Secure Payment Confirmation

Leveraging Payment Request and Web Authentication for low-friction authentication during payments

Ian Jacobs, August 2020

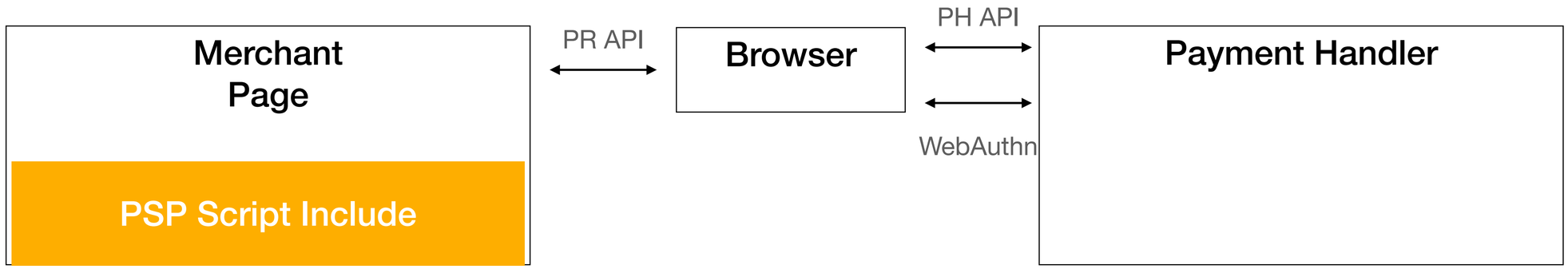
Scope

- This presentation focuses on the integration of Web Authentication into Payment Request, specifically with an EMV® 3-D Secure authentication flow in mind.
- Our expectation is that a general version of this approach would work with other authentication protocols as well.

Pre Payment Request

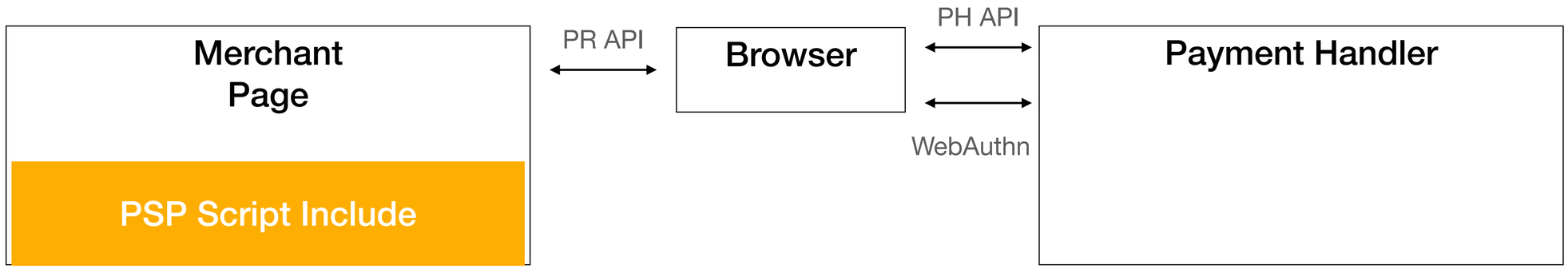
1) Collect card data in Web form
2) Get 3DS Method URL from card issuer/ACS, embed script which sends fingerprint data and transaction id to ACS.
3) Send transaction id to ACS in AReq
4) Receive ARes
5) If step-up required, embed iframe from ACS for step-up

Secure Payment Confirmation (Authentication Only, Enrollment, with Payment Handlers)



1) Collect card data in Web form
2) Get 3DS Method URL from card issuer/ACS, embed script which sends fingerprint data and transaction id to ACS.
3) Send transaction id to ACS in AReq
4) Receive ARes with fallback challenge URL
5) When step-up required, call PR API with fallback challenge URL
6) Call challenge URL in modal window
7) Prompt user to enroll FIDO authenticator with ACS/issuer for future transactions
8) ACS sends RReq and closes modal window

Secure Payment Confirmation (Authentication Only, Transaction, with Payment Handlers)



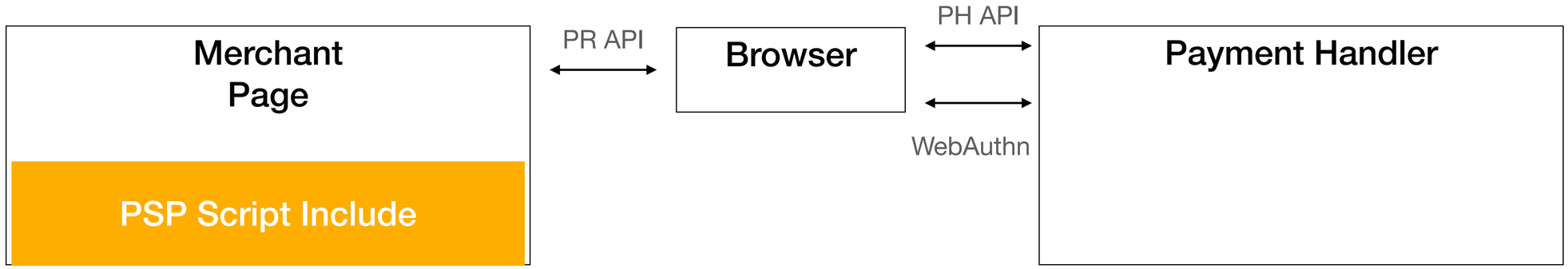
1) Collect card data in Web form
2) Get 3DS Method URL from card issuer/ACS, embed script which sends fingerprint data and transaction id to ACS.
3) Send transaction id to ACS in AReq
4) Receive ARes including credential IDs and fallback challenge URL
5) When step-up required, call PR API with credential IDs

6) Ask Browser to do WebAuthn using credential IDs. Note that Merchant, not ACS/issuer is the relying party

7) If WebAuthn succeeds, then done. Otherwise call PR API with fallback challenge URL

8) Call challenge URL in modal window

Secure Payment Confirmation
(Instrument Selection and Authentication, Transaction, with Payment Handlers)

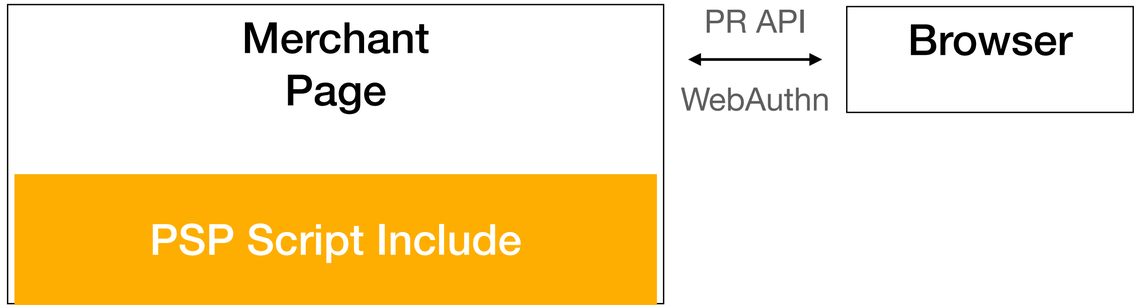


1) Call PR API with supported payment methods

2) Display matching instruments
3) Launch payment handler that owns selected instrument

4) Based on selected instrument, get 3DS Method URL from card issuer/ACS, embed script which sends fingerprint data and transaction id to ACS.
5) Send transaction id to ACS in AReq
6) Receive ARes including credential IDs and fallback challenge URL
7) When step-up required, ask Browser to do WebAuthn using credential IDs.
8) Return WebAuthn assertion or (if failure) call fallback challenge URL

Secure Payment Confirmation
(Instrument Selection and Authentication, Transaction, without Payment Handlers)



1) Call PR API with supported payment methods

2) Display matching instruments
3) Fire event to provide information about selected instrument

4) Based on selected instrument, get 3DS Method URL from card issuer/ACS, embed script which sends fingerprint data and transaction id to ACS. Instrument information must enable PSP to identify the ACS.
5) Send transaction id to ACS in AReq
6) Receive ARes including credential IDs and fallback challenge URL
7) When step-up required, update PR API call with credential IDs

8) WebAuthn using credential IDs. Return assertion or failure.

9) Use WebAuthn response or call fallback challenge URL

Additional Proposals

- #15 Alternative SPC Flow
  - Works with or without instrument selection
  - Relies on Payment Apps (from relying party, e.g., ACS or issuer)

- #17 No Payment Handler Flow

Resources

- Mockups
- Secure Payment Confirmation proposal
- Call for feedback