EMV® Secure Remote Commerce

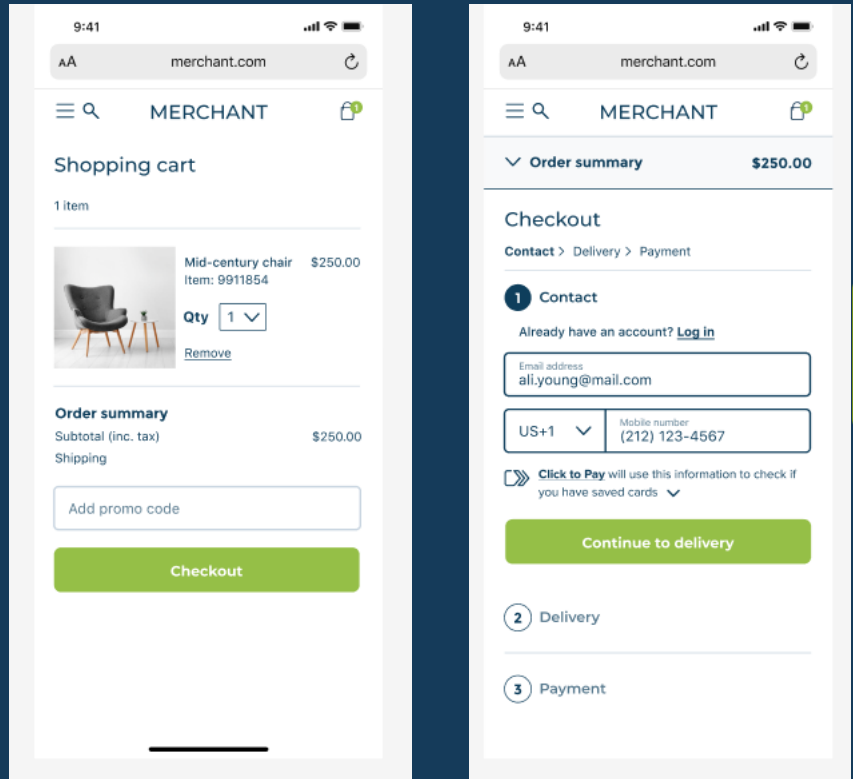Clinton Allen, Chair, SRCWG

WPWG Remote Meetings

Separate Recognition from Authentication
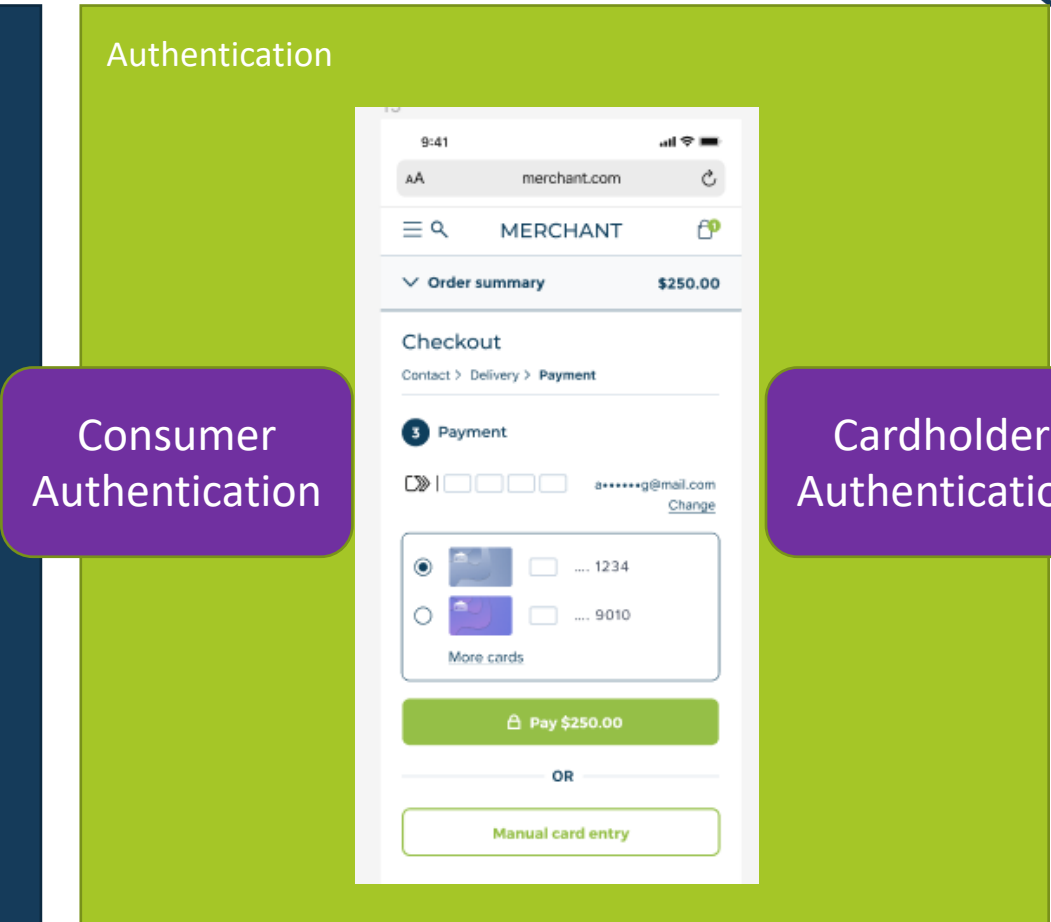

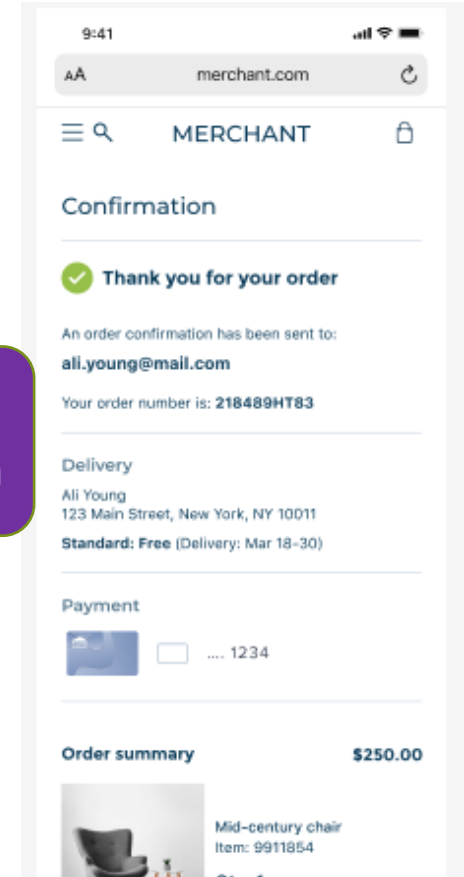Recognition
- Cookie
- Recognition Domain
- FedCM?

Consumer Authentication
- SMS_OTP
- EMAIL_OTP
- APP_OTP

Cardholder Authentication
- 3DS
- WebAuthn
- SPC

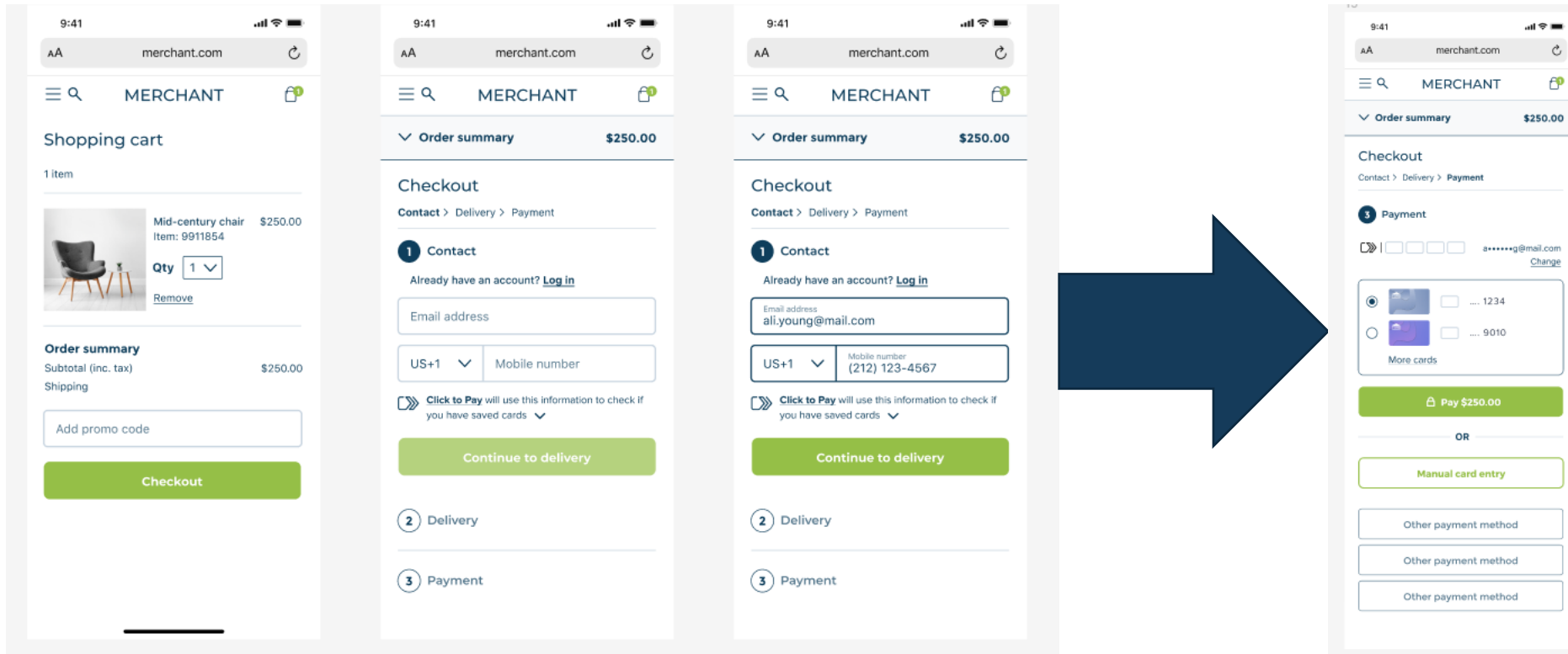# EMVCo / W3C Payment Related Objectives

- **Recognition**
  - Domain Based Recognition (Recognition Domain)
  - FedCM
- **Authentication**
  - SRC + SPC
    - UI/UX Screens
    - Sequence Diagram
  - SRC + WebAuthn
    - UI/UX Screens
    - Sequence Diagram

Recognition

Domain

FedCM

Recognition - Without Recognition Support from Browser

No Ability to Recognize a Consumer
- No Cookie Access
- No Browser Based Identification

Continue Checkout
- Assume no Consumer Authentication
- Assume no Shipping
- Select Card Complete Checkout

Recognition – With Recognition Support from Browser
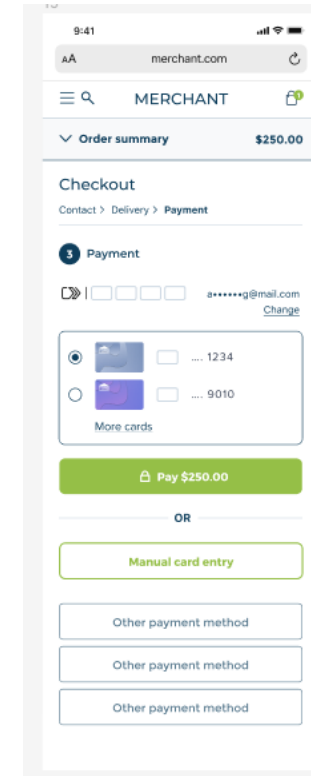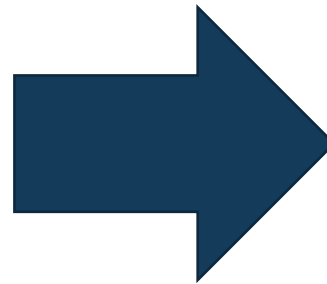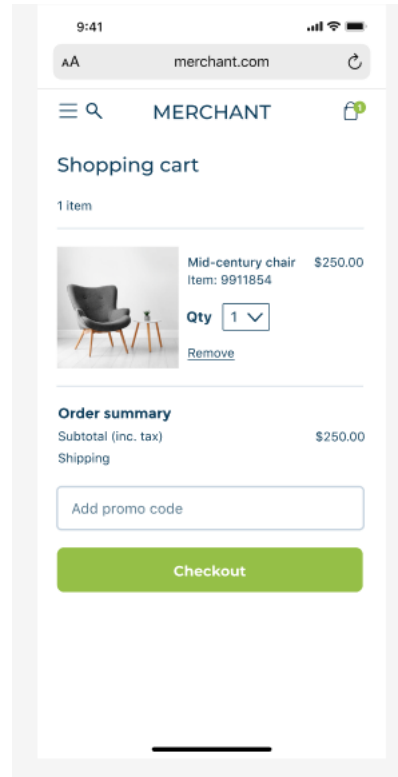
No Ability to Recognize a Consumer
- Recognition Domain
- FedCM?

Continue Checkout
- Assume no Consumer Authentication
- Assume no Shipping
- Select Card Complete Checkout

Recognition – Options

EMVCo.

First Checkout ➡ **Store Recognition Information**

Cross Origin Recognition
- Device based
- Works across multiple Merchants (Domains)
- Required 3rd Party Cookie Access

Domain Recognition
- Device based
- Works across multiple Merchants (Domains)
- 3rd Party Cookie Access NOT required

Fed CM
- Federated Credential Management allows users to login to websites with their federated accounts in a privacy preserving manner

Merchant Recognition
- Device based
- Works within a single Merchant (Domain)
- 3rd Party Cookie Access NOT required

Retrieve Recognition Information ➡ Second Checkout

Recognition - Consumer Experience with Checkout

Horizontal Recognition
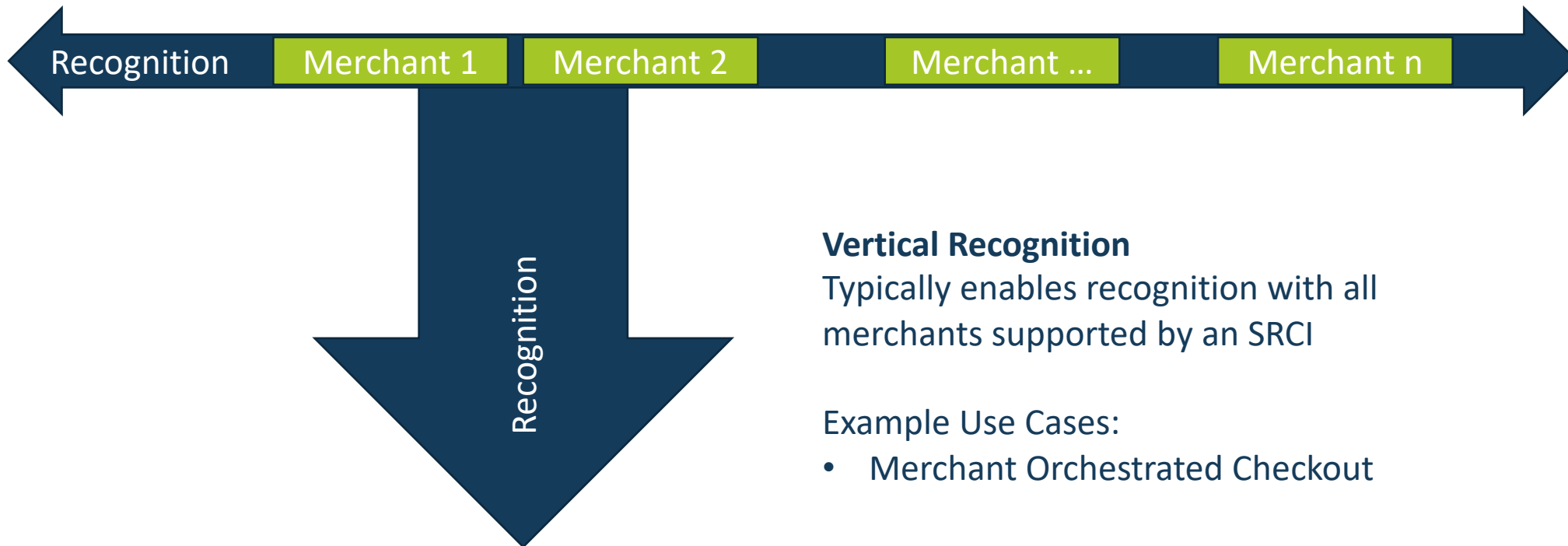Typically enables recognition across a consumer's journey across merchants

Example Use Cases:
- Recognition Domain
- SRC Orchestrated Checkout (Remembered)
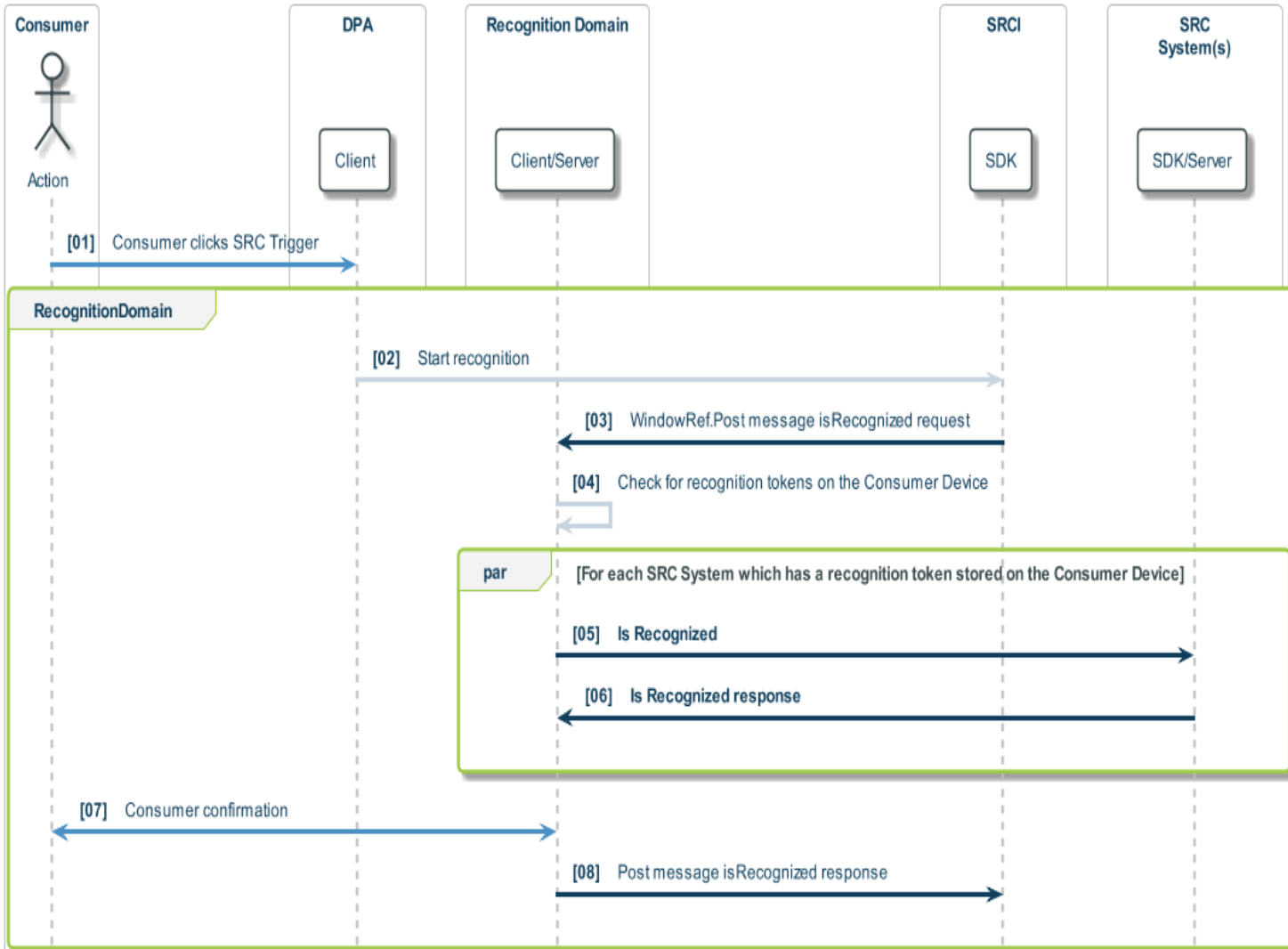- FedCM

| Recognition | Merchant 1 | Merchant 2 | Merchant ... | Merchant n |

Recognition

Vertical Recognition
Typically enables recognition with all merchants supported by an SRCI

Example Use Cases:
- Merchant Orchestrated Checkout
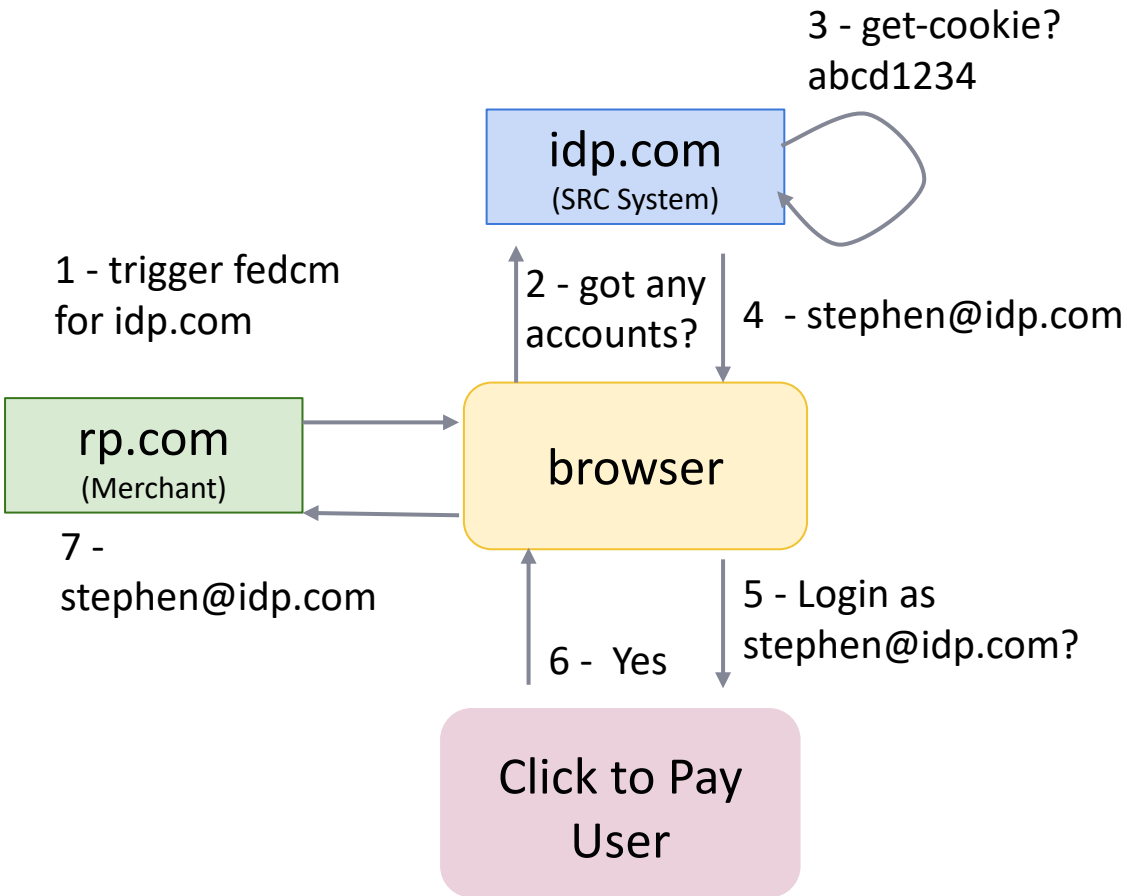
Recognition - Domain

01. The Consumer chooses the Click to Pay Trigger as the payment method

02. The SRCI starts the recognition process

03. The SRCI makes a cross origin Post Message IsRecognized call to the recognition domain windows reference.

04. The recognition domain checks the availability of recognition tokens for the browser on the Consumer Device

There are two possible outcomes from Step [04]:

• At least one recognition token is available, in which case the flow continues with Step [05]

• No recognition tokens are available, in which case the flow continues with Step [08]

05. The recognition domain calls the Is Recognized operation for each SRC System where a recognition token is available.

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

07. If the recognition domain has received any Federated ID Tokens, there is an interaction between the recognition domain and the Consumer (for example, the recognition domain presents the account(s) that were recognised and the Consumer clicks "Continue")

08. The recognition domain returns any Federated ID Tokens in the Post Message IsRecognized response

Recognition- FedCM

3 - get-cookie?
abcd1234

idp.com
(SRC System)

1 - trigger fedcm
for idp.com

2 - got any
accounts?

4 - stephen@idp.com

rp.com
(Merchant)

browser

7 -
stephen@idp.com

5 - Login as
stephen@idp.com?

6 - Yes

Click to Pay
User

- The browser enforces isolation, which allows IDP to access 1p cookies.
- The IDP does not know who is asking.
- There is a privacy issue - what happens if there is no account?
- FedCM will always require user understanding and consent
- returning flows will at least show the user something
- RP.com passes a list of IDPs to the browser
- browser talks to each idp.com (SRC system)
- Issues
  - Demo provided card list rather than login names (Good or Bad)?
  - Messsaging of "you are being logged in" is confusing
  - one issue here is that you might of N identical identities

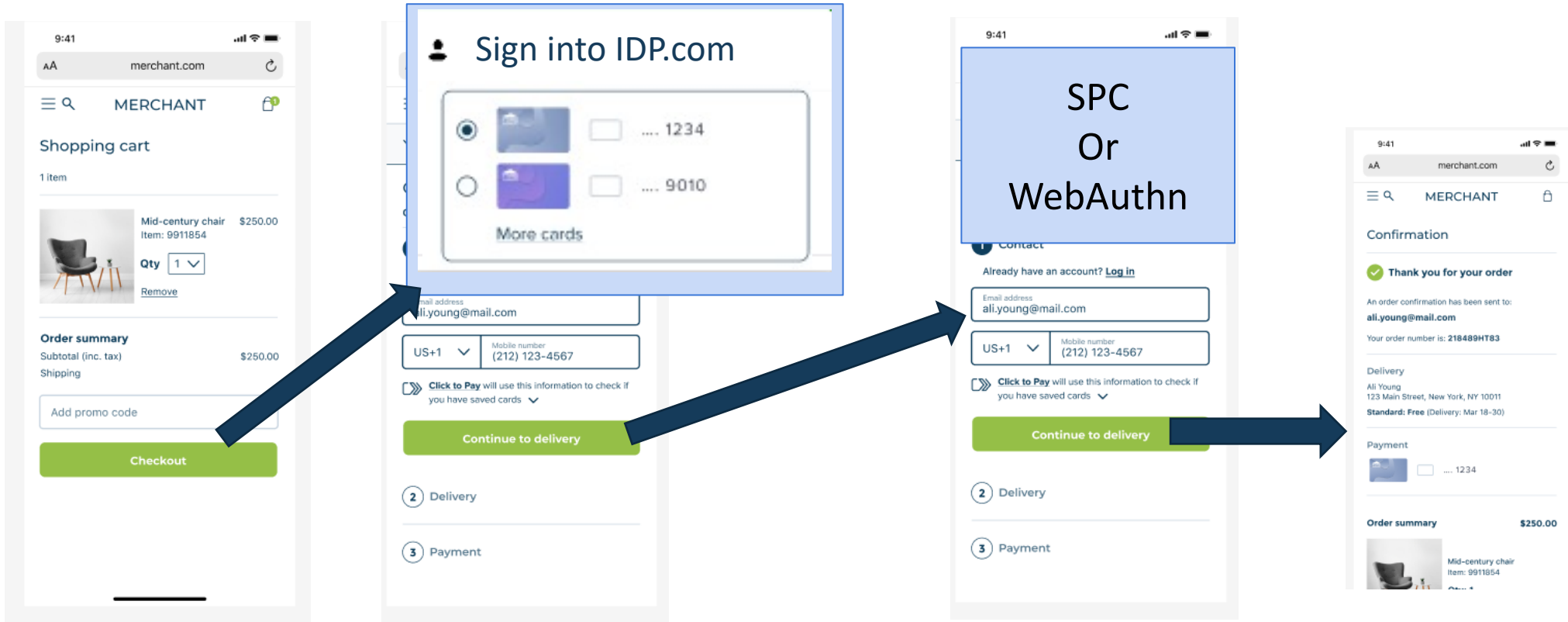# Recognition – FedCM - Email or Phone?

Trigger FedCM

Sign In
- Sign into what?
- Sign in with an Email?
Phone?

Continue Checkout
- Confusing to "sign in again"
- Assume no Shipping
- Select Card Complete Checkout

Recognition – FedCM - Card

Trigger FedCM

Sign In
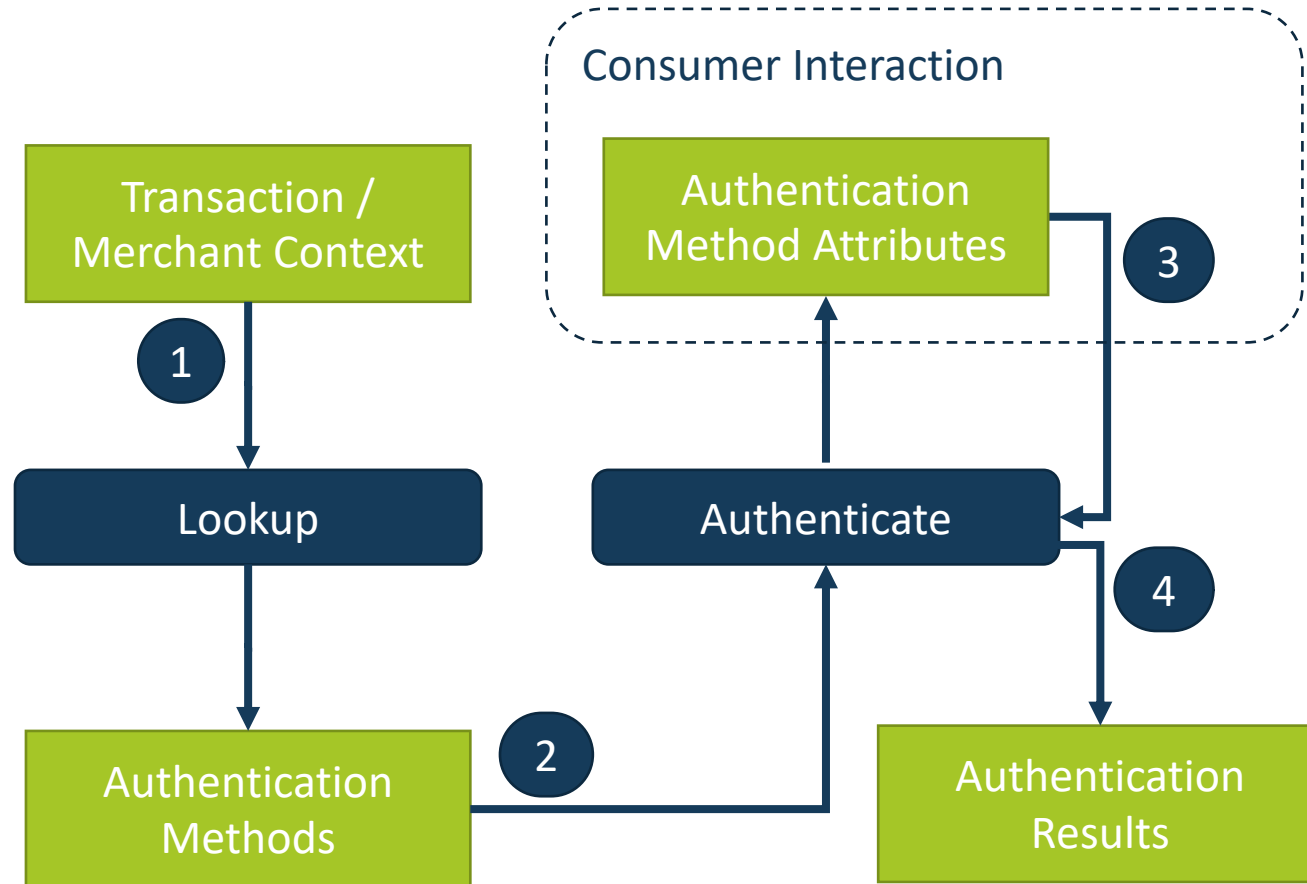- Sign into what? (CTP?)
- Sign in with a Card?

**Continue Checkout**
- Assume no Shipping

Authentication

SPC

WebAuthn

SRC Authentication Facilitation Service – 1.3

Consumer Interaction

Transaction / Merchant Context → **1** → Lookup → **2** → Authentication Methods

Authentication Method Attributes → **3**

Authenticate → **4** → Authentication Results

1. Request lookup of Authentication Methods Available
   - Information Sent
     - Transaction Details
     - Merchant Details
2. SRCS Responds with list of available methods from the available options
   - SMS_OTP
   - EMAIL_OTP
   - APP_OTP
   - 3DS
   - CSC_VALIDATION
   - APP_AUTHENTICATON
   - ADDRESS_VERIFICATION
   - FIDO
   - SPC
   - MANAGED_AUTHENTICATION
3. Authenticate operation can:
   - Initiate a multi-step authentication
   - Complete in-band validation
   - Check progress / status
4. Authentication Results Available

Reference Flow – SRC with SPC
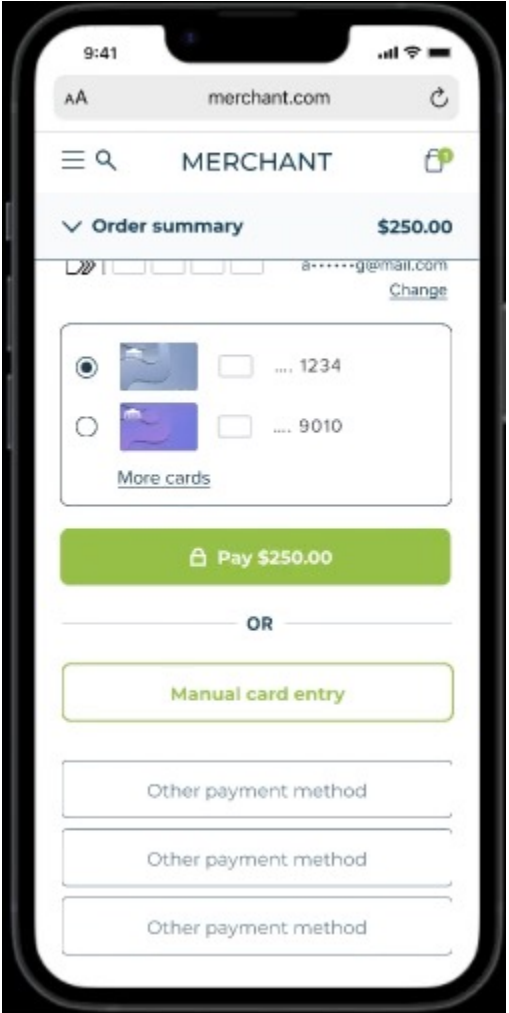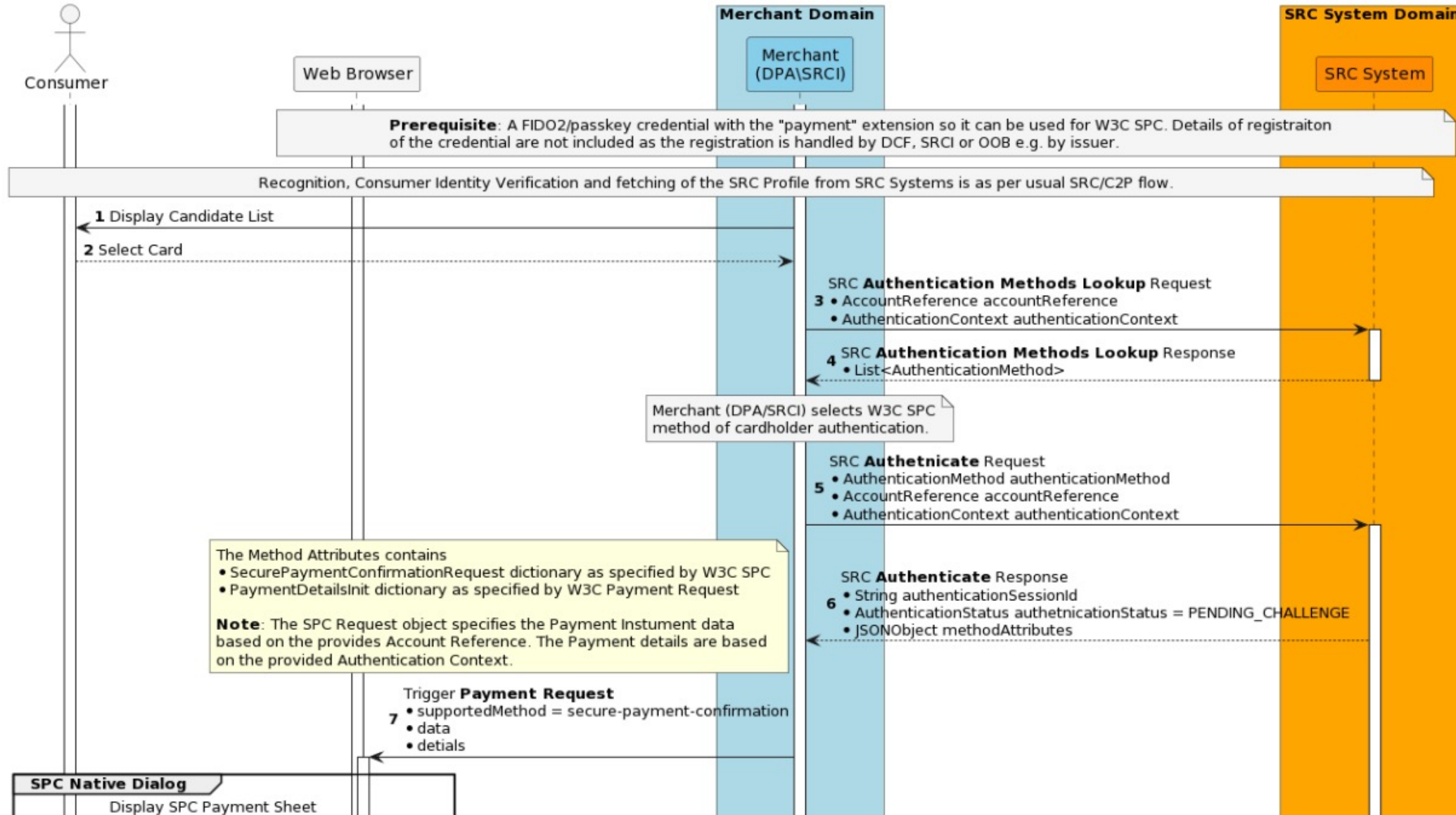
SRC Authentication Facilitation Service – SPC
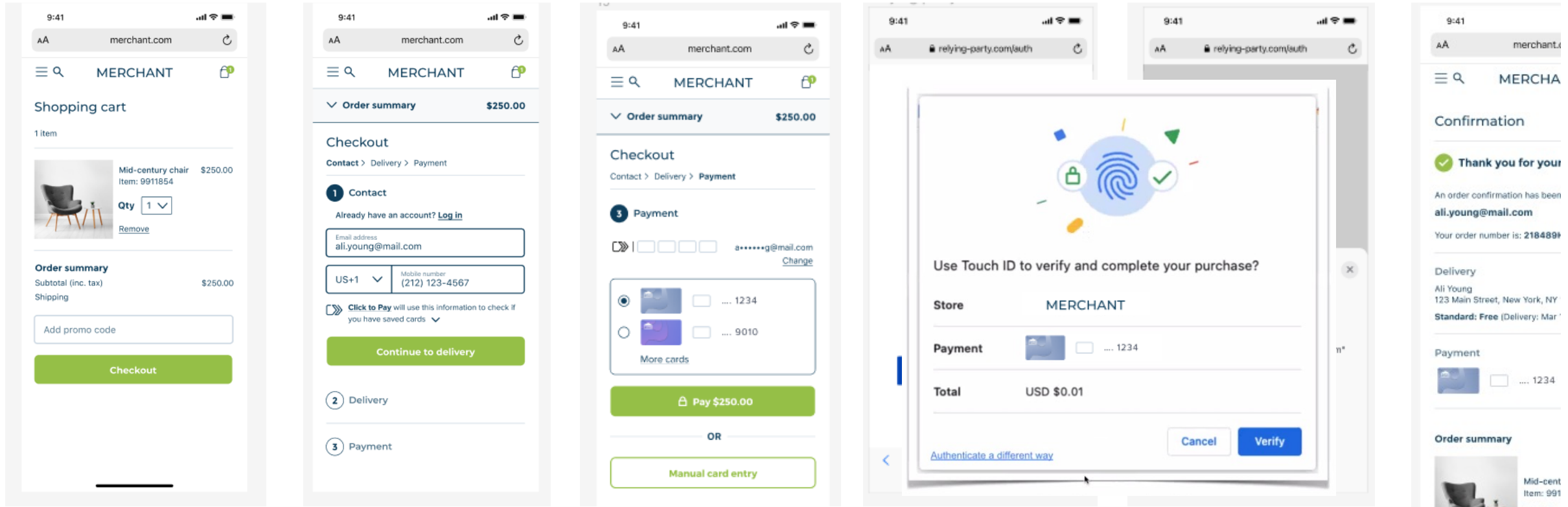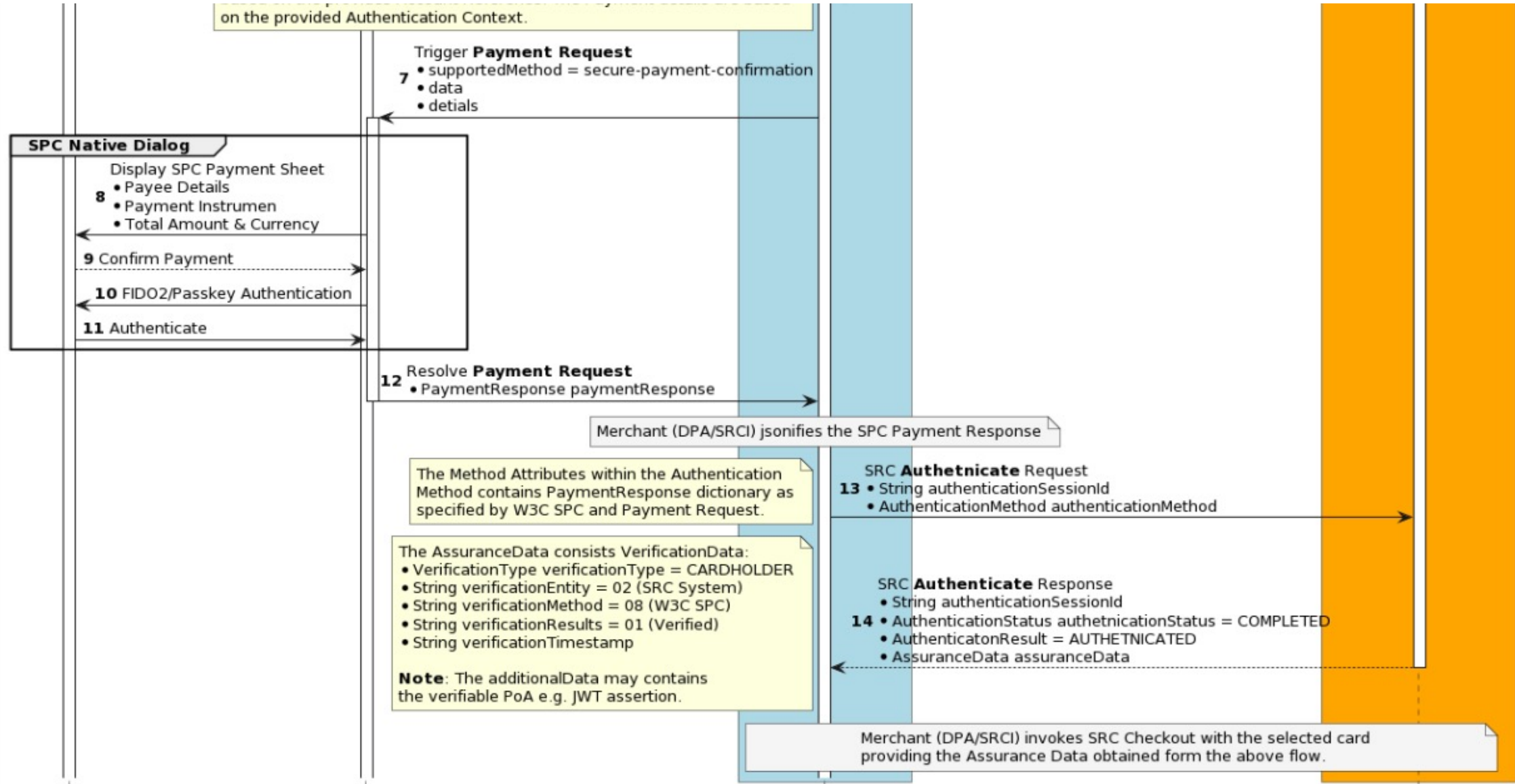

Sequence Diagrams to Follow

Proposed

SRC Authentication Facilitation Service – SPC Sequence

W3C W3C Secure Payment Specification - Merchant Initiated

17

SRC Authentication Facilitation Service – SPC Sequence

on the provided Authentication Context.

Trigger **Payment Request**
7 • supportedMethod = secure-payment-confirmation
• data
• detials

SPC Native Dialog

Display SPC Payment Sheet
8 • Payee Details
• Payment Instrumen
• Total Amount & Currency

9 Confirm Payment

10 FIDO2/Passkey Authentication

11 Authenticate

Resolve **Payment Request**
12 • PaymentResponse paymentResponse

Merchant (DPA/SRCI) jsonifies the SPC Payment Response

The Method Attributes within the Authentication Method contains PaymentResponse dictionary as specified by W3C SPC and Payment Request.

SRC **Authetnicate** Request
13 • String authenticationSessionId
• AuthenticationMethod authenticationMethod

The AssuranceData consists VerificationData:
• VerificationType verificationType = CARDHOLDER
• String verificationEntity = 02 (SRC System)
• String verificationMethod = 08 (W3C SPC)
• String verificationResults = 01 (Verified)
• String verificationTimestamp

Note: The additionalData may contains the verifiable PoA e.g. JWT assertion.

SRC **Authenticate** Response
• String authenticationSessionId
14 • AuthenticationStatus authetnicationStatus = COMPLETED
• AuthenticatonResult = AUTHETNICATED
• AssuranceData assuranceData

Merchant (DPA/SRCI) invokes SRC Checkout with the selected card providing the Assurance Data obtained form the above flow.

Thank you

For more information, visit www.emvco.com

- Official specification and supporting material portal

- General and technical FAQs

- Virtual and in-person meeting details

- EMVCo approved products and accredited labs

- White papers and best practice guides

Follow us on LinkedIn and Twitter