



**EMV®**

# **Secure Remote Commerce**

---

## **Specification – API**

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 1.2:

- Minor editorial changes throughout the document, with sections and tables renumbered where necessary
- Edits to account for the deprecation of the SRC Data Dictionary
- Section 2.1 Complex Data Objects has been reorganised so that it is in alphabetical order, with the following complex data objects added:
  - AccountReference (Section 2.1.3)
  - AuthenticationContext (Section 2.1.8)
  - AuthenticationMethod (Section 2.1.9)
  - BusinessIdentification (Section 2.1.10)
  - ComplianceResource (Section 2.1.14)
  - RecognitionData (Section 2.1.43)
  - UriData (Section 2.1.47)
- Section 2.1 Complex Data Objects, the following has been deprecated:
  - Consent (Section 2.1.18)
- Section 2.1 Complex Data Objects, the following have been modified:
  - Address (Section 2.1.5): updated description to data element state
  - AssuranceData (Section 2.1.7): new data element eci added
  - ComplianceSettings (Section 2.1.15): individual data elements replaced with a list of ComplianceResources
  - DigitalCardData (Section 2.1.24): new data element authenticationMethods added
  - DpaData (Section 2.1.27): dpaUri made conditional (from optional) and seven new data elements (merchantCountryCode, businessId, merchantName, merchantCategoryCode, acquirerId, acquirerBin, dpaPanDataRequested) added
  - DpaTransactionOptions (Section 2.1.28): two new data elements (cardholderNameRequested, consumerNationalIdentifierRequested) added
  - MaskedAddress (Section 2.1.35): updated description to data element state

- MaskedCard (Section 2.1.36): four new data elements (`enrollmentReferenceData`, `cofEligible`, `maskedCardholderFullName`, `maskedCardholderFirstName`, `maskedCardholderLastName`, `complianceSettings`) added
- MaskedConsumer (Section 2.1.37): new data element `pendingEvents` added
- Payload (Section 2.1.39): new data element `consumerNationalIdentifier` added
- VerificationData (Section 2.1.46): new data element `methodResults` added
- Section 2.2 Individual Attributes has been deleted. Following the introduction of the new table structure for the individual APIs in version 1.2, descriptions for individual data elements are included within the APIs themselves. Therefore Section 2.2 is no longer required, since the information can be found elsewhere.
- Section 2.2 JSON Attributes has been added to describe the attributes of specific JSON objects
- Section 2.3 Enumerations, the following have been added or modified:
  - Action
  - AuthenticationReason
  - AuthenticationMethodType
  - AuthenticationSubject
  - AuthenticationStatus
  - AuthenticationResult
  - BindingStatus
  - CardPendingEvent: the PENDING\_SCA value has been deprecated and replaced with the PENDING\_CARDHOLDER\_AUTHENTICATION value and the PENDING\_CSC value has been added
  - ComplianceType: the ComplianceType enumeration replaces the individual data elements within the complex data object ComplianceSettings (Section 2.1.15), with the addition of REMEMBER\_ME, which supersedes the `cookie` data element in ComplianceSettings
  - ConsumerPendingEvent
  - DcfActionCode: the PENDING\_AUTHENTICATION value has been added
  - EnrollmentReferenceType: the COF\_REFERENCE\_ID value has been added
  - UriType
- Section 3.1.2 Token Claims, an additional value `merchant_rememberme` has been added to the amr claim

- Section 5.1 API Principles, the following subsections have been added:
  - Section 5.1.5.1 Recognition Token JWT
  - Section 5.1.7 API Tables
- Section 5 Server-Side API (Sections 5.2 to 5.11) and Section 6 Notification Service (Sections 6.2 to 6.5), each API has had the existing table structure replaced, where applicable, with individual tables for:
  - HTTP Verb, Path and Parameters
  - Query Parameters
  - Request Body
  - Response Body
  - HTTP Status Codes
- Section 5 Server-Side API, the following Services and their APIs have been added:
  - Authentication Facilitation Service (Section 5.8)
  - Retrieve Latest Compliance Resources Service (Section 5.10)
  - Management Service (Section 5.11)
- Section 5 Server-Side API, the following Services and their APIs have been changed:
  - Card Enrolment Response Body (Section 5.2.1) `appInstanceId` deprecated and replaced by `recognitionToken`
  - Add Consumer Identities Request Body (Section 5.4.2) `encryptedConsumer` added
  - Add Consumer Identities Response Body (Section 5.4.2) `appInstanceId` deprecated and replaced by `recognitionToken`
  - Unbind App Instance Query Parameters (Section 5.4.3) `appInstanceId` deprecated and replaced by `recognitionToken`
  - Confirmation Request Body (Section 5.6.1) `assuranceData` deprecated
  - Identity Lookup Body (Section 5.7.1) `lastUsedCardTimestamp` added
  - Initiate Identity Validation Response Body (Section 5.7.2) `authenticationAppUri` added
  - Complete Identity Validation Response Body (Section 5.7.3) `maskedCard` added
  - Is Recognized Query Parameters (Section 5.7.4) `appInstanceId` deprecated and replaced by `recognitionTokens`
  - Is Recognized Response Body (Section 5.7.4) `appInstanceId` deprecated and replaced by `recognitionToken`, `recognitionDomainName` added
- Section 6 Notification Service, the following Services and their APIs have been added:

- Authentication Event Notification (Section 6.4)
- The following Annex has been added:
  - Annex B 3DS Data

# Contents

<b>Legal Notice .....</b>	i
<b>Revision Log – Version 1.3.....</b>	ii
<b>Contents .....</b>	vi
<b>Tables .....</b>	x
<b>1 Introduction .....</b>	1
1.1 Scope .....	1
1.2 Constraints .....	1
1.3 Audience .....	1
1.4 References .....	2
1.4.1 Normative References .....	2
1.4.2 Published EMVCo Documents .....	2
1.5 Definitions.....	3
1.6 Notational Conventions.....	4
1.6.1 Abbreviations .....	4
1.6.2 Terminology and Conventions.....	4
<b>2 Data Dictionary.....</b>	5
2.1 Complex Data Objects.....	5
2.1.1 AcceptanceChannelData .....	5
2.1.2 AcceptanceChannelRelatedData .....	6
2.1.3 AccountReference .....	6
2.1.4 AdditionalAmount.....	7
2.1.5 Address .....	7
2.1.6 AppInstance.....	9
2.1.7 AssuranceData .....	10
2.1.8 AuthenticationContext.....	17
2.1.9 AuthenticationMethod .....	18
2.1.10 BusinessIdentification .....	19
2.1.11 Card.....	20
2.1.12 CardholderData .....	21
2.1.13 CommunicationsConsent.....	22
2.1.14 ComplianceResource.....	23
2.1.15 ComplianceSettings .....	23
2.1.16 ConfirmationData DEPRECATED .....	24
2.1.17 ConfirmationData2 .....	26
2.1.18 Consent DEPRECATED .....	28
2.1.19 Consumer .....	29

2.1.20 ConsumerIdentity.....	30
2.1.21 Dcf .....	30
2.1.22 DeliveryContactDetails.....	31
2.1.23 DeviceData .....	32
2.1.24 DigitalCardData .....	32
2.1.25 DigitalCardFeature.....	34
2.1.26 DigitalCardUpdateNotification .....	34
2.1.27 DpaData .....	35
2.1.28 DpaTransactionOptions .....	38
2.1.29 DynamicData .....	41
2.1.30 EnrollmentReferenceData.....	42
2.1.31 Error.....	42
2.1.32 ErrorDetail.....	43
2.1.33 EventHistory .....	43
2.1.34 IdentityValidationChannel .....	44
2.1.35 MaskedAddress .....	45
2.1.36 MaskedCard .....	46
2.1.37 MaskedConsumer.....	50
2.1.38 MaskedConsumerIdentity .....	52
2.1.39 Payload.....	53
2.1.40 PaymentOptions .....	59
2.1.41 PaymentToken.....	59
2.1.42 PhoneNumber.....	60
2.1.43 RecognitionData .....	60
2.1.44 SrcProfile .....	61
2.1.45 TransactionAmount.....	62
2.1.46 VerificationData .....	63
2.1.47 UriData .....	69
2.2 JSON Attributes.....	69
2.2.1 Authentication Facilitation .....	69
2.3 Enumerations .....	72
2.4 Signed Checkout Objects .....	76
2.4.1 Checkout Request JWS .....	76
2.4.2 Checkout Payload Response.....	79
2.4.3 JWS JOSE Header .....	83
2.5 Masking Rule.....	84
<b>3 Federated Identity .....</b>	<b>85</b>
3.1 Authorisation Token.....	85
3.1.1 Token Header .....	85
3.1.2 Token Claims.....	86

3.1.3 Notes on Authentication .....	90
<b>4 SRCI – DCF Interaction .....</b>	<b>92</b>
4.1 Interaction Mechanisms.....	92
4.2 Launch The DCF .....	93
4.3 Redirect back to SRCI .....	93
<b>5 Server-Side API .....</b>	<b>96</b>
5.1 API Principles .....	96
5.1.1 Common HTTP Status Codes.....	96
5.1.2 Error Handling.....	97
5.1.3 Conditionality of Data.....	97
5.1.4 Authorisation.....	97
5.1.5 Recognition.....	97
5.1.6 API Access Control.....	99
5.1.7 API Tables .....	99
5.2 Card Service.....	99
5.2.1 Card Enrolment.....	99
5.2.2 Delete Card.....	103
5.2.3 Add Billing Address.....	105
5.2.4 Get Card Data.....	107
5.3 Address Service .....	108
5.3.1 Add Shipping Address .....	108
5.3.2 Delete Shipping Address.....	110
5.4 SRC Profile Service .....	111
5.4.1 Prepare SRC Profile .....	111
5.4.2 Add Consumer Identities.....	114
5.4.3 Unbind App Instance.....	117
5.5 Checkout Service .....	118
5.5.1 Prepare Checkout Data.....	118
5.5.2 Checkout .....	121
5.5.3 Get Payload.....	126
5.5.4 Make Payment.....	128
5.6 Confirmation Service .....	129
5.6.1 Confirmation .....	129
5.7 Identity Service.....	131
5.7.1 Identity Lookup .....	131
5.7.2 Initiate Identity Validation .....	132
5.7.3 Complete Identity Validation .....	134

5.7.4 Is Recognized .....	136
5.8 Authentication Facilitation Service .....	138
5.8.1 Authentication Methods Lookup .....	138
5.8.2 Authenticate.....	140
5.9 Public Keys Retrieval Service .....	142
5.9.1 Public Key Retrieval.....	143
5.10 Retrieve Latest Compliance Resources Service .....	144
5.10.1 Latest Compliance Resources Retrieval .....	145
5.11 Management Service.....	146
5.11.1 DPA Registration .....	146
<b>6 Notification Service.....</b>	<b>148</b>
6.1 Notifications Principles.....	148
6.1.1 Data Delivery Modes.....	148
6.1.2 Standard HTTP Status Codes.....	148
6.2 Card Update Event Notification.....	149
6.3 Identity Validation Completion Event Notification.....	150
6.4 Authentication Event Notification .....	153
6.5 Payment Notification.....	154
<b>Annex A EMVCo Specification Mapping.....</b>	<b>156</b>
A.1 Merchant-Presented Mode – QR Code Payload.....	156
A.1.1 SRC Data Elements .....	156
A.1.2 QR Code specific Data Elements for Seller Data .....	157
A.1.3 QR Code specific Data Elements for Consumer Data.....	158
A.1.4 QR Code Specific Data Elements for Additional Amounts .....	162
<b>Annex B 3DS Data.....</b>	<b>165</b>
B.1 3DS Input Data.....	165
B.2 3DS Output Data .....	166

## Tables

Table 1.1: Normative References.....	2
Table 1.2: EMVCo References.....	2
Table 2.1: AcceptanceChannelData.....	5
Table 2.2: AcceptanceChannelRelatedData.....	6
Table 2.3: AccountReference.....	6
Table 2.4: AdditionalAmount .....	7
Table 2.5: Address.....	7
Table 2.6: ApplInstance .....	9
Table 2.7: AssuranceData.....	10
Table 2.8: AuthenticationContext .....	17
Table 2.9: AuthenticationMethod.....	18
Table 2.10: BusinessIdentification.....	19
Table 2.11: Card .....	20
Table 2.12: CardholderData .....	21
Table 2.13: CommunicationsConsent .....	22
Table 2.14: ComplianceResource .....	23
Table 2.15: ComplianceSettings .....	23
Table 2.16: ConfirmationData DEPRECATED .....	24
Table 2.17: ConfirmationData2 .....	26
Table 2.18: Consent DEPRECATED.....	28
Table 2.19: Consumer.....	29
Table 2.20: ConsumerIdentity .....	30
Table 2.21: Dcf.....	30
Table 2.22: DeliveryContactDetails .....	31
Table 2.23: DeviceData.....	32
Table 2.24: DigitalCardData .....	32
Table 2.25: DigitalCardFeature .....	34
Table 2.26: DigitalCardUpdateNotification.....	34
Table 2.27: DpaData .....	35
Table 2.28: DpaTransactionOptions .....	38
Table 2.29: DynamicData.....	41
Table 2.30: EnrollmentReferenceData .....	42
Table 2.31: Error .....	42
Table 2.32: ErrorDetail .....	43
Table 2.33: EventHistory .....	43
Table 2.34: IdentityValidationChannel .....	44
Table 2.35: MaskedAddress.....	45
Table 2.36: MaskedCard.....	46
Table 2.37: MaskedConsumer .....	50
Table 2.38: MaskedConsumerIdentity .....	52

Table 2.39: Payload .....	53
Table 2.40: PaymentOptions.....	59
Table 2.41: PaymentToken .....	59
Table 2.42: PhoneNumber .....	60
Table 2.43: RecognitionData.....	60
Table 2.44: SrcProfile.....	61
Table 2.45: TransactionAmount .....	62
Table 2.46: VerificationData .....	63
Table 2.47: VerificationData Values .....	64
Table 2.48: UriData .....	69
Table 2.49: JSON Attributes for CSC_VALIDATION .....	70
Table 2.50: JSON Attributes for SMS OTP, EMAIL OTP, APP OTP.....	70
Table 2.51: JSON Attributes for ADDRESS_VERIFICATION.....	70
Table 2.52: JSON Attributes for SPC (Authenticate response).....	71
Table 2.53: JSON Attributes for SPC (Authenticate request).....	71
Table 2.54: JSON Attributes for 3DS.....	71
Table 2.55: JSON Attributes for Consumer Authentication.....	72
Table 2.56: Enumerations .....	72
Table 2.57: Checkout Request JOSE Header .....	76
Table 2.58: Checkout Request Claim Set.....	77
Table 2.59: Checkout Payload Response .....	79
Table 2.60: JWS JOSE Header.....	83
Table 3.1: JOSE Header .....	85
Table 3.2: Federated ID Token Claim Set .....	86
Table 4.1: Error Codes.....	94
Table 5.1: Recognition Token Claim Set .....	98
Table 5.2.1: Card Enrolment Definition – HTTP Verb, Path and Parameters.....	100
Table 5.2.2: Card Enrolment Definition – Request Body .....	100
Table 5.2.3: Card Enrolment Definition – Response Body.....	102
Table 5.2.4: Card Enrolment Definition – HTTP Status Codes .....	103
Table 5.2.5: Delete Card Definition – HTTP Verb, Path and Parameters.....	103
Table 5.2.6: Delete Card Definition – Query Parameters.....	103
Table 5.2.7: Delete Card Definition – Response Body.....	104
Table 5.2.8: Delete Card Definition – HTTP Status Codes .....	104
Table 5.2.9: Add Billing Address Definition – HTTP Verb, Path and Parameters...	105
Table 5.2.10: Add Billing Address Definition – Request Body.....	105
Table 5.2.11: Add Billing Address Definition – Response Body.....	106
Table 5.2.12: Add Billing Address Definition – HTTP Status Codes .....	106
Table 5.2.13: Get Card Data Definition – HTTP Verb, Path and Parameters.....	107
Table 5.2.14: Get Card Data Definition – Query Parameters.....	107
Table 5.2.15: Get Card Data Definition – Response Body.....	108
Table 5.2.16: Get Card Data Definition – HTTP Status Codes .....	108

Table 5.3.1: Add Shipping Address Definition – HTTP Verb, Path and Parameters	108
Table 5.3.2: Add Shipping Address Definition – Request Body .....	109
Table 5.3.3: Add Shipping Address Definition – Response Body .....	109
Table 5.3.4: Add Shipping Address Definition – HTTP Status Codes .....	110
Table 5.3.5: Delete Shipping Address Definition – HTTP Verb, Path and Parameters	110
Table 5.3.6: Delete Shipping Address Definition – Query Parameters.....	110
Table 5.3.7: Delete Shipping Address Definition – Response Body.....	111
Table 5.3.8: Delete Shipping Address Definition – HTTP Status Codes .....	111
Table 5.4.1: Prepare SRC Profile Definition – HTTP Verb, Path and Parameters .	112
Table 5.4.2: Prepare SRC Profile Definition – Request Body .....	112
Table 5.4.3: Prepare SRC Profile Definition – Response Body .....	113
Table 5.4.4: Prepare SRC Profile Definition – HTTP Status Codes .....	114
Table 5.4.5: Add Consumer Identities Definition – HTTP Verb, Path and Parameters	114
Table 5.4.6: Add Consumer Identities Definition – Request Body.....	115
Table 5.4.7: Add Consumer Identities Definition – Response Body.....	116
Table 5.4.8: Add Consumer Identities Definition – HTTP Status Codes .....	116
Table 5.4.9: Unbind App Instance Definition – HTTP Verb, Path and Parameters.	117
Table 5.4.10: Unbind App Instance Definition – Query Parameters.....	117
Table 5.4.11: Unbind App Instance Definition – Response Body.....	118
Table 5.4.12: Unbind App Instance Definition – HTTP Status Codes .....	118
Table 5.5.1: Prepare Checkout Data Definition – HTTP Verb, Path and Parameters	119
Table 5.5.2: Prepare Checkout Data Definition – Request Body .....	119
Table 5.5.3: Prepare Checkout Data Definition – Response Body.....	121
Table 5.5.4: Prepare Checkout Data Definition – HTTP Status Codes .....	121
Table 5.5.5: Checkout Definition – HTTP Verb, Path and Parameters .....	122
Table 5.5.6: Checkout Definition – Request Body .....	122
Table 5.5.7: Checkout Definition – Request Body .....	123
Table 5.5.8: Checkout Definition – Response Body .....	125
Table 5.5.9: Checkout Definition – HTTP Status Codes .....	126
Table 5.5.10: Get Payload Definition – HTTP Verb, Path and Parameters .....	126
Table 5.5.11: Get Payload Definition – Query Parameters .....	126
Table 5.5.12: Get Payload Definition – Response Body .....	128
Table 5.5.13: Get Payload Definition – HTTP Status Codes.....	128
Table 5.5.14: Make Payment Definition – HTTP Verb, Path and Parameters.....	128
Table 5.5.15: Make Payment Definition – Request Body.....	128
Table 5.5.16: Make Payment Definition – HTTP Status Codes .....	129
Table 5.6.1: Confirmation Definition – HTTP Verb, Path and Parameters .....	129
Table 5.6.2: Confirmation Definition – Request Body .....	129
Table 5.6.3: Confirmation Definition – HTTP Status Codes .....	130
Table 5.7.1: Identity Lookup Definition – HTTP Verb, Path and Parameters .....	131
Table 5.7.2: Identity Lookup Definition – Request Body .....	131
Table 5.7.3: Identity Lookup Definition – Response Body .....	132

Table 5.7.4: Identity Lookup Definition – HTTP Status Codes .....	132
Table 5.7.5: Initiate Identity Validation Definition – HTTP Verb, Path and Parameters	133
Table 5.7.6: Initiate Identity Validation Definition – Request Body .....	133
Table 5.7.7: Initiate Identity Validation Definition – Response Body .....	133
Table 5.7.8: Initiate Identity Validation Definition – HTTP Status Codes.....	134
Table 5.7.9: Complete Identity Validation Definition – HTTP Verb, Path and Parameters	134
Table 5.7.10: Complete Identity Validation Definition – Request Body .....	135
Table 5.7.11: Complete Identity Validation Definition – Response Headers .....	135
Table 5.7.12: Complete Identity Validation Definition – Response Body .....	135
Table 5.7.13: Complete Identity Validation Definition – HTTP Status Codes .....	136
Table 5.7.14: Is Recognized Definition – HTTP Verb, Path and Parameters .....	136
Table 5.7.15: Is Recognized Definition – Query Parameters .....	136
Table 5.7.16: Is Recognized Definition – Response Body .....	137
Table 5.7.17: Is Recognized Definition – HTTP Status Codes.....	138
Table 5.8.1: Authentication Methods Lookup Definition – HTTP Verb, Path and Parameters .....	138
Table 5.8.2: Authentication Methods Lookup Definition – Request Body.....	139
Table 5.8.3: Authentication Methods Lookup Definition – Response Body .....	139
Table 5.8.4: Authentication Methods Lookup Definition – HTTP Status Codes ....	140
Table 5.8.5: Authenticate Definition – HTTP Verb, Path and Parameters.....	140
Table 5.8.6: Authenticate Definition – Request Body .....	140
Table 5.8.7: Authenticate Definition – Response Body.....	141
Table 5.8.8: Authenticate Definition – Response Headers .....	142
Table 5.8.9: Authenticate Definition – HTTP Status Codes .....	142
Table 5.9.1: Public Key Retrieval Definition – HTTP Verb, Path and Parameters..	143
Table 5.9.2: Public Key Retrieval Definition – Response Body.....	144
Table 5.9.3: Public Key Retrieval Definition – HTTP Status Codes .....	144
Table 5.10.1: Latest Compliance Resources Retrieval Definition – HTTP Verb, Path and Parameters .....	145
Table 5.10.2: Latest Compliance Resources Retrieval Definition – Request Body	145
Table 5.10.3: Latest Compliance Resources Retrieval Definition – Response Body	145
Table 5.10.4: Latest Compliance Resources Retrieval Definition – HTTP Status Codes	146
Table 5.11.1: DPA Registration Definition – HTTP Verb, Path and Parameters ...	146
Table 5.11.2: DPA Registration Definition – Request Body .....	146
Table 5.11.3: DPA Registration Definition – Response Body .....	147
Table 5.11.4: DPA Registration Definition – HTTP Status Codes.....	147
Table 6.1: Standard HTTP Status Codes .....	149
Table 6.2.1: Card Update Event Notification Definition – HTTP Verb, Path and Parameters .....	150
Table 6.2.2: Card Update Event Notification Definition – Request Body.....	150
Table 6.2.3: Card Update Event Notification Definition – HTTP Status Codes.....	150
Table 6.3.1: Identity Validation Completion Event Notification Definition – HTTP Verb, Path and Parameters .....	151

---

Table 6.3.2: Identity Validation Completion Event Notification Definition – Request Body	151
Table 6.3.3: Identity Validation Completion Event Notification Definition – HTTP Status Codes.....	151
Table 6.4.1: Authentication Event Notification Definition – HTTP Verb, Path and Parameters .....	153
Table 6.4.2: Authentication Completion Event Notification Definition – Request Body	153
Table 6.4.3: Authentication Completion Event Notification Definition – HTTP Status Codes .....	154
Table 6.5.1: Payment Notification Definition – HTTP Verb, Path and Parameters.	154
Table 6.5.2: Payment Notification Definition – Request Body.....	154
Table 6.5.3: Payment Notification Definition – HTTP Status Codes.....	155
Table A.1: SRC API Usage for QR Code Payload.....	158
Table A.2: SRC API Usage for Bill Number.....	158
Table A.3: SRC API Usage for Mobile Number .....	159
Table A.4: SRC API Usage for Store Label .....	159
Table A.5: SRC API Usage for Loyalty Number .....	159
Table A.6: SRC API Usage for Reference Label .....	160
Table A.7: SRC API Usage for Customer Label .....	160
Table A.8: SRC API Usage for Terminal Label.....	160
Table A.9: SRC API Usage for Purpose of Transaction.....	161
Table A.10: SRC API Usage for Email .....	161
Table A.11: SRC API Usage for Phone Number .....	162
Table A.12: SRC API Usage for Address .....	162
Table A.13: SRC API Usage for Tip .....	163
Table A.14: SRC API Usage for Convenience Fee .....	163
Table A.15: SRC API Usage for Sub Total .....	164
Table B.1: 3DS Input Data .....	165
Table B.2: 3DS Output Data.....	166

# 1 Introduction

Secure Remote Commerce (SRC) is an evolution of remote commerce that provides for secure and interoperable card acceptance established through a standard specification.

This document, the EMV® Secure Remote Commerce Specification – API, (hereafter the “SRC API Specification”), contains server-based APIs which can be used to securely build interfaces between SRC Systems and SRC System Participants. It is intended to be used in conjunction with the SRC Specifications (see Section 1.4.2 Published EMVCo Documents).

## 1.1 Scope

The SRC API Specification describes APIs to be used for the transmission of data between SRC Systems and SRC System Participants. These APIs are based on the following assumptions:

- The server-based APIs provide a toolkit for SRC System Participants
- They are not intended to provide context for all scenarios or use cases, and individual SRC Systems are responsible for creating implementation instructions for their SRC System Participants
- They do not preclude an SRC System from providing additional technical components to support their implementations
- The EMV SRC API specification offers levels of optionality for implementers of the specifications to add security layers based on the SRC solution provider’s own security requirements and risk controls

## 1.2 Constraints

The SRC API Specification is designed to work within the constraints described in the SRC Core Specification. In particular, the SRC API Specification or any implementation of the SRC API Specification is not intended to replace or interfere with any international, regional, national or local laws and regulations; those governing requirements supersede any industry standards.

## 1.3 Audience

This document is intended for use by SRC Systems and SRC System Participants.

## 1.4 References

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

### 1.4.1 Normative References

The standards in Table 1.1 may be associated with the SRC API Specification.

**Table 1.1: Normative References**

Reference	Publication Name
ISO 3166	Country Codes — ISO 3166
ISO 4217	Currency Codes — ISO 4217
ISO/IEC 7812	Identification cards — Identification of issuers
RFC 3447	Public-Key Cryptography Standards ( <a href="https://tools.ietf.org/html/rfc3447">https://tools.ietf.org/html/rfc3447</a> )
RFC 7515	JSON Web Signature ( <a href="https://tools.ietf.org/html/rfc7515">https://tools.ietf.org/html/rfc7515</a> )
RFC 7516	JSON Web Encryption ( <a href="https://tools.ietf.org/html/rfc7516">https://tools.ietf.org/html/rfc7516</a> )
RFC 7517	JSON Web Key ( <a href="https://tools.ietf.org/html/rfc7517">https://tools.ietf.org/html/rfc7517</a> )
RFC 7518	JSON Web Algorithms ( <a href="https://tools.ietf.org/html/rfc7518">https://tools.ietf.org/html/rfc7518</a> )
RFC 7519	JSON Web Token ( <a href="https://tools.ietf.org/html/rfc7519">https://tools.ietf.org/html/rfc7519</a> )

### 1.4.2 Published EMVCo Documents

The documents in Table 1.2 are related to or are associated with SRC and are located at [www.emvco.com](http://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

Reference	Publication Name
Merchant-Presented Mode	EMV® QR Code Specification for Payment Systems (EMV QRCPS) – Merchant-Presented Mode
Payment Tokenisation	EMV® Payment Tokenisation Specification – Technical Framework
SRC Core Specification	EMV® Secure Remote Commerce Specification
SRC Reproduction Requirements	EMV® Secure Remote Commerce (SRC): Click to Pay Icon Reproduction Requirements
SRC UI Guidelines and Requirements	EMV® Secure Remote Commerce Specification – User Interface Guidelines and Requirements
SRC JavaScript SDK	EMV® Secure Remote Commerce Specification – JavaScript SDK
SRC Version Management	EMV® Secure Remote Commerce Version Management for SRC API and SRC JavaScript SDK Specifications
SRC Use Cases	EMV® Secure Remote Commerce Use Cases

Collectively, the term SRC Specifications refers to:

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

## 1.5 Definitions

For the definition of the terms used in the SRC API Specification, refer to Table 1.3: Definitions in the SRC Core Specification. For definitions of data elements refer to Section 2 Data Dictionary.

## 1.6 Notational Conventions

### 1.6.1 Abbreviations

For the definition of the abbreviations used in the SRC API Specification, refer to Section 1.9.1 Abbreviations in the SRC Core Specification.

### 1.6.2 Terminology and Conventions

For the definition of the terminology and conventions used in the SRC API Specification, refer to Section 1.9.2 Terminology and Conventions in the SRC Core Specification.

## 2 Data Dictionary

### 2.1 Complex Data Objects

Table 2.1 to Table 2.48 introduce the common data objects used across the APIs defined in the SRC API Specification. Each table defines a single data object.

The column headed R/C/O in each table refers to whether the data element is required, conditional or optional. The following notation is used:

- R = Required – always present
- C = Conditional – present under certain conditions (as specified in the description)
- O = Optional – can be present

#### 2.1.1 AcceptanceChannelData

**Table 2.1: AcceptanceChannelData**

Data Element	R/C/O	Constraints	Description
<b>consumerData</b> Type: JSONObject	C	Acceptance channel specific	Consumer supplied data, either manually entered (or supplied by other means, e.g. voice, camera etc.) or previously stored <b>Conditionality:</b> At least one of consumerData or sellerData is required
<b>sellerData</b> Type: JSONObject	C	Acceptance channel specific	Seller supplied data supplied over the acceptance channel technology, or other means <b>Conditionality:</b> At least one of consumerData or sellerData is required

## 2.1.2 AcceptanceChannelRelatedData

**Table 2.2: AcceptanceChannelRelatedData**

Data Element	R/C/O	Constraints	Description
<b>acceptanceChannelType</b> Type: AcceptanceChannelType	R	See AcceptanceChan nelType	Type of acceptance channel
<b>acceptanceChannelTechnol ogy</b> Type: AcceptanceChannelTechnolog y	O	See AcceptanceChan nelTechnology	Technology used to transmit/receive the acceptance channel data
<b>acceptanceChannelData</b> Type: AcceptanceChannelData	R	See AcceptanceChan nelData	Acceptance channel data

## 2.1.3 AccountReference

**Table 2.3: AccountReference**

Data Element	R/C/O	Constraints	Description
<b>srcDigitalCardId</b> Type: String	C	Max Length = 36	Reference identifier to the Digital Card representing the PAN or Payment Token  <b>Conditionality:</b> Required when consumerIdentity is not present
<b>consumerIdentity</b> Type: ConsumerIdentity	C	See ConsumerIdentity	Primary verifiable Consumer Identity within an SRC Profile (e.g. an email address or a mobile phone number)  <b>Conditionality:</b> Required when srcDigitalCardId is not present

## 2.1.4 AdditionalAmount

**Table 2.4: AdditionalAmount**

Data Element	R/C/O	Constraints	Description
<b>additionalAmountType</b> Type: AdditionalAmountType	R	See AdditionalAmount Type	Type of additional amount
<b>additionalAmountValue</b> Type: String	R		Value of the additional amount

## 2.1.5 Address

**Table 2.5: Address**

Data Element	R/C/O	Constraints	Description
<b>addressId</b> Type: String	O	UUID	Reference identifier of the address
<b>name</b> Type: String	O	Max Length = 100	Name of the Consumer
<b>line1</b> Type: String	C	Max Length = 75	Address line 1 <b>Conditionality:</b> Required when used with the DPA Registration operation in the Management Service APIs
<b>line2</b> Type: String	O	Max Length = 75	Address line 2
<b>line3</b> Type: String	O	Max Length = 75	Address line 3

Data Element	R/C/O	Constraints	Description
<b>city</b> Type: String	C	Max Length = 50	<p>Address city</p> <p><b>Conditionality:</b> When used with the DPA Registration operation in the Management Service APIs at least one of the following is required:</p> <ul style="list-style-type: none"> <li>• both <code>city</code> and <code>state</code></li> <li>• <code>zip</code></li> </ul>
<b>state</b> Type: String	C	Max Length = 30	<p>Address state</p> <p>Recommendation to support ISO 3166-2 format i.e. made up of ISO 3166-1 alpha 2 country code, followed by an alphanumeric string of 3 characters representing the state or sub-division</p> <p><b>Conditionality:</b> When used with the DPA Registration operation in the Management Service APIs at least one of the following is required:</p> <ul style="list-style-type: none"> <li>• both <code>city</code> and <code>state</code></li> <li>• <code>zip</code></li> </ul>
<b>zip</b> Type: String	C	Max Length = 16	<p>Address zip/postal code</p> <p><b>Conditionality:</b> When used with the DPA Registration operation in the Management Service APIs at least one of the following is required:</p> <ul style="list-style-type: none"> <li>• both <code>city</code> and <code>state</code></li> <li>• <code>zip</code></li> </ul>

Data Element	R/C/O	Constraints	Description
<b>countryCode</b> Type: String	C	ISO 3166-1 alpha-2 country code	Address country code <b>Conditionality:</b> Required when used with the DPA Registration operation in the Management Service APIs
<b>deliveryContactDetails</b> Type: DeliveryContactDetails	O	See DeliveryContactDetails	Delivery contact details
<b>createTime</b> Type: String (Numeric)	O	UTC time in Unix epoch format	Date and time the address was created
<b>lastUsedTime</b> Type: String (Numeric)	O	UTC time in Unix epoch format	Date and time the address was last used

## 2.1.6 AppInstance

**Table 2.6: AppInstance**

Data Element	R/C/O	Constraints	Description
<b>userAgent</b> Type: String	C	N/A	User agent string of the connecting client application <b>Conditionality:</b> <ul style="list-style-type: none"> <li>Required for browsers</li> <li>Optional for non-browsers</li> </ul>
<b>applicationName</b> Type: String	O	Max Length = 255	Name of the connecting client application
<b>countryCode</b> Type: String	O	ISO 3166-1 alpha-2 country code	The country where the Consumer is accessing the service from
<b>deviceData</b> Type: DeviceData	O	See DeviceData	Device specific data

## 2.1.7 AssuranceData

**Table 2.7: AssuranceData**

Data Element	R/C/O	Constraints	Description
<b>verificationData</b> Type: List<VerificationData>	R	See VerificationData	Set of verification data structures relating to different types of assurance
<b>eci</b> Type: String	O	Max Length = 2	Payment System-specific value to indicate the results of the attempt to authenticate the Cardholder
<b>cardVerificationEntity</b> Type: String (Numeric)  DEPRECATED	O	Length = 2	Entity performing card verification. Valid values are:  <ul style="list-style-type: none"> <li>• 01 SRC Initiator</li> <li>• 02 SRC System</li> <li>• 03 SRCPI</li> <li>• 04 DCF</li> <li>• 05 DPA</li> <li>• 06 -99 Others</li> </ul>
<b>cardVerificationMethod</b> Type: String (Numeric)  DEPRECATED	O	Length = 2	Card verification check to validate that the PAN is active and valid at the Card Issuer. Valid values are:  <ul style="list-style-type: none"> <li>• 01 \$0 authorisation, or single unit of currency authorisation</li> <li>• 02 Card Verification Number validation</li> <li>• 03 Postal code and address verification, where supported</li> <li>• 04 -20 EMVCo future use</li> <li>• 21 -99 SRC System specific</li> </ul>

Data Element	R/C/O	Constraints	Description
<b>cardVerificationResults</b> Type: String (Numeric)  DEPRECATED	Ø	Length = 2	Verification status of the PAN. Valid values are: <ul style="list-style-type: none"><li>• 01 Verified</li><li>• 02 Not Verified</li><li>• 03 Not performed</li><li>• 04 - 20 EMVCo future use</li><li>• 21 - 99 SRC System specific</li></ul>
<b>cardVerificationTimestamp</b> Type: String (Numeric)  DEPRECATED	Ø	UTC time in Unix epoch format	Date and time when the card verification was conducted
<b>cardAssuranceData</b> Type: String  DEPRECATED	Ø		Data collected that is associated with the PAN and presented to the SRC System
<b>cardholderAuthenticationEntity</b> Type: String  DEPRECATED	Ø	Max Length = 64	Entity performing Cardholder authentication

Data Element	R/C/O	Constraints	Description
<b>cardholderAuthenticationMethod</b>  Type: String (Numeric)  DEPRECATED	Ø	Length = 2	Card Issuer verification of the Cardholder. Valid values are: <ul style="list-style-type: none"><li>• 01 Use of a 3-D Secure ACS</li><li>• 02 Mobile banking verification of the Cardholder with an authentication code</li><li>• 03 Federated login systems</li><li>• 04 A shared secret between the Card Issuer and the Cardholder such as One Time Passcode (OTP), activation code</li><li>• 05 -20 EMVCo future use</li><li>• 21 - 99 SRC System specific</li></ul>
<b>cardholderAuthenticationResults</b>  Type: String (Numeric)  DEPRECATED	Ø	Length = 2	Indicates whether the Cardholder was verified or not, and what the results are when verified. <ul style="list-style-type: none"><li>• 01 Verified</li><li>• 02 Not Verified</li><li>• 03 Not performed</li><li>• 04 -20 EMVCo future use</li><li>• 21 - 99 SRC System specific</li></ul>
<b>cardholderAuthenticationTimestamp</b>  Type: String (Numeric)  DEPRECATED	Ø	UTC time in Unix epoch format	Date and time when the Cardholder authentication was conducted

Data Element	R/C/O	Constraints	Description
<b>cardholderAssuranceData</b> Type: String DEPRECATED	Ø		Data collected that is associated with the Cardholder and presented to the SRC System
<b>consumerVerificationEntity</b> Type: String DEPRECATED	Ø	Max Length = 64	Entity performing Consumer verification
<b>consumerVerificationMethod</b> Type: String (Numeric) DEPRECATED	Ø	Length = 2	The verification method used to verify Consumer credential. Valid values are: <ul style="list-style-type: none"> <li>• 01 Static Passcode</li> <li>• 02 SMS One Time Passcode (OTP)</li> <li>• 03 Keyfob or EMV cardreader One Time Passcode (OTP)</li> <li>• 04 Application One Time Passcode (OTP)</li> <li>• 05 One Time Passcode (OTP) Other</li> <li>• 06 Knowledge Based Authentication (KBA)</li> <li>• 07 Out of Band Biometrics</li> <li>• 08 Out of Band Login</li> <li>• 09 Out of Band Other</li> <li>• 10 Risk-Based</li> <li>• 11 Other</li> <li>• 12 - 99 EMVCo future use</li> </ul>

Data Element	R/C/O	Constraints	Description
<b>consumerVerificationResult</b> <del>s</del> Type: String (Numeric) DEPRECATED	Ø	Length = 2	Indicates whether the Consumer was verified or not, and what the results are when verified. Valid values are: <ul style="list-style-type: none"><li>• 01 Verified</li><li>• 02 Not Verified</li><li>• 03 Not performed</li><li>• 04 - 20 EMVCo future use</li><li>• 21 - 99 SRC System specific</li></ul>
<b>consumerVerificationTimestamp</b> <del>s</del> Type: String (Numeric) DEPRECATED	Ø	UTC time in Unix epoch format	Date and time when the Consumer verification was conducted
<b>consumerAssuranceData</b> <del>s</del> Type: String DEPRECATED	Ø		Data collected that is associated with the Consumer for assurance purposes
<b>deviceVerificationEntity</b> <del>s</del> Type: String (Numeric) DEPRECATED	Ø	Length = 2	Entity performing device verification. The valid values are: <ul style="list-style-type: none"><li>• 01 SRC Initiator</li><li>• 02 SRC System</li><li>• 03 SRCPI</li><li>• 04 DCF</li><li>• 05 DPA</li><li>• 06 - 99 Others</li></ul>

Data Element	R/C/O	Constraints	Description
<b>deviceVerificationMethod</b> Type: String (Numeric)  DEPRECATED	Ø	Length = 2	Verification method used to verify Consumer Device information. Valid values are: <ul style="list-style-type: none"><li>• 01 - 20 EMVCo future use</li><li>• 21 - 99 SRC System specific</li></ul>
<b>deviceVerificationResults</b> Type: String (Numeric)  DEPRECATED	Ø	Length = 2	Indicates whether the device was verified or not, and what the results are when verified. Valid values are: <ul style="list-style-type: none"><li>• 01 Verified</li><li>• 02 Not Verified</li><li>• 03 Not performed</li><li>• 04 - 20 EMVCo future use</li><li>• 21 - 99 SRC System specific</li></ul>
<b>deviceVerificationTimestamp</b> Type: String (Numeric)  DEPRECATED	Ø	UTC time in Unix epoch format	Date and time when the device verification was conducted
<b>deviceAssuranceData</b> Type: String  DEPRECATED	Ø		Data collected that is associated with the device for assurance purposes

Data Element	R/C/O	Constraints	Description
<del><b>relationshipVerificationEntity</b></del>  Type: String (Numeric)  DEPRECATED	Ø	Length = 2	Entity performing relationship verification of a combination of data. The valid values are: <ul style="list-style-type: none"><li>• 01 SRC Initiator</li><li>• 02 SRC System</li><li>• 03 SRCPI</li><li>• 04 DCF</li><li>• 05 DPA</li><li>• 06-99 Others</li></ul>
<del><b>relationshipVerificationMethod</b></del>  Type: String (Numeric)  DEPRECATED	Ø	Max Length = 2	Verification method used to verify information associated with the relationship
<del><b>relationshipVerificationResults</b></del>  Type: String (Numeric)  DEPRECATED	Ø	Max Length = 2	Results of the verification of the relationship of a combination of data
<del><b>relationshipVerificationTimeStamp</b></del>  Type: String (Numeric)  DEPRECATED	Ø	UTC time in Unix epoch format	Date and time when the relationship verification was conducted
<del><b>relationshipAssuranceData</b></del>  Type: String  DEPRECATED	Ø		Data collected that is associated with the binding relationship for assurance purposes

## 2.1.8 AuthenticationContext

**Table 2.8: AuthenticationContext**

Data Element	R/C/O	Constraints	Description
<b>authenticationReasons</b> Type: List<AuthenticationReason>	R	See AuthenticationReason	
<b>srcDpald</b> Type: String	C	Max length = 255	<b>Conditionality:</b> When authenticationReasons contains TRANSACTION_AUTHENTICATION exactly one of srcDpald or dpaData must be provided
<b>dpaData</b> Type: DpaData	C		
<b>dpaTransactionOptions</b> Type: DpaTransactionOptions	C	See DpaTransactionOptions	Conditionality: Required when authenticationReasons contains TRANSACTION_AUTHENTICATION. In this case, dpaTransactionOptions must contain the same data that is supplied in Checkout
<b>acquirerMerchantId</b> Type: String	O	Max Length = 35	Acquirer-assigned Merchant identifier
<b>acquirerBIN</b> Type: String	O	Max Length = 11	Acquirer identification code as assigned by the Directory Server receiving the AReq message
<b>merchantName</b> Type: String	O		Merchant name assigned by the Acquirer or Payment System

## 2.1.9 AuthenticationMethod

**Table 2.9: AuthenticationMethod**

Data Element	R/C/O	Constraints	Description
<b>authenticationMethodType</b> Type: AuthenticationMethodType	R	See AuthenticationMethodType	
<b>authenticationSubject</b> Type: AuthenticationSubject	R	See AuthenticationSubject	
<b>uriData</b> Type: UriData	O	See UriData	URI associated with the authentication method (only valid in the Authentication Method Lookup response)  When authentication is invoked by launching the URI then AssuranceData, AuthenticationStatus, AuthenticationResult and any relevant session ids should be provided back asynchronously when authentication completes.  It can be achieved by cross origin post message between the windows i.e. the caller and the authenticator.

Data Element	R/C/O	Constraints	Description
<b>authenticationCredentialReference</b> Type: String	O	Max Length = 255	May be provided by the identity provider once an authentication is initiated to qualify the nature of the authentication method (e.g. for SMS OTP, this may include the masked mobile number "***-***-1234", which can be displayed to the Consumer to aid method selection)
<b>methodAttributes</b> Type: JSONObject	O		Attributes associated with the authenticationMethod Type (see Section 2.2.1 Authentication Facilitation)

## 2.1.10 BusinessIdentification

**Table 2.10: BusinessIdentification**

Data Element	R/C/O	Constraints	Description
<b>businessIdentificationType</b> Type: String	C	Max Length = 50	<b>Conditionality:</b> Required when acquirerMerchantId is not present or when businessIdentificationValue is present
<b>businessIdentificationValue</b> Type: String	C	Max Length = 30	<b>Conditionality:</b> Required when acquirerMerchantId is not present or when businessIdentificationType is present
<b>acquirerMerchantId</b> Type: String	O	Max Length = 35	Acquirer-assigned merchant identifier.

## 2.1.11 Card

**Table 2.11: Card**

Data Element	R/C/O	Constraints	Description
<b>primaryAccountNumber</b> Type: String (Numeric)	R	Min Length = 9 Max Length = 19	Primary Account Number. A variable length, ISO/IEC 7812-compliant account number that is generated within account ranges associated with a BIN by a Card Issuer
<b>panExpirationMonth</b> Type: String (Numeric)	C	Length = 2	Expiration month expressed as a two-digit month (MM) <b>Conditionality:</b> Required when specified for the Card (PAN)
<b>panExpirationYear</b> Type: String (Numeric)	C	Length = 4	Expiration year expressed as a four-digit calendar year (YYYY) <b>Conditionality:</b> Required when specified for the Card (PAN)
<b>cardSecurityCode</b> Type: String (Numeric)	O	Length = 3 or 4	Card security code
<b>cardholderFullName</b> Type: String	O	Max Length = 100	Cardholder name
<b>cardholderFirstName</b> Type: String	O	Max Length = 50	Cardholder first name
<b>cardholderLastName</b> Type: String	O	Max Length = 50	Cardholder last name
<b>billingAddress</b> Type: Address	O	See Address	Billing address

Data Element	R/C/O	Constraints	Description
<b>paymentAccountReference</b> Type: String	O	Max Length = 29	A non-financial reference assigned to each unique PAN and used to link a payment account represented by that PAN to affiliated Payment Tokens
<b>customerServiceEmailAddresses</b> Type: String	O	Max Length = 255	Customer service email address
<b>customerServicePhoneNumber</b> Type: PhoneNumber	O	See PhoneNumber	Customer service phone number
<b>customerServiceUri</b> Type: String	O	Max Length = 1024	Customer service webpage URI

### 2.1.12 CardholderData

**Table 2.12: CardholderData**

Data Element	R/C/O	Constraints	Description
<b>fullName</b> Type: String	O	Max Length = 100	Cardholder name
<b>firstName</b> Type: String	O	Max Length = 50	Cardholder first name
<b>lastName</b> Type: String	O	Max Length = 50	Cardholder last name

Data Element	R/C/O	Constraints	Description
<b>issuerIdentity</b> Type: String	O	Max Length = 64	Cardholder identity as known by the Card Issuer. This generally enables access to an application, website or other. Examples include username/email address/mobile number
<b>emailAddress</b> Type: String	O	Max Length = 255	Cardholder email address. This is Cardholder generated and represents contact or notification data
<b>mobileNumber</b> Type: PhoneNumber	O	See PhoneNumber	Cardholder mobile phone number
<b>billingPhoneNumber</b> Type: PhoneNumber	O	See PhoneNumber	Cardholder billing phone number

### 2.1.13 CommunicationsConsent

Table 2.13: CommunicationsConsent

Data Element	R/C/O	Constraints	Description
<b>communicationsOptIn</b> Type: Boolean	O	Boolean	Consumer's communications opt in preference.
<b>affiliateCommunicationsOptIn</b> Type: Boolean	O	Boolean	Consumer's affiliate communications opt in preference
<b>allowEmail</b> Type: Boolean	O	Boolean	Consumer's preference for receiving communications via email
<b>allowText</b> Type: Boolean	O	Boolean	Consumer's preference for receiving communications via SMS

Data Element	R/C/O	Constraints	Description
<b>allowCall</b> Type: Boolean	O	Boolean	Consumer's preference for receiving communications via voice calls
<b>allowPush</b> Type: Boolean	O	Boolean	Consumer's preference for receiving communications via a notification channel

## 2.1.14 ComplianceResource

**Table 2.14: ComplianceResource**

Data Element	R/C/O	Constraints	Description
<b>complianceType</b> Type: ComplianceType	R	See ComplianceType	
<b>uri</b> Type: String	R	Max Length = 1024	URI
<b>version</b> Type: String	O	Max Length = 10	Version
<b>datePublished</b> Type: String	O	UTC time in Unix epoch format	Date resource was published

## 2.1.15 ComplianceSettings

**Table 2.15: ComplianceSettings**

Data Element	R/C/O	Constraints	Description
<b>complianceResources</b> Type: List<ComplianceResource>	R	See ComplianceResource	
<b>privacy</b> Type: Consent  DEPRECATED	O	See Consent	Consent wording for privacy policy

Data Element	R/C/O	Constraints	Description
<del>tnc</del> Type: Consent DEPRECATED	Ø	See Consent	Consent wording for T&Cs policy
<del>cookie</del> Type: Consent DEPRECATED	Ø	See Consent	Consent wording for cookie policy
<del>geoLocation</del> Type: Consent DEPRECATED	Ø	See Consent	Consent wording for geolocation policy
<b>communications</b> Type: CommunicationsConsent	O	See Communications Consent	Indicates the Consumer's consent to receive communications

### 2.1.16 ConfirmationData DEPRECATED

*Replaced by ConfirmationData2 (Section 2.1.17)*

**Table 2.16: ConfirmationData DEPRECATED**

Data Element	R/C/O	Constraints	Description
<del>checkoutEventType</del> Type: String (Numeric) DEPRECATED	Ø	Length = 2	Event type associated with the update. Valid values are: <ul style="list-style-type: none"><li>• 01 Authorise</li><li>• 02 Capture</li><li>• 03 Refund</li><li>• 04 Cancel</li><li>• 05 Fraud</li><li>• 06 Chargeback</li><li>• 07 Other</li></ul>

Data Element	R/C/O	Constraints	Description
<b>checkoutEventStatus</b> Type: String (Numeric)  DEPRECATED	Ø	Length = 2	Event type associated with the order. Valid values are: <ul style="list-style-type: none"><li>• 01 Created</li><li>• 02 Confirmed</li><li>• 03 Cancelled</li><li>• 04 Fraud Cancelled</li><li>• 05 Others</li><li>• 06 - 50 EMVCo future use</li><li>• 51 - 99 SRC System specific</li></ul>
<b>confirmationStatus</b> Type: String (Numeric)  DEPRECATED	Ø	Length = 2	Status of the event as provided by the SRC Initiator in the Confirmation message. Valid values are: <ul style="list-style-type: none"><li>• 01 Success</li><li>• 02 Failure</li><li>• 03 Other</li></ul>
<b>confirmationReason</b> Type: String  DEPRECATED	Ø	Max Length = 64	Description of the reason for the event associated with the order
<b>confirmationTimestamp</b> Type: String (Numeric)  DEPRECATED	Ø	UTC time in Unix epoch format	Date and time of the event completion corresponding to the Confirmation event by the SRC Initiator
<b>networkAuthorizationCode</b> Type: String  DEPRECATED	Ø	Max Length = 25	Authorisation code associated with an approved transaction
<b>networkTransactionIdentifier</b> Type: String  DEPRECATED	Ø	Max Length = 25	Unique authorisation related tracing value assigned by a Payment Network and provided in an authorisation response

Data Element	R/C/O	Constraints	Description
<b>paymentNetworkReference</b> Type: String DEPRECATED	Ø	Max Length = 25	Transaction identifier as provided by a Payment Network after authorisation has been complete
<b>assuranceData</b> Type: AssuranceData DEPRECATED	Ø	See AssuranceData	Assurance data
<b>transactionAmount</b> Type: TransactionAmount DEPRECATED	Ø	See TransactionAmount	Amount of the transaction

### 2.1.17 ConfirmationData2

**Table 2.17: ConfirmationData2**

Data Element	R/C/O	Constraints	Description
<b>checkoutEventType</b> Type: String (Numeric)	R	Length = 2	<p>Event type associated with the confirmation. Valid values are:</p> <ul style="list-style-type: none"> <li>• 00 Place Order</li> <li>• 01 Authorise</li> <li>• 02 Capture</li> <li>• 03 Refund</li> <li>• 04 Cancel (Auth Reversal)</li> <li>• 05 Fraud</li> <li>• 06 Chargeback</li> <li>• 07 Cancel before Auth</li> <li>• 08 Auth for account validation</li> <li>• 09 – 50 EMVCo future use</li> <li>• 51 – 99 SRC System specific</li> </ul>

Data Element	R/C/O	Constraints	Description
<b>checkoutEventStatus</b> Type: String (Numeric)	O	Length = 2	Event status associated with the order. Valid values are: <ul style="list-style-type: none"><li>• 01 Created</li><li>• 02 Confirmed</li><li>• 03 Cancelled</li><li>• 04 Fraud Cancelled</li><li>• 05 Others</li><li>• 06 – 50 EMVCo future use</li><li>• 51 – 99 SRC System specific</li></ul>
<b>confirmationStatus</b> Type: String (Numeric)	R	Length = 2	Status related to the <code>checkoutEventType</code> as provided by the SRC Initiator. Valid values are: <ul style="list-style-type: none"><li>• 01 Success</li><li>• 02 Failure</li><li>• 03 Other</li><li>• 04 Timeout</li></ul>
<b>confirmationReason</b> Type: String	O	Max Length = 64	Description of the reason for the event associated with the order
<b>confirmationTimestamp</b> Type: String (Numeric)	R	UTC time in Unix epoch format	Date and time of the event set by the SRC Initiator
<b>networkAuthorizationCode</b> Type: String	C	Max Length = 25	Authorisation code associated with an approved transaction  <b>Conditionality:</b> Required when the value of: <ul style="list-style-type: none"><li>• <code>checkoutEventType</code> is set to 01 (Authorize) or 03 (Refund); and</li><li>• <code>confirmationStatus</code> is set to 01 (Success)</li></ul>

Data Element	R/C/O	Constraints	Description
<b>networkTransactionIdentifier</b> Type: String	O	Max Length = 25	Unique authorisation related tracing identifier assigned by a Payment Network and provided in an payment authorisation response
<b>paymentNetworkReference</b> Type: String	O	Max Length = 25	Transaction identifier as provided by a Payment Network payment authorisation has been completed
<b>assuranceData</b> Type: AssuranceData	O	See AssuranceData	Assurance data
<b>transactionAmount</b> Type: TransactionAmount	C	See TransactionAmount	Amount of the transaction <b>Conditionality:</b> Required when the value of: <ul style="list-style-type: none"> <li>• checkoutEventType is set to 01 (Authorize) or 03 (Refund); and</li> <li>• confirmationStatus is set to 01 (Success)</li> </ul>

### 2.1.18 Consent DEPRECATED

**Table 2.18: Consent DEPRECATED**

Data Element	R/C/O	Constraints	Description
<b>acceptedVersion</b> Type: String DEPRECATED	O	Max Length = 10	Version accepted by the Consumer
<b>latestVersion</b> Type: String DEPRECATED	O	Max Length = 10	Latest version

Data Element	R/C/O	Constraints	Description
<b>latestVersionUri</b> Type: String DEPRECATED	O	Max Length = 1024	URI of the latest version

## 2.1.19 Consumer

**Table 2.19: Consumer**

Data Element	R/C/O	Constraints	Description
<b>consumerIdentity</b> Type: ConsumerIdentity	R	See ConsumerIdentity	Primary verifiable Consumer Identity within an SRC Profile (e.g. an email address or a mobile phone number)
<b>emailAddress</b> Type: String	O	Max Length = 255	Consumer-provided email address
<b>mobileNumber</b> Type: PhoneNumber	O	See PhoneNumber	Consumer-provided mobile number
<b>nationalIdentifier</b> Type: String	O	Max Length = 20	Geographic-specific, nationally-provided identifier for the Consumer
<b>countryCode</b> Type: String	O	ISO 3166-1 alpha-2 country code	Consumer-provided country code
<b>languageCode</b> Type: String	O	ISO 639-1 Code	Consumer-provided language choice
<b>firstName</b> Type: String	O	Max Length = 50	Consumer-provided first name
<b>lastName</b> Type: String	O	Max Length = 50	Consumer-provided last name

Data Element	R/C/O	Constraints	Description
<b>fullName</b> Type: String	O	Max Length = 100	Consumer-provided full name

## 2.1.20 ConsumerIdentity

**Table 2.20: ConsumerIdentity**

Data Element	R/C/O	Constraints	Description
<b>identityProvider</b> Type: IdentityProvider	O	See IdentityProvider	Entity or organisation that collected and verified the Consumer Identity
<b>identityType</b> Type: ConsumerIdentityType	R	See ConsumerIdentity Type	Type of Consumer Identity transmitted or collected
<b>identityValue</b> Type: String	R	Max Length = 255	Consumer Identity value that corresponds to the Consumer Identity Type

## 2.1.21 Dcf

**Table 2.21: Dcf**

Data Element	R/C/O	Constraints	Description
<b>applicationType</b> Type: ApplicationType	O	See ApplicationType	Type of the environment of the DCF
<b>uri</b> Type: String	O	Max Length = 1024	DCF URI as provided by DCF
<b>logoUri</b> Type: String	O	Max Length = 1024	Logo image URI provided by the DCF to support presentation

Data Element	R/C/O	Constraints	Description
<b>name</b> Type: String	O	Max Length = 60	Legal Name of DCF Onboarded to the SRC System

## 2.1.22 DeliveryContactDetails

**Table 2.22: DeliveryContactDetails**

Data Element	R/C/O	Constraints	Description
<b>contactFullName</b> Type: String	O	Max Length = 100	Consumer-provided name of the contact person
<b>contactPhoneNumber</b> Type: PhoneNumber	O	See PhoneNumber	Consumer-provided phone number of the contact person
<b>numberIsVoiceOnly</b> Type: Boolean	C		Indicates that the phone number provided is not capable of receiving text messages.  <b>Conditionality:</b> Required when contactPhoneNumber is provided
<b>contactEmailAddress</b> Type: email	O	See Email	Consumer-provided email address of the contact person
<b>instructions</b> Type: String	O	Max Length = 1024	Consumer-provided delivery instructions

## 2.1.23 DeviceData

**Table 2.23: DeviceData**

Data Element	R/C/O	Constraints	Description
<b>type</b> Type: String	O	Max Length = 255	Type of device being used. Example values are: <ul style="list-style-type: none"><li>• Mobile Phone</li><li>• Tablet</li><li>• Laptop</li><li>• Personal Assistant</li><li>• Connected Auto</li><li>• Home Appliance</li><li>• Wearable</li><li>• Stationary Computer</li><li>• E-Reader</li><li>• Handheld Gaming Devices</li><li>• Other</li></ul>
<b>manufacturer</b> Type: String	O	Max Length = 255	Manufacturer of the device
<b>brand</b> Type: String	O	Max Length = 255	Brand name of the device
<b>model</b> Type: String	O	Max Length = 255	Specific model of the device

## 2.1.24 DigitalCardData

**Table 2.24: DigitalCardData**

Data Element	R/C/O	Constraints	Description
<b>status</b> Type: DigitalCardStatus	R	See DigitalCardStatus	State of the Digital Card

Data Element	R/C/O	Constraints	Description
<b>presentationName</b> Type: String	O	Max Length = 64	Presentation text created by the Consumer to enable recognition of the PAN. This value is defined by the Consumer (e.g. nickname)
<b>descriptorName</b> Type: String	R	Max Length = 64	Presentation text defined by the SRC Programme that describes the PAN presented as a Digital Card
<b>artUri</b> Type: String	R	Max Length = 1024	URI that hosts the Card Art image to be used for presentation purposes. Can be provided by SRCPI
<b>artHeight</b> Type: String (Numeric)	O		Height of the card art in pixels
<b>artWidth</b> Type: String (Numeric)	O		Width of the card art in pixels
<b>pendingEvents</b> Type: List<CardPendingEvent>	C	See CardPendingEvent	Set of events that are pending completion <b>Conditionality:</b> Required when the value of <code>status</code> is set to PENDING
<b>authenticationMethods</b> List<AuthenticationMethod>	O	See AuthenticationMethod	List of available authentication methods May be provided when SRC System identifies a need to perform verification

## 2.1.25 DigitalCardFeature

**Table 2.25: DigitalCardFeature**

Data Element	R/C/O	Constraints	Description
<b>content</b> Type: String	R	Max Length = 1024	Content of the Digital Card Feature. The value is specific for the contentType
<b>contentType</b> Type: DigitalCardFeatureContentType	R	See DigitalCardFeatureContentType	Type of the content of the Digital Card Feature
<b>style</b> Type: String	O	Max Length = 1024	URI of a CSS style sheet that describes how to present a Digital Card Feature
<b>width</b> Type: String (Numeric)	O		Width to be applied to display of a Digital Card Feature image
<b>height</b> Type: String (Numeric)	O		Height to be applied to display of a Digital Card Feature image

## 2.1.26 DigitalCardUpdateNotification

**Table 2.26: DigitalCardUpdateNotification**

Data Element	R/C/O	Constraints	Description
<b>serviceId</b> Type: String	O	Max Length = 255	Service identifier associated to an SRC System specific configuration
<b>srcDigitalCardId</b> Type: String	C	Max Length = 36	Identifier of the updated card <b>Conditionality:</b> Required when maskedCard is not present

Data Element	R/C/O	Constraints	Description
<b>authorization</b> Type: String	O		First Party Token that may be provided if the <code>maskedCard</code> is not present
<b>maskedCard</b> Type: MaskedCard	C	See MaskedCard	Updated masked card data <b>Conditionality:</b> Required when <code>srcDigitalCardId</code> is not present
<b>eventTimestamp</b> Type: String (Numeric)	R	UTC time in Unix epoch format	Date and time of the card update event
<b>srcCorrelationId</b> Type: String	O	Max Length = 256	SRC Correlation Id corresponding to this SRC checkout transaction. May be provided if the notification occurs during checkout
<b>reason</b> Type: String	O	Max length = 255	Reason for the update of the card

### 2.1.27 DpaData

Table 2.27: DpaData

Data Element	R/C/O	Constraints	Description
<b>dpaPresentationName</b> Type: String	O	Max Length = 60	Merchant company name associated with the DPA to be used for presentation purposes within the user experience
<b>dpaAddress</b> Type: Address	O	See Address	DPA business address
<b>dpaName</b> Type: String	R	Max Length = 60	Legal name of registered DPA
<b>dpaEmailAddress</b> Type: String	O	Max Length = 255	DPA contact email address

Data Element	R/C/O	Constraints	Description
<b>dpaPhoneNumber</b> Type: PhoneNumber	O	See PhoneNumber	DPA contact phone number
<b>dpaLogoUri</b> Type: String	O	Max Length = 1024	URI of the logo of the DPA
<b>dpaSupportEmailAddress</b> Type: String	O	Max Length = 255	DPA support contact email address
<b>dpaSupportPhoneNumber</b> Type: PhoneNumber	O	See PhoneNumber	DPA support contact phone number
<b>dpaSupportUri</b> Type: String	O	Max Length = 1024	DPA's support URI
<b>dpaUri</b> Type: String	C	Max Length = 1024	A suitable unique DPA identifier. May contain the DPA business website URI or mobile application identifier in reversed domain notation or any other suitable unique DPA identifier  <b>Conditionality:</b> Required when used with the DPA Registration operation in the Management Service APIs
<b>applicationType</b> Type: ApplicationType	O	See ApplicationType	Type of DPA
<b>merchantAccountInformation</b> Type: String	O	Max Length = 1024	Implementation specific account information for an alternative acceptance channel

Data Element	R/C/O	Constraints	Description
<b>merchantCountryCode</b> Type: String	C	ISO 3166-1 alpha-2 country code	The country code associated with the site or application that implements SRC  <b>Conditionality:</b> Required when used with the DPA Registration operation in the Management Service APIs
<b>businessId</b> Type: BusinessIdentification	C	See BusinessIdentification	<b>Conditionality:</b> Required when used with the DPA Registration operation in the Management Service APIs
<b>merchantName</b> Type: String	O	Max Length = 40	Merchant name assigned by the Acquirer or Payment System, for 3DS usage only; may be different from dpaName
<b>merchantCategoryCode</b> Type: String	O	Max Length = 10	
<b>acquirerId</b> Type: String	O	Max Length = 50	
<b>acquirerBin</b> Type: String	O	Max Length = 11	Acquiring institution identification code as assigned by the 3DS Directory Server receiving the AReq message, for 3DS usage only
<b>dpaPanDataRequested</b> Type: Boolean	O		Indicates that the merchant requests PAN-based data in the payload. Valid values are: <ul style="list-style-type: none"><li>• true</li><li>• false (default)</li></ul>

## 2.1.28 DpaTransactionOptions

**Table 2.28: DpaTransactionOptions**

Data Element	R/C/O	Constraints	Description
<b>transactionAmount</b> Type: TransactionAmount	C	See TransactionAmount	The amount of the transaction  <b>Conditionality:</b> Required when 3DS is to be performed by SRC System (i.e. the value of threeDsPreference is set to ONBEHALF)
<b>transactionType</b> Type: TransactionType	O	See TransactionType	Type of transaction
<b>deliveryMethod</b> Type: DeliveryMethod	O	See DeliveryMethod	An indication of the manner in which the purchased goods are to be delivered, independent of the dpaBillingPreference or dpaShippingPreference data elements
<b>dpaBillingPreference</b> Type: AddressPreference	O	See AddressPreference	Type of billing address required
<b>dpaAcceptedBillingCountries</b> Type: List<String>	O	Array of country codes in ISO 3166-1 alpha-2 format	Billing restrictions.  Payments from all the listed billing countries are accepted  For example: ["US","CA","AU"]  An empty list or the absence of this data element means that all countries are accepted.

Data Element	R/C/O	Constraints	Description
<b>dpaShippingPreference</b> Type: AddressPreference	O	See AddressPreference	Type of shipping address required
<b>dpaAcceptedShippingCountries</b> Type: List<String>	O	Array of country codes in ISO 3166-1 alpha-2 format	Shipping restrictions. Shipping region country codes that limits the selection of eligible shipping addresses  For example: ["US","CA","AU"]  An empty list or the absence of this data element means that all countries are accepted.
<b>consumerEmailAddressRequested</b> Type: Boolean	O		Indicates whether the DPA expects the Consumer email address to be returned in the SRC Payload
<b>consumerNameRequested</b> Type: Boolean	O		Indicates whether the DPA expects the Consumer name to be returned in the SRC Payload
<b>consumerPhoneNumberRequested</b> Type: Boolean	O		Indicates whether the DPA expects the Consumer phone number to be returned in the SRC Payload
<b>cardholderNameRequested</b> Type: Boolean	O		Indicates whether the DPA expects the Cardholder name to be returned in the SRC Payload

Data Element	R/C/O	Constraints	Description
<b>consumerNationalIdentifierRequested</b> Type: Boolean	O		Indicates whether the DPA expects the Consumer National Identifier to be returned in the SRC Payload
<b>merchantCategoryCode</b> Type: String	O	Length = 4	Describes the merchant's type of business, product or service
<b>merchantCountryCode</b> Type: String	O	ISO 3166-1alpha-2 country code	Country code of the merchant
<b>merchantOrderId</b> Type: String	O	UUID	Digital Payment Application generated order/invoice number corresponding to a Consumer purchase
<b>threeDsPreference</b> Type: ThreeDsPreference	R	See ThreeDsPreference	Merchant's 3DS preferences. This data element is not related to the Authentication Facilitation Service API operations and SDK methods
<b>threeDsInputData</b> Type: JSONObject	C		Merchant's 3DS input data <b>Conditionality:</b> Required when 3DS is to be performed by SRC System (i.e. the value of threeDsPreference is set to ONBEHALF)
<b>srcTokenrequestData</b> Type: JSONObject	O		Token specific data provided by the merchant
<b>paymentOptions</b> Type: List<PaymentOptions>	O	See PaymentOptions	Specifies the Dynamic Data requirement for the payload creation

Data Element	R/C/O	Constraints	Description
<b>dpaLocale</b> Type: String	O	ISO language country pair. [ISO 639-1 Code] [ISO 3166-1 alpha-2 country code]	Merchant's preferred locale. For example: ["en_US", "fr_CA"]
<b>customInputData</b> Type: JSONObject	O		Extensible container that allows DPA to pass SRC System-specific data to the SRC System
<b>orderType</b> Type: String	O	Length = 255	Type of the order
<b>confirmPayment</b> Type: Boolean	O		Default value: <code>false</code> <ul style="list-style-type: none"> <li>DCF is expected to prompt the Consumer to confirm payment when value is set to <code>true</code></li> <li>DPA is expected to prompt the Consumer to confirm payment when value is set to <code>false</code></li> </ul>

## 2.1.29 DynamicData

**Table 2.29: DynamicData**

Data Element	R/C/O	Constraints	Description
<b>dynamicDataValue</b> Type: String	C		Value of the dynamic data <b>Conditionality:</b> Required when the value of <code>dynamicDataType</code> is not set to <code>NONE</code>

Data Element	R/C/O	Constraints	Description
<b>dynamicDataType</b> Type: DynamicDataType	R	See DynamicDataType	Type of the Dynamic Data
<b>dynamicDataExpiration</b> Type: String (Numeric)	O	UTC time in Unix epoch format	Date and time at which the Dynamic Data expires

### 2.1.30 EnrollmentReferenceData

**Table 2.30: EnrollmentReferenceData**

Data Element	R/C/O	Constraints	Description
<b>enrollmentReferenceld</b> Type: String	R	Max Length = 256	Identifier of the enrolment reference
<b>enrollmentReferenceType</b> Type: EnrollmentReferenceType	R	See EnrollmentReferenceType	Type of the enrolment reference
<b>enrollmentReferenceProvider</b> Type: String	O	Max Length = 256	Provider of the enrolment reference

### 2.1.31 Error

**Table 2.31: Error**

Data Element	R/C/O	Constraints	Description
<b>status</b> Type: Numeric	R	Length = 3	HTTP status code to categorise the errors
<b>reason</b> Type: String	R	Max Length = 32	Error reason as associated with the HTTP status code
<b>message</b> Type: String	R	Max Length = 255	Error message as associated with the HTTP status code

Data Element	R/C/O	Constraints	Description
<b>errorDetail</b> Type: List<ErrorDetail>	O	See ErrorDetail	Error details

### 2.1.32 ErrorDetail

**Table 2.32: ErrorDetail**

Data Element	R/C/O	Constraints	Description
<b>reason</b> Type: String	O	Max Length = 32	Error reason
<b>source</b> Type: String	O	Max Length = 255	Name of the source which generated this error
<b>message</b> Type: String	O	Max Length = 255	Error message
<b>sourceType</b> Type: String	O	Max Length = 32	Type of the source

### 2.1.33 EventHistory

**Table 2.33: EventHistory**

Data Element	R/C/O	Constraints	Description
<b>ageOfSrcPanEnrolmentSinceCreated</b> Type: String (Numeric)	O	Max Length = 5	Age, in days, since the PAN was enrolled in the SRC System
<b>srcAgeSinceLastSuccessfulTransaction</b> Type: String (Numeric)	O	Max Length = 5	Age, in days, since the PAN/Digital Card/SRC Profile was successfully used for a transaction
<b>ageOfSrcRelationship</b> Type: String (Numeric)	O	Max Length = 5	Age, in days, of the SRC Profile in the SRC System

Data Element	R/C/O	Constraints	Description
<b>ageOfConsumerRelationship</b> Type: String (Numeric)	O	Max Length = 5	Age, in days, since the Consumer profile binding event occurred at the SRC Profile
<b>billingAndShippingRelations hip</b> Type: String	O	Length = 2	Relationship between the Cardholder billing and shipping information. Valid values are: <ul style="list-style-type: none"> <li>• 01 Same as Cardholder's billing address</li> <li>• 02 Consumer's preferred shipping address</li> <li>• 03 Consumer other address</li> </ul>
<b>shippingAddressUsageNew</b> Type: String (Numeric)	O	UTC time in Unix epoch format	Date when the shipping address used for this transaction was first used with the SRC Initiator
<b>ageOfShippingAddressUsag e</b> Type: String (Numeric)	O	Max Length = 5	Age, in days, since shipping address used for this transaction was first used by the SRC Initiator

### 2.1.34 IdentityValidationChannel

Table 2.34: IdentityValidationChannel

Data Element	R/C/O	Constraints	Description
<b>validationChannelId</b> Type: String	R	Max Length = 36	Reference identifier of the validation channel
<b>identityProvider</b> Type: IdentityProvider	O	See IdentityProvider	Entity or organisation that can validate the identity

Data Element	R/C/O	Constraints	Description
<b>identityType</b> Type: IdentityValidationChannelType	R	See IdentityValidation ChannelType	Type of the identity validation channel (e.g. email, SMS)
<b>maskedValidationChannel</b> Type: String	O	Max Length = 255	Masked identity validation channel (e.g. masked email, masked mobile number)

### 2.1.35 MaskedAddress

**Table 2.35: MaskedAddress**

Data Element	R/C/O	Constraints	Description
<b>addressId</b> Type: String	R	UUID	Identifier used to point to the address
<b>name</b> Type: String	O	Max Length = 100	Name of the individual receiving the delivered goods or service. Only applicable for the shipping address
<b>line1</b> Type: String	O	Max Length = 75	Address line 1
<b>line2</b> Type: String	O	Max Length = 75	Address line 2
<b>line3</b> Type: String	O	Max Length = 75	Address line 3
<b>city</b> Type: String	O	Max Length = 50	Address city

Data Element	R/C/O	Constraints	Description
<b>state</b> Type: String	O	Max Length = 30	Address state Recommendation to support ISO 3166-2 format i.e. made up of ISO 3166-1 alpha 2 country code, followed by an alphanumeric string of 3 characters representing the state or sub-division
<b>countryCode</b> Type: String	O	ISO 3166-1 alpha-2 country code	Address country code
<b>zip</b> Type: String	O	Max Length = 16	Address zip/postal code
<b>createTime</b> Type: String (Numeric)	O	UTC time in Unix epoch format	Date and time the address was created
<b>lastUsedTime</b> Type: String (Numeric)	O	UTC time in Unix epoch format	Date and time the address was last used

### 2.1.36 MaskedCard

**Table 2.36: MaskedCard**

Data Element	R/C/O	Constraints	Description
<b>srcDigitalCardId</b> Type: String	C	Max Length = 36	Reference identifier to the Digital Card representing the PAN or Payment Token <b>Conditionality:</b> <ul style="list-style-type: none"> <li>Required when returned to an SRCI or DCF</li> <li>Optional when returned to an SRCPI</li> </ul>

Data Element	R/C/O	Constraints	Description
<b>enrollmentReferenceData</b> Type: EnrollmentReferenceData	O	See EnrollmentReferenceData	Contains enrolment reference identifier as per the enrolment reference type
<b>cofEligible</b> Type: Boolean	O		Indicates that the card is eligible for the Merchant Digital Card-on-File use case
<b>srcPaymentCardId</b> Type: String	C	Max Length = 36	Reference identifier to the PAN that enables the SRC System to communicate with the SRCPI without transmitting the actual PAN. It is associated with the SRC Profile to which the Payment Card belongs and is unique within an SRC System  <b>Conditionality:</b> Required when returned to the SRCPI
<b>panBin</b> Type: String (Numeric)	R	Max Length = PAN Length - 10	First significant digits of the PAN in an unmasked form
<b>panLastFour</b> Type: String (Numeric)	R	Length = 4	Last four digits of the PAN in an unmasked form
<b>tokenBinRange</b> Type: String (Numeric)	C	Max Length = Payment Token Length - 10	Specific BIN range or subset of the BIN Range that has been designated only for the purpose of issuing Payment Tokens in an unmasked form  <b>Conditionality:</b> Required when a Payment Token is used

Data Element	R/C/O	Constraints	Description
<b>tokenLastFour</b> Type: String (Numeric)	C	Length = 4	Last four digits of the Payment Token in an unmasked form  <b>Conditionality:</b> Required when a Payment Token is used
<b>digitalCardData</b> Type: DigitalCardData	R	See DigitalCardData	Contains Digital Card information that is used in the acceptance environment and user interface. It refers to the actual PAN or Payment Token without disclosing either
<b>maskedCardholderFullName</b> Type: String	O	Max Length = 100	Masked Cardholder name
<b>maskedCardholderFirstName</b> Type: String	O	Max Length = 50	Masked Cardholder first name
<b>maskedCardholderLastName</b> Type: String	O	Max Length = 50	Masked Cardholder last name
<b>panExpirationMonth</b> Type: String (Numeric)	C	Length = 2	Expiration month expressed as a two-digit month (MM) used for presentation purposes  <b>Conditionality:</b> Required when specified for the card (PAN)

Data Element	R/C/O	Constraints	Description
<b>panExpirationYear</b> Type: String (Numeric)	C	Length = 4	Expiration year expressed as four-digit calendar year (YYYY), used for presentation purposes <b>Conditionality:</b> Required when specified for the card (PAN)
<b>paymentCardDescriptor</b> Type: String	O	Max Length = 32	Conveys the card brand, and will be a free-form string, to be defined within an SRC Programme
<b>paymentCardType</b> Type: String	O	Max Length = 32	Conveys the card type
<b>digitalCardFeatures</b> Type: List<DigitalCardFeature>	O	See DigitalCardFeature	Attributes related to the Digital Card Features that should be displayed to the Consumer
<b>countryCode</b> Type: String	O	ISO 3166-1 alpha-2 country code	Country code of issuance associated with the Card Issuer's BIN license
<b>maskedBillingAddress</b> Type: MaskedAddress	O	See MaskedAddress	Masked billing address associated with the card
<b>complianceSettings</b> Type: ComplianceSettings	O	See ComplianceSettings	Consumer compliance settings
<b>dcf</b> Type: Dcf	O	See Dcf	Digital Card Facilitator associated with the card
<b>serviceId</b> Type: String	O	Max Length = 255	Service identifier associated to an SRC System specific configuration

Data Element	R/C/O	Constraints	Description
<b>paymentAccountReference</b> Type: String	O	Max Length = 29	A non-financial reference assigned to each unique PAN and used to link a payment account represented by that PAN to affiliated Payment Tokens
<b>customerServiceEmailAddress</b> Type: String	O	Max Length = 255	Customer service email address
<b>customerServicePhoneNumber</b> Type: PhoneNumber	O	See PhoneNumber	Customer service phone number
<b>customerServiceUri</b> Type: String	O	Max Length = 1024	Customer service webpage URI
<b>dateOfCardCreated</b> Type: String (Numeric)	R	UTC time in Unix epoch format	Date when card was enrolled into the SRC System
<b>dateOfCardLastUsed</b> Type: String (Numeric)	O	UTC time in Unix epoch format	Date when card was last used for an SRC transaction

### 2.1.37 MaskedConsumer

**Table 2.37: MaskedConsumer**

Data Element	R/C/O	Constraints	Description
<b>srcConsumerId</b> Type: String	O	UUID	Reference identifier generated by the SRC System
<b>pendingEvents</b> Type: List<ConsumerPendingEvent>	O	See ConsumerPendingEvent	Set of events that are pending completion (e.g. re-acceptance of consent)

Data Element	R/C/O	Constraints	Description
<b>maskedConsumerIdentity</b> Type: MaskedConsumerIdentity	R	See MaskedConsumerIdentity	Masked value of the primary verifiable Consumer Identity within an SRC Profile (e.g. an email address or a mobile phone number)
<b>maskedEmailAddress</b> Type: String	O	Max Length = 255	Masked Consumer email address
<b>maskedMobileNumber</b> Type: PhoneNumber	O	See PhoneNumber	Masked Consumer mobile phone number
<b>maskedNationalIdentifier</b> Type: String	O	Max Length = 20	Masked Consumer national identifier
<b>complianceSettings</b> Type: ComplianceSettings	O	See ComplianceSettings	Consumer compliance settings
<b>countryCode</b> Type: String	O	ISO 3166-1 alpha-2 country code	Consumer-provided country code
<b>languageCode</b> Type: String	O	ISO 639-1 Code	Consumer-provided language choice
<b>status</b> Type: ConsumerStatus	R	See ConsumerStatus	Current status of the Consumer
<b>maskedFirstName</b> Type: String	O	Max Length = 50	Masked Consumer first name
<b>maskedLastName</b> Type: String	O	Max Length = 50	Masked Consumer last name
<b>maskedFullname</b> Type: String	O	Max Length = 100	Masked Consumer name

Data Element	R/C/O	Constraints	Description
<b>dateConsumerAdded</b> Type: String (Numeric)	R	UTC time in Unix epoch format	Date Consumer was added to the SRC System
<b>dateConsumerLastUsed</b> Type: String (Numeric)	O	UTC time in Unix epoch format	Date Consumer last transacted as determined by the SRC System

### 2.1.38 MaskedConsumerIdentity

Table 2.38: MaskedConsumerIdentity

Data Element	R/C/O	Constraints	Description
<b>identityProvider</b> Type: IdentityProvider	O	See IdentityProvider	Entity or organisation that collected and verifies the Consumer Identity
<b>identityType</b> Type: ConsumerIdentityType	R	See ConsumerIdentity Type	Type of Consumer Identity transmitted or collected
<b>maskedIdentityValue</b> Type: String	R	Max Length = 255	Masked Consumer Identity value (e.g. masked email address or masked mobile phone number)

## 2.1.39 Payload

**Table 2.39: Payload**

Data Element	R/C/O	Constraints	Description
<b>card</b> Type: Card	C	See Card	<p>Card data associated with the PAN used for the purchase</p> <p><b>Conditionality:</b> Required when the:</p> <ul style="list-style-type: none"> <li>• value of the relevant data element of type <code>PayloadTypeIndicator</code> was set to <code>FULL</code> or <code>PAYMENT</code>; and</li> <li>• SRC System determines that a PAN-based payload must be returned.</li> </ul> <p>A <code>card</code> is required if a <code>token</code> is not present. <code>card</code> and <code>token</code> are mutually exclusive</p>

Data Element	R/C/O	Constraints	Description
<b>token</b> Type: PaymentToken	C	See PaymentToken	<p>Payment Token data associated with the PAN used for the purchase</p> <p><b>Conditionality:</b> Required when the:</p> <ul style="list-style-type: none"> <li>• Value of the relevant data element of type PayloadTypeIndicator was set to FULL or PAYMENT; and</li> <li>• SRC System determines that a Payment Token-based payload must be returned</li> </ul> <p>A token is required if a card is not present. card and token are mutually exclusive</p>
<b>shippingAddress</b> Type: Address	C	See Address	<p>Shipping address as required for the delivery of the goods/services being purchased</p> <p><b>Conditionality:</b> Required when:</p> <ul style="list-style-type: none"> <li>• The value of the relevant data element of type PayloadTypeIndicator was set to FULL or NON_PAYMENT; and</li> <li>• Identified shipping address is available in the SRC Profile; and</li> <li>• Shipping address was requested (based on dpaShippingPreference)</li> </ul>

Data Element	R/C/O	Constraints	Description
<b>consumerEmailAddress</b> Type: String	C	Max Length = 255	Consumer-provided email address <b>Conditionality:</b> Required when: <ul style="list-style-type: none"> <li>The value of the relevant data element of type <code>PayloadTypeIndicator</code> was set to <code>FULL</code> or <code>NON_PAYMENT</code>; and</li> <li>Email address is available in the SRC Profile; and</li> <li>Email address was requested (<code>consumerEmailAddressRequested</code> set to true)</li> </ul>
<b>consumerFirstName</b> Type: String	C	Max Length = 50	Consumer-provided first name <b>Conditionality:</b> Required when: <ul style="list-style-type: none"> <li>The value of the relevant data element of type <code>PayloadTypeIndicator</code> was set to <code>FULL</code> or <code>NON_PAYMENT</code>; and</li> <li>Consumer first name is available in the SRC Profile; and</li> <li>Consumer name was requested (<code>consumerNameRequested</code> set to true)</li> </ul>

Data Element	R/C/O	Constraints	Description
<b>consumerLastName</b> Type: String	C	Max Length = 50	Consumer-provided last name <b>Conditionality:</b> Required when: <ul style="list-style-type: none"> <li>The value of the relevant data element of type <code>PayloadTypeIndicator</code> or was set to <code>FULL</code> or <code>NON_PAYMENT</code>; and</li> <li>Consumer last name is available in the SRC Profile; and</li> <li>Consumer name was requested (<code>consumerNameRequested</code> set to <code>true</code>)</li> </ul>
<b>consumerFullName</b> Type: String	C	Max Length = 100	Consumer-provided name <b>Conditionality:</b> Required when: <ul style="list-style-type: none"> <li>The value of the relevant data element of type <code>PayloadTypeIndicator</code> or was set to <code>FULL</code> or <code>NON_PAYMENT</code>; and</li> <li>Consumer name is available in the SRC Profile; and</li> <li>Consumer name was requested (<code>consumerNameRequested</code> set to <code>true</code>)</li> </ul>

Data Element	R/C/O	Constraints	Description
<b>consumerMobileNumber</b> Type: PhoneNumber	C	See Phonenumber	Consumer-provided mobile number  <b>Conditionality:</b> Required when: <ul style="list-style-type: none"> <li>• The value of the relevant data element of type PayloadTypeIndicator was set to FULL or NON_PAYMENT; and</li> <li>• Consumer mobile number is available in the SRC Profile; and</li> <li>• Consumer mobile number is requested (consumerPhoneNumberRequested set to true)</li> </ul>
<b>consumerNationalIdentifier</b> Type: String	O	Max Length = 20	Consumer National Identifier as available in SRC Profile
<b>srcTokenResultsData</b> Type: JSONObject	O		SRC System specific Token data
<b>dynamicData</b> Type: List<DynamicData>	R	See DynamicData	Dynamic data, generated using the dynamicDataType preference indicated in paymentOptions

Data Element	R/C/O	Constraints	Description
<b>billingAddress</b> Type: Address	C	See Address	<p>Billing address associated with the card used for the purchase</p> <p><b>Conditionality:</b> Required when:</p> <ul style="list-style-type: none"> <li>• The value of the relevant data element of type PayloadTypeIndicator was set to FULL or NON_PAYMENT; and</li> <li>• Billing address is available in the SRC Profile; and</li> <li>• Billing address was requested (based on dpaBillingPreference or statically derived using the default configured during DPA Registration)</li> </ul>
<b>threeDsOutputData</b> Type: JSONObject	C		<p>Result of 3DS payment authentication</p> <p><b>Conditionality:</b> Required when:</p> <ul style="list-style-type: none"> <li>• the value for threeDsPreference was set to ONBEHALF; and</li> <li>• 3DS authentication has been performed</li> </ul>

## 2.1.40 PaymentOptions

**Table 2.40: PaymentOptions**

Data Element	R/C/O	Constraints	Description
<b>dpaDynamicDataTtlMinutes</b> Type: String (Numeric)	O		Requested “Time to Live” (expiry period) of the Dynamic Data, specified in minutes
<b>dynamicDataType</b> Type: DynamicDataType	O	See DynamicDataType	Type of Dynamic Data required in the payload

## 2.1.41 PaymentToken

**Table 2.41: PaymentToken**

Data Element	R/C/O	Constraints	Description
<b>paymentToken</b> Type: String	R	ISO/IEC 7812 format	Payment Token
<b>tokenExpirationMonth</b> Type: String (Numeric)	C	Length = 2	Expiration month expressed as a two-digit month (MM) <b>Conditionality:</b> Required when specified for the Payment Token
<b>tokenExpirationYear</b> Type: String (Numeric)	C	Length = 4	Expiration year expressed as a four-digit calendar year (YYYY) <b>Conditionality:</b> Required when specified for the Payment Token
<b>cardholderFullName</b> Type: String	O	Max Length = 100	Cardholder name

Data Element	R/C/O	Constraints	Description
<b>cardholderFirstName</b> Type: String	O	Max Length = 50	Cardholder first name
<b>cardholderLastName</b> Type: String	O	Max Length = 50	Cardholder last name
<b>paymentAccountReference</b> Type: String	O	Max Length = 29	A non-financial reference assigned to each unique PAN and used to link a payment account represented by that PAN to affiliated Payment Tokens

## 2.1.42 PhoneNumber

**Table 2.42: PhoneNumber**

Data Element	R/C/O	Constraints	Description
<b>countryCode</b> Type: String	R	Min Length = 1 Max Length = 4	Phone number country code as defined by the International Telecommunication Union
<b>phoneNumber</b> Type: String	R	Min Length = 4 Max Length = 14	Phone number without country code

## 2.1.43 RecognitionData

**Table 2.43: RecognitionData**

Data Element	R/C/O	Constraints	Description
<b>srcCorrelationId</b> Type: String	O	Max Length = 256	Unique identifier generated by an SRC System

<b>idTokens</b> Type: List<JWT>	C		List of the Federated ID Tokens issued by the SRC System based on the successful recognition of the instance of the returning Consumer's web browser.  <b>Conditionality:</b> If the instance of the web browser has been recognised, at least a single Federated ID Token shall be provided in the list
<b>srcSystemUri</b> Type: String	C	Case sensitive URI using the https scheme that contains scheme and full qualified domain name of the host only	SRC System URI to identify the SRC System that generates the srcCorrelationId  <b>Conditionality:</b> Required when srcCorrelationId is provided and idTokens is not provided

## 2.1.44 SrcProfile

**Table 2.44: SrcProfile**

Data Element	R/C/O	Constraints	Description
<b>maskedCards</b> Type: List<MaskedCard>	O	See MaskedCard	Masked card data associated with the SRC Profile
<b>maskedShippingAddresses</b> Type: List<MaskedAddress>	O	See MaskedAddress	Masked shipping address data associated with the SRC Profile

Data Element	R/C/O	Constraints	Description
<b>maskedConsumer</b> Type: MaskedConsumer	C	See MaskedConsumer	Masked Consumer data associated with the SRC Profile  <b>Conditionality:</b> Required for non-device bound SRC Profiles
<b>authorization</b> Type: String	R		First party authorisation token as defined in Section 5.1.4 Authorisation

## 2.1.45 TransactionAmount

**Table 2.45: TransactionAmount**

Data Element	R/C/O	Constraints	Description
<b>transactionAmount</b> Type: Number	R	Max Length = 18	Amount of the transaction represented as a floating-point number
<b>transactionCurrencyCode</b> Type: String	R	ISO 4217 currency code	Currency in which the transaction amount is expressed. It is up to the SRC Programme to determine whether the currency code is: <ul style="list-style-type: none"><li>• Alphabetic</li><li>• Numeric</li><li>• Both</li></ul>
<b>additionalAmounts</b> Type: List<AdditionalAmount>	O		A list of additional amounts related to the transaction

## 2.1.46 VerificationData

**Table 2.46: VerificationData**

Data Element	R/C/O	Constraints	Description
<b>verificationType</b> Type: VerificationType	R	See VerificationType	Type of the verification data
<b>verificationEntity</b> Type: String (Numeric)	R	Length = 2	Entity performing the verification  See Table 2.47
<b>verificationEvents</b> Type: List<String (Numeric)>	O	Array of two digit codes as defined in Table 2.47	Event where the verification occurred  See Table 2.47
<b>verificationMethod</b> Type: String (Numeric)	R	Length = 2	Method of the verification  See Table 2.47
<b>verificationResults</b> Type: String (Numeric)	R	Length = 2	Result of the verification  See Table 2.47
<b>verificationTimestamp</b> Type: String (Numeric)	R	UTC time in Unix epoch format	Date and time when the verification was conducted
<b>methodResults</b> Type: JSONObject	O		Attributes associated with the authentication method (see Section 2.2.1 Authentication Facilitation)
<b>additionalData</b> Type: String	O		Data collected during the verification process

The VerificationData structure can contain data relating to various entities within the SRC Specifications. Table 2.47 provides valid values for individual attributes of the structure, depending on the type of the verification.

**Table 2.47: VerificationData Values**

<b>Verification Type</b>	<b>Verification Entity</b>	<b>Verification Event</b>	<b>Verification Method</b>	<b>Verification Results</b>
CARD	<p>Entity performing or initiating card verification. Valid values are:</p> <ul style="list-style-type: none"> <li>• 01 SRC Initiator</li> <li>• 02 SRC System</li> <li>• 03 SRCPI</li> <li>• 04 DCF</li> <li>• 05 DPA</li> <li>• 06– 20 EMVCo future use</li> <li>• 21 – 99 SRC System specific</li> </ul>	<p>Event where the verification occurred. Valid values are:</p> <ul style="list-style-type: none"> <li>• 01 – 20 EMVCo future use</li> <li>• 21 – 99 SRC System specific</li> </ul>	<p>Validates that the PAN is active and valid at the Card Issuer. Valid values are:</p> <ul style="list-style-type: none"> <li>• 01 \$0 authorisation, or single unit of currency authorisation</li> <li>• 02 Card Verification Number validation</li> <li>• 03 Postal code and address verification, where supported</li> <li>• 04 – 09 EMVCo future use</li> <li>• 10 Card Issuer Account Verification</li> <li>• 11 Card Issuer Interactive Cardholder Authentication – 1 Factor</li> <li>• 12 Card Issuer Interactive Cardholder Authentication – 2 Factor</li> <li>• 13 Card Issuer Risk Oriented Non-Interactive Cardholder Authentication</li> <li>• 14 Card Issuer Asserted Authentication</li> <li>• 15 – 20 EMVCo future use</li> <li>• 21 – 99 SRC System specific</li> </ul>	<p>Verification status of the PAN. Valid values are:</p> <ul style="list-style-type: none"> <li>• 01 Verified</li> <li>• 02 Not Verified</li> <li>• 03 Not performed</li> <li>• 04 Not Required</li> <li>• 05 – 20 EMVCo future use</li> <li>• 21 – 99 SRC System specific</li> </ul>

<b>Verification Type</b>	<b>Verification Entity</b>	<b>Verification Event</b>	<b>Verification Method</b>	<b>Verification Results</b>
CARDHOLDER	<p>Entity performing or initiating Cardholder authentication. Valid values are:</p> <ul style="list-style-type: none"> <li>• 01 SRC Initiator</li> <li>• 02 SRC System</li> <li>• 03 SRCPI</li> <li>• 04 DCF</li> <li>• 05 DPA</li> <li>• 06– 20 EMVCo future use</li> <li>• 21 – 99 SRC System specific</li> </ul>	<p>Event where the verification occurred. Valid values are:</p> <ul style="list-style-type: none"> <li>• 01 Payment transaction</li> <li>• 02 Add card/Card enrolment</li> <li>• 03 SRC Profile Access</li> <li>• 04 Account Verification</li> <li>• 05 – 20 EMVCo future use</li> <li>• 21 – 99 SRC System specific</li> </ul>	<p>Card Issuer verification of the Cardholder. Valid values are:</p> <ul style="list-style-type: none"> <li>• 01 Use of an EMV 3-D Secure ACS</li> <li>• 02 App based authentication</li> <li>• 03 Federated login systems</li> <li>• 04 A shared secret between the Card Issuer and the Cardholder such as One Time Passcode (OTP), activation code</li> <li>• 05 No authentication</li> <li>• 06 Proprietary method of authentication</li> <li>• 07 FIDO2</li> <li>• 08 SPC</li> <li>• 09 – 20 EMVCo future use</li> <li>• 21 – 99 SRC System specific</li> </ul>	<p>Indicates whether the Cardholder was verified or not, and what the results are when verified. Valid values are:</p> <ul style="list-style-type: none"> <li>• 01 Verified</li> <li>• 02 Not Verified</li> <li>• 03 Not performed</li> <li>• 04 Not required</li> <li>• 05 – 20 EMVCo future use</li> <li>• 21 – 99 SRC System specific</li> </ul>

<b>Verification Type</b>	<b>Verification Entity</b>	<b>Verification Event</b>	<b>Verification Method</b>	<b>Verification Results</b>
CONSUMER	<p>Entity performing or initiating Consumer verification. Valid values are:</p> <ul style="list-style-type: none"> <li>• 01 SRC Initiator</li> <li>• 02 SRC System</li> <li>• 03 SRCPI</li> <li>• 04 DCF</li> <li>• 05 DPA</li> <li>• 06– 20 EMVCo future use</li> <li>• 21 – 99 SRC System specific</li> </ul>	<p>Event where the verification occurred. Valid values are:</p> <ul style="list-style-type: none"> <li>• 01 – 20 EMVCo future use</li> <li>• 21 – 99 SRC System specific</li> </ul>	<p>Verification method used to verify the Consumer credential. Valid values are:</p> <ul style="list-style-type: none"> <li>• 01 Static Passcode</li> <li>• 02 SMS One Time Passcode (OTP)</li> <li>• 03 Keyfob or EMV cardreader One Time Passcode (OTP)</li> <li>• 04 Application One Time Passcode (OTP)</li> <li>• 05 One Time Passcode (OTP) Other</li> <li>• 06 Knowledge Based Authentication (KBA)</li> <li>• 07 Out of Band Biometrics</li> <li>• 08 Out of Band Login</li> <li>• 09 Out of Band Other</li> <li>• 10 Risk-Based</li> <li>• 11 Other</li> <li>• 12 FIDO2</li> <li>• 13 – 20 EMVCo future use</li> <li>• 21 – 99 SRC System specific</li> </ul>	<p>Indicates whether the Consumer was verified or not, and what the results are when verified. Valid values are:</p> <ul style="list-style-type: none"> <li>• 01 Verified</li> <li>• 02 Not Verified</li> <li>• 03 Not performed</li> <li>• 04 Not Required</li> <li>• 05 – 20 EMVCo future use</li> <li>• 21 – 99 SRC System specific</li> </ul>

<b>Verification Type</b>	<b>Verification Entity</b>	<b>Verification Event</b>	<b>Verification Method</b>	<b>Verification Results</b>
DEVICE	<p>Entity performing or initiating Device verification. Valid values are:</p> <ul style="list-style-type: none"> <li>• 01 SRC Initiator</li> <li>• 02 SRC System</li> <li>• 03 SRCPI</li> <li>• 04 DCF</li> <li>• 05 DPA</li> <li>• 06– 20 EMVCo future use</li> <li>• 21 – 99 SRC System specific</li> </ul>	<p>Event where the verification occurred. Valid values are:</p> <ul style="list-style-type: none"> <li>• 01 – 20 EMVCo future use</li> <li>• 21 – 99 SRC System specific</li> </ul>	<p>Verification method used to verify Consumer Device information. Valid values are:</p> <ul style="list-style-type: none"> <li>• 01 App Binding (App Instance ID)</li> <li>• 02 – 20 EMVCo future use</li> <li>• 21 – 99 SRC System specific</li> </ul>	<p>Indicates whether the device was verified or not, and what the results are when verified. Valid values are:</p> <ul style="list-style-type: none"> <li>• 01 Verified</li> <li>• 02 Not Verified</li> <li>• 03 Not performed</li> <li>• 04 Not Required</li> <li>• 05 – 20 EMVCo future use</li> <li>• 21 – 99 SRC System specific</li> </ul>

Verification Type	Verification Entity	Verification Event	Verification Method	Verification Results
RELATIONSHIP	<p>Entity performing or initiating relationship verification of a combination of data.</p> <p>Valid values are:</p> <ul style="list-style-type: none"><li>• 01 SRC Initiator</li><li>• 02 SRC System</li><li>• 03 SRCPI</li><li>• 04 DCF</li><li>• 05 DPA</li><li>• 06– 20 EMVCo future use</li><li>• 21 – 99 SRC System specific</li></ul>	<p>Event where the verification occurred.</p> <p>Valid values are:</p> <ul style="list-style-type: none"><li>• 01 – 20 EMVCo future use</li><li>• 21 – 99 SRC System specific</li></ul>	Verification method used to verify information associated with the relationship.	Results of the verification of the relationship of a combination of data.

### 2.1.47 UriData

**Table 2.48: UriData**

Data Element	R/C/O	Constraints	Description
<b>uri</b> Type: String	R	Max Length = 2048	URI
<b>uriType</b> Type: UriType	R	See UriType	

## 2.2 JSON Attributes

### 2.2.1 Authentication Facilitation

This section describes the JSON attributes used with the `methodAttributes` and `methodResults` data structures for the Authentication Facilitation Service (Section 5.8) and equivalent SDK methods (see SRC JavaScript SDK). Optionally, they may be used in other API services and equivalent SDK methods where authentication is required.

The contents of `methodAttributes` / `methodResults` depends on the value of `authenticationMethodType` and on the API operation / SDK method being called.

`methodAttributes` is included as follows:

- Within the Authenticate response
- As part of AuthenticationMethod within the:
  - Authentication Methods Lookup response
  - Authenticate request

`methodResults` is part of `VerificationData` which is part of `AssuranceData`, which is returned in the following:

- Authentication Methods Lookup response
- Authenticate response

When the `authenticationMethodType` is `CSC_VALIDATION` then `methodAttributes` in the `Authenticate` request is given in Table 2.49.

**Table 2.49: JSON Attributes for CSC\_VALIDATION**

Data Element	R/C/O	Constraints	Description
<b>cardSecurityCode</b> Type: String	R	Length = 3 or 4	Card Security Code

When the authenticationMethodType is one of:

- SMS OTP
- EMAIL OTP
- APP OTP

then methodAttributes in the Authenticate request is given in Table 2.50.

**Table 2.50: JSON Attributes for SMS OTP, EMAIL OTP, APP OTP**

Data Element	R/C/O	Constraints	Description
<b>otpValue</b> Type: String	R	Max Length = 16	OTP value

When the authenticationMethodType is ADDRESS\_VERIFICATION then methodAttributes in the Authenticate request is given in Table 2.51.

**Table 2.51: JSON Attributes for ADDRESS\_VERIFICATION**

Data Element	R/C/O	Constraints	Description
<b>billingAddress</b> Type: Address	R	See Address	Billing address data

When the authenticationMethodType is SPC then methodAttributes is as follows:

- Table 2.52: Authenticate response
- Table 2.53: Authenticate request

The JSON objects in Table 2.52 and Table 2.53 are defined in the W3C specification Secure Payment Confirmation (see <https://www.w3.org/TR/secure-payment-confirmation/> for more details).

**Table 2.52: JSON Attributes for SPC (Authenticate response)**

Data Element	R/C/O	Constraints	Description
<b>spcRequest</b> Type: JSONObject	R		See W3C specification Secure Payment Confirmation

**Table 2.53: JSON Attributes for SPC (Authenticate request)**

Data Element	R/C/O	Constraints	Description
<b>spcResponse</b> Type: JSONObject	R		See W3C specification Secure Payment Confirmation

When the authenticationMethodType is 3DS, then methodAttributes / methodResults contains threeDsData as shown in Table 2.54. Examples of the contents of threeDsData for various API operations / SDK methods are given below, but threeDsData may contain other data as specified in the EMV 3-D Secure Specification.

Within methodAttributes, threeDsData may contain:

- Authentication Methods Lookup response: 3DS method related data (e.g. threeDsMethodUrl<sup>1</sup>)
- Authenticate response: ACS related data if step-up is required (e.g. acsSignedContent<sup>1</sup>)

Within methodResults, threeDsData may contain data such as tranStatus and tranStatusReason when 3DS is completed:

- Authenticate response

**Table 2.54: JSON Attributes for 3DS**

Data Element	R/C/O	Constraints	Description
<b>threeDsData</b> Type: JSONObject	R		See EMV 3-D Secure Specification for detailed data objects

<sup>1</sup> These data elements are defined in EMV 3DS

When authentication is successfully completed for an authenticationsubject of CONSUMER, then methodResults in AssuranceData includes the federated identity token as shown in Table 2.55.

**Table 2.55: JSON Attributes for Consumer Authentication**

Data Element	R/C/O	Constraints	Description
<b>idtoken</b> Type: JWT	R	See Section 3 Federated Identity	Federated identity token

## 2.3 Enumerations

Note: the enumeration values set out below are not exhaustive. Other values may be added in future versions of this SRC API Specification, or may be defined within the scope of a specific implementation.

**Table 2.56: Enumerations**

Name	Valid Values
<b>AcceptanceChannelType</b>	<ul style="list-style-type: none"> <li>• EMV_MERCHANT_PRESENTED_MODE</li> </ul>
<b>AcceptanceChannelTechnology</b>	<ul style="list-style-type: none"> <li>• QR_CODE</li> </ul>
<b>Action</b>	<ul style="list-style-type: none"> <li>• ACTIVATION</li> <li>• DEACTIVATION</li> <li>• REGISTRATION</li> <li>• UPDATE</li> </ul>
<b>AdditionalAmountType</b>	<ul style="list-style-type: none"> <li>• TIP</li> <li>• CONVENIENCE_FEE</li> <li>• SUB_TOTAL</li> </ul>
<b>AddressPreference</b>	<ul style="list-style-type: none"> <li>• NONE</li> <li>• FULL</li> <li>• POSTAL_COUNTRY</li> </ul>

Name	Valid Values
<b>ApplicationType</b>	<ul style="list-style-type: none"> <li>• IOT_DEVICE</li> <li>• MOBILE_APP</li> <li>• WEB_BROWSER</li> <li>• OTHER</li> </ul>
<b>AuthenticationReason</b>	<ul style="list-style-type: none"> <li>• CARD_VERIFICATION</li> <li>• CONSUMER_IDENTITY_VALIDATION</li> <li>• ENROL_FINANCIAL_INSTRUMENT</li> <li>• TRANSACTION_AUTHENTICATION</li> </ul>
<b>AuthenticationMethodType</b>	<ul style="list-style-type: none"> <li>• SMS OTP</li> <li>• EMAIL OTP</li> <li>• APP OTP</li> <li>• 3DS</li> <li>• CSC_VALIDATION</li> <li>• APP_AUTHENTICATON</li> <li>• ADDRESS_VERIFICATION</li> <li>• FIDO2</li> <li>• SPC</li> <li>• MANAGED_AUTHENTICATION</li> </ul>
<b>AuthenticationSubject</b>	<ul style="list-style-type: none"> <li>• CARDHOLDER</li> <li>• CONSUMER</li> <li>• CARD</li> </ul>
<b>AuthenticationStatus</b>	<ul style="list-style-type: none"> <li>• COMPLETE</li> <li>• PENDING</li> <li>• PENDING_CHALLENGE</li> <li>• CANCELLED</li> <li>• EXPIRED</li> <li>• NOT_SUPPORTED</li> </ul>
<b>AuthenticationResult</b>	<ul style="list-style-type: none"> <li>• AUTHENTICATED</li> <li>• NOT_AUTHENTICATED</li> </ul>
<b>BindingStatus</b>	<ul style="list-style-type: none"> <li>• BIND</li> <li>• UNBIND</li> </ul>
<b>CardDeletionReason</b>	<ul style="list-style-type: none"> <li>• SUSPECTED_FRAUD</li> <li>• ACCOUNT_CLOSED</li> </ul>

Name	Valid Values
<b>CardPendingEvent</b>	<ul style="list-style-type: none"> <li>PENDING_AVIS</li> <li>PENDING_CSC</li> <li>PENDING_CONSUMER_IDV</li> <li>PENDING_SCA (DEPRECATED) <i>replaced by</i></li> <li>PENDING_CARDHOLDER_AUTHENTICATION</li> </ul>
<b>ComplianceType</b>	<ul style="list-style-type: none"> <li>PRIVACY_POLICY</li> <li>REMEMBER_ME</li> <li>TERMS_AND_CONDITIONS</li> <li>COOKIE</li> <li>GEOLOCATION</li> </ul>
<b>ConsumerIdentityType</b>	<ul style="list-style-type: none"> <li>EMAIL_ADDRESS</li> <li>MOBILE_PHONE_NUMBER</li> </ul>
<b>ConsumerPendingEvent</b>	<ul style="list-style-type: none"> <li>PENDING_RE_CONSENT</li> </ul>
<b>ConsumerStatus</b>	<ul style="list-style-type: none"> <li>ACTIVE</li> <li>SUSPENDED</li> <li>LOCKED</li> </ul>
<b>DcfActionCode</b>	<ul style="list-style-type: none"> <li>COMPLETE</li> <li>PENDING_AUTHENTICATION</li> <li>CHANGE_CARD</li> <li>ADD_CARD</li> <li>SWITCH_CONSUMER</li> <li>CANCEL</li> <li>ERROR</li> </ul>
<b>DeliveryMethod</b>	<ul style="list-style-type: none"> <li>NO_DELIVERY</li> <li>ADDRESS_BILLING</li> <li>ADDRESS_ON_FILE</li> <li>ADDRESS_OTHER</li> <li>PICKUP</li> <li>ELECTRONIC</li> </ul>
<b>DigitalCardFeatureContent Type</b>	<ul style="list-style-type: none"> <li>TEXT_STRING</li> <li>IMAGE_URL</li> <li>CONTENT_URL</li> <li>LINK_URL</li> </ul>

Name	Valid Values
<b>DigitalCardStatus</b>	<ul style="list-style-type: none"> <li>• ACTIVE</li> <li>• SUSPENDED</li> <li>• EXPIRED</li> <li>• PENDING</li> <li>• CANCELLED</li> </ul>
<b>DynamicDataType</b>	<ul style="list-style-type: none"> <li>• CARD_APPLICATION_CRYPTogram_SHORT_FORM</li> <li>• CARD_APPLICATION_CRYPTogram_LONG_FORM</li> <li>• DYNAMIC_CARD_SECURITY_CODE</li> <li>• CARDHOLDER_AUTHENTICATION_CRYPTogram</li> <li>• NONE</li> </ul>
<b>EnrollmentReferenceType</b>	<ul style="list-style-type: none"> <li>• SRC_DIGITAL_CARD_ID</li> <li>• SRC_PAYMENT_CARD_ID</li> <li>• COF_REFERENCE_ID</li> </ul>
<b>IdentityProvider</b>	<ul style="list-style-type: none"> <li>• SRC</li> </ul>
<b>IdentityValidationChannel Type</b>	<ul style="list-style-type: none"> <li>• EMAIL</li> <li>• SMS</li> <li>• OUT_OF_BAND</li> </ul>
<b>Origin</b>	<ul style="list-style-type: none"> <li>• CARDHOLDER</li> <li>• MERCHANT</li> <li>• ISSUER</li> </ul>
<b>PayloadTypeIndicator</b>	<ul style="list-style-type: none"> <li>• SUMMARY</li> <li>• FULL</li> <li>• PAYMENT</li> <li>• NON_PAYMENT</li> </ul>
<b>SrciActionCode</b>	<ul style="list-style-type: none"> <li>• NEW_USER</li> <li>• AUTH_FAILED</li> <li>• AUTH_SKIPPED</li> </ul>
<b>ThreeDsPreference</b>	<ul style="list-style-type: none"> <li>• NONE</li> <li>• SELF</li> <li>• ONBEHALF</li> </ul>

Name	Valid Values
<b>TransactionType</b>	<ul style="list-style-type: none"> <li>PURCHASE</li> <li>BILL_PAYMENT</li> <li>MONEY_TRANSFER</li> <li>DISBURSEMENT</li> <li>P2P</li> </ul>
<b>UriType</b>	<ul style="list-style-type: none"> <li>APP_URI</li> <li>WEB_URI</li> </ul>
<b>VerificationType</b>	<ul style="list-style-type: none"> <li>CARD</li> <li>CARDHOLDER</li> <li>CONSUMER</li> <li>DEVICE</li> <li>RELATIONSHIP</li> </ul>

## 2.4 Signed Checkout Objects

### 2.4.1 Checkout Request JWS

The Checkout Request JWS is a signed object generated by the SRC System for the SRCI front-end to pass to the DCF front-end. The SRC System can subsequently recognise/verify this JWS when it is provided by the DCF front-end in the Checkout operation.

Note: The language within the descriptions in Table 2.57 and Table 2.58 is taken directly from the relevant RFC.

**Table 2.57: Checkout Request JOSE Header**

Parameter Name	R/C/O	Description
alg	R	<p>Algorithm used to digitally sign the payload according to RFC 7518 Section 3.1:</p> <ul style="list-style-type: none"> <li>‘None’ is not supported.</li> <li>‘PS256’ is preferred to ‘RS256’ following the recommendation in RFC 3447</li> </ul>
kid	R	Key ID of the cryptographic public key of the signing SRC System.

		Relying party SHOULD use the key ID to select the appropriate key to verify the signature.  The key type of the public key identified by the key ID MUST match the type of the signing algorithm.
--	--	---

**Table 2.58: Checkout Request Claim Set**

Claim Name	Cardinality	Notes
iss	1	Value has to be URI or other identifier of the SRC System that generated this JWS. The format of the identifier is specific to SRC Programme.  Sample value of the URI: <a href="https://srcsystem1.com">https://srcsystem1.com</a>
exp	1	Expiration time in UTC and unix/epoch format. This is useful for the cases where the transaction is abandoned and the JWS can be used for one-time attack, where jti cannot help.
iat	1	Issuance time in UTC and unix/epoch format  Time at which the JWS was issued. This should not be before the current date/time.
jti	0..1	Provides a unique identifier for the JWS. The value is a case-sensitive string. This helps against replay attacks
jti_IDToken	0..1	Populated from the idToken_JWT.jti, if the authorisation is the idToken
srcInitiatorId	1	Identifier of the SRCI assigned during Onboarding Type: String
maskedCard	1	Masked Digital Card information Type: MaskedCard
maskedConsumer	0..1	Masked Consumer information Type: MaskedConsumer
maskedShippingAddresses	0..n	Array of masked shipping addresses Type: List<MaskedAddress>

Claim Name	Cardinality	Notes
authorization	0..1	First Party Token Type: String
srcCorrelationId	1	Unique identifier corresponding to the present checkout session. A new one is generated by the SRC System if not provided in the input Type: String
srciTransactionId	0..1	Transactional identifier provided by the SRCI. Populated if provided in the input Type: String
srcDpald	0..1	Identifier of the DPA. Populated if provided in the input Type: String
dpaData	0..1	Data associated with the DPA Type: DpaData
dpaTransactionOptions	1	Transaction options as provided by the DPA Type: DpaTransactionOptions
assuranceData	0..1	Assurance data related to the checkout flow. Populated if provided in the input Type: AssuranceData
checkoutRequestUri	1	The URI that the SRCI will use to invoke the DCF. This can be same as or derived from the checkoutRequestUri in the request body Type: String
checkoutResponseUri	1	The URI that the DCF will use to redirect back to the SRCI after the transaction is completed or cancelled or failed. Provided by SRCI during Onboarding Type: String
serviceId	0..1	Service identifier Type: String

Claim Name	Cardinality	Notes
payloadTypeIndicatorCheckout	0..1	Type of encrypted payload to be returned in the Checkout operation response Type: PayloadTypeIndicator
payloadTypeIndicatorPayload	0..1	Type of encrypted payload to be created for the retrieval by the Get Payload operation Type: PayloadTypeIndicator
recipientIdCheckout	0..1	Recipient identifier of the encrypted payload known to the SRC System (as provided in the Checkout operation response) for the intended recipient Type: String
recipientIdPayload	0..1	Recipient identifier of the encrypted payload known to the SRC System (as retrieved by the Get Payload operation) for the intended recipient Type: String

#### 2.4.2 Checkout Payload Response

Table 2.59 defines a data type of `CheckoutPayloadResponse`.

**Table 2.59: Checkout Payload Response**

Data Element	R/C/O	Constraints	Description
<b>srcCorrelationId</b> Type: String	C	Max Length = 256	Unique identifier generated by an SRC System  <b>Conditionality:</b> <ul style="list-style-type: none"> <li>Required for the Checkout and Make Payment operations</li> <li>Optional for the Get Payload operation</li> </ul>

Data Element	R/C/O	Constraints	Description
<b>srciTransactionId</b> Type: String	C	Max Length = 255	Transactional identifier provided by the SRCI  <b>Conditionality:</b> Required when received in the request
<b>srcDpald</b> Type: String	O	Max Length = 255	Identifier of the DPA generated by SRC System based on the previously provided dpaData or generated during the DPA Registration process
<b>dpaData</b> Type: DpaData	C	See DpaData	Data associated with the DPA  <b>Conditionality:</b> <ul style="list-style-type: none"> <li>• Required for the Make Payment operation</li> <li>• Optional for the Checkout and Get Payload operations</li> </ul>
<b>maskedConsumer</b> Type: MaskedConsumer	C	See MaskedConsumer	Masked Consumer data associated with the SRC Profile  <b>Conditionality:</b> <ul style="list-style-type: none"> <li>• Required for the Checkout and Get Payload operations if the associated SRC Profile contains Consumer data</li> <li>• Optional for the Make Payment operation</li> </ul>

Data Element	R/C/O	Constraints	Description
<b>maskedCard</b> Type: MaskedCard	C	See MaskedCard	Masked card data  <b>Conditionality:</b> <ul style="list-style-type: none"> <li>Required for the Checkout and Get Payload operations</li> <li>Optional for the Make Payment operation</li> </ul>
<b>shippingAddressZip</b> Type: String	C	Max Length = 16	Zip or postal code of selected shipping address  <b>Conditionality:</b> Required, depending on the <code>dpaShippingPreference</code> option in the <code>dpaTransactionOptions</code> structure and if either a <code>shippingAddressId</code> or <code>shippingAddress</code> object was present in the Checkout operation request
<b>shippingAddressCountryCode</b> Type: String	C	ISO 3166-1 alpha-2 country code	Country code of selected shipping address  <b>Conditionality:</b> Required, depending on the <code>dpaShippingPreference</code> option in the <code>dpaTransactionOptions</code> structure and if either a <code>shippingAddressId</code> or <code>shippingAddress</code> object was present in the Checkout operation request
<b>customOutputData</b> Type: JSONObject	O		SRC System-specific data
<b>assuranceData</b> Type: AssuranceData	O	See AssuranceData	Assurance data related to the checkout flow

Data Element	R/C/O	Constraints	Description
<b>eventHistory</b> Type: EventHistory	O	See EventHistory	Event history related to the checkout flow
<b>payload</b> Type: JWE<JWS<Payload>>  DEPRECATED	C	See Payload	<p>SRC Payload. Signed by prior to being encrypted for the specific recipient</p> <p><b>Conditionality:</b> Refer to the response definitions for the Checkout operation (see Section 5.5.2 Checkout) and the Get Payload operation (see Section 5.5.3 Get Payload)</p>
<b>encryptedSignedPayload</b> Type: JWE<JWS<Payload>>	C	See Payload	<p>SRC Payload. Signed by prior to being encrypted for the specific recipient</p> <p><b>Conditionality:</b> Refer to the response definitions for the Checkout operation (see Section 5.5.2 Checkout) and the Get Payload operation (see Section 5.5.3 Get Payload)</p> <p>encryptedSignedPayload and encryptedPayload are mutually exclusive</p>

Data Element	R/C/O	Constraints	Description
<b>encryptedPayload</b> Type: JWE<Payload>	C	See Payload	<p>SRC Payload. Encrypted for the specific recipient</p> <p><b>Conditionality:</b> Refer to the response definitions for the Checkout operation (see Section 5.5.2 Checkout) and the Get Payload operation (see Section 5.5.3 Get Payload)</p> <p>encryptedSignedPayload and encryptedPayload are mutually exclusive</p>
<b>dpaTransactionOptions</b> Type: DpaTransactionOption	O	See DpaTransactionOptions	Transaction options as provided by the DPA
<b>acceptanceChannelRelatedData</b> Type: AcceptanceChannelRelatedData	O	See AcceptanceChannelRelatedData	Data related to the acceptance channel

#### 2.4.3 JWS JOSE Header

The JWS structure for the signed data elements of type CheckoutPayloadResponse and Payload contains the protected JOSE header as specified in Table 2.60.

Note: The language within the descriptions in Table 2.60 is taken directly from the relevant RFC.

**Table 2.60: JWS JOSE Header**

Parameter Name	R/C/O	Description
alg	R	Algorithm used to digitally sign the payload according to RFC 7518 Section 3.1:

<b>Parameter Name</b>	<b>R/C/O</b>	<b>Description</b>
		<ul style="list-style-type: none"> <li>‘None’ is not supported.</li> <li>‘PS256’ is preferred to ‘RS256’ following the recommendation in RFC 3447</li> </ul>
kid	R	<p>Key ID of the cryptographic public key of the signing SRC System. Relying party SHOULD use the key ID to select the appropriate key to verify the signature.</p> <p>The key type of the public key identified by the key ID MUST match the type of the signing algorithm</p>
iss	R	<p>Issuer identifier. The value is a case sensitive URI using the https scheme that contains scheme and full qualified domain name of the host only.</p> <p>Sample value of the URI: <a href="https://srcsystem1.com">https://srcsystem1.com</a></p>
jti	R	A pseudo-random value used as nonce. The value is a case-sensitive string
iat	R	Issuance timestamp in UTC and Unix/epoch format

## 2.5 Masking Rule

All masked objects should follow the masking rules as defined in the SRC Core Specification.

## 3 Federated Identity

The concept of federated identity enables collaborating SRC Systems to reduce friction by sharing the results of a successfully validated Consumer Identity. This Section describes a federated token that supports the notion of federated digital identity and authorisation. A Federated ID Token is issued by the SRC System as a digitally signed attestation that the identity of the requestor has been validated.

### 3.1 Authorisation Token

By default, the digital authorisation is a JSON Web Token (JWT) in line with RFC 7519 and compatible with OpenID Connect ID Token.

Each token needs to be digitally signed by the SRC System that issued the token. Relying parties (e.g. other SRC Systems) need to be able to validate this token using the issuing SRC System's public key. Signature has to be compliant with JSON Web Signature (JWS) specification RFC 7515.

#### 3.1.1 Token Header

The header of the JWT has to be compliant with the JOSE Header as specified by RFC 7519. Table 3.1 describes the JOSE Header.

**Table 3.1: JOSE Header**

Parameter Name	R/C/O	Description
alg	R	<p>Algorithm used to digitally sign the payload according to RFC 7518 Section 3.1:</p> <ul style="list-style-type: none"> <li>• ‘None’ is not supported</li> <li>• ‘PS256’ is preferred to ‘RS256’ following the recommendation in RFC 3447</li> </ul>
kid	R	<p>Key ID for the SRC System public key to be used to verify the signature.</p> <p>Relying party SHOULD use the Key ID to select the appropriate key to verify the signature.</p> <p>The key type of the public key identified by the Key ID MUST match the type of the signing algorithm</p>

<b>Parameter Name</b>	<b>R/C/O</b>	<b>Description</b>
typ	R	Media type of the token. For JWT tokens the value should be <code>JWT+ext.id_token</code>

### 3.1.2 Token Claims

The Federated ID Token represents digitally signed attestation that a Consumer has been identified by an SRC System. The token contains Consumer Identities that allow other SRC Systems to identify the corresponding SRC Profile.

**Table 3.2: Federated ID Token Claim Set**

<b>Claim Name</b>	<b>Cardinality</b>	<b>Notes</b>
<b>Public Claims</b>		
iss	1	<p>Issuer identifier for the Issuer of the response.</p> <p>Identifiers MUST BE in the form of case sensitive URI using the https scheme that contains scheme and full qualified domain name of the host only.</p> <p>Sample value of the URI:  <a href="https://srcsystem1.com">https://srcsystem1.com</a></p>
sub	1	<p>Subject Identifier. A locally unique and never reassigned identifier within the Issuer for the end user (Consumer), which is intended to be consumed by the Client, e.g., 24400320 or AitOawyewNvutrJUqsvl6qs7A4.</p> <p>It MUST NOT exceed 255 ASCII characters in length. The sub value is a case sensitive string.</p> <p>SRC System-specific primary identifier of the Consumer that MAY BE used to locate Consumer's SRC Profile.</p>
aud	1..n	JSON Array of the audience(s) that this ID Token is intended for.

Claim Name	Cardinality	Notes
		<p>It MUST contain the identifier of the requestor (SRCI or DCF) as the first element of the array. It MUST also contain identifiers for participating SRC Systems as audiences.</p> <p>Identifiers MUST BE in the form of case sensitive URLs using the https scheme that contains scheme and full qualified domain name of the host only.</p> <p>Sample value of the array: ["https://srci.com", "https://srcsystem1.com", "https://srcsystem2.com", "https://srcsystem3.com"]</p>
exp	1	<p>Expiration time on or after which the ID Token SHOULD NOT be accepted for processing. The processing of this parameter requires that the current date/time MUST be before the expiration date/time listed in the value.</p> <p>Implementers MAY provide for some small leeway, usually no more than a few minutes, to account for clock skew.</p> <p>Its value is a JSON number representing the number of seconds from 1970-01-01T0:0:0Z as measured in UTC until the date/time. See RFC 3339 [RFC3339] for details regarding date/times in general and UTC in particular.</p> <p>Minimum expiration timestamp SHOULD BE 15 minutes from the issued-at timestamp.</p>
iat	1	<p>Time at which the ID Token was issued. Its value is a JSON number representing the number of seconds from 1970-01-01T0:0:0Z as measured in UTC until the date/time.</p> <p>This MAY BE before current date/time, i.e., an SRC System may cache tokens up to close to the expiration time of the token.</p>
jti	0..1	<p>The "jti" (JWT ID) claim provides a unique identifier for the JWT. The value is a case-sensitive string.</p>

Claim Name	Cardinality	Notes
auth_time	0..1	<p>Time when the end user authentication occurred. Its value is a JSON number representing the number of seconds from 1970-01-01T0:0:0Z as measured in UTC until the date/time.</p> <p>Value of the claim reflects the time when the user actually provided the credentials for authentication on this specific browser or app instance: A validated token MUST be issued if and only if a channel was validated on this specific browser or app instance.</p>
amr	0..n	<p>List of methods end user was authenticated with.</p> <p>JSON array of strings that are identifiers for authentication methods used in the authentication. For instance, values might indicate that both password and OTP authentication methods were used. The amr value is an array of case sensitive strings.</p> <p>The authentication method used when the user actually provided the credentials for authentication on this specific browser or app instance: A validated token MUST be issued if and only if a channel was validated on this specific browser or app instance.</p> <p>For the specific details of each of the values, see:</p> <p><a href="https://tools.ietf.org/html/draft-ietf-oauth-amr-values-04#page-3">https://tools.ietf.org/html/draft-ietf-oauth-amr-values-04#page-3</a></p> <p>Additional values for SRC are:</p> <ul style="list-style-type: none"> <li>• sms_otp</li> <li>• email_otp</li> <li>• merchant_rememberme</li> </ul>

Claim Name	Cardinality	Notes
<b>Standard ID Token Claims</b>		
phone_number	0..1	<p>Obfuscated end user's preferred mobile phone number. Underlying phone number value MUST conform with E.164 [E.164] format except that the leading "+" special character MUST be excluded.</p> <p>Used by Relying Party to help to identify a matching SRC Profile.</p> <p>The Relying Party MUST NOT rely upon this value being unique.</p>
phone_number_verified	0..1	<p><code>true</code> if the end user's phone number has been verified; otherwise <code>false</code>.</p> <p>When this claim value is <code>true</code>, this means that the OP (OpenID Provider) took affirmative steps to ensure that this phone number was controlled by the end user at the time the verification was performed. The means by which a phone number is verified is context-specific, and dependent upon the trust framework or contractual agreements within which the parties are operating.</p> <p>The Relying Party MUST NOT rely upon this value being unique.</p> <p>For SRC, this value MUST be <code>true</code> only if the OP can deterministically confirm that the phone number was verified by the user authenticated on this specific browser or app instance.</p>
email	0..1	<p>Obfuscated end user's preferred e-mail address. Underlying email address value MUST conform to the RFC 5322 addr-spec syntax simplified to all lowercase characters.</p> <p>Used by Relying Party to help to identify a matching SRC Profile.</p> <p>The Relying Party MUST NOT rely upon this value being unique.</p>

Claim Name	Cardinality	Notes
email_verified	0..1	<p>true if the end user's e-mail address has been verified; otherwise false.</p> <p>When this claim value is true, this means that the OP took affirmative steps to ensure that this e-mail address was controlled by the end user at the time the verification was performed. The means by which an e-mail address is verified is context-specific, and dependent upon the trust framework or contractual agreements within which the parties are operating.</p> <p>For SRC, this value MUST be true only if the OP can deterministically confirm that the email address was verified by the user authenticated on this specific browser or app instance.</p>
<b>Private Claims</b>		
src_phone_number_mask	0..1	<p>Masked Consumer mobile phone number. This MUST use E.164 format with SRC-specific masking rules.</p> <p>Used by the Relying Party to properly render the UI and allow a frictionless user experience.</p>
src_email_mask	0..1	<p>Masked Consumer e-mail address in RFC 5322 format with SRC-specific masking rules.</p> <p>Used by the Relying Party to properly render the UI and allow a frictionless user experience.</p>

### 3.1.3 Notes on Authentication

Note that:

- The auth\_time claim is not correlated with the iat claim
- The amr claim is optional. If value is not specified, the end user cannot be assumed as authenticated
- The auth\_time claim SHOULD BE present only if the amr claim is present
- The auth\_time claim MUST always represent the time at which a consumer-interactive authentication method was performed (e.g. email\_otp or sms\_otp)

- The `auth_time` claim MUST NOT represent a consumer-transparent authentication method (e.g. swk or rbd)
- The `amr` claim array MUST present authentication methods in order from oldest to most recent
- When the `amr` claim contains a list of different authentication methods the `auth_time` claim shall correspond to the most recent interactive authentication method from the `amr` list

## 4 SRCI – DCF Interaction

As part of a checkout flow, an SRCI may be required to invoke the DCF to support necessary aspects of the checkout user experience. Upon completion of these steps, the DCF can return control back to the SRCI.

The SRCI and DCF will not know each other directly, however. The URIs will be provided by the SRC System to the SRCI and the DCF to invoke each other for native or browser environments.

The following are the use cases to be addressed here:

- The recognized Consumer (with an `idToken`), card list is presented by the SRCI and the Consumer chooses a card. The appropriate DCF for that Digital Card is invoked by the SRCI using the URI provided by the SRC System
- The recognized Consumer (with an `idToken`), card list is presented by the SRCI and the Consumer chooses to add a new card. The appropriate default DCF for that SRC System is invoked by the SRCI using the URI provided by the SRC System
- The unrecognized Consumer (no `idToken`) adds a new card. The appropriate default DCF for that SRC System is invoked by the SRCI using the URI provided by the SRC System

All the above use cases should be addressed for the following:

- Browser and native (iOS/Android) use cases
- Support the following action/result scenarios from DCF to SRCI:
  - Change Consumer
  - Change Card
  - Add Card
  - Cancel Checkout
  - Successful Checkout
  - Error

### 4.1 Interaction Mechanisms

There can be various possible technical implementation approaches to support these interactions. The example flow is illustrative only to help the reader understand the concept, however actual implementations will differ due to security principles and policies.

The sequence of calls are as follows:

- SRCI front end (e.g. JavaScript from the SRCI that executes in the Consumer's browser) calls the SRC System back end to create the Checkout Request JWS and get the DCF URI
- The SRCI front end launches the DCF front end (e.g. JavaScript from the DCF that executes in the Consumer's browser) using the `checkoutRequestUri`
- After the transaction is completed, the DCF front end sends control to the SRCI using the `checkoutResponseUri` obtained from the Checkout Request JWS

## 4.2 Launch The DCF

This is the mechanism for the SRCI to launch a DCF from the given DCF URI using the Checkout Request JWS.

```
{checkoutRequestUri}?action={actionCode}&IDToken={idToken}#{checkoutRequestJws}
```

The `actionCode`, if passed from the SRCI to the DCF, is expected to be one of the following:

- NEW\_USER: if specified, will advise the DCF that the Consumer entered the flow for Enrolment
- AUTH\_FAILED: if specified, will advise the DCF that the Consumer failed identity validation with no attempts remaining
- AUTH\_SKIPPED: if specified, will advise the DCF that the Consumer chose to skip identity validation

The DCF application would need to read the Checkout Request JWS from the URI fragment using `document.location` (in case of the browser) or using native code (in case of a native mobile app). Note that the `idToken` might not be present in scenarios such as an unrecognised Consumer adding a new card.

The usage of fragment has the benefit of not having to pass the contents of Checkout Request JWS through the network.

There can be more suitable methods like Android Intents to launch the DCF for certain native environments like Android. In those cases, the implementer can choose to use those platform-specific methods.

## 4.3 Redirect back to SRCI

After the transaction is processed, the control needs to be handed back to the SRCI from the DCF.

This is done using the `checkoutResponseUri` derived from the above-mentioned JWS.

For non-error scenarios:

```
{checkoutRequestJws.checkoutResponseUri}?action={actionCode}&IDToken={idToken}#{checkoutResponse}
```

The `checkoutResponse` is the signed data element of type `CheckoutPayloadReponse` as returned by the `Checkout` operation. Note that `checkoutResponse` will be present only when the content of `actionCode` has a value of `COMPLETE`.

The `idToken` is conditional in the response URI fragment and is present only when the Consumer successfully completes identity validation and the Consumer chooses to add/change card.

There might be more suitable methods like Android Intents to redirect back to the SRCI for certain native environments like Android. In those cases, the implementer can choose to use those platform-specific methods.

The valid values of `actionCode` are as follows:

- `COMPLETE`: DCF processing completed normally
- `CHANGE_CARD`: Consumer wishes to select an alternative card
- `ADD_CARD`: Consumer wishes to add a new card
- `SWITCH_CONSUMER`: Consumer wishes to change account profile / identity
- `CANCEL`: Consumer wishes to cancel the flow
- `ERROR`: an error was detected and the DCF processing cannot continue

For error scenarios:

```
{checkoutRequestJws.checkoutResponseUri}?action=ERROR&error={errorCode}&errorDescription={errorDescription}
```

The error codes and description values are defined in Table 4.1.

**Table 4.1: Error Codes**

Name	R/C/O	Description	
<b>errorCode</b> Type: string	R	Code for the error. Used by the API client for error handling.	
		<b>Error</b>	<b>Comments</b>
		TERMS_AND_CONDITIONS_NOT_ACCEPTED	Terms and Conditions are not accepted

		ACCT_INACCESSIBLE	User account is disabled or locked out
		AUTH_INVALID	Client is not authorised to make this request
		AUTH_ERROR	Unrecognised client
		SERVICE_ERROR	Unexpected server error
		INVALID_REQUEST	This error can result when the checkoutRequestJws format or contents are invalid (due to invalid signature, etc.)
<b>errorDescription</b> Type: string	O	Description of the error message. Should not be used for display purposes since this message is not localised. However, it could be used for logging and debugging purposes.	

# 5 Server-Side API

## 5.1 API Principles

- The server-side API is designed as a set of web services where each API endpoint represents an operation to be performed
- All request and response data elements are sent in the JSON (JavaScript Object Notation) data-interchange format
- Each endpoint in the API specifies the HTTP Method used to perform the required operation
- All data elements or parameters of type String in requests and responses, or within complex data objects are UTF-8 encoded
- All actionable fields MUST be provided as part of the request parameters (path, query or body). Only meta data must be carried in the headers. This ensures that the SDK and API spec have similar function signatures and that actionable fields can be included as part of cryptographic signatures to control against data tampering as well as repudiation claims

### 5.1.1 Common HTTP Status Codes

The following common HTTP status codes are defined:

- 200: OK, the request was successful; details are included in the response body
- 202: Accepted, e.g. card details have been accepted by Enrolment service, but enrolment is outstanding, dependent upon further checks, identified by response data
- 204: No content, the service completed successfully and there is no content to be returned
- 400: Bad request, see `Error` object for details, e.g. identifies a malformed or invalid request
- 401: Unauthorised, see `Error` object for details, e.g. authorisation token validation failure
- 403: Forbidden, see `Error` object for details, e.g. client identity (origin) not validated
- 404: Not found, see `Error` object for details, e.g. the reference to the SRC Profile in the request data was not found
- 409: Conflict, see `Error` object for details, e.g. the submitted Consumer Identity(s) are already bound to an established SRC Profile
- 500: Internal server error, see `Error` object for details

### 5.1.2 Error Handling

In case an API service call response contains an HTTP error status code (4xx, 5xx), then the response body contains only an `Error` object that includes details about the error.

### 5.1.3 Conditionality of Data

Definitions of data conditionality for the APIs are provided based on successful outcomes for those APIs. In case of error outcomes, only an `error` object is returned.

### 5.1.4 Authorisation

The SRC System uses an authorisation object provided by the API client to identify if there is an existing SRC Profile on which to perform the API operation and determine whether identity validation must occur.

The SRC System supports two categories of authorisation objects:

- **Federated ID Token:** A Federated ID Token is a digitally signed attestation that the identity of the requestor has been validated by an SRC System. A Federated ID Token issued by one SRC System may be sent by the client to any other participating SRC System
- **First Party Token:** An opaque first party token issued and recognised by the same SRC System. The content and structure of these tokens is out of scope of the specification

The authorisation objects may be provided by the API client as HTTP header value, e.g. `Authorisation`, or in the body of HTTP request as explicitly defined by the respective operation, or through other mechanism depending on the integration model and specificity of the individual operation.

### 5.1.5 Recognition

The SRC System binds device/app identifiers to an SRC Profile to enable the relevant SRC Profile to be determined when device/app identifiers are provided in an API request. Once the relevant SRC Profile has been determined, the SRC System performs additional identity verification if necessary. An SRC System that recognises, and can validate, the associated Consumer Identity, returns a Federated ID Token that may be sent by the client to any other participating SRC System.

The `Is Recognized` API (Section 5.7.4) provides two mechanisms for recognising the device and/or app depending on the specific calling client:

- **Implicit cookie-based recognition:** the HTTP client (e.g. web browser) may provide a secure HTTP cookie (containing a First Party Token) in the HTTP header that enables the SRC System to identify an SRC Profile

- Explicit token-based recognition: the SRC Initiator may provide one or more `recognitionToken` JWTs explicitly in the request body.

The SRC System issues a Federated ID Token after successful verification of the tokens described above, and after any necessary additional identity validation.

### 5.1.5.1 Recognition Token JWT

The recognition token JWT represents the Device Identity bound to the specific SRC Profile. It is a first party token issued by the SRC System and is intended to be sent to the same SRC System as the explicit recognition token.

The recognition token JWT should be structured as JSON Web Token (JWT) in line with RFC 7519 and should contain at least the claim as described in Table 5.1.

Note: The language within the notes in Table 5.1 is taken directly from the relevant RFC.

**Table 5.1: Recognition Token Claim Set**

Claim Name	Cardinality	Notes
iss	1	<p>Issuer of the recognition token JWT.</p> <p>Identifiers MUST BE in the form of case sensitive URI using the https scheme that contains scheme and full qualified domain name of the host only.</p> <p>Sample value of the URI:  <a href="https://srcsystem1.com">https://srcsystem1.com</a></p>
exp	1	Expiration time of the recognition token JWT.
sub	1	<p>Subject Identifier.</p> <p>A locally unique and never reassigned identifier within the Issuer for the end user (Consumer), which is intended to be consumed by the Client, e.g., 24400320 or AitOawyewNvutruJUqsvl6qs7A4.</p> <p>It MUST NOT exceed 255 ASCII characters in length. The sub value is a case sensitive string.</p>

In addition to the claim required by this SRC API Specification, each SRC System may specify its own claims.

### 5.1.6 API Access Control

Access to all APIs must be protected using an authorisation mechanism defined by the SRC System. For server-to-server API access, mutually authenticated TLS connections are generally recommended. For browser-to-server APIs, besides the server authenticated TLS connection, SRC Systems may choose to implement additional access protection models, in order to authenticate that all incoming requests are generated by Onboarded SRC System Participants.

Refer to Annex A Security Guidelines of the SRC Core Specification for more details on the various security credentials used in TLS connections, along with different versions and cipher suites.

### 5.1.7 API Tables

In the following sections, API tables are only shown for the elements of the API which have content. For example, if an API does not have a response body, no response body table will be shown.

## 5.2 Card Service

Card Service supports Payment Card digitisation. It covers operations to enrol a card, delete a card, to add a billing address card to a previously enrolled card and to retrieve a Digital Card and related masked card data.

### 5.2.1 Card Enrolment

The Card Enrolment operation 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. Note that the Digital Card maybe associated with a specific merchant for certain use cases.

If an existing SRC Profile is identified, a Digital Card (associated with an underlying PAN) will be added to that SRC Profile. In the case that an SRC Profile cannot be identified, the SRC System will either create a new SRC Profile based on the Consumer Identity provided, or the Digital Card will be enrolled in an unbounded state. An unbound Digital Card can be bound to an SRC Profile in a subsequent Add Consumer Identities operation, leveraging a first party opaque authorisation token provided in response to this operation.

The `serviceId` can be used for extended functionality as defined by the SRC System (e.g. to indicate to the SRC System that this Digital Card is the merchant Digital Card-on-file for the merchant associated with `srcDpaId`).

**Table 5.2.1: Card Enrolment Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	POST
<b>Path</b>	/cards
<b>Parameters</b>	None

**Table 5.2.2: Card Enrolment Definition – Request Body**

Data Element	R/C/O	Notes
<b>srcClientId</b> Type: String	R	Reference identifier of the connecting client (Max length = 255)
<b>srcDpald</b> Type: String	C	Reference identifier of the DPA (Max length = 255)  Must be provided if the calling client is an SRCI
<b>srcCorrelationId</b> Type: String	C	Unique identifier generated by an SRC System (Max length = 256)  Must be provided if available within the present checkout session (e.g. received in an earlier response during the present session), otherwise a new checkout session will be initiated
<b>serviceId</b> Type: String	O	Service identifier associated to an SRC System specific configuration (Max length = 255)
<b>srciTxAuditId</b> Type: String	O	Transactional identifier provided by the SRCI (Max length = 255)
<b>srcTokenRequestData</b> Type: JSONObject	O	
<b>threeDsInputData</b> Type: JSONObject	O	Input data for 3DS processing

Data Element	R/C/O	Notes
<b>assuranceData</b> Type: AssuranceData	O	
<b>consumer</b> Type: Consumer	C	
<b>encryptedConsumer</b> Type: JWE<Consumer>	C	Either none or one of consumer or encryptedConsumer must be provided
<b>applInstance</b> Type: ApplInstance	O	
<b>digitalCardData</b> Type: DigitalCardData	O	
<b>cardholderData</b> Type: CardholderData	C	Either none or one of cardholderData or encryptedCardholderData must be provided
<b>encryptedCardholderData</b> Type: JWE<CardholderData>	C	
<b>complianceSettings</b> Type: ComplianceSettings	O	
<b>cardSource</b> Type: Origin	O	Indicates the entity performing the Enrolment
<b>card</b> Type: Card	C	
<b>encryptedCard</b> Type: JWE<Card>	C	Exactly one of "card", "srcDigitalCardId", or "encryptedCard" must be provided
<b>srcDigitalCardId</b> Type: String  DEPRECATED  <b>Replaced by</b>	C	<b>Conditionality changed to</b>  Exactly one of card, encryptedCard or enrollmentReferenceData must be provided
<b>enrollmentReferenceData</b> Type: EnrollmentReferenceData	C	

If the operation is processed successfully, the response body in Table 5.2.3 will be returned.

**Table 5.2.3: Card Enrolment Definition – Response Body**

Data Element	R/C/O	Notes
<b>srcCorrelationId</b> Type: String	O	Unique identifier generated by an SRC System (Max length = 256)
<b>maskedCard</b> Type: MaskedCard	R	
<b>maskedConsumer</b> Type: MaskedConsumer	C	Must be provided if consumer was provided in the request
<b>authorization</b> Type: String	C	Must be provided if no authorization was provided in the request
<b>appInstanceId</b> Type: String  DEPRECATED	C	Must be provided if appInstance was provided in the request
<b>recognitionToken</b> Type: JWT	C	Long-lived First Party Token representing a device or app bound to the SRC Profile (Max length = 1024)  Must be provided if appInstance was provided in the request

**Table 5.2.4: Card Enrolment Definition – HTTP Status Codes**

<b>Code</b>	<b>Description</b>
200	The operation is processed successfully and the card is enrolled
202	The operation is processed successfully, but the card is pending further checks or authentication which must be performed before Enrolment can be completed
4xx – 5xx	See Common HTTP Status Codes (Section 5.1.1)

## 5.2.2 Delete Card

The Delete Card operation deletes a Digital Card from an SRC Profile.

If the parameter `cardId` is a Payment Card Identifier provided by the SRCPI, the relationship of that identifier to Digital Cards is SRC System specific.

**Table 5.2.5: Delete Card Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	DELETE
<b>Path</b>	/cards/{cardId}
<b>Parameters</b>	<code>cardId</code> : Value: may be <code>srcDigitalCardId</code> or <code>srcPaymentCardId</code> , Required

**Table 5.2.6: Delete Card Definition – Query Parameters**

<b>Data Element</b>	<b>R/C/O</b>	<b>Notes</b>
<b>srcClientId</b> Type: String	R	Reference identifier of the connecting client (Max length = 255)
<b>srcDpald</b> Type: String	C	Reference identifier of the DPA (Max length = 255)  Must be provided if the calling client is an SRCI

Data Element	R/C/O	Notes
<b>srcCorrelationId</b> Type: String	C	Unique identifier generated by an SRC System (Max length = 256)  Must be provided if available within the present checkout session (e.g. received in an earlier response during the present session), otherwise a new checkout session will be initiated
<b>serviceId</b> Type: String	O	Service identifier associated to an SRC System specific configuration (Max length = 255)
<b>srciTransactionId</b> Type: String	O	Transactional identifier provided by the SRCI (Max length = 255)
<b>requestor</b> Type: Origin	O	Indicates the original entity requesting deletion of the card from the SRC Profile.  Note: the requestor may be different than the API client identified by the <code>srcClientId</code>
<b>reason</b> Type: CardDeletionReason	O	Reason of the card deletion request

If the operation is processed successfully, the response body in Table 5.2.7 will be returned.

**Table 5.2.7: Delete Card Definition – Response Body**

Data Element	R/C/O	Notes
<b>srcCorrelationId</b> Type: String	O	Unique identifier generated by an SRC System (Max length = 256)

**Table 5.2.8: Delete Card Definition – HTTP Status Codes**

Code	Description
200	The operation is processed successfully and the card is deleted

Code	Description
404	Not found, see <code>Error</code> object for details, e.g. content of <code>cardId</code> not recognised
4xx – 5xx	See Common HTTP Status Codes (Section 5.1.1)

### 5.2.3 Add Billing Address

The Add Billing Address operation adds a billing address to an SRC Profile.

**Table 5.2.9: Add Billing Address Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	POST
<b>Path</b>	/cards/{cardId}/address
<b>Parameters</b>	cardId: Value: <code>srcDigitalCardId</code> or <code>srcPaymentCardId</code> , Required

**Table 5.2.10: Add Billing Address Definition – Request Body**

Data Element	R/C/O	Notes
<b>srcClientId</b> Type: String	R	Reference identifier of the connecting client (Max length = 255)
<b>srcDpald</b> Type: String	C	Reference identifier of the DPA (Max length = 255)  Must be provided if the calling client is an SRCI
<b>srcCorrelationId</b> Type: String	C	Unique identifier generated by an SRC System (Max length = 256)  Must be provided if available within the present checkout session (e.g. received in an earlier response during the present session), otherwise a new checkout session will be initiated

Data Element	R/C/O	Notes
<b>serviceId</b> Type: String	O	Service identifier associated to an SRC System specific configuration (Max length = 255)
<b>srciTransactionId</b> Type: String	O	Transactional identifier provided by the SRCI (Max length = 255)
<b>billingAddress</b> Type: Address	R	
<b>setAsShippingAddress</b> Type: Boolean	O	If set to <code>true</code> , the shipping address is also created and is set to the same as the billing address

If the operation is processed successfully, the response body in Table 5.2.11 will be returned.

**Table 5.2.11: Add Billing Address Definition – Response Body**

Data Element	R/C/O	Notes
<b>srcCorrelationId</b> Type: String	O	Unique identifier generated by an SRC System (Max length = 256)
<b>maskedCard</b> Type: MaskedCard	R	
<b>maskedShippingAddress</b> Type: MaskedAddress	C	Must be provided if <code>setAsShippingAddress</code> in the request was set to <code>true</code>

**Table 5.2.12: Add Billing Address Definition – HTTP Status Codes**

Code	Description
200	The operation is processed successfully and the masked card details are included in the response body
404	Not found, see <code>error</code> object for details, e.g. the digital card referenced in the request data was not found
4xx – 5xx	See Common HTTP Status Codes (Section 5.1.1)

### 5.2.4 Get Card Data

The Get Card Data operation allows an SRC Participant to retrieve a Digital Card and related masked card data.

**Table 5.2.13: Get Card Data Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	GET
<b>Path</b>	/cards/{cardId}
<b>Parameters</b>	cardId: Value: srcDigitalCardId, Required

**Table 5.2.14: Get Card Data Definition – Query Parameters**

Data Element	R/C/O	Notes
<b>srcClientId</b> Type: String	R	Reference identifier of the connecting client (Max length = 255)
<b>srcDpalId</b> Type: String	C	Reference identifier of the DPA (Max length = 255)  Must be provided if the calling client is an SRCI
<b>srcCorrelationId</b> Type: String	C	Unique identifier generated by an SRC System (Max length = 256)  Must be provided if available within the present checkout session (e.g. received in an earlier response during the present session), otherwise a new checkout session will be initiated
<b>serviceId</b> Type: String	O	Service identifier associated to an SRC System specific configuration (Max length = 255)
<b>srcITransactionId</b> Type: String	O	Transactional identifier provided by the SRCI (Max length = 255)

If the operation is processed successfully, the response body in Table 5.2.15 will be returned.

**Table 5.2.15: Get Card Data Definition – Response Body**

Data Element	R/C/O	Notes
<b>maskedCard</b> Type: MaskedCard	R	
<b>srcCorrelationId</b> Type: String	O	Unique identifier generated by an SRC System (Max length = 256)

**Table 5.2.16: Get Card Data Definition – HTTP Status Codes**

Code	Description
200	The operation is processed successfully and the masked card meta-data is included in the response body
4xx – 5xx	See Common HTTP Status Codes (Section 5.1.1)

## 5.3 Address Service

The Address Service enables the management of shipping addresses.

### 5.3.1 Add Shipping Address

The Add Shipping Address operation adds a shipping address to an SRC Profile.

**Table 5.3.1: Add Shipping Address Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	POST
<b>Path</b>	/addresses
<b>Parameters</b>	None

**Table 5.3.2: Add Shipping Address Definition – Request Body**

Data Element	R/C/O	Notes
<b>srcClientId</b> Type: String	R	Reference identifier of the connecting client (Max length = 255)
<b>srcDpald</b> Type: String	C	Reference identifier of the DPA (Max length = 255)  Must be provided if the calling client is an SRCI
<b>srcCorrelationId</b> Type: String	C	Unique identifier generated by an SRC System (Max length = 256)  Must be provided if available within the present checkout session (e.g. received in an earlier response during the present session), otherwise a new checkout session will be initiated
<b>serviceId</b> Type: String	O	Service identifier associated to an SRC System specific configuration (Max length = 255)
<b>srciTransactionId</b> Type: String	O	Transactional identifier provided by the SRCI (Max length = 255)
<b>shippingAddress</b> Type: Address	R	

If the operation is processed successfully, the response body in Table 5.3.3 will be returned.

**Table 5.3.3: Add Shipping Address Definition – Response Body**

Data Element	R/C/O	Notes
<b>srcCorrelationId</b> Type: String	O	Unique identifier generated by an SRC System (Max length = 256)
<b>maskedShippingAddress</b> Type: MaskedAddress	R	

**Table 5.3.4: Add Shipping Address Definition – HTTP Status Codes**

<b>Code</b>	<b>Description</b>
200	The operation is processed successfully and the updated masked card details are included in the response body
4xx – 5xx	See Common HTTP Status Codes (Section 5.1.1)

### 5.3.2 Delete Shipping Address

The Delete Shipping Address operation deletes a shipping address from an SRC Profile.

**Table 5.3.5: Delete Shipping Address Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	DELETE
<b>Path</b>	/addresses/{addressId}
<b>Parameters</b>	addressId: addressId of shipping address to be deleted, Required

**Table 5.3.6: Delete Shipping Address Definition – Query Parameters**

<b>Data Element</b>	<b>R/C/O</b>	<b>Notes</b>
<b>srcClientId</b> Type: String	R	Reference identifier of the connecting client (Max length = 255)
<b>srcDpalId</b> Type: String	C	Reference identifier of the DPA (Max length = 255)  Must be provided if the calling client is an SRCI
<b>srcCorrelationId</b> Type: String	C	Unique identifier generated by an SRC System (Max length = 256)  Must be provided if available within the present checkout session (e.g. received in an earlier response during the present session), otherwise a new checkout session will be initiated

Data Element	R/C/O	Notes
<b>serviceId</b> Type: String	O	Service identifier associated to an SRC System specific configuration (Max length = 255)
<b>srciTransactionId</b> Type: String	O	Transactional identifier provided by the SRCI (Max length = 255)

If the operation is processed successfully, the response body in Table 5.3.7 will be returned.

**Table 5.3.7: Delete Shipping Address Definition – Response Body**

Data Element	R/C/O	Notes
<b>srcCorrelationId</b> Type: String	O	Unique identifier generated by an SRC System (Max length = 256)

**Table 5.3.8: Delete Shipping Address Definition – HTTP Status Codes**

Code	Description
200	The operation is processed successfully and the shipping address is deleted
404	Not found, see <code>Error</code> object for details, e.g. <code>addressId</code> not recognised
4xx – 5xx	See Common HTTP Status Codes (Section 5.1.1)

## 5.4 SRC Profile Service

The SRC Profile Service enables SRC System Participants to retrieve SRC Profiles from SRC Systems and manage binding of identities to SRC Profiles.

### 5.4.1 Prepare SRC Profile

The Prepare SRC Profile operation requests that an SRC System prepare one or more SRC Profile(s) to be returned.

**Table 5.4.1: Prepare SRC Profile Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	POST
<b>Path</b>	/profiles/prepare
<b>Parameters</b>	None

**Table 5.4.2: Prepare SRC Profile Definition – Request Body**

Data Element	R/C/O	Notes
<b>srcClientId</b> Type: String	R	Reference identifier of the connecting client (Max length = 255)
<b>srcDpald</b> Type: String	C	Reference identifier of the DPA (Max length = 255)  Must be provided if the calling client is an SRCI
<b>srcCorrelationId</b> Type: String	C	Unique identifier generated by an SRC System (Max length = 256)  Must be provided if available within the present checkout session (e.g. received in an earlier response during the present session), otherwise a new checkout session will be initiated
<b>serviceId</b> Type: String	O	Service identifier associated to an SRC System specific configuration (Max length = 255)
<b>srciTxAuditId</b> Type: String	O	Transactional identifier provided by the SRCI (Max length = 255)
<b>idTokens</b> Type: List<JWT>	C	

Data Element	R/C/O	Notes
<b>consumerIdentities</b> Type: List<ConsumerIdentity>	C	<p>Either <code>idTokens</code> or <code>consumerIdentities</code> must be provided if:</p> <ul style="list-style-type: none"> <li>The <code>idTokens</code> list carries one or more Federated ID Tokens (used to identify associated SRC Profile(s), and attest that the requester is authorised to access this data)</li> <li>The <code>consumerIdentities</code> list carries one or more Consumer Identities and is used to identify associated SRC Profile(s) (may be used only when the client is trusted and authorised to access the SRC System)</li> </ul>
<b>dpaTransactionOptions</b> Type: DpaTransactionOptions	O	
<b>dpaData</b> Type: DpaData	O	

If the operation is processed successfully, the response body in Table 5.4.3 will be returned.

**Table 5.4.3: Prepare SRC Profile Definition – Response Body**

Data Element	R/C/O	Notes
<b>srcCorrelationId</b> Type: String	O	Unique identifier generated by an SRC System (Max length = 256)
<b>profiles</b> Type: List<SrcProfile>	R	Contains entries if one or more SRC Profiles are found, otherwise an empty list is returned
<b>srcDpald</b> Type: String	C	<p>Reference identifier of the DPA (Max length = 255)</p> <p>Must be provided if the DPA Registration occurred based on the <code>dpaData</code> in the request</p>

**Table 5.4.4: Prepare SRC Profile Definition – HTTP Status Codes**

<b>Code</b>	<b>Description</b>
200	The operation is processed successfully and the SRC Profile details are included in the response body
400	Bad request, see <code>Error</code> object for details. Identifies a malformed or invalid request, including reporting that the <code>srcCorrelationId</code> provided was invalid or not recognised
4xx – 5xx	See Common HTTP Status Codes (Section 5.1.1)

### 5.4.2 Add Consumer Identities

The Add Consumer Identities operation binds a Device Identity (an application instance) or Consumer Identity to an SRC Profile.

In the case that the SRC Profile cannot be located, the SRC System may create a new SRC Profile (based on Consumer details provided in the request) if a previously enrolled unbound Digital Card exists.

The Add Consumer Identifiers operation supports Consumer Identities such as e-mail address, phone number and/or application instance information to support a range of use-cases.

When the type of a provided Consumer Identity is considered to be a primary identity for an SRC Profile (e.g. an email address or phone number), then, if the SRC System detects that an SRC Profile already exists with the same primary identity, the SRC System should respond to the request by advising that an SRC Profile with that identity already exists.

Whether or not a provided Consumer Identity is used to replace an existing identity on an existing SRC Profile is an SRC System implementation decision.

**Table 5.4.5: Add Consumer Identities Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	POST
<b>Path</b>	/profiles
<b>Parameters</b>	None

**Table 5.4.6: Add Consumer Identities Definition – Request Body**

Data Element	R/C/O	Notes
<b>srcClientId</b> Type: String	R	Reference identifier of the connecting client (Max length = 255)
<b>srcDpald</b> Type: String	C	Reference identifier of the DPA (Max length = 255)  Must be provided if the calling client is an SRCI
<b>srcCorrelationId</b> Type: String	C	Unique identifier generated by an SRC System (Max length = 256)  Must be provided if available within the present checkout session (e.g. received in an earlier response during the present session), otherwise a new checkout session will be initiated
<b>serviceId</b> Type: String	O	Service identifier associated to an SRC System specific configuration (Max length = 255)
<b>srciTxAuditId</b> Type: String	O	Transactional identifier provided by the SRCI (Max length = 255)
<b>consumer</b> Type: Consumer	C	One and only one of the following must be provided:
<b>encryptedConsumer</b> Type: JWE<Consumer>	C	<ul style="list-style-type: none"> <li>• appInstance</li> <li>• consumer</li> <li>• encryptedConsumer</li> <li>• consumer <b>and</b> appInstance</li> <li>• encryptedConsumer <b>and</b> appInstance</li> </ul>
<b>appInstance</b> Type: AppInstance	C	
<b>assuranceData</b> Type: AssuranceData	O	
<b>complianceSettings</b> Type: ComplianceSettings	O	

Data Element	R/C/O	Notes
<b>srcDigitalCardId</b> Type: String	C	Must be provided if the request is to establish a new SRC Profile and bind the identifier(s) to a previously enrolled, unbound card

If the operation is processed successfully, the response body in Table 5.4.7 will be returned.

**Table 5.4.7: Add Consumer Identities Definition – Response Body**

Data Element	R/C/O	Notes
<b>srcCorrelationId</b> Type: String	O	Unique identifier generated by an SRC System (Max length = 256)
<b>authorization</b> Type: String	C	Must be provided if consumer was provided in the request  May be provided if appInstance was provided in the request
<b>maskedConsumer</b> Type: MaskedConsumer	C	Must be provided if consumer was provided in the request
<b>appInstanceId</b> Type: String  DEPRECATED	C	<del>Must be provided if appInstance was provided in the request</del>
<b>recognitionToken</b> Type: JWT	C	Long-lived First Party Token representing a device or app bound to the SRC Profile (Max length = 1024)  Must be provided if appInstance was provided in the request

**Table 5.4.8: Add Consumer Identities Definition – HTTP Status Codes**

Code	Description
2xx – 5xx	See Common HTTP Status Codes (Section 5.1.1)

### 5.4.3 Unbind App Instance

The Unbind App Instance operation unbinds a Device Identity (an application instance) from an SRC Profile.

**Table 5.4.9: Unbind App Instance Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	DELETE
<b>Path</b>	/profile/appinstances DEPRECATED <i>Replaced by</i> /profiles/appinstances
<b>Parameters</b>	None

**Table 5.4.10: Unbind App Instance Definition – Query Parameters**

Data Element	R/C/O	Notes
<b>srcClientId</b> Type: String	R	Reference identifier of the connecting client (Max length = 255)
<b>srcDpalId</b> Type: String	C	Reference identifier of the DPA (Max length = 255)  Must be provided if the calling client is an SRCI
<b>srcCorrelationId</b> Type: String	C	Unique identifier generated by an SRC System (Max length = 256)  Must be provided if available within the present checkout session (e.g. received in an earlier response during the present session), otherwise a new checkout session will be initiated.
<b>serviceId</b> Type: String	O	Service identifier associated to an SRC System specific configuration (Max length = 255)
<b>srciTxId</b> Type: String	O	Transactional identifier provided by the SRCI (Max length = 255)

Data Element	R/C/O	Notes
<b>appInstanceId</b> Type: String  DEPRECATED	-O	A unique identifier of an app/device issued by the given SRC System. See details in Section 5.1.5 Recognition
<b>recognitionToken</b> Type: JWT	O	The explicit recognition token issued by the SRC System (Max length = 1024). See details in Section 5.1.5 Recognition

If the operation is processed successfully, the response body in Table 5.4.11 will be returned.

**Table 5.4.11: Unbind App Instance Definition – Response Body**

Data Element	R/C/O	Notes
<b>srcCorrelationId</b> Type: String	O	Unique identifier generated by an SRC System (Max length = 256)

**Table 5.4.12: Unbind App Instance Definition – HTTP Status Codes**

Code	Description
404	Not found, see Error object for details, e.g. <code>recognitionToken</code> provided in the request does not match the SRC Profile
2xx – 5xx	See Common HTTP Status Codes (Section 5.1.1)

## 5.5 Checkout Service

The Checkout Service provides Payment Data and payment related data for a specific checkout. It also allows provisioning of transaction credentials and retrieval or delivery of the `encryptedPayload` or `encryptedSignedPayload` to support a wide range of checkout use cases.

### 5.5.1 Prepare Checkout Data

The Prepare Checkout Data operation allows the SRCI to create a checkout request to fetch the DCF information along with the SRC checkout request JWS for the DCF.

The resulting `checkoutRequestJws` is signed by the SRC System and this structure needs to be passed to the SRC System for Checkout operation.

**Table 5.5.1: Prepare Checkout Data Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	POST
<b>Path</b>	/transaction/preparedata
<b>Parameters</b>	None

**Table 5.5.2: Prepare Checkout Data Definition – Request Body**

Data Element	R/C/O	Notes
<b>srcClientId</b> Type: String	R	Reference identifier of the connecting client (Max length = 255)
<b>srcDpald</b> Type: String	C	Reference identifier of the DPA (Max length = 255)  Must be provided if the calling client is an SRCI
<b>srcCorrelationId</b> Type: String	C	Unique identifier generated by an SRC System (Max length = 256)  Must be provided if available within the present checkout session (e.g. received in an earlier response during the present session), otherwise a new checkout session will be initiated
<b>serviceId</b> Type: String	O	Service identifier associated to an SRC System specific configuration (Max length = 255)
<b>srciTxnId</b> Type: String	O	Transactional identifier provided by the SRCI (Max length = 255)
<b>srcInitiatorId</b> Type: String	R	Reference identifier of the SRCI (Max length = 255)

Data Element	R/C/O	Notes
<b>payloadTypeIndicatorCheckout</b> Type: PayloadTypeIndicator	O	Type of encrypted payload to be returned in the Checkout operation response
<b>payloadTypeIndicatorPayload</b> Type: PayloadTypeIndicator	O	Type of encrypted payload to be created for the retrieval by the Get Payload operation
<b>recipientIdCheckout</b> Type: String	O	Recipient of the encrypted payload known to the SRC System (as provided in the Checkout operation response) for the intended recipient (Max length = 36)
<b>recipientIdPayload</b> Type: String	O	Recipient of the encrypted payload known to the SRC System (as retrieved by the Get Payload operation) for the intended recipient (Max length = 36)
<b>customInputData</b> Type: JSONObject	O	SRC System-specific input data
<b>srcDigitalCardId</b> Type: String	R	
<b>consumerId</b> Type: String  DEPRECATED  <i>Replaced by</i>	C	Must be provided if available within the present checkout session (e.g. received in an earlier API response during the present session)
<b>srcConsumerId</b> Type: String	C	
<b>shippingAddressIds</b> Type: List<String>	O	List of shipping address reference identifiers (each with max length = 256)
<b>authorization</b> Type: String	O	
<b>dpaTransactionOptions</b> Type: DpaTransactionOptions	R	

Data Element	R/C/O	Notes
<b>dpaData</b> Type: DpaData	O	
<b>assuranceData</b> Type: AssuranceData	O	
<b>checkoutResponseUri</b> Type: String	O	Redirection URI for the DCF (Max length = 1024)

If the operation is processed successfully, the response body in Table 5.5.3 will be returned.

**Table 5.5.3: Prepare Checkout Data Definition – Response Body**

Data Element	R/C/O	Notes
<b>srcCorrelationId</b> Type: String	R	Unique identifier generated by an SRC System (Max length = 256)
<b>checkoutRequestJws</b> Type: JWS<CheckoutRequest>	R	The definition of <code>checkoutRequestJws</code> is included in Section 2.4.1 Checkout Request JWS

**Table 5.5.4: Prepare Checkout Data Definition – HTTP Status Codes**

Code	Description
404	Not Found, see <code>Error</code> object for details. Used to indicate the checkout flow does not require redirection to a DCF and the Checkout operation can be performed instead
2xx – 5xx	See Common HTTP Status Codes (Section 5.1.1)

## 5.5.2 Checkout

The Checkout operation utilises the Consumer's chosen Digital Card and details of the current transaction to retrieve Payment Data and payment related data.

If present in the `checkoutResponse` attribute, the `encryptedPayload` or `encryptedSignedPayload` encrypted according to JSON Web Encryption (JWE) specification RFC 7516 and the algorithm used for encryption is according to RFC 7518 Section 4.1.

Note that for the Checkout operation, the content of the request body depends on whether it contains:

- The signed `checkoutRequestJws` object (Table 5.5.6)
- Only unsigned checkout request data (Table 5.5.7)

**Table 5.5.5: Checkout Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	POST
<b>Path</b>	/transaction/credentials
<b>Parameters</b>	None

**Table 5.5.6: Checkout Definition – Request Body**

Table 5.5.6 defines the request body for requests containing the signed `checkoutRequestJws` object.

Data Element	R/C/O	Notes
<b>srcClientId</b> Type: String	R	Reference identifier of the connecting client (Max length = 255)
<b>srcDpalId</b> Type: String	C	Reference identifier of the DPA (Max length = 255)  Must be provided if the calling client is an SRCI
<b>srcCorrelationId</b> Type: String	C	Unique identifier generated by an SRC System (Max length = 256)  Must be provided if available within the present checkout session (e.g. received in an earlier response during the present session), otherwise a new checkout session will be initiated
<b>serviceId</b> Type: String	O	Service identifier associated to an SRC System specific configuration (Max length = 255)

Data Element	R/C/O	Notes
<b>srciTransactionId</b> Type: String	O	Transactional identifier provided by the SRCI (Max length = 255)
<b>shippingAddressId</b> Type: String	O	Shipping address reference identifier (Max length = 256)
<b>shippingAddress</b> Type: Address	O	
<b>acceptanceChannelRelatedData</b> Type: AcceptanceChannelRelatedData	O	
<b>complianceSettings</b> Type: ComplianceSettings	O	
<b>checkoutRequestJws</b> Type: JWS<CheckoutRequest>	R	

**Table 5.5.7: Checkout Definition – Request Body**

Table 5.5.7 defines the request body for requests containing only unsigned checkout request data.

Data Element	R/C/O	Notes
<b>srcClientId</b> Type: String	R	Reference identifier of the connecting client (Max length = 255)
<b>srcDpaId</b> Type: String	C	Reference identifier of the DPA (Max length = 255)
<b>dpaData</b> Type: DpaData	C	Either <code>srcDpaId</code> or <code>dpaData</code> must be provided by the calling client when it is an SRCI

Data Element	R/C/O	Notes
<b>srcCorrelationId</b> Type: String	C	Unique identifier generated by an SRC System (Max length = 256)  Must be provided if available within the present checkout session (e.g. received in an earlier response during the present session), otherwise a new checkout session will be initiated
<b>serviceId</b> Type: String	O	Service identifier associated to an SRC System specific configuration (Max length = 255)
<b>srciTransactionId</b> Type: String	O	Transactional identifier provided by the SRCI (Max length = 255)
<b>payloadTypeIndicatorCheckout</b> Type: PayloadTypeIndicator	O	Type of encrypted payload to be returned in the Checkout operation response
<b>payloadTypeIndicatorPayload</b> Type: PayloadTypeIndicator	O	Type of encrypted payload to be created for the retrieval by the Get Payload operation
<b>recipientIdCheckout</b> Type: String	O	Recipient of the encrypted payload known to the SRC System (as provided in the Checkout operation response) for the intended recipient (Max length = 36)
<b>recipientIdPayload</b> Type: String	O	Recipient of the encrypted payload known to the SRC System (as retrieved by the Get Payload operation) for the intended recipient (Max length = 36)
<b>srcDigitalCardId</b> Type: String	R	
<b>shippingAddressId</b> Type: String	O	Shipping address reference identifier (Max length = 256)
<b>shippingAddress</b> Type: Address	O	

Data Element	R/C/O	Notes
<b>dpaTransactionOptions</b> Type: DpaTransactionOptions	C	<p>Must be provided if:</p> <ul style="list-style-type: none"> <li>• 3DS is to be performed by SRC System; or</li> <li>• Default configuration values are required to be overridden for a given transaction; or</li> </ul> <p>The calculation of Dynamic Data is dependent on knowing the transaction amount</p>
<b>acceptanceChannelRelatedData</b> Type: AcceptanceChannelRelatedData	O	
<b>assuranceData</b> Type: AssuranceData	O	
<b>complianceSettings</b> Type: ComplianceSettings	O	

If the operation is processed successfully, the response body in Table 5.5.8 will be returned.

**Table 5.5.8: Checkout Definition – Response Body**

Data Element	R/C/O	Notes
<b>checkoutResponse</b> Type: JWS<CheckoutPayloadResponse>	R	<p>encryptedPayload or encryptedSignedPayload will be not present within the checkoutResponse (see Table 2.59) when:</p> <ul style="list-style-type: none"> <li>• payloadTypeIndicatorCheckout is set to SUMMARY or</li> <li>• HTTP status code is 202</li> </ul> <p>Note that the value of payloadTypeIndicatorCheckout is either dynamically supplied in the request (query) or statically derived using the default configured during DPA Registration</p>

**Table 5.5.9: Checkout Definition – HTTP Status Codes**

<b>Code</b>	<b>Description</b>
200	The operation is processed successfully and the transaction credential response details are included in the response body
202	The operation is processed successfully and the SUMMARY payload is included in the response body. Further checks or authentication must be performed before checkout can be complete
409	Conflict, see <code>Error</code> object for details. For example, data supplied in <code>dpaTransactionOptions</code> is different from that supplied in <code>authenticationContext</code> in prior calls
4xx – 5xx	See Common HTTP Status Codes (Section 5.1.1)

### 5.5.3 Get Payload

The Get Payload operation returns Payment Data and payment related data to be used in payment authorisation.

The Get Payload operation is a server-side API intended for server-based communication.

**Table 5.5.10: Get Payload Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	GET
<b>Path</b>	/transaction/credentials
<b>Parameters</b>	None

**Table 5.5.11: Get Payload Definition – Query Parameters**

<b>Data Element</b>	<b>R/C/O</b>	<b>Notes</b>
<b>srcClientId</b> Type: String	R	Reference identifier of the connecting client (Max length = 255)

Data Element	R/C/O	Notes
<b>payloadTypeIndicator</b> Type: PayloadTypeIndicator	O	Identifies the type of encrypted payload to be returned.  A value of SUMMARY is invalid for the Get Payload operation
<b>recipientId</b> Type: String	O	Recipient of the encrypted payload known to the SRC System (as provided in the Checkout operation response) for the intended recipient (Max length = 36).  The SRC System will use this value to determine the key used for encryption of the payload
<b>srcDpald</b> Type: String	C	Reference identifier of the DPA (Max length = 255)  Must be provided if the calling client is an SRCI
<b>srcCorrelationId</b> Type: String	R	Unique identifier generated by an SRC System (Max length = 256)
<b>serviceId</b> Type: String	O	Service identifier associated to an SRC System specific configuration (Max length = 255)
<b>srciTxAuditId</b> Type: String	O	Transactional identifier provided by the SRCI (Max length = 255)

If the operation is processed successfully, the response body in Table 5.5.12 will be returned.

This request should return an HTTP Status Code of 400 indicating an invalid request when:

- payloadTypeIndicator in this request or payloadTypeIndicatorPayload in the Checkout operation or checkout() method is set to SUMMARY
- The Card has pending events which prevent a payload being returned

**Table 5.5.12: Get Payload Definition – Response Body**

Data Element	R/C/O	Notes
<b>payloadResponse</b> Type: JWS<CheckoutPayloadResponse>	R	Presence of either the encryptedPayload or encryptedSignedPayload data element within the payloadResponse (see Table 2.59) is always required

**Table 5.5.13: Get Payload Definition – HTTP Status Codes**

Code	Description
200	The operation is processed successfully and the transaction credential response details are included in the response body
4xx – 5xx	See Common HTTP Status Codes (Section 5.1.1)

#### 5.5.4 Make Payment

The Make Payment operation allows an SRC System to send payload information for authorisation purposes directly to a payment SRCI.

**Table 5.5.14: Make Payment Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	POST
<b>Path</b>	/transaction/credentials
<b>Parameters</b>	None

**Table 5.5.15: Make Payment Definition – Request Body**

Data Element	R/C/O	Notes
<b>signedTransactionCredentials</b> Type: JWS<CheckoutPayloadResponse>	R	

**Table 5.5.16: Make Payment Definition – HTTP Status Codes**

<b>Code</b>	<b>Description</b>
2xx – 5xx	See Common HTTP Status Codes (Section 5.1.1)

## 5.6 Confirmation Service

The Confirmation Service enables SRC Participants to notify the SRC System of the checkout or payment results.

### 5.6.1 Confirmation

The Confirmation operation enables SRC Participants to provide a notification of the result of a checkout service (checkout or payment authorisation).

The Confirmation operation is server-side API intended for server-based communication.

**Table 5.6.1: Confirmation Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	POST
<b>Path</b>	/confirmations
<b>Parameters</b>	None

**Table 5.6.2: Confirmation Definition – Request Body**

<b>Data Element</b>	<b>R/C/O</b>	<b>Notes</b>
<b>srcClientId</b> Type: String	R	Reference identifier of the connecting client (Max length = 255)
<b>srcDpald</b> Type: String	C	Reference identifier of the DPA (Max length = 255)  Must be provided if the calling client is an SRCI
<b>srcCorrelationId</b> Type: String	R	Unique identifier generated by an SRC System (Max length = 256)

Data Element	R/C/O	Notes
<b>serviceId</b> Type: String	O	Service identifier associated to an SRC System specific configuration (Max length = 255)
<b>srciTransactionId</b> Type: String	O	Transactional identifier provided by the SRCI (Max length = 255)
<b>assuranceData</b> Type: AssuranceData  DEPRECATED	O	
<b>customData</b> Type: JSONObject	O	
<b>confirmationData</b> Type: ConfirmationData  DEPRECATED  <i>Replaced by</i>  <b>confirmationData2</b> Type: ConfirmationData2	R	
	R	

**Table 5.6.3: Confirmation Definition – HTTP Status Codes**

Code	Description
2xx – 5xx	See Common HTTP Status Codes (Section 5.1.1)

## 5.7 Identity Service

The Identity Service enables operations related to identity recognition, validation of identity and the generation of Federated ID Tokens.

The service allows identity validation to be a two-step process encompassing initiation and completion to allow challenge/response interaction with the Consumer within the SRC experience. It is also possible that an out of band mechanism be used in which case the challenge/response within the SRC experience may not be necessary.

When requested, the SRC System should perform the validation of the identity (to verify possession) regardless of whether the Consumer Identity is associated with an SRC Profile or not.

### 5.7.1 Identity Lookup

The Identity Lookup operation utilises a provided Consumer Identity (email address or mobile phone number) to determine whether it is associated with an SRC Profile.

**Table 5.7.1: Identity Lookup Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	POST
<b>Path</b>	/identities/lookup
<b>Parameters</b>	None

**Table 5.7.2: Identity Lookup Definition – Request Body**

Data Element	R/C/O	Notes
<b>srcClientId</b> Type: String	R	Reference identifier of the connecting client (Max length = 255)
<b>serviceId</b> Type: String	O	Service identifier associated to an SRC System specific configuration (Max length = 255)
<b>consumerIdentity</b> Type: ConsumerIdentity	R	

If the operation is processed successfully, the response body in Table 5.7.3 will be returned.

**Table 5.7.3: Identity Lookup Definition – Response Body**

Data Element	R/C/O	Notes
<b>consumerPresent</b> <del>Type: Boolean</del> DEPRECATED  <i>Replaced by</i>	C	<del>consumerPresent must be provided if the specified Consumer Identity was recognised by the SRC System</del>
<b>consumerPresent1</b> Type: Boolean	R	Indicates whether the Identity Lookup operation was successful or not
<b>idLookupSessionId</b> Type: String	C	Session identifier of format UUID, returned by SRC System following an Identity Lookup operation. Can be used in subsequent Initiate Identity Validation operation
<b>consumerStatus</b> Type: ConsumerStatus	C	<del>consumerStatus, idLookupSessionId and the list of supportedValidationChannels must all be provided if the specified Consumer Identity was recognised by the SRC System</del>
<b>supportedValidationChannels</b> Type: List<IdentityValidationChannel>	C	
<b>lastUsedCardTimestamp</b> Type: String	O	

**Table 5.7.4: Identity Lookup Definition – HTTP Status Codes**

Code	Description
200	The operation is processed successfully and the lookup result is included in the response body
4xx – 5xx	See Common HTTP Status Codes (Section 5.1.1)

## 5.7.2 Initiate Identity Validation

The Initiate Identity Validation operation initiates a process to validate that a Consumer is in the possession of, or has access to, the Consumer Identity claimed.

**Table 5.7.5: Initiate Identity Validation Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	POST
<b>Path</b>	/identities/validation/initiate
<b>Parameters</b>	None

**Table 5.7.6: Initiate Identity Validation Definition – Request Body**

Data Element	R/C/O	Notes
<b>srcClientId</b> Type: String	R	Reference identifier of the connecting client (Max length = 255)
<b>serviceId</b> Type: String	O	Service identifier associated to an SRC System specific configuration (Max length = 255)
<b>idLookupSessionId</b> Type: String	C	Session identifier of format UUID, returned by SRC System following an Identity Lookup operation. Can be used in subsequent Initiate Identity Validation operation
<b>consumerIdentity</b> Type: ConsumerIdentity	C	Exactly one of consumerIdentity or idLookupSessionId must be provided
<b>requestedValidationChannel</b> Type: IdentityValidationChannel	O	

If the operation is processed successfully, the response body in Table 5.7.7 will be returned.

**Table 5.7.7: Initiate Identity Validation Definition – Response Body**

Data Element	R/C/O	Notes
<b>idValidationSessionId</b> Type: String	R	Session identifier of UUID format, returned by SRC System following an Initiate Identity Validation operation. Used in subsequent Complete Identity Validation operation

Data Element	R/C/O	Notes
<b>maskedValidationChannel</b> Type: IdentityValidationChannel	R	
<b>validationMessage</b> Type: String	O	Validation message that needs to be presented to the Consumer for step up authentication (Max length = 255)
<b>supportedValidationChannels</b> Type: List<IdentityValidationChannel>	O	
<b>uriData</b> Type: UriData	O	URI (e.g. Android App link, IOS universal link)

**Table 5.7.8: Initiate Identity Validation Definition – HTTP Status Codes**

Code	Description
200	The operation is processed successfully and the verification request results are included in the response body
404	Not Found, see <code>Error</code> object for details. Used to indicate that the identity provided was not recognised
4xx – 5xx	See Common HTTP Status Codes (Section 5.1.1)

### 5.7.3 Complete Identity Validation

The Complete Identity Validation operation 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.

**Table 5.7.9: Complete Identity Validation Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	POST
<b>Path</b>	/identities/validation/complete
<b>Parameters</b>	None

**Table 5.7.10: Complete Identity Validation Definition – Request Body**

Data Element	R/C/O	Notes
<b>srcClientId</b> Type: String	R	Reference identifier of the connecting client (Max length = 255)
<b>serviceId</b> Type: String	O	Service identifier associated to an SRC System specific configuration (Max length = 255)
<b>idValidationSessionId</b> Type: String	R	Session identifier of UUID format, returned by SRC System following an Initiate Identity Validation operation. Used in subsequent Complete Identity Validation operation
<b>validationData</b> Type: String	C	Validation data (e.g. OTP) as entered by the Consumer as a part of the step up authentication (Max length = 255)  Must be provided if type of identity validation channel was other than OUT_OF_BAND

**Table 5.7.11: Complete Identity Validation Definition – Response Headers**

<b>Header</b>	Retry-After: may be specified by the server when HTTP status code is 202.
---------------	---

If the operation is processed successfully, the response body in Table 5.7.12 will be returned.

**Table 5.7.12: Complete Identity Validation Definition – Response Body**

Data Element	R/C/O	Notes
<b>idToken</b> Type: JWT	R	
<b>maskedCard</b> Type: MaskedCard	O	MaskedCard representing the last used card

**Table 5.7.13: Complete Identity Validation Definition – HTTP Status Codes**

<b>Code</b>	<b>Description</b>
200	The operation is processed successfully, validation of identity has been successfully completed and the Federated ID Token included in the response body
202	OK, validation still in progress and no result yet available
4xx – 5xx	See Common HTTP Status Codes (Section 5.1.1)

#### 5.7.4 Is Recognized

The Is Recognized operation 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.

**Table 5.7.14: Is Recognized Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	GET
<b>Path</b>	/identities/recognize
<b>Parameters</b>	None

**Table 5.7.15: Is Recognized Definition – Query Parameters**

<b>Data Element</b>	<b>R/C/O</b>	<b>Notes</b>
<b>srcClientId</b> Type: String	R	Reference identifier of the connecting client (Max length = 255)
<b>srcDpalId</b> Type: String	C	Reference identifier of the DPA (Max length = 255)  Must be provided if the calling client is an SRCI
<b>serviceId</b> Type: String	O	Service identifier associated to an SRC System specific configuration (Max length = 255)

Data Element	R/C/O	Notes
<b>srciTransactionId</b> Type: String	O	Transactional identifier provided by the SRCI (Max length = 255)
<b>applinstanceid</b> Type: String  DEPRECATED	O	A unique identifier of an app/device issued by the given SRC System. See details in Section 5.1.5 Recognition
<b>recognitionToken</b> Type: JWT	O	An explicit recognition token issued by the SRC System. See details in Section 5.1.5 Recognition

If the operation is processed successfully, the response body in Table 5.7.16 will be returned.

**Table 5.7.16: Is Recognized Definition – Response Body**

Data Element	R/C/O	Notes
<b>srcCorrelationId</b> Type: String	O	Unique identifier generated by an SRC System (Max length = 256)
<b>idTokens</b> Type: List<JWT>	R	Each idToken in the list should be a Federated ID Token <ul style="list-style-type: none"> <li>• If the Consumer Device is recognised, a list of idTokens must be provided, one for each established SRC Profile associated to the recognised Consumer application instance</li> <li>• If the Consumer Device is not recognised, the list must be empty</li> </ul>
<b>applinstanceid</b> Type: String  DEPRECATED	C	Must be supplied if the connecting consumer application instance is recognised by the SRC System
<b>recognitionToken</b> Type: JWT	O	An explicit recognition token issued by the SRC System (Max length = 1024). See details in Section 5.1.5

Data Element	R/C/O	Notes
<b>recognitionDomainName</b> Type: String	O	A redirection to a domain that may facilitate recognition of the Consumer Device (e.g. browser or client application) by the SRC System (Max length = 256)

**Table 5.7.17: Is Recognized Definition – HTTP Status Codes**

Code	Description
200	The operation is processed successfully, the Consumer application instance was recognised and the recognition data is included in the response body
4xx – 5xx	See Common HTTP Status Codes (Section 5.1.1)

## 5.8 Authentication Facilitation Service

The Authentication Facilitation Service provides operations to enable Cardholder, Card and Consumer authentication methods to be performed. Examples include:

- OTP (SMS or email)
- 3DS authentication
- Card Security Code (CSC) validation

The Authentication Methods Lookup operation returns a list of methods that are relevant to the criteria specified by the client, which chooses one of the methods to facilitate the authentication process using the Authenticate operation.

### 5.8.1 Authentication Methods Lookup

The Authentication Methods Lookup operation obtains a proposed list of authentication methods relevant to criteria specified by the client.

**Table 5.8.1: Authentication Methods Lookup Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	POST
<b>Path</b>	/authentications/lookup

<b>Parameters</b>	None
-------------------	------

**Table 5.8.2: Authentication Methods Lookup Definition – Request Body**

Data Element	R/C/O	Notes
<b>srcClientId</b> Type: String	R	Reference identifier of the connecting client (Max length = 255)
<b>serviceId</b> Type: String	O	Service identifier associated to an SRC System specific configuration (Max length = 255)
<b>srcCorrelationId</b> Type: String	O	Unique identifier generated by an SRC System (Max length = 256)
<b>srciTransactionId</b> Type: String	O	Transactional identifier provided by the SRCI (Max length = 255)
<b>accountReference</b> Type: AccountReference	R	
<b>authenticationContext</b> Type: AuthenticationContext	R	

If the operation is processed successfully, the response body in Table 5.8.3 will be returned.

**Table 5.8.3: Authentication Methods Lookup Definition – Response Body**

Data Element	R/C/O	Notes
<b>srcCorrelationId</b> Type: String	O	Unique identifier generated by an SRC System (Max length = 256)
<b>srciTransactionId</b> Type: String	O	Transactional identifier provided by the SRCI (Max length = 255)
<b>authenticationSessionId</b> Type: String	O	
<b>assuranceData</b> Type: AssuranceData	O	

Data Element	R/C/O	Notes
<b>authenticationMethods</b> List<AuthenticationMethod>	R	List of available authentication methods

**Table 5.8.4: Authentication Methods Lookup Definition – HTTP Status Codes**

Code	Description
2xx – 5xx	See Common HTTP Status Codes (Section 5.1.1)

## 5.8.2 Authenticate

The Authenticate operation can:

- Initiate a multi-step authentication based on specified input criteria
- Complete in-band validation, passing validation data for assessment, e.g. OTP value
- Check progress / status of an on-going out-of-band validation, where validation occurs on another channel

In the final case, validation data is not supplied, but the `authenticationSessionId` provides the context.

**Table 5.8.5: Authenticate Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	POST
<b>Path</b>	/authentications/authenticate
<b>Parameters</b>	None

**Table 5.8.6: Authenticate Definition – Request Body**

Data Element	R/C/O	Notes
<b>srcClientId</b> Type: String	R	Reference identifier of the connecting client (Max length = 255)
<b>serviceId</b> Type: String	O	Service identifier associated to an SRC System specific configuration (Max length = 255)

Data Element	R/C/O	Notes
<b>srcCorrelationId</b> Type: String	O	Unique identifier generated by an SRC System (Max length = 256)
<b>srciTransactionId</b> Type: String	O	Transactional identifier provided by the SRCI (Max length = 255)
<b>authenticationSessionId</b> Type: String	C	Must be provided if available from a previously initiated authentication event
<b>accountReference</b> Type: AccountReference	C	Must be provided if authenticationSessionId is not available
<b>authenticationContext</b> Type: AuthenticationContext	C	Must be provided if authenticationSessionId is not available
<b>authenticationMethod</b> Type: AuthenticationMethod	R	

If the operation is processed successfully, the response body in Table 5.8.7 will be returned. If authentication is invoked by using `uriData` provided in `authenticationMethod`, then the data elements in the response body need to be returned asynchronously to SRC Initiator via a cross origin Post Message.

**Table 5.8.7: Authenticate Definition – Response Body**

Data Element	R/C/O	Notes
<b>srcCorrelationId</b> Type: String	O	Unique identifier generated by an SRC System (Max length = 256)
<b>srciTransactionId</b> Type: String	O	Transactional identifier provided by the SRCI (Max length = 255)
<b>authenticationSessionId</b> Type: String	R	
<b>authenticationResult</b> Type: AuthenticationResult	C	Must be provided if authenticationStatus is COMPLETE

Data Element	R/C/O	Notes
<b>authenticationStatus</b> Type: AuthenticationStatus	R	
<b>assuranceData</b> Type: AssuranceData	C	See AssuranceData  Must be provided if authenticationStatus is COMPLETE
<b>methodAttributes</b> Type: JSONObject	C	Any relevant attributes supplied by the SRC System  Must be provided as specified in Section 2.2.1 Authentication Facilitation

**Table 5.8.8: Authenticate Definition – Response Headers**

<b>Header</b>	Retry-After: may be specified by the server when HTTP status code is 202.
---------------	---

**Table 5.8.9: Authenticate Definition – HTTP Status Codes**

Code	Description
202	OK, validation still in progress and no result yet available
409	The supplied authentication method doesn't match the authentication context
2xx – 5xx	See Common HTTP Status Codes (Section 5.1.1)

## 5.9 Public Keys Retrieval Service

The Public Keys Retrieval service enables retrieval of cryptographic public keys from a well-known URI hosted by an SRC System. The keys retrieved are used by other SRC Participants for Federated ID Token and JWS signature verification.

Each SRC System must host cryptographic public keys for retrieval by other SRC Systems and SRC Participants to allow signature verification and encryption in the following cases:

- Federated ID Token is signed JWT in the form of JWS

- `checkoutRequest`, `checkoutResponse`, `payloadResponse` and (optionally) `encryptedSignedPayload` are signed in the form of JWS
- Payment Card and Consumer details presented during Enrolment can be encrypted in the form of JWE

Each SRC System must publish the cryptographic public keys on the web in well-known location to allow discovery of the keys by the relying party. Each key must be easily identifiable so it can be selected by the relying party based on the key ID ("kid") specified in the header of the JWS.

For signature verification, key retrieval and selection process for SRC Systems follows the steps below:

1. The relying party discovers the URI of the signature issuer by examining the JWS content (i.e. "iss") or using some other method.
2. The relying party retrieves the set of public keys available at the well-known path on issuer host as per issuer URI
3. The relying party examines JWS header to discover the key ID ("kid" member) and cryptographic signature algorithm ("alg" member).
4. The relying party selects the corresponding public key that matched the key ID and performs verification of the signature following the algorithm

For encryption, the recipient party should fetch the key from the well-known path based on a pre-agreed key ID.

**Note:** *Symmetric Key Retrieval is not defined in this version of the specification.*

### 5.9.1 Public Key Retrieval

The Public Key Retrieval operation retrieves a set of public keys.

**Table 5.9.1: Public Key Retrieval Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	GET
<b>Path</b>	/keys
<b>Parameters</b>	None

If the operation is processed successfully, the response body in Table 5.9.2 will be returned.

**Table 5.9.2: Public Key Retrieval Definition – Response Body**

Data Element	R/C/O	Notes
<b>keySet</b> Type: JWKS	R	<p>JSON Web Key Set (JWKS) as specified by JSON Web Key standard (RFC 7517).</p> <p>The keyset must specify at least one valid public key.</p> <p>Each key in the keyset must contain the following details:</p> <ul style="list-style-type: none"> <li>• Key ID (“kid”) used for key selection as described in the flow above</li> <li>• Key type (“kty”).</li> </ul> <p>It is also recommended to specify Key Operations (“key_ops”) with value “verify” to indicate the public key intended use.</p> <p>The key is specified as an X.509 certificate chain (“x5c”)</p>

**Table 5.9.3: Public Key Retrieval Definition – HTTP Status Codes**

Code	Description
2xx – 5xx	See Common HTTP Status Codes (Section 5.1.1)

Handling of keys used to encrypt the encryptedPayload or the encryptedSignedPayload returned by SRC Systems is out the scope of the SRC Specifications. The encryption algorithms and keys should be specified by SRC Programme.

## 5.10 Retrieve Latest Compliance Resources Service

The Retrieve Latest Compliance Resources service allows the retrieval of latest compliance resource URI for consent from a well-known URI hosted by an SRC System.

### 5.10.1 Latest Compliance Resources Retrieval

The Latest Compliance Resources Retrieval operation retrieves the latest compliance resource URI for consent from a well-known URI hosted by an SRC System.

**Table 5.10.1: Latest Compliance Resources Retrieval Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	POST
<b>Path</b>	/compliance
<b>Parameters</b>	None

**Table 5.10.2: Latest Compliance Resources Retrieval Definition – Request Body**

Data Element	R/C/O	Notes
<b>encryptedCard</b> Type: JWE<Card>	C	Either encryptedCard or srcDigitalCardId must be provided, but not both
<b>srcDigitalCardId</b> Type: String (Numeric)	C	
<b>srcClientId</b> Type: String	R	Reference identifier of the connecting client (Max length = 255)
<b>dpaLocale</b> Type: String	O	

If the operation is processed successfully, the response body in Table 5.10.3 will be returned.

**Table 5.10.3: Latest Compliance Resources Retrieval Definition – Response Body**

Data Element	R/C/O	Notes
complianceResources Type: list<ComplianceResource>	R	

**Table 5.10.4: Latest Compliance Resources Retrieval Definition – HTTP Status Codes**

<b>Code</b>	<b>Description</b>
2xx – 5xx	See Common HTTP Status Codes (Section 5.1.1)

## 5.11 Management Service

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

### 5.11.1 DPA Registration

The DPA Registration operation is provided for an SRC Initiator to register a DPA in the SRC System. After successful registration, the `srcDpaId` returned by SRC System can be used by SRC Initiator in future operations.

**Table 5.11.1: DPA Registration Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	POST
<b>Path</b>	/dpas
<b>Parameters</b>	None

**Table 5.11.2: DPA Registration Definition – Request Body**

<b>Data Element</b>	<b>R/C/O</b>	<b>Notes</b>
<b>srcInitiatorId</b> Type: String	R	Reference identifier of the SRCI (Max length = 255)
<b>serviceId</b> Type: String	O	Service identifier associated to an SRC System specific configuration (Max length = 255)
<b>action</b> Type: Action	R	

Data Element	R/C/O	Notes
<b>srcDpaID</b> Type: String	C	Reference identifier of the DPA (Max length = 255)  Must be provided if <code>action</code> is one of: <ul style="list-style-type: none"><li>• ACTIVATION</li><li>• DEACTIVATION</li><li>• UPDATE</li></ul>
<b>dpaData</b> Type: DpaData	C	Must be provided only when <code>action</code> is one of: <ul style="list-style-type: none"><li>• REGISTRATION</li><li>• UPDATE</li></ul>

If the operation is processed successfully, the response body in Table 5.11.3 will be returned.

**Table 5.11.3: DPA Registration Definition – Response Body**

Data Element	R/C/O	Notes
<b>srcDpaID</b> Type: String	R	Reference identifier of the DPA (Max length = 255)

**Table 5.11.4: DPA Registration Definition – HTTP Status Codes**

Code	Description
2xx – 5xx	See Common HTTP Status Codes (Section 5.1.1)

# 6 Notification Service

The Notification service enables outbound messages sent by the SRC System when specific events occur.

## 6.1 Notifications Principles

The notifications are sent as HTTP POST messages to the specific endpoint. The SRC System must support HTTPS and use it as default.

The SRC System maintains a registry of the SRC Participants (notification subscribers) for any given event. Each notification subscriber must be Onboarded to the SRC System and the base URIL of the notification subscriber's server provided as configuration data. The Onboarding and configuration of the notification subscribers are out of scope of this document.

Each notification defines a specific path that should be appended to the base URIL specified for the notification subscriber.

The “Success” HTTP status code indicates to the SRC System that the notification has been received, acknowledged and understood. In case of an error, client or server, the entity which contains an explanation of the error should be provided.

### 6.1.1 Data Delivery Modes

Where applicable, the following two data delivery models should be considered:

- Push Model – where the SRC System includes the data in the body of the notification. The notification subscriber receives the full set of data associated with the event that triggered the notification
- Push-Pull Model – where the SRC System only includes a specific entity identifier or session identifier (and optionally a First Party Token) in the request body of the notification. The notification subscriber willing to act on the notification received should refer to the specific API to fetch the data associated with the event that triggered the notification

The SRC System may support either one or both data delivery models.

### 6.1.2 Standard HTTP Status Codes

For the notifications the standard classes of HTTP status codes should be used by the server hosting subscriber's notification endpoint. These are described in Table 6.1.

**Table 6.1: Standard HTTP Status Codes**

<b>Code Class</b>	<b>Type</b>	<b>Description</b>
2XX	Success	This class of status codes indicates the notification was received by the subscriber, understood, accepted.
3XX	Redirection	Indicates that further action may be taken by the SRC System in order to fulfil the delivery of notification. SRC System is under no obligation to follow the actions indicated.
4XX	Client Error	Intended for cases in which the SRC System originating the notification seems to have encountered an error and therefore the subscriber's endpoint cannot acknowledge the reception of the notification.
5XX	Server Error	Indicate cases in which the subscriber's server is aware that it has encountered an error or is otherwise incapable of handling the notification.

In case of the error HTTP codes, the subscriber's server should include a standard Error entity containing an explanation of the error situation.

Support for individual HTTP codes for the classes given above is optional for the SRC System.

## 6.2 Card Update Event Notification

The Card Update Event notification sends a message to subscribers when a Digital Card's information has been modified or updated.

Each notification must specify the timestamp of the event and must contain the reason for the modification or update.

The SRC System may support two notification delivery models:

- The request body may contain the `maskedCard` object representing the updated Digital Card, or
- The request body may only contain the `srcDigitalCardId` along with the optional authorization (a First Party Token). The subscriber may then fetch the `maskedCard` object using the Get Card Data operation

**Table 6.2.1: Card Update Event Notification Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	POST
<b>Path</b>	/notifications/cards
<b>Parameters</b>	None

**Table 6.2.2: Card Update Event Notification Definition – Request Body**

Data Element	R/C/O	Notes
<b>digitalCardUpdateNotifications</b> Type: List<DigitalCardUpdateNotification>	R	

**Table 6.2.3: Card Update Event Notification Definition – HTTP Status Codes**

Code	Description
204	No Content, the subscriber acknowledges the receipt of the notification
400	Bad Request, the request body has been malformed or otherwise prohibits the subscriber to process the notification
2xx – 5xx	See Standard HTTP Status Codes (Section 6.1.2)

## 6.3 Identity Validation Completion Event Notification

The Identity Validation Complete 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.

The SRC System may support two notification delivery models:

- The request body may contain a Federated ID Token; or
- The request body may contain an `idValidationSessionId` along with the optional authorization (a First Party Token). The subscriber may fetch the Federated ID Token using the Complete Identity Validation operation

**Table 6.3.1: Identity Validation Completion Event Notification Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	POST
<b>Path</b>	/notifications/identities/validation/complete
<b>Parameters</b>	None

**Table 6.3.2: Identity Validation Completion Event Notification Definition – Request Body**

Data Element	R/C/O	Notes
<b>idValidationSessionId</b> Type: String	R	Session identifier of UUID format, returned by SRC System following an Initiate Identity Validation operation. Used in subsequent Complete Identity Validation operation
<b>idToken</b> Type: JWT  <b>error</b> Type: Error	C  C	Either <code>idToken</code> or <code>error</code> must be provided if the subscriber is configured in the push model
<b>maskedCard</b> Type: MaskedCard	O	MaskedCard representing the last used card
<b>authorization</b> Type: String	O	

**Table 6.3.3: Identity Validation Completion Event Notification Definition – HTTP Status Codes**

Code	Description
204	No Content, the subscriber acknowledges the receipt of the notification
400	Bad Request, the request body has been malformed or otherwise prohibits the subscriber to process the notification

Code	Description
2xx – 5xx	See Standard HTTP Status Codes (Section 6.1.2)

## 6.4 Authentication Event Notification

The Authentication Event Notification sends a message to subscribers when an authentication event is completed (`authenticationStatus` is set to COMPLETE).

**Table 6.4.1: Authentication Event Notification Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	POST
<b>Path</b>	/notifications/authentications
<b>Parameters</b>	None

**Table 6.4.2: Authentication Event Notification Definition – Request Body**

Data Element	R/C/O	Notes
<b>authenticationSessionId</b> Type: String	R	
<b>srcCorrelationId</b> Type: String	O	Unique identifier generated by an SRC System (Max length = 256)
<b>srciTransactionId</b> Type: String	O	Transactional identifier provided by the SRCI (Max length = 255)
<b>authenticationResult</b> Type: AuthenticationResult	C	Must be provided if <code>authenticationStatus</code> is COMPLETE
<b>authenticationStatus</b> Type: Authenticationstatus	R	
<b>assuranceData</b> Type: AssuranceData	C	See AssuranceData Must be provided if <code>authenticationStatus</code> is COMPLETE

**Table 6.4.3: Authentication Event Notification Definition – HTTP Status Codes**

<b>Code</b>	<b>Description</b>
204	No Content, the subscriber acknowledges the receipt of the notification
400	Bad Request, the request body has been malformed or otherwise prohibits the subscriber to process the notification
2xx – 5xx	See Standard HTTP Status Codes (Section 6.1.2)

## 6.5 Payment Notification

The Payment Notification sends a message to subscribers when an SRC System has received a confirmation of payment authorisation.

Each Payment Notification must specify the timestamp of the payment completion event and must contain the status of the payment authorisation.

**Table 6.5.1: Payment Notification Definition – HTTP Verb, Path and Parameters**

<b>HTTP Verb</b>	POST
<b>Path</b>	/notifications/payment
<b>Parameters</b>	None

**Table 6.5.2: Payment Notification Definition – Request Body**

<b>Data Element</b>	<b>R/C/O</b>	<b>Notes</b>
<b>srcCorrelationId</b> Type: String	R	Unique identifier generated by an SRC System (Max length = 256)
<b>srciTransactionId</b> Type: String	O	Transactional identifier provided by the SRCI (Max length = 255)
<b>serviceId</b> Type: String	O	Service identifier associated to an SRC System specific configuration (Max length = 255)

Data Element	R/C/O	Notes
<b>srcDigitalCardId</b> Type: String	O	
<b>confirmationData2</b> Type: ConfirmationData2	R	
<b>customData</b> Type: JSONObject	O	

**Table 6.5.3: Payment Notification Definition – HTTP Status Codes**

Code	Description
204	No Content, the subscriber acknowledges the receipt of the notification
400	Bad Request, the request body has been malformed or otherwise prohibits the subscriber to process the notification
4xx – 5xx	See Standard HTTP Status Codes (Section 6.1.2)

## Annex A EMVCo Specification Mapping

This Annex describes the mapping of data from other EMVCo specifications to these SRC Specifications. It provides a level of interoperability for an implementation using another EMVCo specification to use SRC to process such a transaction.

### A.1 Merchant-Presented Mode – QR Code Payload

Annex A.1 describes the mapping of data from the QR Code Payload described in the Merchant-Presented Mode specification (EMV® QR Code Specification for Payment Systems (EMV QRCPS) – Merchant-Presented Mode). As per the Merchant-Presented Mode specification, this describes any conversion of data necessary as well as any additional data needed to process the transaction.

The mapping is described from the perspective of the Mobile Application consuming a QR Code Payload and building the SRC data elements to be populated to SRC API input parameters and SRC JavaScript SDK attributes. The descriptions below all assume that the QR Code Payload complies with the Merchant-Presented Mode specification.

#### A.1.1 SRC Data Elements

The following SRC data elements, parameters, objects or attributes are populated with Merchant-Presented Mode QR specific data. Based on the mapping described, when processing a Merchant-Presented Mode QR Code payment transaction using SRC, `acceptanceChannelRelatedData` is a required input parameter or attribute in the relevant SRC API operation or SRC JavaScript SDK method.

##### Transaction Amount

The `transactionAmount` data element of the `TransactionAmount` object is populated with:

- The transaction amount; or
- When there is also a tip or convenience fee (see Annex A.1.4 QR Code Specific Data Elements for Additional Amounts), the sum of the transaction amount and the tip or convenience fee

The value of the transaction amount is dependent on the presence of the Transaction Amount (ID “54”) in the QR Code Payload.

- If present, the transaction amount referred to above is the value present in Transaction Amount (ID “54”) in the QR Code Payload

- If not present, the transaction amount referred to above is the Consumer-entered amount

### **Transaction Currency**

The `transactionCurrency` data element of the `TransactionAmount` object is populated with the Transaction Currency (ID “53”) in the QR Code Payload.

### **Acceptance Channel Type**

The `acceptanceChannelType` data element of the `AcceptanceChannelRelatedData` object is populated with the value of `EMV_MERCHANT_PRESENTED_MODE`

### **Acceptance Channel Technology**

The `acceptanceChannelTechnology` data element of the `AcceptanceChannelRelatedData` object is populated with the value of `QR_CODE`.

### **Digital Payment Application Data**

The `merchantAccountInformation` data element of the `DpaData` object is populated with the Merchant Account Information (IDs “02” to “51”) of the QR Code Payload. It is only necessary to populate the content of the ID relevant to the receiving SRC System, which is based on which SRC System maintains the Digital Card selected for the specific transaction:

- ID “02” or “03” for the Visa SRC System
- ID “04” and “05” for the Mastercard SRC System
- ID “09” or “10” for the Discover SRC System
- ID “11” and “12” for the Amex SRC System
- ID “13” or “14” for the JCB SRC System
- ID “15” and “16” for the Union Pay SRC System

## **A.1.2 QR Code specific Data Elements for Seller Data**

The following data element is defined specifically for the `sellerData` object which is a data element of the `AcceptanceChannelData` object (see Table 2.1).

### **QR Code Payload**

Always populated with the full content of the QR Code Payload.

**Table A.1: SRC API Usage for QR Code Payload**

<b>qrCodePayload</b>	
Type	String
Constraint	Maximum length of 2048
Present in object	sellerData

### A.1.3 QR Code specific Data Elements for Consumer Data

The following data elements are defined specifically for the `consumerData` object which is a data element of the `AcceptanceChannelData` object (see Table 2.1). Consumer Data will only be present and populated if one or more of the following data objects are indicated within the QR Code Payload

#### **Bill Number**

Populated with a Consumer-entered bill number if the Bill Number (ID “01”), with a value of “\*\*\*”, is present within the Additional Data Field Template (ID “62”) of the QR Code Payload.

**Table A.2: SRC API Usage for Bill Number**

<b>billNumber</b>	
Type	String
Constraint	Maximum length of 25
Present in object	consumerData

#### **Mobile Number**

Populated with a Consumer-entered mobile number if the Mobile Number (ID “02”), with a value of “\*\*\*”, is present within the Additional Data Field Template (ID “62”) of the QR Code Payload.

**Table A.3: SRC API Usage for Mobile Number**

<b>mobileNumber</b>	
Type	String
Constraint	Maximum length of 25
Present in object	consumerData

**Store Label**

Populated with a Consumer-entered store label if the Store Label (ID “03”), with a value of “\*\*\*”, is present within the Additional Data Field Template (ID “62”) of the QR Code Payload.

**Table A.4: SRC API Usage for Store Label**

<b>storeLabel</b>	
Type	String
Constraint	Maximum length of 25
Present in object	consumerData

**Loyalty Number**

Populated with a Consumer-entered loyalty number if the Loyalty Number (ID “04”), with a value of “\*\*\*”, is present within the Additional Data Field Template (ID “62”) of the QR Code Payload.

**Table A.5: SRC API Usage for Loyalty Number**

<b>loyaltyNumber</b>	
Type	String
Constraint	Maximum length of 25
Present in object	consumerData

**Reference Label**

Populated with a Consumer-entered reference label if the Reference Label (ID “05”), with a value of “\*\*\*”, is present within the Additional Data Field Template (ID “62”) of the QR Code Payload.

**Table A.6: SRC API Usage for Reference Label**

<b>referenceLabel</b>	
Type	String
Constraint	Maximum length of 25
Present in object	consumerData

**Customer Label**

Populated with a Consumer-entered Customer label if the Customer Label (ID “06”), with a value of “\*\*\*”, is present within the Additional Data Field Template (ID “62”) of the QR Code Payload.

**Table A.7: SRC API Usage for Customer Label**

<b>customerLabel</b>	
Type	String
Constraint	Maximum length of 25
Present in object	consumerData

**Terminal Label**

Populated with a Consumer-entered terminal label if the Terminal Label (ID “07”), with a value of “\*\*\*”, is present within the Additional Data Field Template (ID “62”) of the QR Code Payload.

**Table A.8: SRC API Usage for Terminal Label**

<b>terminalLabel</b>	
Type	String
Constraint	Maximum length of 25

<b>terminalLabel</b>	
Present in object	consumerData

### **Purpose of Transaction**

Populated with a Consumer-entered transaction purpose if the Purpose of Transaction (ID “08”), with a value of “\*\*\*”, is present within the Additional Data Field Template (ID “62”) of the QR Code Payload.

**Table A.9: SRC API Usage for Purpose of Transaction**

<b>purposeOfTransaction</b>	
Type	String
Constraint	Maximum length of 25
Present in object	consumerData

### **Email**

Populated with an email known to the Mobile Application if the Additional Consumer Data Request (ID “09”), with a value containing the character “E”, is present within the Additional Data Field Template (ID “62”) of the QR Code Payload.

**Table A.10: SRC API Usage for Email**

<b>email</b>	
Type	String
Constraint	Maximum length of 255
Present in object	consumerData

### **Phone Number**

Populated with an mobile number known to the Mobile Application if the Additional Consumer Data Request (ID “09”), with a value containing the character “M”, is present within the Additional Data Field Template (ID “62”) of the QR Code Payload.

**Table A.11: SRC API Usage for Phone Number**

<b>phoneNumber</b>	
Type	String
Constraint	A length ranging from 4 to 14
Present in object	consumerData

**Address**

Populated with an address known to the Mobile Application if the Additional Consumer Data Request (ID “09”), with a value containing the character “A”, is present within the Additional Data Field Template (ID “62”) of the QR Code Payload.

**Table A.12: SRC API Usage for Address**

<b>address</b>	
Type	String
Constraint	Maximum length of 2048
Present in object	consumerData

**A.1.4 QR Code Specific Data Elements for Additional Amounts**

The following data elements are defined specifically for the `additionalAmounts` list which is a data element the `TransactionAmount` object (see Table 2.45).

**Tip**

A floating-point number only populated with a Consumer-entered tip value if Tip or Convenience Indicator (ID “55”), containing a value of “01”, is present within the QR Data Payload.

If present with the relevant value, populate an entry of the `additionalAmounts` list with the values in Table A.13.

**Table A.13: SRC API Usage for Tip**

Data Element	Value
additionalAmountType	TIP
additionalAmountValue	Consumer entered tip value

**Convenience Fee**

A floating-point number only populated if the Tip or Convenience Indicator (ID “55”), containing a value of “02” or “03”, is present within the QR Data Payload.

If present with the relevant values, populate an entry of the `additionalAmounts` list with the values in Table A.14.

**Table A.14: SRC API Usage for Convenience Fee**

Data Element	Value
additionalAmountType	CONVENIENCE_FEE
additionalAmountValue	If the value of ID “55” is: <ul style="list-style-type: none"> <li>• “02” then populate with the content of the Value of Convenience Fee Fixed (ID “56”) present within the QR Data Payload (converted to a floating-point number)</li> <li>• “03” then populate with a Mobile Application calculated value, equal to a percentage of the Sub Total. The percentage used for the calculation is the Convenience Fee Percentage (ID “57”) value present in the QR Code Payload</li> </ul>

**Sub Total**

A floating-point number only populated if one of the above `tip` or `convenienceFee` data elements is populated.

If a `tip` or `convenienceFee` data elements is populated, then populate an entry of the `additionalAmounts` list with the values in Table A.15.

**Table A.15: SRC API Usage for Sub Total**

Data Element	Value
additionalAmountType	SUB_TOTAL
additionalAmountValue	Either the: <ul style="list-style-type: none"><li>• Transaction Amount (ID “54”) if present in the QR Code Payload (converted to a floating-point number); or</li><li>• Consumer-entered amount if the Transaction Amount (ID “54”) is not present in the QR Code Payload</li></ul>

## Annex B 3DS Data

This Annex describes the additional data elements required specifically for 3DS Input Data and 3DS Output Data when `threeDsPreference` in `DpaTransactionOptions` is set to `ONBEHALF`.

Note: data elements defined in this Annex may be duplicates of data elements defined elsewhere in this specification.

### B.1 3DS Input Data

The `threeDsInputData` object is defined as `JSONObject` type and is populated with the data elements as defined in the 3DS Specification. This includes, but is not necessarily limited to, those data elements shown in Table B.1.

**Table B.1: 3DS Input Data**

Name	Constraints	Description
<b>acquirerMerchantId</b> Type: String	Max Length = 35	Acquirer-assigned merchant identifier. This may be the same value that is used in authorisation requests sent on behalf of the 3DS Requestor and is represented in ISO 8583 formatting requirements
<b>acquirerBIN</b> Type: String	Max Length = 11	Acquiring institution identification code as assigned by the DS receiving the AReq message
<b>merchantName</b> Type: String	Max Length = 40	Merchant name assigned by the Acquirer or Payment System
<b>merchantCategoryCode</b> Type: String	Length = 4	Describes the merchant's type of business, product or service (mcc)

Name	Constraints	Description
<b>merchantCountryCode</b> Type: String	ISO 3166-1alpha-2 country code	Country code of the merchant

## B.2 3DS Output Data

The `threeDsOutputData` object of the `Payload` object is defined as `JSONObject` type and is populated with data elements as defined in the 3DS Specification. This includes, but is not necessarily limited to, the data elements shown in Table B.2.

**Table B.2: 3DS Output Data**

Name	Constraints	Description
<b>authenticationValue</b> Type: String	Max Length = 28 A 20-byte value that has been BASE64 encoded	Payment System-specific value provided by the ACS or the DS using an algorithm defined by the Payment System.  Authentication Value may be used to provide proof of authentication
<b>eci</b> Type: String	Max Length = 2	Payment System-specific value provided by the ACS or the DS to indicate the results of the attempt to authenticate the Cardholder
<b>transStatus</b> Type: String	Max Length = 1 See 3DS Specification for more details	Indicates whether a transaction qualifies as an authenticated transaction or account verification
<b>transStatusReason</b> Type: String	Max Length = 2 See 3DS Specification for more details	Provides information on why the Transaction Status field has the specified value

Name	Constraints	Description
<b>dsTransId</b> Type: String	Max Length = 36	Universally unique transaction identifier assigned by the DS to identify a single transaction
<b>acsTransId</b> Type: String	Max Length = 36	Universally unique transaction identifier assigned by the ACS to identify a single transaction

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