

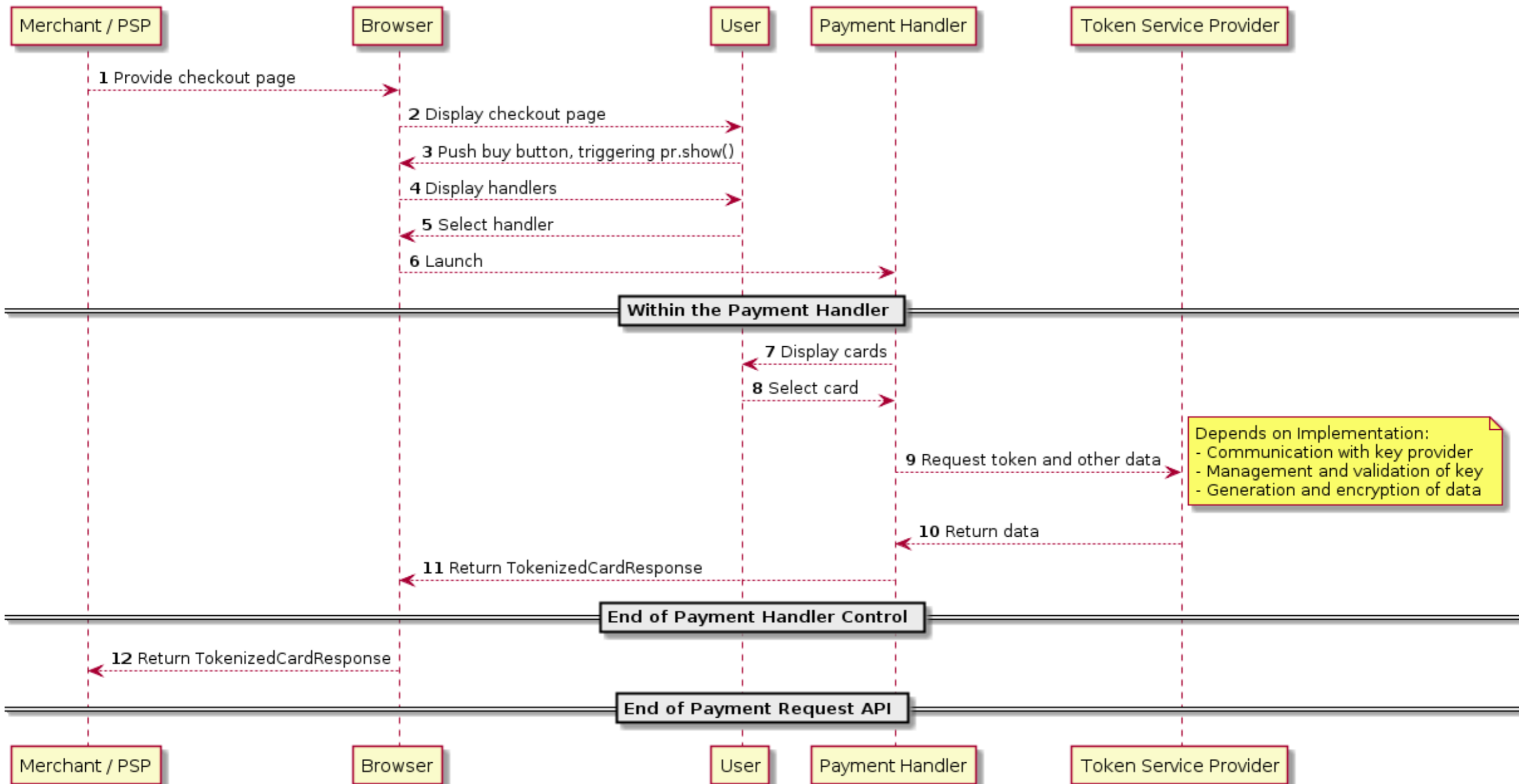
Tokenization and Payment Request API

Ian Jacobs, 8 March 2018

Goals

- Lower fraud improve user privacy by reducing exposure of cardholder PANs in payment flows.
- Lower front-end integration cost of leveraging network tokens.
- Improve security and potentially lower PCI-DSS burden for merchants.

Flow



Since TPAC (Nov '17)

Updates to Tokenized Card Payment Specification

- New data model based on Mastercard experimentation and feedback from Visa.
 - Distinguishes displayable response data from sensitive data used for payment
 - Intends to leverage the task force's encryption work (work in progress).
- Greater clarity about scope, prerequisites
- Added a response example
- Updated references and flow diagram
- Issue markers added
- New FAQ questions in tokenization wiki

Encryption

- The sensitive parts of the response data will be encrypted using a key acquired with a keyProviderURL.
- The task force's encryption proposal currently refers to JOSE JWE.
 - Manu has suggested we look at JSON LD options.
 - AdrianHB has suggested we consider a limited profile of algorithms, and also mentioned cleartext JWS.
- What key formats are allowed?
- The proposal is not specific enough on how to leverage JWE, so we are looking for crypto experts and developers to help us flesh out the proposal.

Token properties

- Issue 25: To improve **payment handler matching**, would it be useful if request data described acceptable tokens by property? For example:
 - One time v. recurring use
 - Authorized for specific amounts v. variable amounts
 - Authorized for immediate use v. any time in the future
 - Authorized for partial shipments
 - Attached to a specific merchant or transaction type
- Acceptable token properties may be established through prior out-of-band registration, in which matching on TSP identifier may be appropriate.

Reference Basic Card?

- Some Basic Card members are reused (supportedNetworks, supportedTypes, cardNumber, etc.).
- Issue 17: Should Tokenization include by reference or define again (and stay in sync)?
- Is the WPWG planning to formally deprecate Basic Card?

Other Issues

- #31, #32: Do we need more information about payment handler TSP relationship?
- #36: Document threat model
- #27: Is this specification for network tokens only or more general?

Next steps

- March/April: Get more implementation experience, solidify encryption proposal
- Mid-April: Discuss progress at FTF meeting
- April/May: Call for consensus to advance to FPWD
- Questions:
 - Will browsers want to implement this natively?
 - Will *Pay systems want to converge on this?
 - Who will want to implement this?