EMV®
Secure Remote Commerce

Specification

Version 1.3

December 2022

Legal Notice

The EMV® Specifications are provided “AS IS” without warranties of any kind, and EMVCo neither assumes nor accepts any liability for any errors or omissions contained in these Specifications. EMVCO DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AS TO THESE SPECIFICATIONS.

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

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

Revision Log – Version 1.3

The following changes have been made to the document since the publication of version 1.1. Note that there is no version 1.2 of the document.

- Minor Editorial changes
- Changes to account for the deprecation of the SRC Data Dictionary
- Changes to reference the publication of SRC Use Cases
- Removal of description of deprecation (now in SRC Version Management)
- Addition of the following to Section 9.2 Payment Operations
  - Make Payment (push payment)
- Addition of the following Sections:
  - 10.4 Authentication Facilitation
  - 10.5 Management Service
  - 10.6 Notification
- Addition of the following services to Section 11.1.1 SRC API Operations
  - Authentication Facilitation Service
  - Management Service
  - Notification Service
- Addition of the following methods to Section 11.2.1 SRC JavaScript SDK Methods
  - addBillingAddress()
  - authenticationMethodsLookup()
  - authenticate()

Contents

Figures

Tables

1 Introduction

Secure Remote Commerce (SRC) is an evolution of remote commerce that provides for secure and interoperable card acceptance established through a common set of specifications (collectively known as the SRC Specifications).

1.1 Background

Internet-based commerce, known as remote commerce, became available in the 1990s and has continued to grow in popularity as a purchasing environment for Consumers. The remote commerce environment involves the purchase of goods or services through an interaction between a Consumer and a merchant on a Consumer Device. Remote commerce is serviced by a wide variety of stakeholders and is typically enabled through the Consumer entry of Primary Account Number (PAN) data into a merchant's shopping application or commerce provider's website. The current environment has many different integration models and practices. The variety of implementations and the lack of common specifications for this environment results in fragmentation, complexity, and inconsistency for ecosystem stakeholders.

EMVCo's chip specifications have been very successful in driving down counterfeit fraud at the point of sale (POS), enabling cryptograms or other transaction unique data to be transmitted and verified in the transaction. This enables better risk management of the transaction which has led to increased Consumer confidence in card payments and provided the pre-conditions for significant long-term global growth of electronic payments using card accounts. This has been a major benefit to all stakeholders in the payment ecosystem.

While security of payments in the physical terminal environment have improved with the introduction of EMV® specifications, there have been no such specifications for the remote commerce environment. As remote commerce becomes increasingly targeted and susceptible to compromise, it is important to establish common specifications that protect ecosystem stakeholders.

The popularity of remote commerce as a purchasing environment continues to increase with innovation targeted to drive engagement and convenience enabled through new technology and new Consumer Devices.

Although many merchant shopping applications have enabled a card-on-file methodology, the basic method of delivery of the Payment Card is largely insecure and unauthenticated. While account data storage standards such as Payment Card Industry Data Security Standards (PCI DSS) have been a staple in this environment, there is no common specification to address the functional interactions and transmission of data between the participants.

There is growing concern that the lack of uniformity in remote commerce creates opportunity for bad actors and hinders the progress made by the payment ecosystem to reduce payment-related fraud.

An industry transition from a dependency on Consumer entry of PAN data can be accomplished by providing an SRC specification that meets the needs of all stakeholders involved.

1.2 Opportunity

A secure and interoperable specification for transmission of Payment Data, rather than the Consumer entry of Payment Data, has the potential to increase transaction security while simplifying integration for merchants and commerce platforms. There is the opportunity to facilitate more secure methods of remote commerce through:

- Minimising the number of times Consumers enter their Payment Data
- Minimising the local storage of static Payment Data or Personal Identifiable Information
- Supporting common verification of the Consumer to enable access to established Payment Data
- Introducing Dynamic Data to protect the integrity of the Payment Data
- Encryption of Payment Data
- Providing transparency in the transaction data available between the participants to facilitate identity validation and Consumer Device identification to enable enhanced fraud management
- Streamlining integrations between industry participants using a common set of API and SDK specifications

1.3 Scope

This document, the EMVCo Secure Remote Commerce Specification, (hereafter the "Specification"), along with the associated SRC specifications (hereafter the "SRC Specifications", see Section 1.7.2 Published EMVCo Documents) describe the functional behaviour of SRC as well as the interactions and data exchanges among SRC Participants.

In scope for SRC:

- Preparation and assertion of Payment Data delivered to a merchant or commerce provider using a payment-enabled application for a remote commerce payment interaction

- Common SRC API and SRC JavaScript SDK specifications ("EMV® Secure Remote Commerce Specification – API" and "EMV® Secure Remote Commerce Specification – JavaScript SDK"), which include data fields and services to provide consistency and reduce integration complexity by SRC System Participants for the enablement of a remote commerce payment interaction
- Guidance on the interaction and connectivity infrastructure necessary for SRC System Participants to interface with SRC System
- Presentation of visual elements ("EMV® Secure Remote Commerce Specification – User Interface Guidelines and Requirements") that enable Customer selection and recognition of an SRC enabled experience provided by a payment-enabled application

Out of scope for SRC:

- Card-present transactions initiated by an EMV chip application and terminal interaction
- Card-not-present transactions where no Consumer Device is utilised, except for those that are Merchant-Initiated Transactions
- Product definitions and commercial products provided directly to Consumers
- Changes required by participants or to messages within a Payment Networks authorisation, clearing and settlement processes
- Payments initiated from anything other than a Payment Card
- Payment processing interactions including, but not limited to, the submission of an authorisation, reversal, or capture transactions
- Changes to transaction routing or processing choices by Payment System participants
- Eligibility requirements for participation
- Merchant experience guidance or mandates
- Compliance or policy requirements defined by SRC product implementations or SRC Programmes

The SRC Specifications:

- Can be adopted to meet the unique payment ecosystem requirements of international, regional, national or local implementations
- Do not include messages, formats and use case requirements based on implementation details
- Are not designed to mandate, incentivise, or define commercial rules, requirements or policies for the implementation of SRC solutions by international, regional, national or local Payment Systems

1.4 Objectives

The objectives of SRC include:

- Streamlining integrations in remote commerce by:
  - Enabling simplified and efficient integration and interfaces between SRC System Participants
  - Creating guidelines for a recognisable trigger (Click to Pay) to initiate checkout
  - Providing common API and JavaScript SDK specifications that enable integration of industry participants to perform remote commerce
  - Creating common guidelines for card selection within checkout
  - Enabling consistency in the delivery of Payment Data to the merchant to facilitate post-checkout processing and payment authorisation
- Interoperability in the remote commerce environment by:
  - Facilitating interoperable remote transactions
  - Enabling the use and integration of other EMV technologies such as Payment Tokenisation and EMV® 3-D Secure authentication by a variety of SRC Participants to improve the protection and use of Payment Data
- Increasing security in remote commerce by:
  - Maintaining integrity of Payment Data using transactionally unique Dynamic Data
  - Decreasing vulnerability of shopping websites and mobile shopping applications by replacing PAN data with reference information that will enable the secure and consistent transmission of Payment Data and related checkout data
  - Introducing encryption during the exchange of Payment Data between SRC Participants
  - Enabling transparency in the data exchanged between the participants to facilitate improved Consumer Identity validation results and enhanced Consumer recognition
  - Supporting common Assurance to enable access to established Payment Data
  - Enabling federated recognition and authentication of Consumers using a unique Consumer Identity (or supporting common Consumer verification to enable access to established Payment Data)
- Improving benefits to merchants by:
  - Reducing shopping cart abandonment by using a Consumer Identity to access Payment Data, decreasing the need for repetitive manual PAN entries

- Increasing approval rates for remote commerce transactions by reducing fraud
- Delivering a common digital representation of the Consumer account data to merchants

1.5 Constraints

The SRC Specifications are designed to work within a number of constraints of the payment ecosystem, including roles of various entities, transaction flows, and associated payment use cases. These constraints include, but are not limited, to the following:

- The SRC Specifications or any implementation of the SRC Specifications are not intended to replace or interfere with any international, regional, national or local laws and regulations; those governing requirements supersede any industry standards
- An entity providing SRC payment authorisation capability must be cognisant of the payment processing environment in which that service is provided, and ensure that the introduction of SRC does not have an adverse effect on existing processes
- The SRC Specifications do not prescribe any single implementation approach, but describe functions and protocols and the interactions between an SRC System and its SRC Participants

1.6 Audience

This document is intended for the participants in an ecosystem where SRC is implemented.

1.7 References

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

1.7.1 Normative References

The standards in Table 1.1 may be associated with SRC.

Table 1.1: Normative References

Reference	Publication Name
ISO 3166	Country Codes — ISO 3166

Reference	Publication Name
ISO 4217	Currency Codes — ISO 4217
ISO 8583	Financial transaction card originated messages — Interchange message specifications (1987, 1993, 2003 and other variants where appropriate)
RFC 3447	Public-Key Cryptography Standards
RFC 5246	Transport Layer Security (TLS) Protocol
RFC 5322	Internet Message Format
RFC 7516	JSON Web Encryption
RFC 7518	JSON Web Algorithms
RFC 7519	JSON Web Token
OpenID	OpenID Connect Core
Secure Payment Confirmation	W3C specification Secure Payment Confirmation

1.7.2 Published EMVCo Documents

The documents in Table 1.2 are related to or are associated with SRC and are located at 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
Merchant-Presented Mode	EMV® QR Code Specification for Payment Systems (EMV QRCPS) – Merchant-Presented Mode
Payment Tokenisation Technical Framework	EMV® Payment Tokenisation Specification – Technical Framework

Reference	Publication Name
Payment Tokenisation A Guide to Use Cases	EMV® Payment Tokenisation – A Guide to Use Cases
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
SRC Use Cases	EMV® Secure Remote Commerce Use Cases
Transaction Types	EMV® Best Practices Document – Recommendations for EMV Processing for Industry-Specific Transaction Types

Collectively, the term SRC Specifications refers to:

- SRC Core Specification (this document)
- SRC Reproduction Requirements
- SRC UI Guidelines and Requirements
- SRC API
- SRC JavaScript SDK
- SRC Version Management

1.8 Definitions

The definitions contained within this document apply only to the context of the SRC Specifications and are not representative of other uses outside of the scope of the SRC Specifications. Local market differences in terminology may exist, and these are not reflected in the SRC Specifications.

The following terms as defined in Table 1.3 are used in the SRC Specifications.

Table 1.3: Definitions

Term	Definition
Assurance	An assertion of an authentic identity claim(s) provided by SRC Participants for Consumer, Device, Cardholder, Card and/or Relationship identity(s).
Binding	The process that establishes the relationships to an SRC Profile.
Cardholder	An individual that has been issued a financial account provisioned to a Payment Card by a Card Issuer, where a Payment Card is used as a PAN or a Payment Token for purchases.
Cardholder-Initiated Transaction	A transaction where the Cardholder directly interacts with the Digital Payment Application using a Digital Card.
Card Art	A visual representation of the Digital Card.
Card Issuer	A financial institution or its Third Party Service Provider that issues a Payment Card to Cardholders.
Click to Pay Icon	A visual representation that identifies that SRC is available to the Customer.
Consumer	An individual with an existing SRC Profile using the services provided within SRC.
Consumer Device	A Consumer-operated device such as a smartphone, laptop, personal computer, tablet, or voice-activated digital assistant or any application running on a device.
Consumer Identity	A unique value provided by the Consumer to associate the Consumer with a specific SRC Profile.
Customer	An individual making a purchase using a Digital Payment Application.
Device Identity	A combination of attributes enabling the identification of a Consumer Device.
Digital Card	A digital representation of a Payment Card.

Term	Definition
Digital Card Facilitator (DCF)	The SRC System Participant which provides a Consumer with access to Digital Card related data and other optional services.
Digital Card Feature	A card benefit provided by the Card Issuer or SRC System and associated with a Digital Card.
Digital Payment Application (DPA)	A payment-enabled application that enables the initial interaction of a Customer with a merchant, marketplace or other service provider in order to use SRC to pay for goods or services through a Consumer Device.
Dynamic Data	A value unique to a transaction used to protect the integrity of the Payment Data.
EMV 3-D Secure	EMV 3-D Secure authentication is a three-domain model where the acquirer domain and issuer domain are connected by an interoperability domain for the purpose of authenticating a Cardholder or providing verification of their identity during a transaction. Refer to EMV 3-D Secure Protocol and Core Functions Specification.
Enrolment	The process of associating a PAN with an existing or new SRC Profile.
Federated ID Token	A digitally signed attestation that the Consumer Identity has been verified by an SRC System.
First Party Token	An opaque first party authorisation token issued and recognised by the same SRC System.
Merchant-Initiated Transaction	A transaction that relates to a previous Cardholder-Initiated Transaction but conducted without Cardholder participation.
Onboarding	The process that establishes credentials that enable an SRC System Participant to interact with an SRC System.
Payment Card	A payment credential created by a Card Issuer or their agent for a Cardholder to enable a financial transaction. A Payment Card contains Payment Data.
Payment Data	A PAN or Payment Token required to initiate a payment authorisation request.

Term	Definition
Payment Network	An entity that operates an electronic system for payment transaction processing, including operating a network switch for purposes of completing payment authorisation, clearing, and settlement for one or more Payment System(s).
Payment System	An entity that maintains a consumer-facing brand and provides branding guidelines, inclusive of branding requirements for issuers and merchant acceptance environments, may distribute IINs/BINs, defines rules and guidelines for Payment System participants, and develops products and respective product requirements for Payment System participants that are derived from a variety of technologies.
Payment Token	A surrogate value for a PAN that is an ISO/IEC 7812-compliant numeric issued from a designated Token BIN or Token BIN Range that must pass basic validation rules of a PAN.
Payment Tokenisation	A specific form of tokenisation whereby Payment Tokens are requested, generated, issued, provisioned, and processed as a surrogate for PANs. Refer to EMV Payment Tokenisation Specification – Technical Framework.
Primary Account Number (PAN)	An ISO/IEC 7812-compliant account number that is generated within account ranges associated with a PAN BIN or PAN BIN Range by a Card Issuer.
Registration	The process by which a Digital Payment Application is identified by an SRC Initiator to an SRC System.
SRC Candidate List	A list of Digital Cards and related data that are eligible for a specific checkout.
SRC Initiator	The SRC System Participant which presents an SRC Candidate List and potentially facilitates the retrieval of Payment Data.
SRC Participant	An Onboarded or Registered entity that participates in SRC.
SRC Participating Issuer (SRCPI)	A Card Issuer that has its Payment Cards enrolled in SRC Systems.
SRC Profile	A collection of data within an SRC System comprising a primary Consumer Identity and optional data elements such as Payment Card(s), Digital Card(s), Consumer information, and Device Identity(s).

Term	Definition
SRC Programme	Responsible for the policies and processes associated with the oversight of SRC Participants within an SRC System.
SRC System	A technical platform that manages an SRC Profile for each enrolled Consumer and facilitates the payment information exchange among all SRC System Participants.
SRC System Participant	An entity that is Onboarded to an SRC System.
SRC Trigger	The point of initialisation for checkout which may accompany a Click to Pay Icon.

1.9 Notational Conventions

1.9.1 Abbreviations

The abbreviations listed in Table 1.4 are used in the SRC Specifications.

Table 1.4: Abbreviations

Abbreviation	Description
3DS	EMV 3-D Secure
ACS	Access Control Server
API	Application Programming Interface
AReq	Authorisation Request
ARes	Authorisation Response
AVS	Address Verification Service
BIN	Bank Identification Number
CDCVM	Consumer Device Cardholder Verification Method
CSC	Card Security Code

Abbreviation	Description
DCF	Digital Card Facilitator
DPA	Digital Payment Application
FIDO	Fast Identity Online
ID&V	Identification and Verification
IIN	Issuer Identification Number
IoT	Internet of Things
JSON	JavaScript Object Notation
JWE	JSON Web Encryption
JWS	JSON Web Signature
KBA	Knowledge Based Authentication
OTP	One Time Passcode
PAN	Primary Account Number
PCI DSS	Payment Card Industry Data Security Standards
PII	Personally Identifiable Information
QR	Quick Response
SCA	Strong Customer Authentication
SDK	Software Development Kit
SPC	Secure Payment Confirmation
SRC	Secure Remote Commerce
SRCI	Secure Remote Commerce Initiator
SRCPI	Secure Remote Commerce Participating Issuer
T&Cs	Terms & Conditions

Abbreviation	Description
TLS	Transport Layer Security
TSP	Token Service Provider
UI	User Interface
UTC	Coordinated Universal Time

1.9.2 Terminology and Conventions

The following words are used in the SRC Specification and have a specific meaning:

SHALL/MUST

Defines a product or system capability which is mandatory.

MAY

Defines a product or system capability which is optional or a statement which is informative only and is out of scope for the Specification.

SHOULD

Defines a product or system capability which is recommended.

The following conventions apply:

Defined Terms, Operations, Methods and Data Elements

The SRC Specifications use capitalisations, camel case and different fonts, with the following conventions, to refer to:

- Defined terms (see Table 1.3) are capitalised with no other qualification (e.g. Digital Card Facilitator)
- SRC API operations are capitalised and followed by the word “operation” (e.g. Checkout operation)
- SRC JavaScript SDK methods are in camel case and followed by “() method” (e.g. enrollCard() method)
- SRC API and SRC JavaScript SDK complex data objects are capitalised and in Courier New font (e.g. `DigitalCardData`)
- SRC API and SRC JavaScript SDK data elements are in camel case and Courier New font (e.g. `srcCorrelationId`)
- Booleans are in lower case and in Courier New font (e.g. `true`)

2 Overview

Secure Remote Commerce (SRC) offers an approach to promote security and interoperability within the card payment experience in a remote payment environment. SRC facilitates the delivery of interoperable Payment Data to a merchant, during checkout, in order for the merchant to process a payment.

The core tenets of SRC are:

- Consumer Awareness: the Consumer is aware that an SRC experience is occurring when initiating checkout
- Consumer Recognition: the ability for a Consumer to be recognised and authenticated using a unique Consumer Identity
- Card Selection: presentation of an SRC Candidate List to a recognised Consumer in order to select a card
- Consumer Review & Confirmation of Checkout: presentation of all related payment information to be edited and confirmed by the Consumer
- Payload Delivery: providing Payment Data and transactionally unique Dynamic Data to authorised participants in order to facilitate payment authorisation

A brief description of the entities involved in SRC is given in Table 2.1.

Table 2.1: SRC Entities

Entity	Description
SRC Programme	Responsible for the policies and processes associated with the oversight of SRC Participants within an SRC System.
SRC System	A technical platform that manages an SRC Profile for each enrolled Consumer and facilitates the payment information exchange among all SRC System Participants.
SRC Initiator	The SRC System Participant which presents an SRC Candidate List and potentially facilitates the retrieval of Payment Data.
Digital Card Facilitator	The SRC System Participant which provides a Consumer with access to Digital Card related data and other optional services.
SRC Participating Issuer	A Card Issuer that has its Payment Cards enrolled in SRC Systems.
Digital Payment Application	A payment-enabled application that enables the initial interaction of a Customer with a Merchant, marketplace or other service provider in order to use SRC to pay for goods or services through a Consumer Device.

Enabling innovation requires flexibility in the user experience to support a variety of different use cases. At the same time, consistency across some elements help deliver streamlined user experiences across SRC Programmes which drive increased conversion and better repeat experiences.

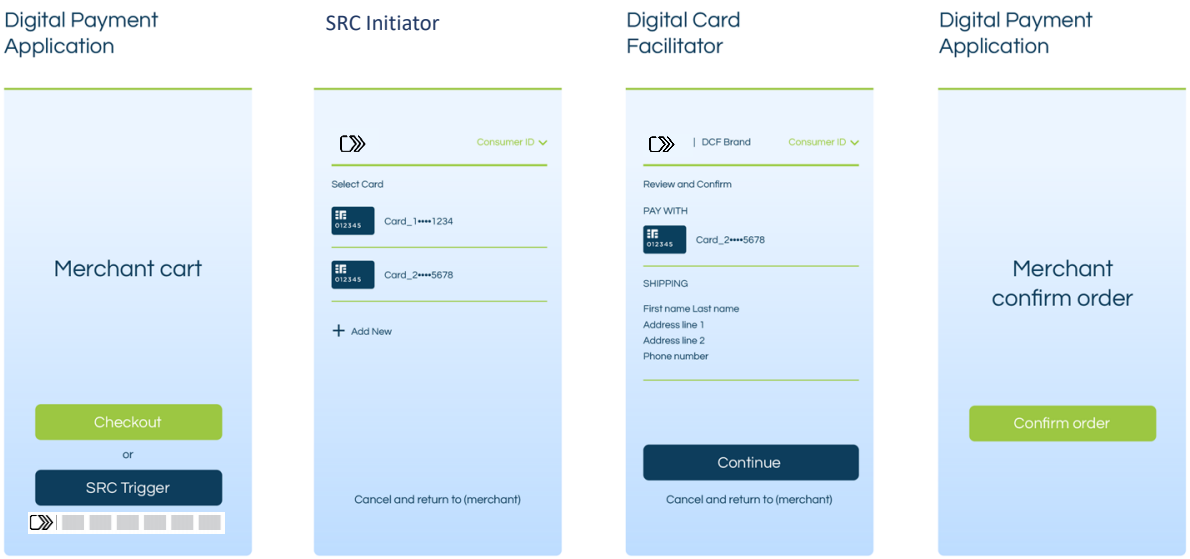
The SRC UI Guidelines and Requirements describe the common presentation elements of the user experience supported within SRC. These include:

- SRC Trigger
- Input for Consumer Identity
- Consumer Assurance
- SRC Candidate List
- Payment method and Cardholder information confirmation

The user experience for SRC is completed when the checkout process returns control to the Digital Payment Application.

An example flow for a remembered Consumer is shown in Figure 2.1.

Figure 2.1: Example Consumer Flow



When a Consumer indicates an intent to complete a purchase, the following specific actions are enabled:

- Initialisation: presentation of an SRC Trigger within the Digital Payment Application that indicates to the Customer that an SRC experience is available. The SRC Trigger (Checkout button or SRC Trigger button above) is the point of interaction that activates the SRC experience
- Card selection: presentation by the SRC Initiator of the SRC Candidate List that enables the Consumer to select the Digital Card to be used for payment
- Consumer review: presentation by the Digital Card Facilitator of confirmation information that includes:
  - Delivery Information: personal data (that may be changed by the Consumer) that accompanies a purchase
  - Acknowledgement: validation of the selected Digital Card and personal data
- Merchant completion: return of the user experience to the Digital Payment Application that will indicate any next steps necessary to process payment.

SRC Systems assess whether additional Assurance is needed to perform a specific action. This assessment is use case specific and determined by the policies of the SRC Programme. For example, additional Assurance could be attempted to authenticate the Consumer Identity.

In addition, the SRC Use Cases document describes various use case examples under the categories of:

- Enrolment

- Checkout (SRC and Merchant)
- Management Service
- Recognition
- Authentication Facilitation

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 may use certain functions enabled by the SRC API or SRC JavaScript SDK in an SRC System specific way to enable the desired experience.

3 SRC Participants

This Section provides details on the various SRC Participants, their roles and how they interact to enable SRC experiences.

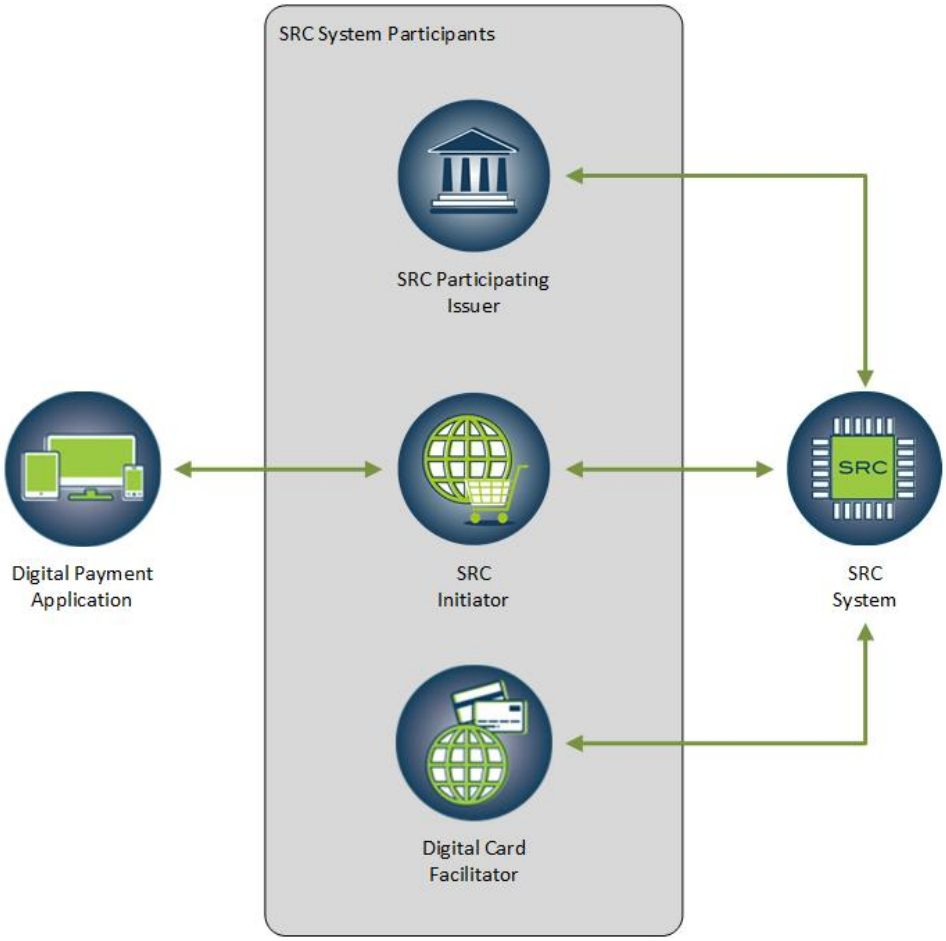
While the SRC Specifications provide flexibility for participation, they do not:

- Prescribe which entities can act as which SRC System Participant
- Define new actors or suggest modifications to existing relationships between payment ecosystem participants.

Note that as shown in Figure 3.1, the SRC Specifications distinguish between:

- SRC Participants, encompassing the SRC System, SRC Initiator, Digital Card Facilitator, Digital Payment Application and the SRC Participating Issuer
- SRC System Participants, encompassing entities that interact directly with the SRC System (SRC Initiator, Digital Card Facilitator and the SRC Participating Issuer)

Figure 3.1: SRC Participants



3.1 SRC Programme

An SRC Programme is established by a business entity responsible for the policies, requirements and processes associated with the oversight of participating SRC Systems and all SRC Participants.

Examples of policies, requirements, and processes that could be established by an SRC Programme include, but are not limited to, the following:

- Onboarding and configuration for SRC System Participants
- Registration and configuration for Digital Payment Applications
- Enrolment of Consumers and Payment Cards into an SRC System
- Visual guidance for SRC System Participants
- Supported Assurance methods
- Use and management of Payment Data
- On-going operation and maintenance of participating SRC Systems
- Lifecycle management of configuration data
- Security policies for SRC Systems and SRC Participants
- Performance requirements for SRC Systems and SRC Participants
- Policies for usage of the SRC API and the SRC JavaScript SDK
- Types of checkout supported
- Criteria that define the relationship of Digital Cards to Digital Card Facilitators

3.2 SRC System

An SRC System is a technical platform that is established by a business entity. It manages an SRC Profile for each enrolled Consumer and facilitates the payment information exchange among all SRC System Participants.

An SRC System is responsible for implementing SRC Programme policies, requirements and processes. These responsibilities may include but are not limited to:

- Onboarding, management and integration of SRC System Participants
- Registration, management and integration of Digital Payment Applications
- Orchestration of the checkout experience
- Creation and management of SRC Profiles
- Ensuring adequate controls of Personally Identifiable Information (PII) data

- Federating ID Token management with other SRC Systems and/or other identity providers
- Configurations related to the use of unique Dynamic Data in Payment Data
- Delivering Payment Data in accordance with established Payment System and Payment Network transaction processing requirements
- Implementing the functions defined in the SRC API and SRC JavaScript SDK in accordance with the requirements of the SRC Programme
- Maintaining and distributing a JavaScript SDK
- Hosting a recognition subdomain to enable Consumer recognition for browsers

3.3 SRC Initiator

An SRC Initiator provides the following functionality:

- Registration of Digital Payment Application(s)
  - The SRC Initiator manages Registration for its participating Digital Payment Applications
  - A Digital Payment Application can be Registered by multiple SRC Initiators.
- Integration with SRC System(s)
  - An SRC Initiator may provide support for a specific technology (e.g. web, mobile application, IoT services)
  - An SRC Initiator may implement recognition subdomain functionality to allow Consumer recognition for browser-based use cases

SRC Initiators also provide payment and/or non-payment functions. In some cases, an entity may provide all functions of an SRC Initiator. In other cases, functions may be split between entities:

- Payment functions (Section 9 Payment Enablement)
  - Receives Payment Data from an SRC System
  - Entities that provide payment services on behalf of merchants can be SRC Initiators in their own right. Such entities indicate which merchant they are servicing by providing the appropriate Digital Payment Application configuration data to SRC Systems
  - Provides payment confirmation to the SRC System
- Non-Payment functions (Section 10 Non-Payment Functions)

- Initiation of checkout, presentation of SRC Candidate List (see Section 8.3.1 SRC Profile Retrieval) and completion of checkout
- Provides checkout confirmation to the SRC System
- Transmits and receives checkout data on behalf of a Digital Payment Application to SRC Systems indicating transaction details and service elections

3.4 Digital Card Facilitator

The Digital Card Facilitator provides access to Consumer data such as billing address, shipping addresses and other data tied to a specific Consumer Identity, provided it is relevant to, and requested by, various SRC Participants.

In Secure Remote Commerce, Digital Card Facilitators are responsible for providing the ability to Consumers to review and confirm the Digital Card and payment-related data associated with a specific checkout.

3.5 SRC Participating Issuer (SRCPI)

An SRC Participating Issuer is configured in each SRC System to establish eligibility and enable Enrolment of its Cardholders and their related PANs.

An SRC Participating Issuer may:

- Identify its BIN and or BIN ranges eligible to participate in SRC so that eligibility can be determined by the SRC System
- Provide Card Art and other data that is used to surface the Digital Card to the Consumer
- Determine the default Digital Card Facilitator(s)
- Provide Assurance method preferences to be used during an Enrolment or checkout
- Provide Enrolment data to the SRC System to facilitate Cardholder participation in SRC

The SRC Participating Issuer also manages other business processes related to Enrolment defined by the SRC Programme.

3.6 Digital Payment Application

A Digital Payment Application enables the initial interaction of a Customer with a merchant. A Digital Payment Application can be any payment-enabled application such as a website, mobile application or IoT device. Participation of the Digital Payment Application is based on the following:

- Relationship with SRC Initiator(s): Each Digital Payment Application integrates with one or more SRC Initiators. As part of integration, the SRC Initiator may register the Digital Payment Application for participation in each SRC System
- Selection of Digital Payment Application(s): The merchant, or any other commerce provider, selects which of its Digital Payment Applications will participate in one or more SRC System(s) through one or more SRC Initiator(s)
- SRC Trigger: The requirement to support a specific SRC Trigger is defined by the SRC Programme and the types of checkout supported as described in Section 8.2 SRC Trigger

Merchants can elect to integrate with multiple front-end SRC Initiators (shopping carts, gateway providers etc.) and need to consider implications for their Digital Payment Application and SRC experience.

A Digital Payment Application provides the following functionality:

- Presenting an SRC Trigger and providing indication of which SRC Systems it supports to the Consumer
- Invoking one or more SRC Initiators
- Conveying data to SRC Initiators indicating transaction details and service elections, which may include but is not limited to Payment Tokenisation and EMV 3-D Secure payment authentication
- Providing checkout confirmation information to the SRC Initiator

4 Onboarding and Registration

SRC Participants are established within an SRC Programme through a series of set-up events orchestrated by the SRC System. Once established, the SRC System continues to manage SRC Participants' data throughout their life cycle. The establishment and subsequent management of SRC Participants occur using the following set-up events provided by SRC Systems:

- Onboarding of SRC System Participants
- Registration of Digital Payment Applications

For each of the above events, the SRC Systems stores configuration settings and, as allowed by the SRC API or SRC JavaScript SDK, configuration data can be overridden during checkout and payment.

While these events are orchestrated by the SRC System, the data requirements, processes and methods associated with Onboarding and Registration are outside the scope of the SRC Specifications. For example, an SRC System may use batch processes, automated tools or portals to enable manual entry of data, or a combination of these to facilitate Onboarding or Registration.

4.1 Onboarding of SRC System Participants

Onboarding establishes:

- The relationship between the SRC System Participants and SRC Systems
- Credentials that enable the interaction between the SRC System Participants and the SRC Systems

Onboarding to SRC Systems is supported for the following SRC System Participants:

- Digital Card Facilitator
- SRC Initiator
- SRC Participating Issuer

The following may be performed by an SRC System during Onboarding:

- Obtain business-related information from each SRC System Participant.
- Generate unique reference identifiers for each SRC System Participant
- Exchange keys with SRC System Participants to enable signing and verification (e.g. JWS) and application-level encryption (e.g. JWE)

- Establish settings for features and services offered by the SRC System for checkout and payment
- Management of transaction settings for Payment Tokenisation and payment authentication using EMV 3-D Secure
- Manage configurations for each SRC System Participant such as:
  - Unique reference identifiers for every SRC Participant in the SRC System
  - Adding and managing relevant configuration details
  - Allowing access to SRC Profile data

4.2 Registration of Digital Payment Application

Registration establishes the identity of the Digital Payment Applications within the SRC Systems through the Digital Payment Application's related and previously Onboarded SRC Initiator(s).

SRC Systems may require that the Digital Payment Application has been Registered before it initiates a checkout. For these SRC Systems, SRC Initiator(s) are required to provide the necessary Digital Payment Application data for each of the Digital Payment Application(s) they service. As a Digital Payment Application may have a relationship with multiple SRC Initiators, each SRC Initiator will perform a separate Registration. At a high level, Registration involves the establishment of a unique reference identifier and configuration settings for each Digital Payment Application within each SRC System.

For SRC Systems that do not require the Digital Payment Application to be Registered prior to checkout, the necessary Digital Payment Application data is provided during checkout.

For SRC Systems that require the Digital Payment Application to be Registered prior to checkout, the optional Management Service APIs are available in Section 10.5 Management Service.

5 SRC Profile and Digital Card

This Section describes the SRC Profile and Digital Card.

5.1 SRC Profile

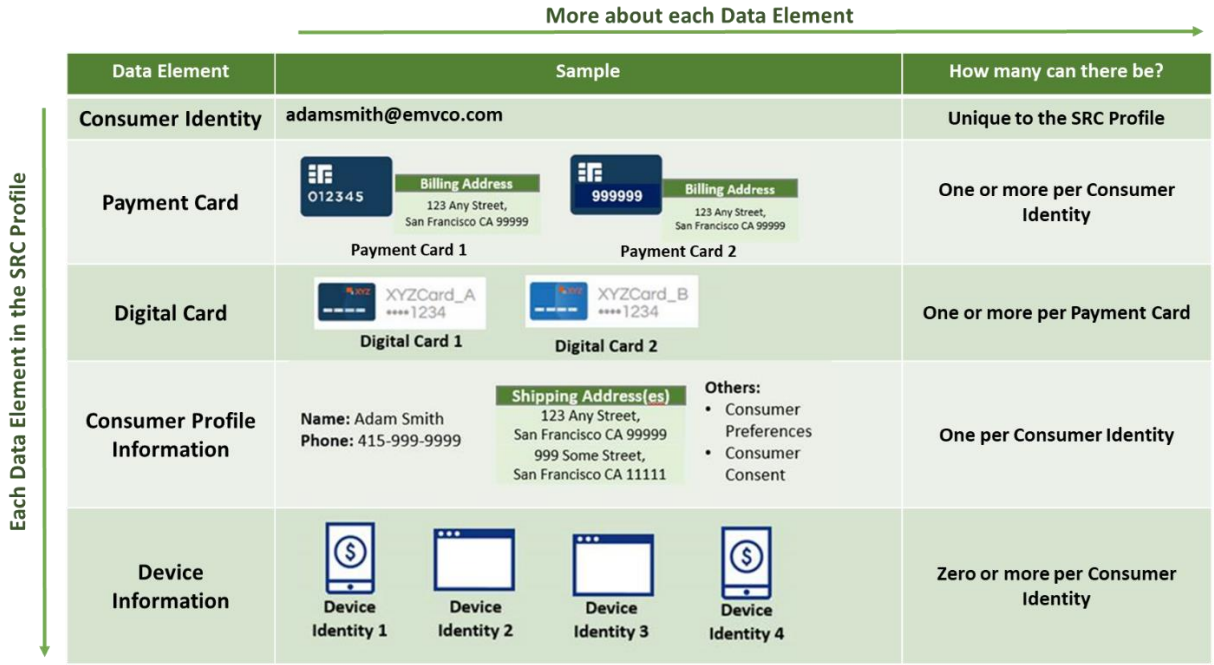
Each SRC System creates and manages SRC Profiles. Each SRC Profile has a primary Consumer Identity, which the Consumer uses to access the SRC Profile, and optional data elements which can include:

- Payment Card(s)
- Digital Card(s)
- Consumer information
- Device Identity(s)

While an SRC Profile is created during Enrolment, it may be added to and/or managed during subsequent SRC interactions.

Figure 5.1 shows the relationships between the main data elements within the SRC Profile.

Figure 5.1: SRC Profile Organisation



Note: more details on data elements can be found in the SRC API.

The initial SRC Profile is created during Enrolment. The SRC System then manages the SRC Profile throughout its life. This includes:

- Adding new data elements (e.g. Consumer adds a new Payment Card)
- Updating content of existing data elements (e.g. Consumer changes a shipping address)
- Deleting existing data elements (e.g. Consumer removes a device from the SRC Profile)

Changes to the SRC Profile can occur due to any of the following:

- Enrolment
- Binding
- Lifecycle mangement

How the SRC Profile data is configured, or managed, by the SRC System is outside the scope of the SRC Specifications.

When the SRC System provides an SRC Profile to an SRC System Participant, the results are dependent on the following:

- Policies and requirements of the SRC Programme
- Configured selections of the Digital Payment Applications, Consumers, and SRC Participating Issuers.
- Capabilities and services available for the Digital Card Facilitators

The above may also affect the level of data provided for a Digital Card as presented content can affect Customer usability, and the overall user experience.

5.2 Digital Card

The Digital Card represents the underlying PAN (Payment Card or Payment Token) within SRC. It is used for:

- All communication with the Consumer/Cardholder such as purchase receipts, order confirmation pages, emails, text messages, chat-bots, messenger platforms, etc.
- Enabling the Consumer to make a selection from the SRC Candidate List

Accompanying the Digital Card is a visual version of the Payment Card commonly referred to as Card Art.

An SRC System may also manage Digital Card Features. These enable the SRC System and/or the Card Issuer to present a card benefit to the Consumer at checkout. Some examples of card benefits may include, but are not limited to:

- Complimentary memberships
- Concierge services
- Event ticket protection
- Extended warranty

How Digital Card Features are received and managed by the SRC System is out of scope of the SRC Specifications.

5.3 Data Obfuscation

Within SRC, Consumer PII data such as name, address, email address or phone number should be obfuscated when presented. It is the responsibility of the SRC Participants to ensure that the communication and presentation of PII data related to the Digital Card or Consumer is obfuscated as required by local regulations, SRC Programme policies and Payment System policies.

Obfuscation of information may be achieved by following the masking rules and best practices defined in Annex B Data Obfuscation. The masking rules and best practices ensure obfuscation of data is conducted in a consistent manner that enables the Consumer to recognise their information while limiting the potential for others to determine the PII data.

6 Card Services

This Section describes:

- Enrolment of a PAN in an SRC System
- Management of enrolled PANs
- Management of the SRC Profile

6.1 Enrolment

Typically, an SRC Participating Issuer drives Enrolment by providing Cardholder PAN(s) and associated Consumer Identities to an SRC System. However, Digital Card Facilitators and SRC Initiators, based on SRC Programme participation policies, can also initiate Enrolment. The Cardholder must provide consent to participate in SRC by electing or confirming Enrolment of its PAN(s) in an SRC System.

If an SRC Profile already exists for the Cardholder, then when a PAN is Enrolled, it will be associated with the existing SRC Profile, otherwise the SRC System will create a new SRC Profile.

An SRC System may support proprietary batch processes for Enrolment, allowing simultaneous Enrolment of more than one PAN. Batch Enrolment details are not in scope of this Specification.

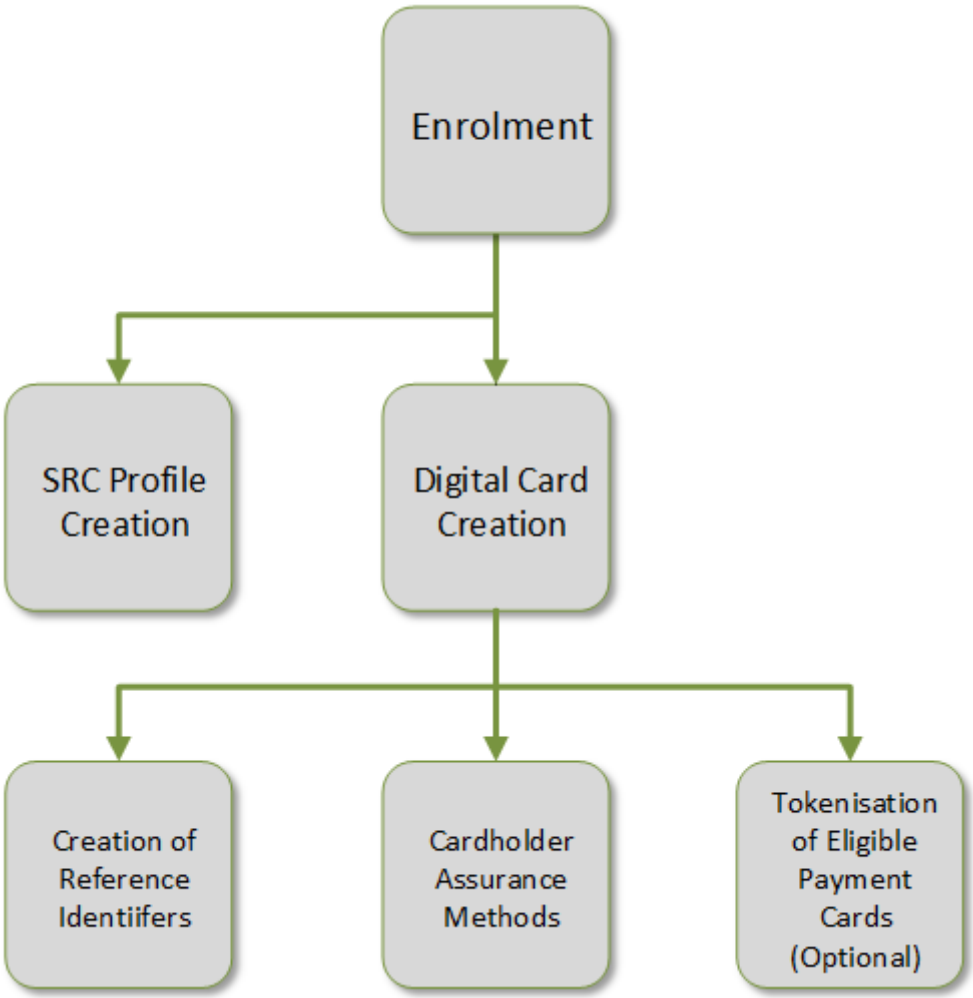
The SRC API and SRC JavaScript SDK define operations/methods to facilitate Enrolment, which are shown in Table 6.1.

Table 6.1: Enrolment Operations/Methods

Specification	API/SDK Operation/Method
SRC API	Card Enrolment
SRC Java Script SDK	enrollCard() checkout()

The functions associated with Enrolment are shown in Figure 6.1.

Figure 6.1: Enrolment



6.1.1 SRC Profile Creation

When creating an SRC Profile, the SRC System includes assigned values as well as information provided by the Consumer. As a minimum, each SRC Profile must have:

- A Consumer Identity
- A unique identifier for the SRC Profile

Examples of additional information contained within an SRC Profile are given in Figure 5.1.

The SRC System will also keep a record of when the SRC Profile was created.

6.1.2 Digital Card Creation

The SRC System creates Digital Card instances of the Payment Card associated with the underlying PAN. When creating a Digital Card, the SRC System includes assigned values as well as Payment Card and Cardholder information such as:

- An SRC System specific reference identifier for each Digital Card and Payment Card
- Payment Data (a Payment Token may be requested for the PAN during Enrolment)
- BIN and last four digits of Payment Data
- Digital Card presentation information (Card Art)
- Cardholder Assurance methods associated with the Digital Card

The SRC System will also keep a record of when the Digital Card was created.

Note: Payment Tokenisation – A Guide to Use Cases gives example use cases showing how SRC can combine with Payment Tokenisation to issue a Payment Token for the PAN during Enrolment.

6.2 Managing Digital Cards

The SRC API and SRC JavaScript SDK provide a number of operations/methods to allow an SRC System to manage Digital Cards.

6.2.1 Delete Card

Table 6.2 shows the operations/methods defined by SRC API and SRC JavaScript SDK to delete a Digital Card from an SRC Profile.

Table 6.2: Delete Card Operations/Methods

Specification	API/SDK Operation/Method
SRC API	Delete Card
SRC JavaScript SDK	deleteCard()

6.2.2 Add Billing Address

Table 6.3 shows the operation defined by SRC API to add a billing address to an SRC Profile.

Table 6.3: Add Billing Address Operations/Methods

Specification	API/SDK Operation/Method
SRC API	Add Billing Address
SRC JavaScript SDK	N/A

7 Identity Management

This Section describes how the Consumer Identity and Device Identity are recognised and managed within SRC.

7.1 Identity Recognition

Identity recognition occurs when a Consumer Identity or Device Identity is presented to an SRC System and is performed prior to enabling access to the SRC Profile.

Functions such as Checkout and SRC Candidate List retrieval require successful recognition of the available identity(s) before enabling access to the associated SRC Profile:

- Device Identity recognition: determines if the provided Device Identity is associated with, and has authorised access to, an existing SRC Profile. Device Identity recognition may be performed prior to Consumer Identity recognition
- Consumer Identity recognition: determines if the provided Consumer Identity is associated with, and has authorised access to, an existing SRC Profile
- Additional identity recognition information: if the Device Identity or Consumer Identity is not successfully recognised (i.e. it is not associated with an existing SRC Profile) this may lead to collection of additional information where appropriate

Table 7.1 shows the operations/methods defined by the SRC API and SRC JavaScript SDK to facilitate identity recognition and validation.

Table 7.1 Identity Recognition Operations/Methods

Specification	API/SDK Operation/Method
SRC API	Identity Lookup Initiate Identity Validation Complete Identity Validation Is Recognized
SRC JavaScript SDK	identityLookup() initiateIdentityValidation() completeIdentityValidation() isRecognized()

7.2 Identity Binding

Binding enables the initiation of a recognised, and possibly remembered, experience with the SRC System.

During Enrolment, a primary Consumer Identity, and at least one enrolled Payment Card are bound to an SRC Profile. Additional identities can then be bound to the SRC Profile. Consumers may be required to provide permission for additional Consumer Identities or Device Identities to be bound to an SRC Profile.

Table 7.2 shows the operations/methods defined by the SRC API and SRC JavaScript SDK to facilitate the Binding of Consumer Identities or Device Identities.

Table 7.2 Identity Binding Operations/Methods

Specification	API/SDK Operation/Method
SRC API	Card Enrolment (Binding during Enrolment) Add Consumer Identities (subsequent Binding)
SRC JavaScript SDK	enrollCard() (Binding during Enrolment) checkout() (subsequent Binding)

7.3 Federated Identity

Federated identity enables participating SRC Systems to reduce friction during Checkout by sharing the results of a successful identity recognition by one of the SRC Systems. These results are shared in a Federated ID Token which is:

- A signed JSON Web Token compliant with an OpenID Token format, used in both the SRC API and SRC JavaScript SDK
- Issued by the SRC System that successfully performs identity recognition
- A digitally signed attestation:
  - That the Consumer Identity or Device Identity has been recognised and bound to an SRC Profile
  - Of the primary Consumer Identity bound to the SRC Profile of the issuing SRC System
  - Of claims asserting how the issuing SRC System validated the identity of the Consumer

The Federated ID Token enables participating SRC Systems to:

- Authenticate the origin of the Federated ID Token
- Use the provided Consumer Identity to access an SRC Profile, if present.
- Determine, using their own risk management evaluations, whether additional identity validation is necessary

For security reasons, the provided primary Consumer Identity is obfuscated such that it can only be used by participating SRC Systems with an SRC Profile corresponding to the same Consumer Identity.

7.4 Assurance

Assurance is an assertion from an SRC Participant that an identity or credential verification has already occurred. When accessing an SRC Profile, these assertions may be used in risk management evaluations to determine whether an identity is valid. These assertions can also be used by SRC Participants, or even other entities in the payment ecosystem, to drive risk management decisions and potentially improve the overall user experience.

7.5 Consumer Consent

The SRC System and SRC System Participants may require explicit consent from Consumers to opt in to their SRC related services. Explicit consent may be necessary in order to:

- Facilitate identity management
- Enable improved checkout experiences

8 Checkout

Checkout allows a merchant or commerce provider to request permission to use a payment method for a Consumer's purchase of the merchant's product or service. Checkout may also include:

- Initiation of an SRC checkout or merchant checkout upon invoking an SRC 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
- Payment authentication during checkout

The SRC Specifications do not provide any requirements for payment authentication nor governs 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 (see Section 9 Payment Enablement)

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.

8.1 Types of Checkout

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

- Presence or absence of SRC Participants
- Functions performed by each SRC Participant
- Entities that deliver the user experience
- Trigger mechanism presented to initiate an checkout
- Presence or absence of the Consumer and/or Consumer Device

For the purposes of the SRC Specifications, the following types of checkout are considered for discussion:

- SRC checkout
- Merchant checkout

The SRC checkout and variations on the Merchant checkout are introduced and described in the SRC Use Case document.

The SRC Specifications also support the ability for implementations to provide Cardholder-Initiated and Merchant-Initiated Transactions. These are reliant on unique rules and policies of Payment Systems along with any required Cardholder 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 Cardholder 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 are the result of a previously successful Cardholder-Initiated Transaction

8.1.1 SRC Checkout

SRC checkout is the facilitation of checkout orchestrated by an SRC System in order to simplify and streamline purchase experiences across multiple Digital Payment Applications. It enables Consumers to:

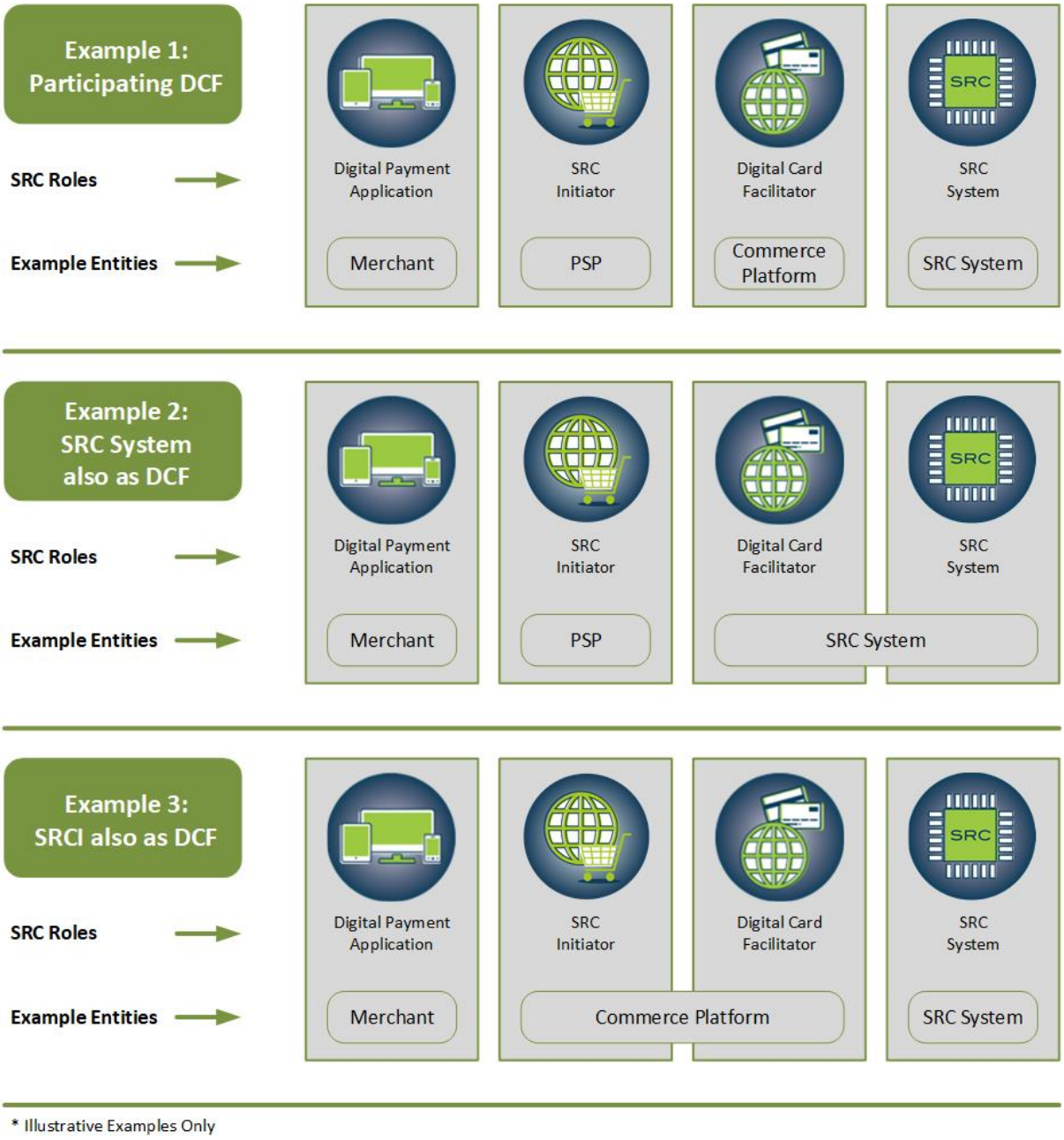
- Access their SRC Profile across participating merchants for single- and repeat uses
- Access Digital Cards for single-use across participating merchants

SRC checkout is characterised by the following:

- Presentation of an SRC Trigger that initiates a checkout experience
- Presentation of terms and conditions to Consumers through a Digital Card Facilitator
- Enablement of access to the SRC Profile or Digital Card(s) by an SRC System
- Management of attributes in the SRC Profile
- Determination of the Digital Card Facilitator for the checkout based on preferences established within the SRC System and the selected Digital Card
- Delivery of payload on completion of checkout by the SRC System

Figure 8.1 gives some checkout examples.

Figure 8.1: Checkout Examples



The examples depict the following scenarios:

- Example 1: Digital Card Facilitator participating in checkout
- Example 2: Digital Card Facilitator provided by the SRC System
- Example 3: Digital Card Facilitator provided by the SRC Initiator where checkout may also be delivered by an entity acting as both SRC Initiator and Digital Card Facilitator, with the Digital Payment Application utilising a separate entity as an SRC Initiator for payload retrieval (as described in Section 3.6 Digital Payment Application)

8.1.2 Merchant Checkout

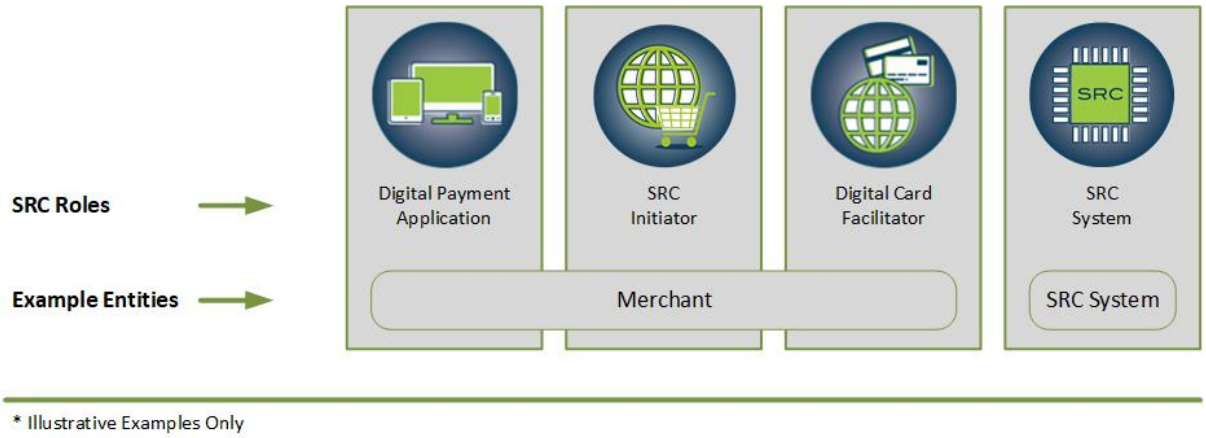
Merchant checkout is a merchant-driven checkout experience that integrates with one or more SRC System(s) to provide simplified, streamlined and repeat purchase experiences across the merchant's Digital Payment Applications.

Merchant checkout is characterised by the following:

- Presentation of an SRC Trigger provided by the Merchant that initiates a checkout experience
- The merchant performing the additional functions of a Digital Card Facilitator and an SRC Initiator
- Presentation of terms and conditions to Consumers by the merchant
- Management of the Consumer Identity by the merchant's Digital Card Facilitator
- Data for Digital Card selection for checkout is provided by the SRC System
- Delivery of payload on completion of checkout by the SRC System
- Usage of consumer data at the merchant additionally being used to provide the user experience

The checkout experience and Cardholder permission for use of Payment Data is controlled by the merchant and is shown by an illustrative example in Figure 8.2.

Figure 8.2: Merchant Checkout



8.2 SRC Trigger

Digital Payment Applications can present an SRC Trigger to indicate to the Customer that an SRC experience is available. The requirement to support a specific SRC Trigger is defined by the SRC Programme and the type of checkout it supports. The SRC Trigger may be a clickable

button, mark, instruction presented, or voice command enabled. When the Click to Pay Icon is used on or in proximity to the SRC Trigger, the SRC Reproduction Requirements need to be followed.

- The SRC Initiator integration software allows Digital Payment Applications to present an SRC Trigger during checkout.
- For Merchant Checkout, the SRC Trigger may be presented by the merchant to initiate checkout
- SRC Triggers will not be present during Merchant-Initiated Transactions

8.3 Checkout Operations/Methods

Table 8.1, Table 8.2 and Table 8.3 show the operations/methods defined by the SRC API and SRC JavaScript SDK to facilitate checkout.

Table 8.1: SRC Profile Retrieval Operations/Methods

Specification	API/SDK Operation/Method
SRC API	Prepare SRC Profile
SRC JavaScript SDK	getSrcProfile()

Table 8.2: Checkout Initiation Operations/Methods

Specification	API/SDK Operation/Method
SRC API	Checkout
SRC JavaScript SDK	checkout()

Table 8.3: Checkout Confirmation Operations/Methods

Specification	API/SDK Operation/Method
SRC API	Confirmation
SRC JavaScript SDK	N/A

Checkout considers the identity of all SRC Participants and uses Digital Payment Application data, enrolled data and configuration settings to enable checkout.

8.3.1 SRC Profile Retrieval

Access to an SRC Profile (see Section 5.1 SRC Profile) is dependent on identity recognition (see Section 7 Identity Management). In the event that identity recognition is not successful, the Consumer may be presented with the option to enrol (see Section 6.1 Enrolment), which leads to the creation of an SRC Profile.

When the SRC System returns an SRC Profile, it provides displayable information associated with each Digital Card, such as Card Art and Digital Card descriptors. The SRC Profile is used by the requesting SRC Initiator to present a Candidate List to the Consumer from which the Consumer can recognise their masked Payment Card during Digital Card selection for checkout purposes. However, when a single SRC Profile containing a single Digital Card is returned, it is not necessary to present an SRC Candidate List.

The `DigitalCardData` (and potentially the `DigitalCardFeatures`) from each received SRC Profile are used to present an SRC Candidate List to the Consumer as described in the SRC UI Guidelines and Requirements. Presentation of optional data is at the discretion of the SRC Initiator as described in the SRC UI Guidelines and Requirements.

`MaskedCard` contains two timestamps (when the Digital Card was last used and when the Digital Card was enrolled) which can be used to order the SRC Candidate List.

When the SRC Systems provide SRC Profiles for multiple Consumer Identities, the presentation of the SRC Candidate List can account for this using either of the following criteria:

- The SRC Candidate List is only displayed after the Consumer's selection of a single Consumer Identity from the full set of Consumer Identities; *or*
- The SRC Candidate List is grouped by Consumer Identity

The SRC System Participant that presents the SRC Candidate List for selection is required to display all SRC Profile Retrieval results that were successfully received from all eligible SRC Systems. The options for determining the display order can use the date that the Digital Card was last used and/or the date that the Digital Card was enrolled.

8.3.2 Checkout Initiation

The SRC Initiator initiates a Checkout operation/checkout() method on behalf of its Digital Payment Application to request information from the SRC System to enable a Consumer purchase.

Checkout initiation:

- Communicates transactional data from a Digital Payment Application to an SRC System
- Varies by use cases provided by the Digital Payment Application
- Is used during a Cardholder-initiated request
- Includes features such as checkout preferences and `DpaTransactionOptions`
- May include an indication of whether the `Payload` is returned in the response or whether it will be requested in a subsequent Get Payload operation
- May include authentication data (for example, 3DS data) in order for the SRC System to facilitate payment authentication on behalf of the Digital Payment Application

On processing a Checkout operation/checkout() method, the SRC System responds to the SRC Initiator including:

- Information from the SRC System to the SRC Initiator that enables the Digital Payment Application to complete the checkout experience for the Consumer (e.g. information required to show a digital receipt to the Consumer may be included)
- A reference identifier for the selected Digital Card which the SRC Initiator can use when requesting Payment Card information in a subsequent Get Payload operation
- Additional resource data such as a Digital Card reference identifier, Card Art and regional data (e.g. postal codes to facilitate the calculation of shipping costs and tax)

If indicated when initiating the Checkout operation/checkout() method, the SRC System also returns:

- The `Payload`
- Authentication data (e.g. 3DS data) indicating the result of payment authentication facilitated by the SRC System

8.3.3 Checkout Confirmation

The SRC Initiator provides confirmation to the SRC System of the outcome of a checkout on behalf of the Digital Payment Application. The `ConfirmationData2` relays whether the Consumer:

- Abandoned the order
- Successfully completed a checkout and agreed to proceed with processing the order

9 Payment Enablement

Payment within SRC denotes a series of events related to the delivery and usage of the SRC Payload during checkout. This is commonly invoked:

- Following checkout of Cardholder-Initiated Transactions
- By merchants during Merchant-Initiated Transactions

The following interactions are involved to facilitate payment:

- `Payload` retrieval
- Payment authentication
- Payment authorisation
- Payment confirmation

While delivery of the `Payload` is orchestrated by the SRC System and `ConfirmationData2` is delivered to the SRC System, payment authentication and payment authorisation are outside the scope of the SRC Specifications. However, they are described here to provide an understanding of how they co-exist with SRC.

9.1 Payment Interactions

9.1.1 Payment Authorisation Preparation

In preparation for payment authorisation, the `Payload` is retrieved from the SRC System by an SRC Initiator:

- During checkout
- Following checkout
- At some future point based on a reference identifier previously received from the SRC System

When providing the `Payload`, the SRC System also provides any additional transaction services requested by the SRC Initiator.

Any request for the `Payload` following checkout includes evidence that a previous SRC interaction occurred, and results in retrieval of all payment-related data associated with the original checkout.

The content of the `Payload` contains payment-related data required for the generation of either a payment authentication request and/or an authorisation request. This always includes:

- A PAN or Payment Token

- Dynamic Data

Additionally, the `Payload` may also include the following information to facilitate payment authorisation:

- Billing address
- Consumer's phone number
- Consumer's name

9.1.2 Payment Authentication

The SRC Specifications do not provide any requirements for payment authentication nor govern activities within it. However, SRC offers Digital Payment Applications the choice to use EMV 3-D Secure to conduct payment authentication in one of the following ways:

- Within an SRC experience (see Section 8 Checkout). The merchant may request that SRC Systems (that provide this service) perform EMV 3-D Secure on behalf of the merchant. In this case, the information required by the SRC System to perform EMV 3-D Secure is provided when initiating the Checkout operation/checkout() method and the payment authentication response provided by an Access Control Server (ACS) is delivered in the `Payload`
- Outside of the SRC experience. Merchants that currently support EMV 3-D Secure use the information contained in the `Payload` as a source of information to enable a payment authentication request to be routed to the ACS

9.1.3 Payment Authorisation

An acquirer or its agent provides routing and authorisation services as part of normal business practices. SRC does not impact the routing or authorisation processes.

Using the data provided in the `Payload`, including Dynamic Data, the SRC Initiator sends, on behalf of the merchant, a request for authorisation through the acquirer. Dynamic Data presented in an authorisation is intended to protect against replication or re-use of the same Payment Data in a subsequent authorisation. Based on configuration and transaction preferences, a Payment Token-based payload (as described in the Payment Tokenisation Technical Framework) can be returned in lieu of a PAN-based payload by the SRC System.

The acquirer routes the authorisation request to its designated Payment Network consistent with current practices. The Payment Network provides the request to the Card Issuer and may provide Card Issuer validation services.

The Payment Network performs its traditional role, which includes, but is not limited to:

- Receiving authorisation requests from the acquirer
- Sending authorisation requests to the Card Issuer

- Providing authorisation responses to the acquirer
- Providing clearing and settlement services to the acquirer and the Card Issuer

Once a transaction is successfully switched to the Card Issuer via a Payment Network, the Card Issuer makes an appropriate authorisation decision and provides an authorisation response that enables the SRC Initiator to initiate a payment confirmation to the appropriate SRC System.

9.1.4 Payment Authorisation Confirmation

After the SRC Initiator has used the payload data in a payment authorisation, it sends `ConfirmationData2` to the SRC System to indicate the outcome of payment authorisation. The SRC System may use the outcome to manage the lifecycle of Payment Data, and to perform risk management related activities.

9.2 Payment Operations

Table 9.1 shows the operations defined by the SRC API to facilitate payment. There are no equivalent methods in the SRC JavaScript SDK.

Table 9.1: Payment Operations/Methods

Specification	API/SDK Operation/Method
SRC API	Get Payload (initiation of payment) Confirmation (payment confirmation) Make Payment (push payment)
SRC JavaScript SDK	N/A

9.2.1 SRC Payload Retrieval

The SRC Initiator can use a Get Payload operation to request information from the SRC System to enable payment.

Initiating a Get Payload operation communicates the following to the SRC System:

- Reference identifiers, as necessary, related to the specific transaction, the entities making use of the `Payload`, or others
- Parameters indicating the level of information that the SRC System should return

On processing a Get Payload operation, the SRC System responds to the SRC Initiator including information to:

- Enable payment authorisation (that is, the `Payload`)
- Facilitate risk management, reporting and auditing of the payment (e.g. masked Consumer and card data, shipping information, event and assurance data and possibly SRC System specific data)

9.2.2 Payment Confirmation

The SRC Initiator can use a Payment Confirmation operation to provide confirmation to the SRC System of the outcome of a payment authorisation. The confirmation relays whether the payment authorisation was a:

- Success
- Failure
- Time out

9.2.3 Make Payment

The SRC System can use a Make Payment operation to send payload information for authorisation purposes directly to a payment SRC Initiator.

10 Non-Payment Functions

In addition to Checkout (Section 8 Checkout) and Payment Enablement (Section 9 Payment Enablement), SRC facilitates three non-payment events. These non-payment events do not require the generation of a full `Payload` (one that includes a `Card` or `PaymentToken`) nor do they directly result in a payment authorisation.

10.1 SRC Profile Retrieval

SRC Profile retrieval allows the SRC Initiator to retrieve SRC Profile information outside the context of checkout. For details, refer to Section 8.3.1 SRC Profile Retrieval.

10.2 Checkout Completion

On successful completion of checkout initiation, the SRC Initiator may retrieve an SRC Payload from the SRC System. In the case of a non-payment SRC Initiator, this `Payload` does not include a `Card` or `PaymentToken` and enables:

- Presentment of a receipt and confirmation to the Consumer for the purposes of checkout completion
- Back-office operations such as order fulfilment and Customer support operations, loyalty management, etc.

For details, refer to Section 8.3.2 Checkout Initiation.

10.3 Non-Payment SRC Payload Retrieval

The SRC Initiator (referred to as a non-payment SRC Initiator), or its underlying Digital Payment Application, may require information contained in the `Payload` but not for payment authorisation purposes. This supports scenarios where a Digital Payment Application has both a payment and non-payment SRC Initiator as described in Section 3.3 SRC Initiator.

10.4 Authentication Facilitation

Authentication facilitation enables the SRC Initiator to use on behalf of services provided by the SRC System for identity and strong Cardholder authentication. For a full list of services available, please see the SRC API.

10.5 Management Service

The Management Service allows an SRC System to provide various management functions to its participants:

- The DPA Registration operation allows an SRC Initiator to register a Digital Payment Application with the SRC System

10.6 Notification

The SRC System can use notification serves to send messages to subscribers when specific events occur. A list of events can be found in Table 11.10.

11 Integration with SRC Systems

The SRC Specifications currently describe and support the following integrations with the SRC System:

- API integration (Section 11.1)
- SDK integration (Section 11.2)

These integrations primarily enable SRC Initiators to carry out SRC checkout and merchant checkout operations for their Digital Payment Applications. In addition, the APIs are available to SRC Participating Issuers and Digital Card Facilitators to perform card, Cardholder, Consumer, and device-related operations.

The SRC Specifications do not prescribe, exclude, or limit individual SRC Systems from providing integration solutions of their choice. The methods by which an SRC Initiator integrates can vary by use case and by the integration solutions provided by an SRC System.

SDK and API integrations can co-exist with each other, depending on the implementation, and when both are used, provide flexibility to SRC System Participants to achieve expected outcomes.

Note: The SRC API and SRC JavaScript SDK may contain deprecated content as data elements, API services and SDK methods. The deprecated content is explicitly marked within the specifications. In these cases, relevant content for this Specification will be deprecated as well. For further information on the deprecation process, refer to the SRC Version Management document.

11.1 SRC API Integration

The SRC API contains server-based APIs which can be used to build interfaces between SRC Systems and SRC System Participants. It enables SRC System Participants to perform individual checkout and payment events. In this integration, the SRC System Participant may integrate with one or more SRC APIs supported by the respective SRC System.

11.1.1 SRC API Operations

The SRC System supports the services and operations described by the SRC API based on its supported use cases. This enables the exchange of data between SRC Systems and SRC System Participants. That is:

- The APIs are server-based
- They are agnostic of the use case that implementations will use them for

- They do not preclude SRC Systems from providing additional technical components to support their implementations
- Multiple levels of data element optionality are offered and, depending on use cases, may be supported by SRC Systems and usable by SRC System Participants (e.g. to enhance security)

The SRC API defines operations which are grouped by service as follows.

Card Service

Card Service supports Payment Card digitisation. It covers the operations shown in Table 11.1.

Table 11.1: SRC API Card Service Operations

Operation	Description
Card Enrolment	Enrols a Consumer and Digital Card (associated with an underlying PAN) to a new SRC Profile, or adds a Digital Card to an existing SRC Profile.
Delete Card	Deletes a Digital Card from an SRC Profile.
Add Billing Address	Adds a billing address to an SRC Profile.
Get Card Data	Allows an SRC Participant to retrieve a Digital Card and related masked card data.

Address Service

Address Service enables the management of shipping addresses. It covers the operations shown in Table 11.2.

Table 11.2: SRC API Address Service Operations

Operation	Description
Add Shipping Address	Adds a shipping address to an SRC Profile.
Delete Shipping Address	Deletes a shipping address from an SRC Profile.

SRC Profile Service

SRC Profile Service enables SRC System Participants to retrieve SRC Profiles from SRC Systems and manage binding of identities to SRC Profiles. It covers the operations shown in Table 11.3.

Table 11.3: SRC API SRC Profile Service Operations

Operation	Description
Prepare SRC Profile	Requests that an SRC System prepare one or more SRC Profile(s) to be returned.
Add Consumer Identities	Binds a Device Identity (an application instance) or Consumer Identity to an SRC Profile.
Unbind App Instance	Unbinds a Device Identity (an application instance) from an SRC Profile.

Checkout Service

Checkout Service provides Payment Data and payment related data for a specific checkout. It covers the operations shown in Table 11.4.

Table 11.4: SRC API Checkout Service Operations

Operation	Description
Checkout	Utilises the Consumer's chosen Digital Card and details of the current transaction to receive Payment Data and payment related data.
Get Payload	Returns Payment Data and payment related data to be used in payment authorisation.
Make Payment	Sends Payment Data and payment related data to be used in payment authorisation purpose to the payment SRC Initiator.

Confirmation Service

Confirmation Service enables SRC Participants to notify the SRC System of the checkout or payment authorisation results. It covers the single operation shown in Table 11.5.

Table 11.5: SRC API Confirmation Service Operations

Operation	Description
Confirmation	Enables SRC Participants to provide a notification of the result of a checkout service (checkout or payment authorisation).

Identity Service

Identity Service enables operations related to identity recognition, validation of identity and the generation of Federated ID Tokens. It covers the operations shown in Table 11.6.

Table 11.6: SRC API Identity Service Operations

Operation	Description
Identity Lookup	Utilises a provided Consumer Identity (email address or mobile phone number) to determine whether it is associated with an SRC Profile.
Initiate Identity Validation	Initiates a process to validate that a Consumer is in possession of, or has access to, the Consumer Identity claimed.
Complete Identity Validation	Determines whether data, provided by the Consumer as part of a second step of an identity validation process, is valid. It can also be used to check whether an out-of-band service was successful.
Is Recognized	Uses a Device Identity (derived from a First Party Token) to determine whether it is bound to an SRC Profile and, if so, returns a Federated ID Token.

Public Keys Retrieval Service

Public Keys Retrieval Service enables retrieval of cryptographic public keys from a well-known URL hosted by an SRC System. The keys retrieved are used by other SRC Participants for Federated ID Token and JWS signature verification. It covers the single operation shown in Table 11.7.

Table 11.7: SRC API Public Keys Retrieval Service Operations

Operation	Description
Public Key Retrieval	Retrieves a set of public keys.

Authentication Facilitation Service

Authentication Facilitation Service facilitates methods for identity and strong Cardholder authentication. It covers the operations shown in Table 11.8.

Table 11.8: SRC API Authentication Facilitation Operations

Operation	Description
Authentication Methods Lookup	Returns a list of methods that are relevant to the criteria specified by the client.
Authenticate	Initiates and completes an authentication based on specific input criteria. This API may be called multiple times depending on the authentication method.

Management Service

Management Service facilitates methods for registering SRC Participants It covers the operations shown in Table 11.10.

Table 11.9: SRC API Management Service Operations

Operation	Description
DPA Registration	After successful registration, the `srcDpaId` returned by SRC System can be used by SRC Initiator in future operations

Notification Service

Notification Service enables outbound messages sent by the SRC System when specific events occur. It covers the operations shown in Table 11.10.

Table 11.10: SRC API Notification Service Operations

Operation	Description
Card Update Event Notification	Sends a message to subscribers when a Digital Card's information has been modified or updated.

Operation	Description
Identity Validation Completion Event Notification	Sends a message to subscribers when an SRC System determines, or is itself notified, that an out-of-band identity validation service has completed.
Authentication Event Notification	Sends a message to subscribers when an authentication event is completed.
Payment Notification	Sends a message to subscribers when an SRC System has received a confirmation of authorisation.

11.2 SRC JavaScript SDK Integration

The SRC JavaScript SDK is intended to create seamless SRC checkout functions within a Digital Payment Application. When an SRC Initiator integrates with more than one SRC System, it provides integration software to their Digital Payment Applications which is an aggregation of the SRC JavaScript SDK(s) provided by each SRC System. This SRC Initiator integration software facilitates SRC checkout interactions for Cardholder-Initiated Transactions within each Digital Payment Application.

The key components of the integration software for an SRC checkout include:

- Integration of multiple SRC JavaScript SDKs provided by each SRC System supported by the SRC Initiator
- One SRC Trigger rendered by the SRC Initiator for all of the SRC System integrations combined (see Section 8.2 SRC Trigger)

The user experience and underlying functionality of the SRC Initiator integration software allows:

- Remembered, recognised and unrecognised experiences through identity recognition and identity binding
- Management of Federated Identity between SRC Systems to facilitate identity recognition
- Identified Consumers to access their SRC Profiles at one or more SRC System(s)
- Ability for Consumers to enrol and/or manage Digital Cards
- Selection of Digital Card and Cardholder data that enables the purchase to complete
- Return of the SRC Payload

11.2.1 SRC JavaScript SDK Methods

The SRC JavaScript SDK describes one example for an SDK provided by an SRC System which can be aggregated within SRC Initiator integration software. The SRC JavaScript SDK is specifically tailored to support the Consumer-initiated checkout use case in the merchant e-commerce environment via the web channel (browser). The SDK can utilise server-based SRC APIs or SRC System proprietary APIs to interface with the respective SRC System.

The SRC JavaScript SDK is comprised of the methods shown in Table 11.11.

Table 11.11: SRC JavaScript SDK Methods

Method	Description
init()	Initialises each SRC System's SDK in a common state.
isRecognized()	Uses a Device Identity (derived from a First Party Token) to determine whether it is bound to an SRC Profile and, if so, returns a Federated ID Token.
getSrcProfile()	Takes a list of Federated ID Tokens and returns SRC Profile data to enable card selection.
identityLookup()	Uses a provided Consumer Identity (email address or mobile phone number) to determine whether it is associated with an SRC Profile.
initiateIdentityValidation()	Initiate a process to validate that the Consumer is in possession of, or has access to, the Consumer Identity claimed.
completeIdentityValidation()	Determines whether data, provided by the Consumer as part of a second step of an identity validation process, is valid. It can also be used to check whether an out-of-band service was successful.
enrollCard()	Enrols a new PAN to the SRC System during checkout.
checkout()	Performs checkout using the specified Digital Card or PAN.
deleteCard()	Deletes a Digital Card from an SRC Profile.
unbindAppInstance()	Unbinds a Device Identity from an SRC Profile.
addBillingAddress()	Adds or updates the billing address for a given Digital Card.

Method	Description
authenticationMethods Lookup()	Obtains a proposed list of authentication methods relevant to the criteria specified by the client.
authenticate()	Initiates and completes an authentication based on specified input criteria.

12 SRC Security Considerations

SRC enhances the security of online payment transactions and privacy of personal Consumer data by protecting PII and Payment Data.

The principle means to achieve protection of the vulnerabilities are:

- Payment Data and PII are substituted with reference information that cannot be directly used for payment authorisation, thereby minimising the exposure of Payment Data and the level of additional protection required
- Protection of personal Consumer data and Payment Card through the use of encryption and/or masking
- The use of protected links using industry standard negotiable security protocols for communication between the SRC System and the SRC Participants. The baseline security mechanism for this connection is Transport Layer Security (TLS)
- Support the use of Dynamic Data for the validation and protection of transaction data submitted in the existing authorisation message data field(s). Each Digital Payment Application indicates the types of Dynamic Data supported by its payment authorisation environment (note that support for no Dynamic Data is a valid indicator). It is the responsibility of the SRC System to define the requirements for the generation and validation related to the supported types of Dynamic Data. An SRC Programme provides documentation detailing the mapping requirement for types of Dynamic Data to the authorisation messages established by the Payment Networks
- Support the ability to use and integrate SRC with other EMV technologies such as EMV 3-D Secure Authentication and Payment Tokenisation
- SRC System controls to mitigate against enumeration risks, bot attacks and denial of service attacks

Annex A Security Guidelines

This Annex describes the security credentials that are established during Onboarding and guidance for the usage of TLS.

A.1 Security Credentials

Security credentials are assigned to SRC Participants by the SRC System during Onboarding.

The SRC Specifications assume a baseline of TLS. The TLS credentials may be augmented by implementation-specific security credentials. Table A.1 lists the security credentials used for TLS connections. Details of certificate chains, identifiers, and other certificate attributes are not described in the table since they are SRC System implementation-specific.

Table A.1: SRC Security Credentials for TLS

Security Credential	Type	Description
SRC System Server Certificate (for server to server)	Public Key Certificate	SRC System certificate signed by the certificate authority supporting the SRC System. Used for mutually authenticated TLS connections between servers initiated by the SRC Participant.
SRC System Client Certificate (for server to server)	Public Key Certificate	SRC System certificate signed by the certificate authority supporting the SRC System. Used for mutually authenticated TLS connections between servers initiated by the SRC System.
SRC System Server Certificate (for browser)	Public Key Certificate	SRC System certificate signed by a commercial certificate authority. Used for server authenticated TLS connections to browsers.
SRC Participant Client Certificate (for server to server)	Public Key Certificate	SRC Participant certificate signed by the certificate authority supporting the SRC System. Used for mutual authenticated TLS connections between servers initiated by the SRC Participant. Generated during Onboarding by certificate authority supporting the SRC System for the SRC Participant.

Security Credential	Type	Description
SRC Participant Server Certificate (for server to server)	Public Key Certificate	SRC Participant certificate signed by the certificate authority supporting the SRC System. Used for mutual authenticated TLS connections between servers initiated by the SRC System. Generated during Onboarding by certificate authority supporting the SRC System for the SRC Participant.
Certificate Authority supporting the SRC System Root Public Key	Public Key	Root public key used for mutual authenticated TLS connections. Provided to SRC System Participants by the SRC System.

Table A.2 lists the security credentials used for the signing or encryption functions described within the SRC Specifications. Details of certificate chains, identifiers, and other certificate attributes are not described in the table since they are SRC System implementation-specific. Algorithms for JWE according to RFC 7518 section 4.1. Algorithms for JWS according to RFC 7518 section 3.1 for JWS.

- 'None' is not supported
- PS256 is preferred to RS256 following the recommendation in RFC 3447

Table A.2: SRC Security Credentials for Signing or Encryption Functions

Security Credential	Type	Description
SRC Participant Encryption Key	Encryption Key	The key used for JWE encryption of the Payload. Issued by the SRC Participants to the SRC System during Onboarding. May be a public key or a symmetric key.
SRC System Encryption Key	Encryption Key	The key used for JWE encryption of card data from SRCI to SRC System. Issued by the SRC System to SRC System Participants. This is a public key.
SRC System Authentication Key	Authentication Key	The key used for JWS signatures or MACs created by the SRC System. Issued by the SRC System to SRC System Participants. May be a public key or a symmetric key.

Security Credential	Type	Description
ID Token Authentication Key	Authentication Key	The key used for verification of JWS signatures of Federated ID Tokens. Shared between SRC Systems for use in federated identity. This is a public key.

A.2 Approved TLS Versions

For establishing the links secured by TLS between the SRC System, SRC Initiators, Digital Card Facilitators and SRC Participating Issuers, the following apply.

- TLS version number: V1.2 or higher
- RSA keys: 2048 bits or longer
- ECC keys: 256 bits or longer

A.3 Supported Cipher Suites

Requirements and recommendations for the supported cipher suites are as follows:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

Curve P-256 is to be used and indicated in the cipher suite extension.

The Certificate Authority supporting the SRC System provides client and server certificates.

A.4 Other Cipher Suites

If required for any other reason, additional cipher suites can be supported. Interoperability is the responsibility of the SRC Programme.

A.5 Cipher Suites Not Supported

The following cipher suites are not to be presented or accepted:

- Any cipher suite represented as ‘Null’, ‘Anonymous/Anon’
- Any cipher suite incorporating any of the algorithms ‘RC2’, ‘RC4’, ‘DES’, ‘IDEA’, KRB5’, ‘ARIA’, or ‘MD5’
- Any cipher suite incorporating an export grade algorithm using ‘EXPORT’

- Note: 3DES and SHA-1 are to be phased out and may become unsupported algorithms in future versions of this Specification.

Annex B Data Obfuscation

This Annex describes the rules and best practices for obfuscating data in SRC.

To enforce consistency in masking logic the special character (asterisk) * is used for masking the obfuscated characters being presented.

B.1 Rules for Masked Email Address

Masking only applies to the identifiable username portion of the email address which is before the '@' sign. The domain name portion will always be shown unmasked. When masking, use a constant hash of five characters (*****) at all times to obfuscate the length of the username portion.

If the length of the username portion is seven characters or more, then the first and last character of the username is unmasked and separated by the constant hash. Some examples are:

- johndoe@example.com would be masked as j*****e@example.com
- srcuser12@example.com would be masked as s*****2@example.com
- other.email-with-hyphen@example.com would be masked as o*****n@example.com

If the length of the username portion is six characters or less, then the first character would be unmasked followed by the constant five character hash. Some examples are:

- abcdef@example.com, abcd@example.com, ab@example.com and a@example.com would all be masked as a*****@example.com

B.2 Rules for Masked Phone Numbers

The '+' (indicating the country code), the country code and the trailing three digits are always unmasked. For the remaining digits, these should all be masked except where local recommendations or common practices suggest an alternative masking pattern. Some examples are:

- 1 555 555 0156 would be masked as +1*******156
- 36 55 626 211 would be masked as +36*****211

B.3 Best Practices for Masked Addresses

Masking applies to each of the identifiable fields (or individual words within the field) of the address. This applies to first name, last name, street address line(s), postal code and city. It may also apply to state, province, etc. It does not apply to countries which, will always be shown in clear. When masking, use a constant hash of five characters (*****) at all times to obfuscate the length of the identifiable field/word.

- If the field/word length is seven characters or more, then the first and last character of the field/word is unmasked and separated by the constant hash.
- If the field/word length is six characters or less, then the first character of the field/word would be unmasked followed by the constant hash.
- Any formatting, spaces and special characters (for example, '-', ',' and ' ') are not masked.

Some examples are given in Table B.1.

Table B.1: Examples of Masked Addresses

Unmasked	Masked
Rebecca Schumer 123 Main St Apt 3A Brooklyn, NY 11218 United States of America	R*****a S*****r 1***** M***** S***** A***** 3***** B*****n, NY 1***** United States of America
John Doe 1004 NW 65th Ave Miami FL 33126 USA	J***** D***** 1***** N***** 6***** A***** M***** FL 3***** USA

B.4 Best Practices for Masked PANs

Data used in the presentation of the PAN is created in such a way as to ensure that the masked PAN contains no more than either the first six and last four digits of the PAN or no more than 10 consecutive numeric values of the PAN.

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