Tokenization and Encryption

- Request/Response format
- Encryption
- Flows
- Other tokens
- Issues

https://w3c.github.io/webpayments-methods-tokenization/

Format (Request)

```
{
  supportedMethods: ["tokenized-card"],
    data: {
      supportedNetworks: ['mastercard','visa', 'amex', 'unionpay'],
      supportedTypes: ['credit','debit'],
      keyProviderURL:  'https://pspKeyProvider.example/tokenizedCardPublicKey',
    }
}
```

- Very similar to `basic-card`

Format (Response – clear text)

```
{
  displayLast4: "***6789",
  displayExpiryMonth: "02",
  displayExpiryYear: "22",
  displayNetwork: "mastercard",
  encryptedTokenizedCard: "QWxobHZ4bU4yWkt1QUFFU05GWjRHb0FCRkE9PQ==",
}
```

- Clear data used purely for display

Format (Response – encrypted text)

```
{
  cardNumber: "5413339000001513",
  expiryMonth: "12",
  expiryYear: "20",
  cryptogram: "AlhlvxmN2ZKuAAESNFZ4GoABFA==",
  typeOfCryptogram: "UCAF", // "Universal Card Authentication Field”
  trid: "59812345678",
  eci: "242", // Authorization and final transaction request with UCAF data
}
```

- Encryption details still TBD and could be defined generically

Encryption

- Implementation experience required
- General encryption solution or specific to tokenization?
- Implementation details to be defined (JOSE)

- Issues: https://github.com/w3c/webpayments-crypto/issues
  - Best practice
  - Multi-party flows
  - Generic encryption for PR API

Flows

- Can browser call TSPs to get tokenized card data?
  (Browsers implement the payment method, possibly register as Token Requesters)
- Alternatively, should payment handlers call TSPs?
  (Nothing required from browsers)
- Need analysis of TSP API data requirements vs available data from:
  - PaymentRequest object
  - `tokenized-card` payment method specific data
  - Contextual data from the browser/payment handler

Other tokens to consider

- Issuer tokens
  E.g. Carte Bancaire
- Network tokens
  Is this different to EMV tokens?
- Apple Pay, Samsung Pay, Google Pay, *Pay tokens
  Are these all gateway tokens? Is there value in standardizing these?
- Virtual Cards
  E.g. https://www.capitalone.com/applications/eno/virtualnumbers
- Generic payment tokens (opaque to acquirer)

Issues

https://github.com/w3c/webpayments-methods-tokenization/issues

- Make spec more generic (not card network specific)
- Token characteristics (re-usable, bound to merchant, etc). Can browsers register as Token Requestors?
- Return payee identification data (e.g. PAR). Is this a super-cookie?
- Reference to `basic-card`?