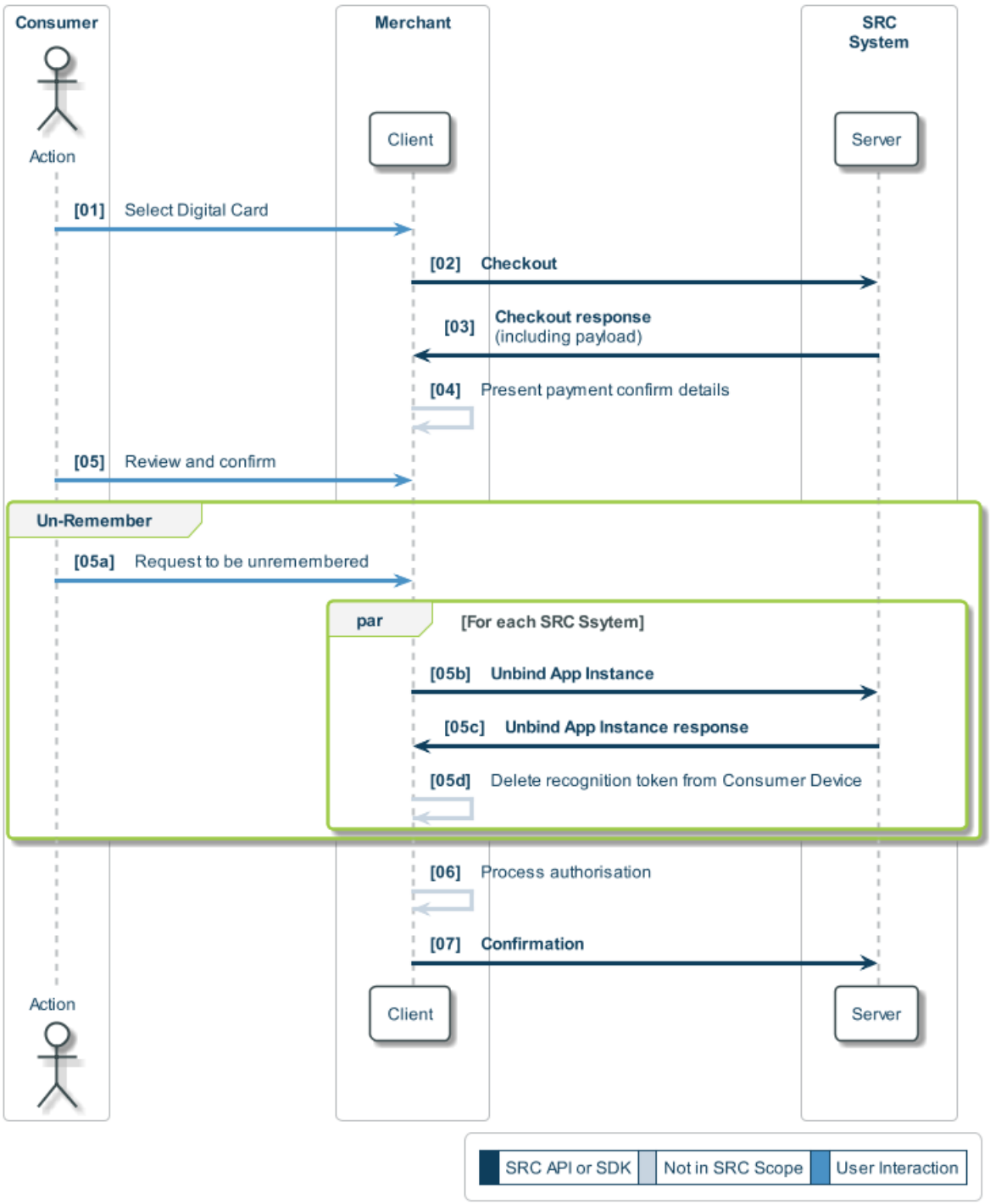
03 Each SRC System responds, indicating whether the Consumer has been recognised by returning a Federated ID Token

The flow then continues through Steps [04] to [06] as described in Section 5.4.2.

10.3.3 Un-Remember

In this use case example, the Consumer choses to be un-remembered at the merchant during checkout following the review and confirmation of the payment. The flow is shown in Figure 10.3 and is the same as the Merchant Orchestrated Checkout (Common Flow) shown in Figure 5.5 (Section 5.4.4) with the steps which differ highlighted in green boxes. Only these steps are explained in the text following the figure.

Figure 10.3: Example Un-Remember Flow



05a Once the Consumer has reviewed and confirmed the purchase, the Consumer requested to be un-remembered on the Consumer Device

05b For each SRC System, the merchant calls the Unbind App Instance operation

05c Each SRC System responds, indicating that the Consumer is un-remembered

05d The merchant removes the corresponding recognition token for the browser on the Consumer Device

The flow then continues through Steps [06] to [07] as described in Section 5.4.4.

11 Last Used Card

Last Used Card describes an optimised checkout flow for an unrecognised returning Consumer to allow the Consumer's last used card (represented by the Masked Card) to be shown as the Consumer's preferred card.

Last Used Card is characterised by the following:

- Presentation of an SRC Trigger that initiates a checkout experience
- The Consumer enters a Consumer Identity as part of identity validation
- Following successful identity validation, the Consumer is presented with the last used card as the preferred card
- The ability of the Consumer to choose to use the last used card or to select another card to proceed with the checkout

11.1 Use Case Overview

The Last Used Card use case consists of the following:

- During an Identity Lookup operation, each SRC System returns a timestamp of the card that was last used
- The Consumer Identity is validated at the SRC System corresponding to the card with the most recent timestamp (i.e. the last used card) using the initiateIdentityValidation() method
- The Complete Identity Validation operation returns the last used card as a Masked Card
- Optionally, the Consumer can choose this card to proceed with the checkout or select another card

There are no variations to this use case.

11.2 Preconditions

The following preconditions apply to this use case:

- The Consumer has:
  - Created an SRC profile
  - Enrolled at least one card
  - Previously used at least one of the enrolled cards to complete a checkout

- The Consumer did not choose to be remembered in the previous checkout (i.e. is an unrecognised returning Consumer)

11.3 Assumptions

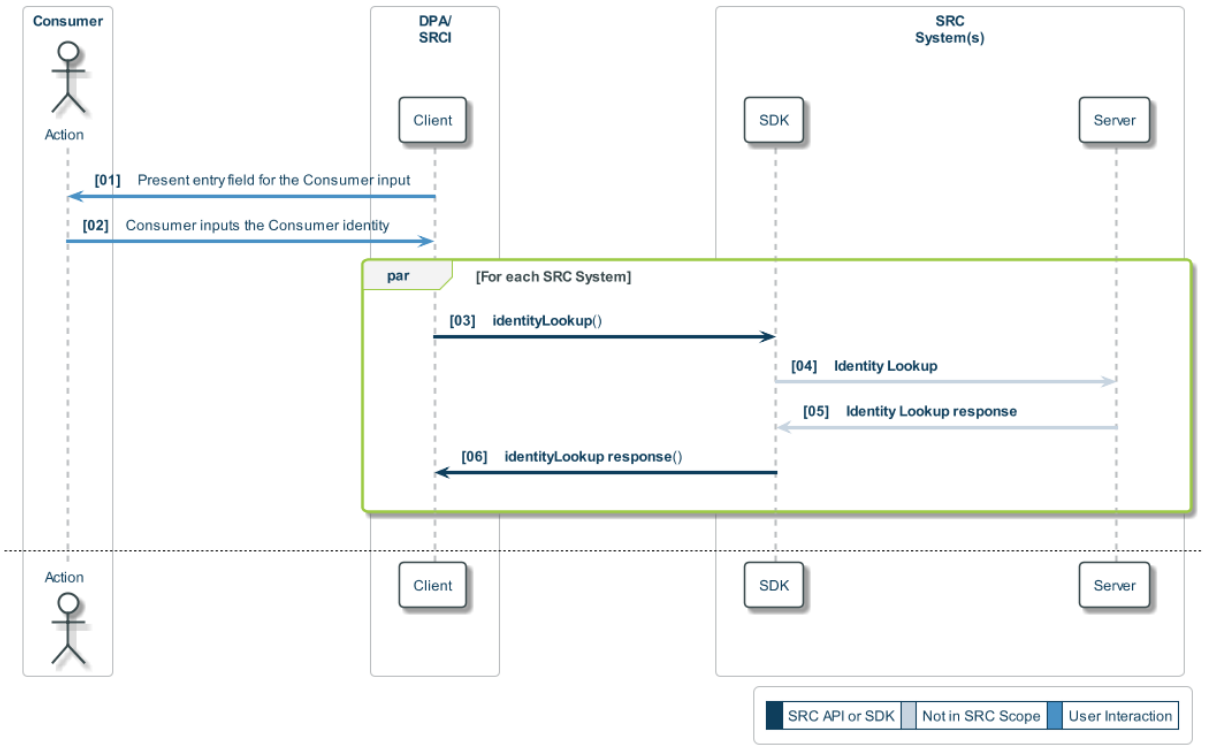
The following assumptions apply:

- The Consumer chooses Click to Pay as the payment method by clicking the SRC Trigger (or equivalent)
- An out of band validation type is used during identity validation

11.4 Sequence Diagrams

An example flow for Last Used Card is shown in Figure 11.1 to Figure 11.3, starting with a returning Consumer undergoing identity validation, which is shown in Figure 11.1.

Figure 11.1: Last Used Card – Example Identity Validation



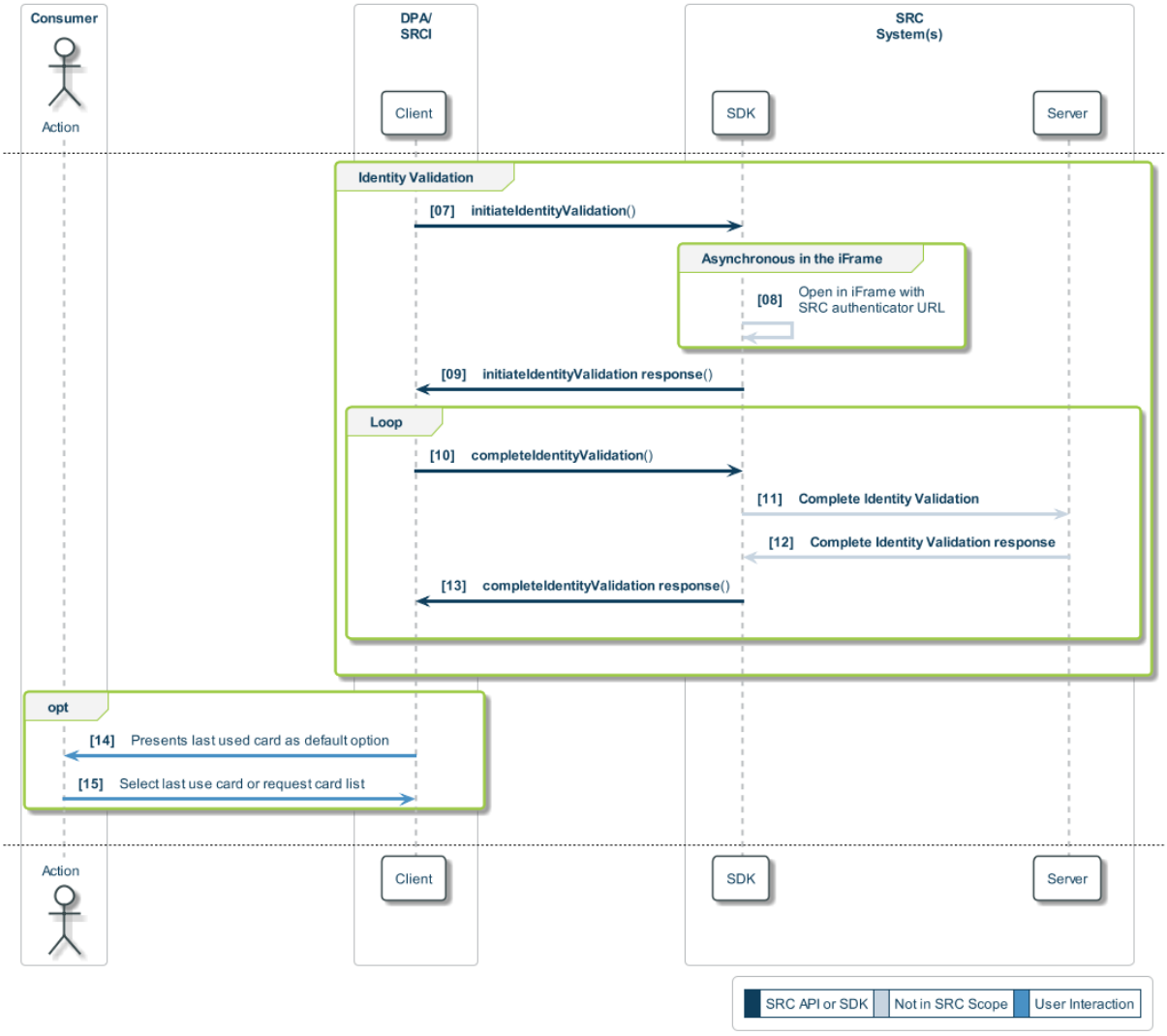
01. The DPA / SRCI presents an entry field for the Consumer Identity

02. The Consumer enters a Consumer Identity (e.g. email)

03. For each SRC System, the DPA / SRCI calls the identityLookup() method using the Consumer Identity provided by the Consumer
04. Each SRC System SDK calls the Identity Lookup operation using the Consumer Identity
05. Each SRC System responds, indicating whether the Consumer Device / Consumer is recognised. If the Consumer is recognised by the SRC System, options for validating the Consumer Identity are provided, along with the timestamp for the card that was most recently used with that SRC System
06. Each SRC System SDK responds, including the last used card timestamp

Once the DPA / SRCI has received responses from all the SRC Systems, it selects the SRC System with the most recent last used card timestamp. The flow then continues in Figure 11.2, which shows identity validation at that SRC System.

Figure 11.2: Last Used Card – Example Identity Validation



07. The DPA / SRCI calls the InitiateIdentityValidation() method of the chosen SRC System
08. The SRC System SDK opens an iFrame to carry out the out of band validation
09. The SRC System SDK responds with a validation session id, indicating that validation is successfully being carried out in the iFrame
10. The DPA / SRCI polls the SRC system using the CompleteIdentityValidation() method
11. The SRC System SDK polls the SRC System using the Complete Identity Validation operation
12. The SRC System responds with the status of the identity validation, including a Federated ID Token and Masked Card once the identify validation has been successfully completed
13. The SRC System SDK responds with the status of the identity validation and, if available, the Federated ID Token and Masked Card representing the last used card

Once identity validation has been successfully completed, the DPA / SRCI can present the Consumer with:

- The last used card as the default option (with the option that the Consumer can select a different card) ; *or*
- The SRC Candidate List, with the last used card shown as the default selection

Last Used Card as Default Option

If the DPA / SRCI presents the last used card to the Consumer as the default option, then the flow continues with Steps [14] to [15]:

14. The DPA / SRCI presents the last used card to the Consumer as the default option
15. The Consumer can either:

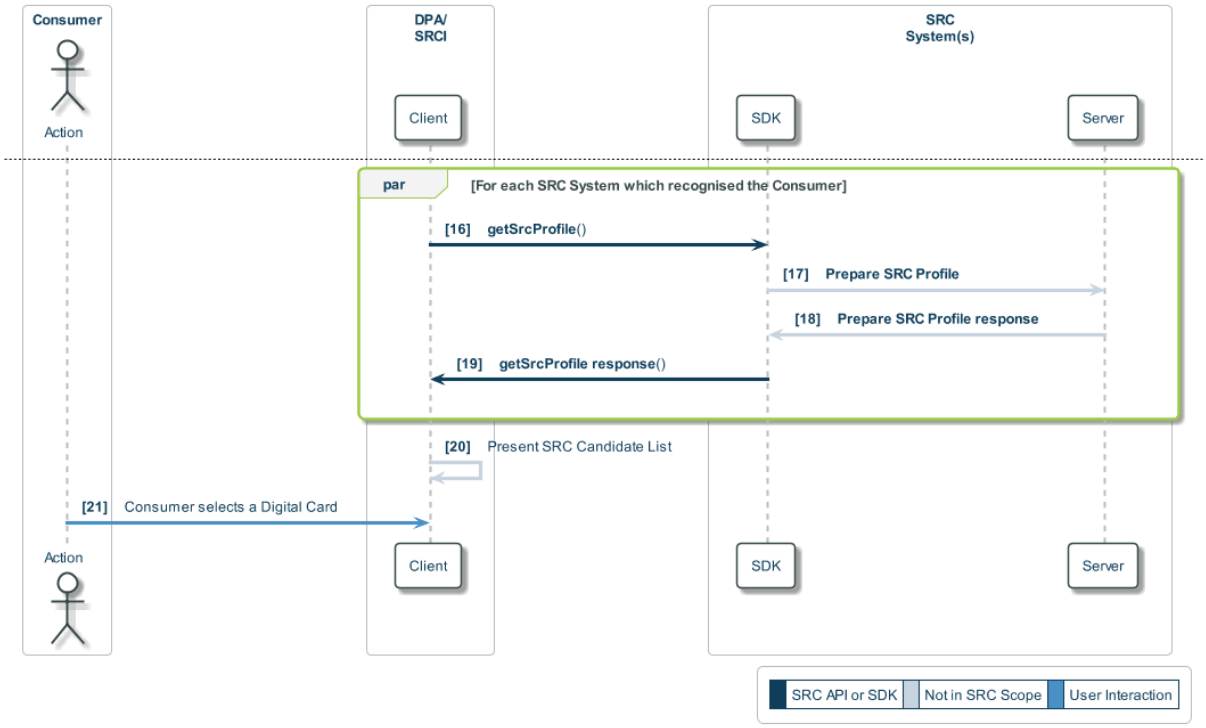
- Select the last used card and proceed to checkout
- Request the option to select a different card

If the Consumer opts for the last used card, the flow proceeds to checkout (not shown). Alternatively, if the Consumer request the option to select a different card, the flow continues in Figure 11.3, which shows the selection of a card by the Consumer.

SRC Candidate List

If the DPA / SRCI presents the SRC Candidate List to the Consumer, then the flow continues in Figure 11.3, skipping Steps [14] to [15].

Figure 11.3: Last Used Card – Example Card Selection



16. For each SRC System which recognised the Consumer, the DPA / SRCI calls the getSrcProfile() method using the returned Federated ID Token
17. Each SRC System SDK calls the Prepare SRC Profile operation
18. The SRC System responds with a list of SRC Profiles
19. Each SRC System SDK responds with a list of SRC Profiles
20. The DPA / SRCI presents the Consumer with the SRC Candidate List. This is comprised of the available Digital Cards from each of the Consumer's SRC Profiles (the DPA / SRCI may present the last used card as the default selection in the SRC Candidate List)
21. The Consumer selects a Digital Card from the SRC Candidate List and proceeds with checkout (not shown in the flow)

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