Web Payments WG

Context for the March/April 2021 F2F

Goals for Payments on the Web

- **Low Friction**
  fewer clicks, swipes, taps, no typing

- **High Security**
  cryptographic certainty, risk-based policies, two-factor authN

- **Strong Privacy**
  only share data as required, always with consent

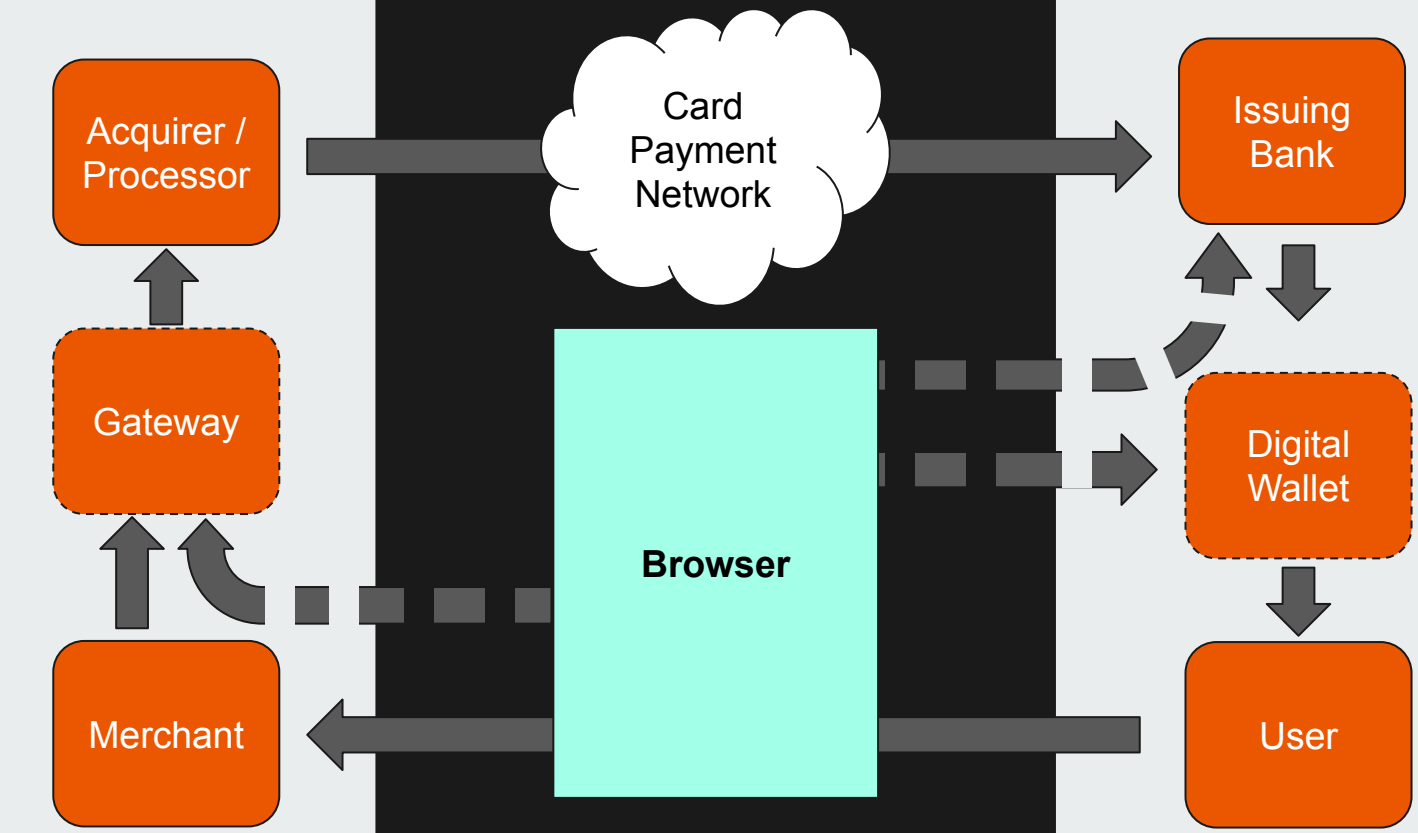
Invariants and Assumptions

- **Origin Security Policy** (browsers use origins to segment security domains)
- **Risk** assessment is facilitated by data collection
- Browsers **limiting 3rd-party access** to data/cookies to prevent tracking

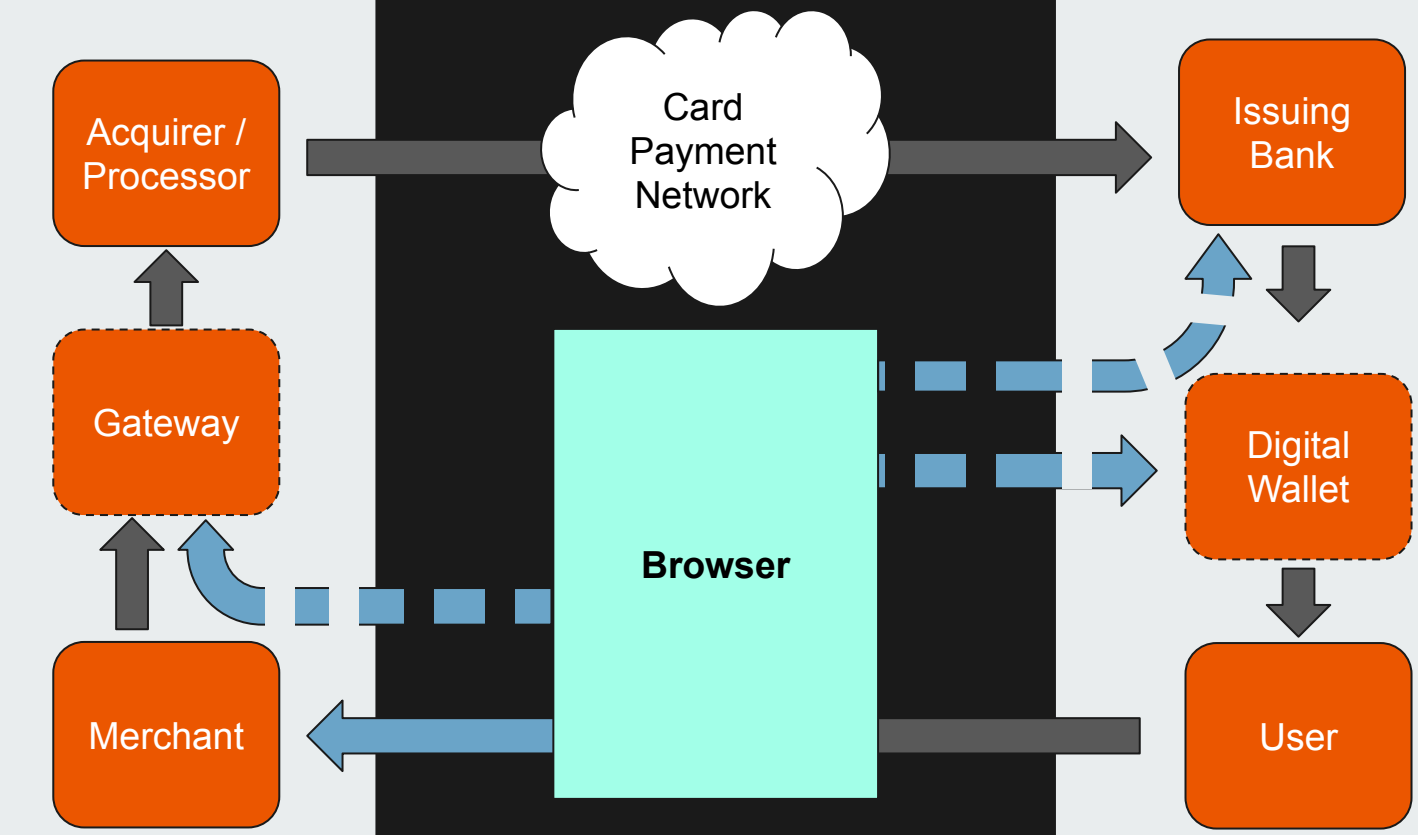
Related tensions in the ecosystem:

- Same Origin Policy (SOP) <-> Payment Initiation often done by 3rd-party from 3rd-party context (iframe)
- Excess data collection is bad for **privacy** <-> Risk assessment consumes as much data as it can get

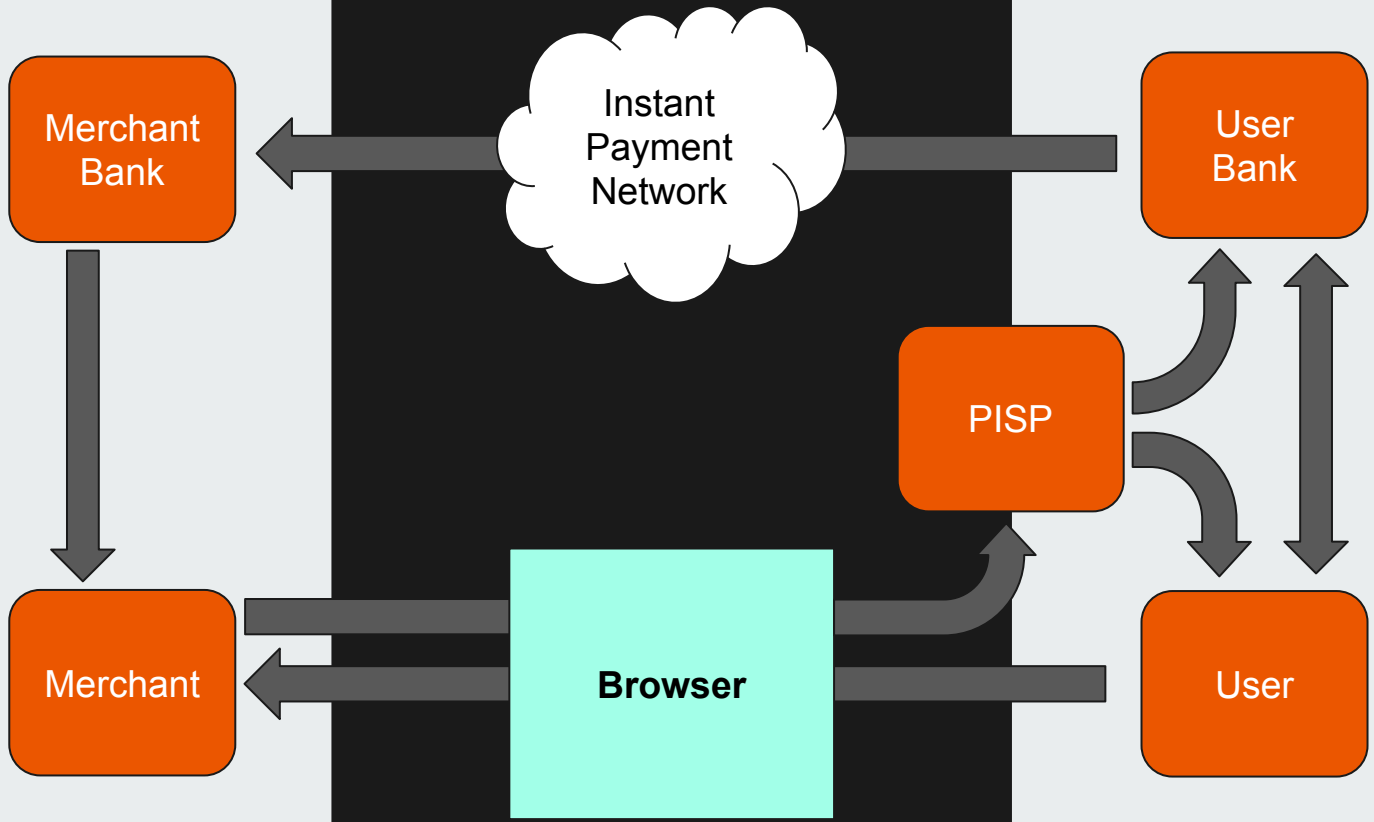
3 domains


Acquirer / Processor
Card Payment Network
Issuing Bank
Gateway
Browser
Digital Wallet
Merchant
User
Merchant
Interoperability
Issuer

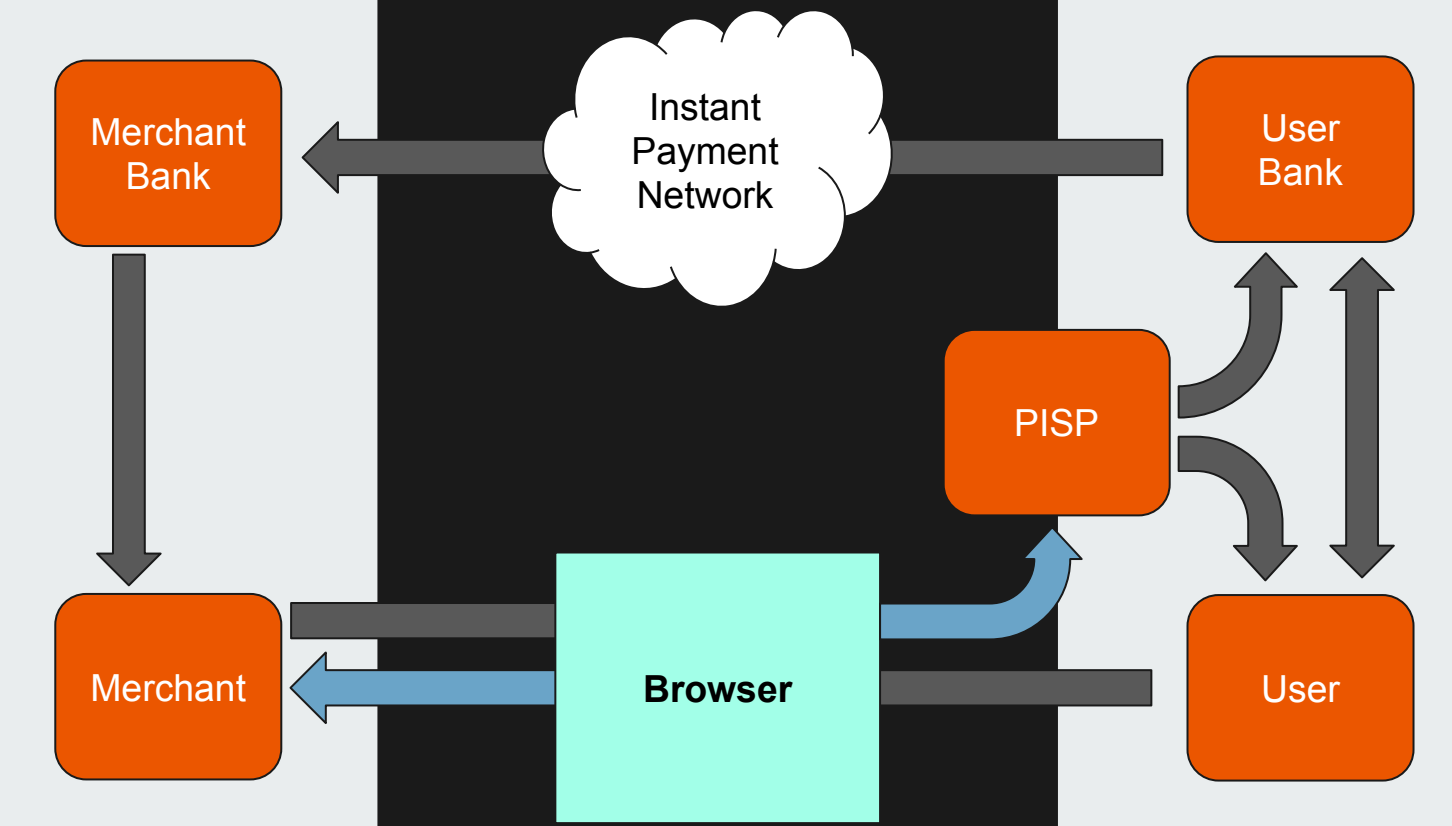
3 domains


Acquirer / Processor
Card Payment Network
Issuing Bank
Gateway
Browser
Digital Wallet
Merchant
User
Merchant
Interoperability
Issuer

3 domains


Merchant Bank
Instant Payment Network
User Bank
PISP
Merchant
Browser
User
Merchant
Interoperability
ASPSP

3 domains


Merchant Bank
Instant Payment Network
User Bank
PISP
Merchant
Browser
User
Merchant
Interoperability
ASPSP

Our Evolving Thesis

Instead of providing a broad cross-origin communication channel, provide **options** to stakeholders

Split the payment user experience into stand-alone functions and provide primitives to cater for each function with standardised browser UX where appropriate:

1. Payment Instrument **Selection/Input**
2. **Authentication** of User and Payment Details
3. **Authorization** of Payment by User

Stakeholders use functions **as required** (all optional) for different flows (mix ‘n match)

Payment Context

Execution inside Payment Handler event OR a Payment Request event

1. Merchant website has called Payment Request API
2. User has been shown **browser rendered payment UI**

Browser can **expose powerful features** and reveal select user data within this context (even to the merchant origin) while maintaining **security** and **privacy**:

- Reveal selected payment instrument/method to merchant
- Invoke WebAuthn from non-RP context
- Allow secure modal window with 1st party context

Browser Primitives exposed in Payment Context

- Secure Payment Confirmation:

  Streamlined secure authentication using WebAuthn + PaymentRequest data

- Payment Instrument Selection:

  Stored identifiers/logos/labels from RP for re-use and low friction

- Secure Modal Window:

  In-context display of cross-origin UI

Order shown is proposed priority

Secure Payment Confirmation (SPC)

- Invoke WebAuthn from payment context with minimal friction
- Display payment details (amount, payee) in authenticator prompt
- Include payment details in signed client data
- Allow non-RP origin to invoke and get attestation from inside payment context
- RP not required to ship UI for authN

Storage/Selection of Payment Instruments

- *A "Payment Cookie" or "Payment Credential"*
  - **icon** and **label** for display in selection lists
  - associated with a **payment method**
  - has a unique non-sensitive **identifier** (URL?) that is shared with merchants and/or Payment Handlers after selection by user
  - can be associated with a **Payment Handler** (or be a Payment Handler)?
- Controlling origin (relying-party) can **enumerate**, **delete** and **add** and link to `PublicKeyCredential`or Payment Handler from top level context
- Managed independently of cookies and storage in browser settings

Secure Modal Window

- Display UI from the RP or PSP origin **in context** (no redirects or pop-ups)
- Superior mobile experience
- Renders **top-level** context (access to cookies and storage)
- Privacy concerns mitigated if UI makes it clear that the window is a new context and new origin (UA must show origin and context - “Paying $5 to abc.com”)