SRC use cases and requirements

W3C FTF March/April 2021

April 1, 2021

Jonathan Grossar, Tomasz Blachowicz

Legal Disclaimer

Information in this presentation or in any report or deliverable provided by Mastercard in connection herewith relating to the projected impact on your financial performance, as well as the results that you may expect generally are estimates only. No assurances are given that any of these projections, estimates or expectations will be achieved, or that the analysis provided is error-free. You acknowledge and agree that inaccuracies and inconsistencies may be inherent in both Mastercard's and your data and systems, and that consequently, the analysis may itself be somewhat inaccurate or inconsistent.

The information, including all forecasts, projections, or indications of financial opportunities are provided to you on an "AS IS" basis for use at your own risk. Mastercard will not be responsible for any action you take as a result of this presentation, or any inaccuracies, inconsistencies, formatting errors, or omissions in this presentation. Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, Mastercard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not Mastercard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, Mastercard specifically disclaims all representations and warranties that any practice or implementation of this document will not infringe any third party patents, copyrights, trade secrets or other rights.

Use of FIDO in Secure Remote Commerce (SRC)

Identity

FIDO can be a frictionless alternative to existing mechanisms that recognize a returning consumer, before the list of cards is displayed for card selection.

Transaction authentication

Consumer authentication during the transaction helps to further secure transactions and/or meet regulatory requirements. FIDO provides Strong Customer Authentication (SCA) with a high level of security and minimizes the friction during the authentication process.

Objective today is to focus on Transaction authentication:

- ***Explore a few SRC use cases where SPC could be used, in which the SRC systems validate FIDO authentication before generating an authenticated payload***
- ***Identify the requirements on SPC to facilitate those use cases***

For illustrative purposes only

Possible consumer journey scenarios to enroll into FIDO

Consumers can enroll in different places

1. SRC system is Relying Party

- Consumers enrolls into FIDO when they are on the network DCF
- An Identification and Verification (ID&V) process can be initiated, for the bank to authenticate the consumer as the legitimate cardholder
- FIDO credentials (Credential ID, Public Key) *and ID of Payment instrument* are associated to the consumer card in SRC system

2. Issuing bank is Relying Party

- Consumer enrolls into FIDO when visiting the bank's web site or app
- The bank authenticates the consumer as the legitimate cardholder, as part of their login process
- With consumer's consent, the bank could share the consumer card and FIDO credentials (Credential ID and Public Key) *and ID of Payment instrument* with the appropriate SRC system

3. Merchant is Relying Party

- Consumer enrolls into FIDO during embedded experience with the merchant
- An ID&V process can be initiated, for the bank to authenticate the consumer as the legitimate cardholder, and SRC system is made aware of the successful ID&V
- With consumer's consent, the merchant could share the FIDO credentials (Credential ID and Public Key) *and ID of Payment instrument* with the appropriate SRC system, for a particular card

For illustrative purposes only

SPC authentication during SRC checkout

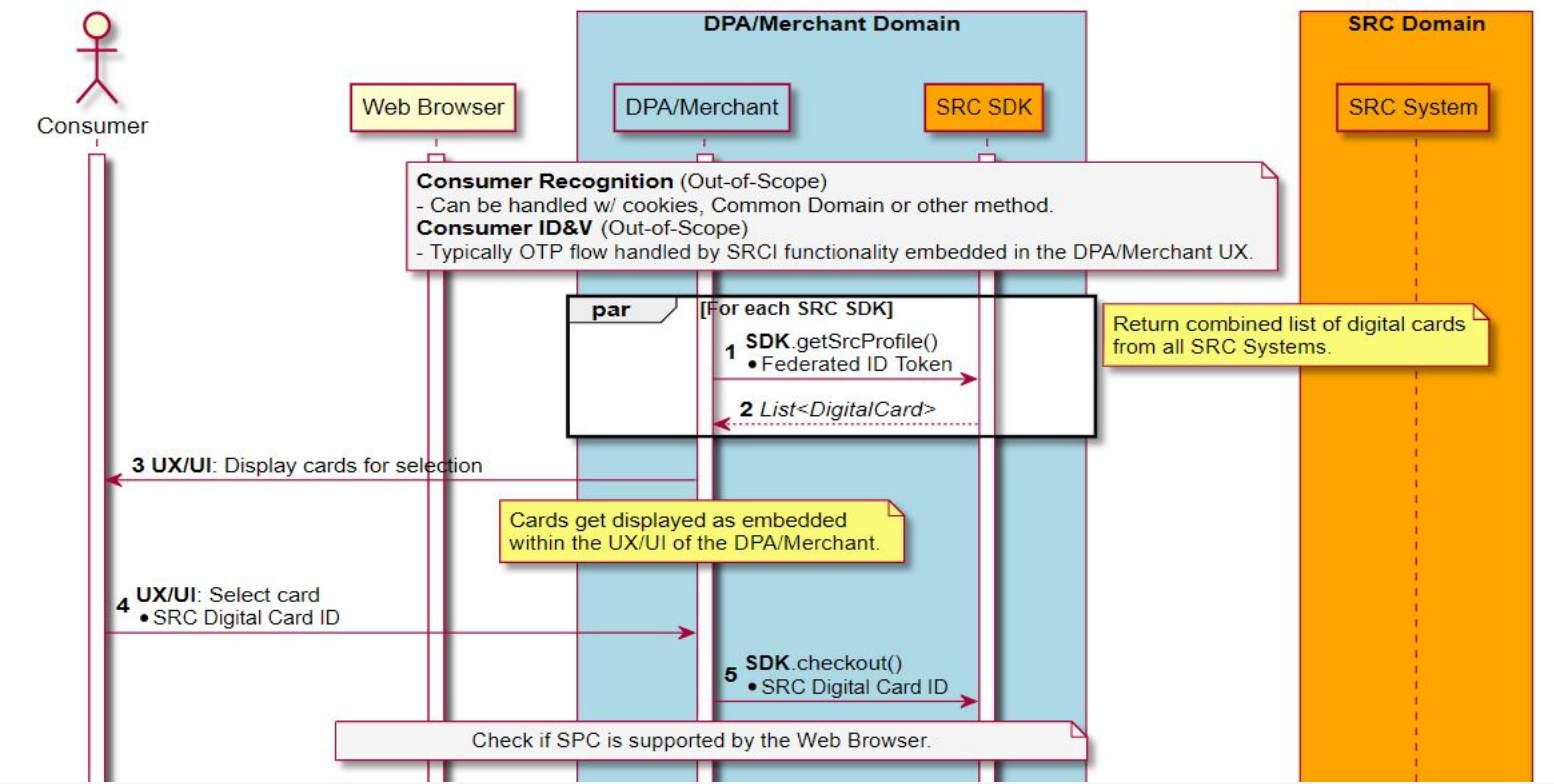
Use of SPC where SRC systems validate FIDO authentication (no EMV 3DS flow)

- After each of the previous enrollment scenarios, where FIDO credentials have been created by the SRC system, the Issuing bank or the merchant, the SRC system stores the FIDO Credential ID(s) *and/or ID(s) of the Payment Instrument*, and Public Key(s) against a payment card
- During the checkout
  - SRCi/DCF retrieves the card profile, the associated *ID(s) of the Payment instrument* and a FIDO Challenge from the SRC system
  - SRCi/DCF uses SPC to authenticate the consumer, by providing *ID(s) of the Payment instrument* and the FIDO challenge to the browser (along with the transaction amount)
  - SRCi/DCF retrieves the FIDO assertion from the browser, submits the FIDO assertion to the SRC system, the SRC system validates the FIDO assertion and generates an authenticated payload

SPC can also be used by the SRCi/DCF with EMV 3DS (Stripe/Chrome demo), in which case the Issuer – not the SRC system – validates FIDO authentication

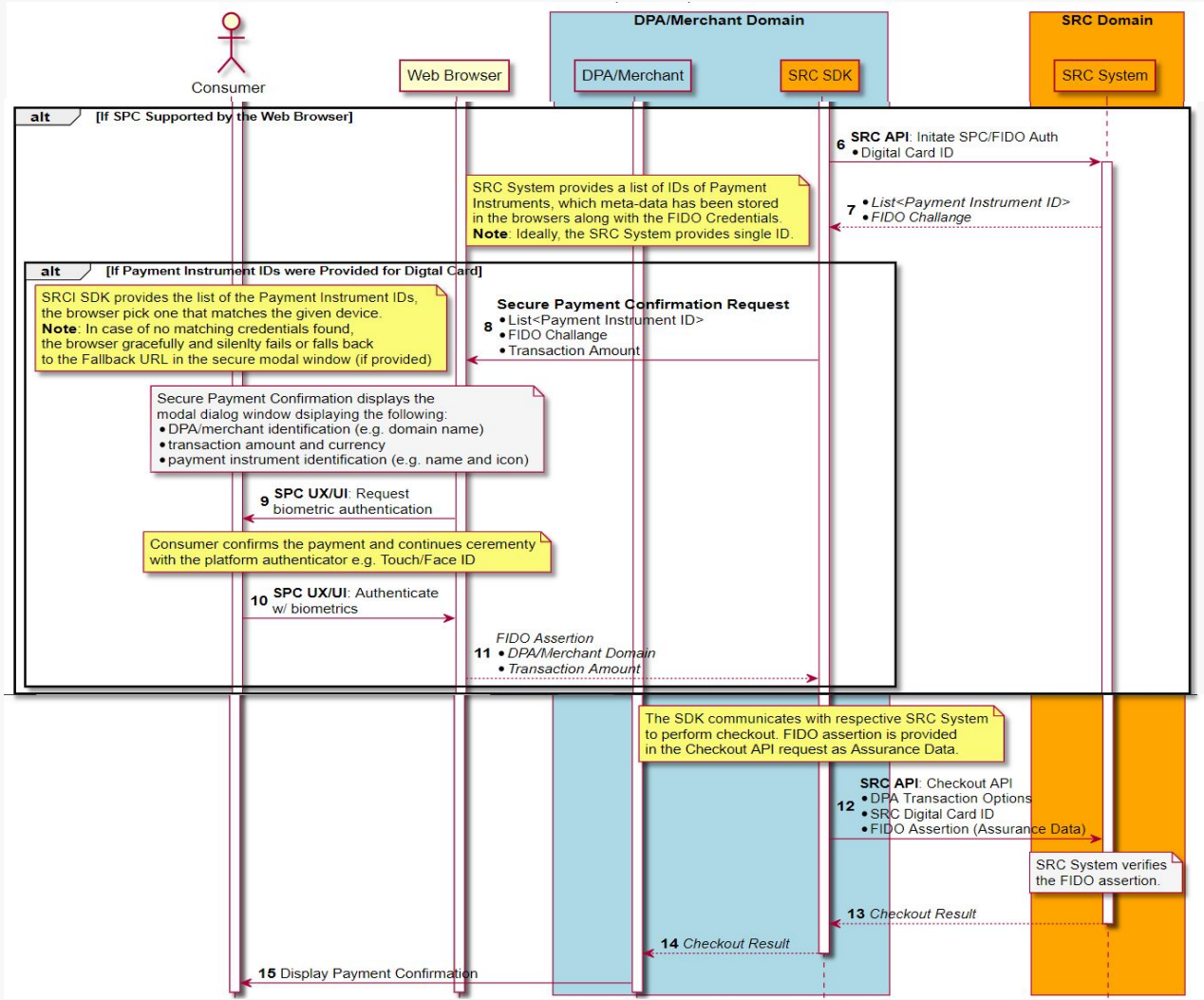
For illustrative purposes only

Existing user recognition and card selection process (before SPC authentication)



For illustrative purposes only

SPC authentication



For illustrative purposes only

SPC authentication requirements

1. There is a mechanism to understand whether the browser supports SPC
2. Non-Relying Party origins can invoke FIDO and retrieve FIDO assertion data
3. At enrollment, the Relying Party creating the FIDO credentials store the card metadata *and the RP ID* in the browser. The browser generates the *ID of the Payment Instrument*.
4. At checkout,
   - the browser's transaction confirmation dialog displays the card metadata, the merchant identification e.g. domain name retrieved by browser from top-level browsing context, and the transaction amount provided in the SPC request
   - the browser performs authentication with the first matching FIDO credential – if no matching FIDO credential can be found, it returns an error or opens a fallback URL.
     - In any case, the messaging in the authentication dialog box should be optimized (in particular in case of error) and (ideally) consistent across browsers.
   - the FIDO assertion data includes merchant URL/identifier and transaction amount in the signature (enforcing dynamic linking)
5. FIDO challenge is not necessarily generated by the Relying Party (in SRC use case the SRC system generates the challenge)

For illustrative purposes only