Secure Payment Confirmation: Design Discussion

danyao@chromium.org

Mar 31, 2021

Presented at WPWG F2F, 2021

Session Goals

So far this week, we heard a lot about the promising business benefits of SPC and ideas on how we can expand them.

Three goals for today:

1. Agree on scope, initial requirements and assumptions for Secure Payment Confirmation Level 1
2. Enumerate key design decisions and major options
3. Identify interest to form a task force to create a public spec draft

Context & Scope

The payment user experience can be split into 3 stand-alone functions (Adrian Hope-Bailie, Mar 29):

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

Secure Payment Confirmation is focused on the 2nd problem: streamlined secure authentication.
The initial Chrome + Stripe pilot tested a baseline user experience that's based on FIDO.

Next step is to formalize the design of the proposed primitives in a way that can also be future-proof.

What is SPC, really?

“Payment Authentication Assertion”[*]

- Proves possession and (optionally) a 2nd factor
- Binds transaction details
- Interoperable across all merchants and payment rails
- Consistent & predictable UX (mediated by the browser)
- Privacy-preserving and strong security

[*] Term coined by Chris Woods in his Mar 29 presentation.

A canonical proof:

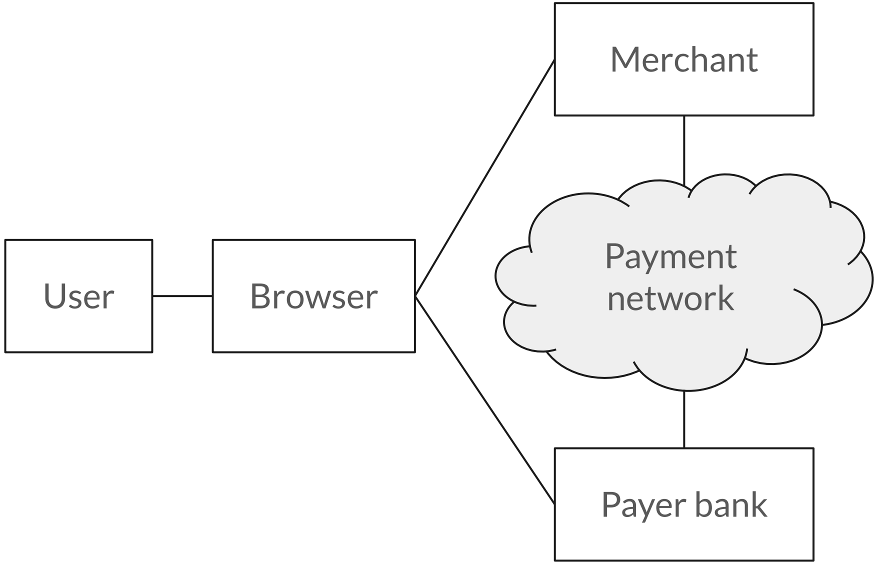
Is this the same device that the user has been associated with?

Is this the same person who has previously been associated with this account?

Have the transaction details been confirmed by the user?

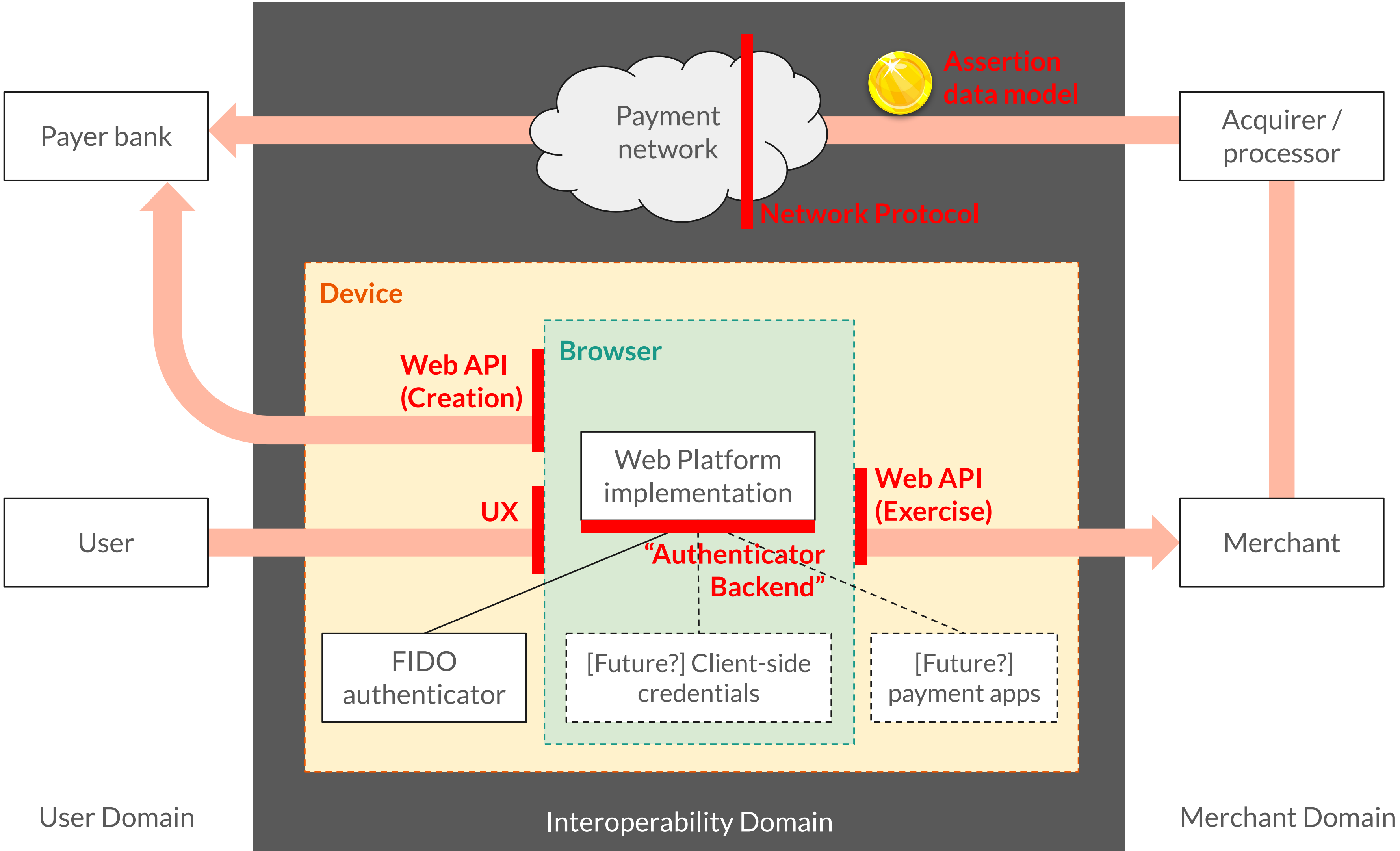
Canonical User Journey

1. User creates a *payment credential* at some point
2. Some time later, user visits merchant A and initiates payment
3. User is challenged to generate a *payment authorization assertion*
4. Payer bank verifies the assertion and authorizes payment.
5. Some time later, user visits merchant B, and passes the payment challenge by generating a *new payment authorization assertion* using *the same payment credential*

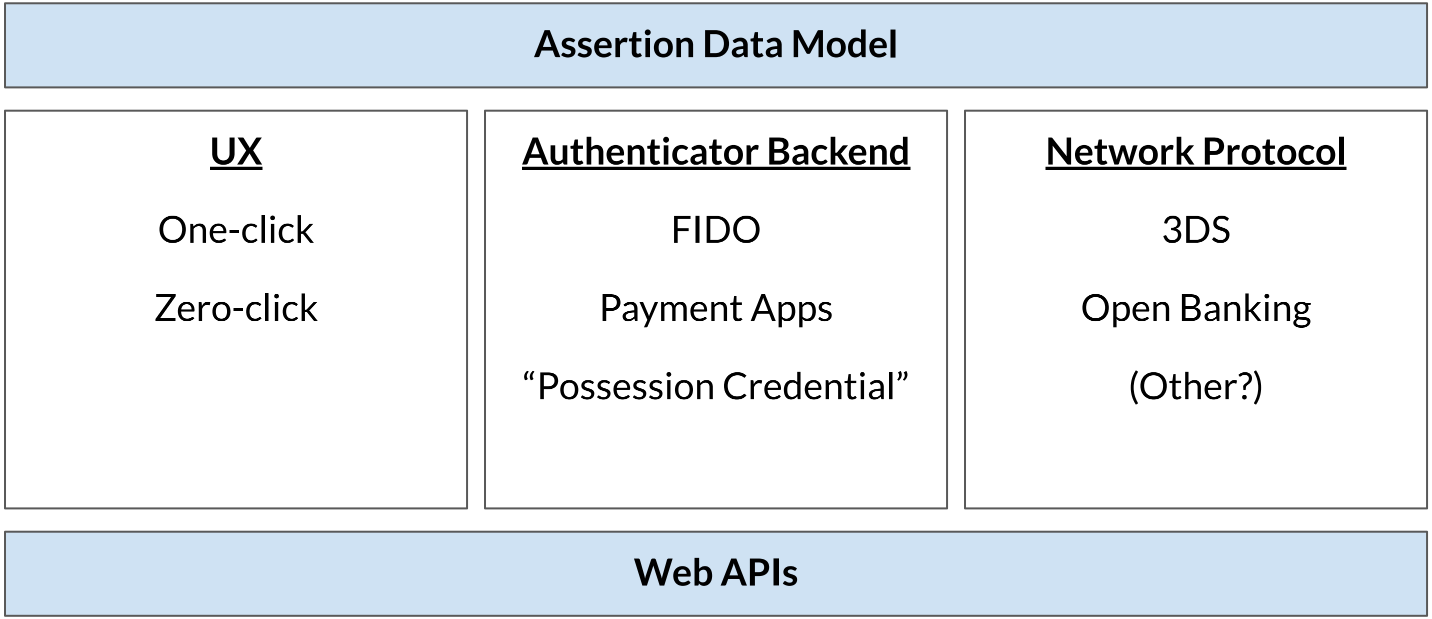


“Payment Authorization Assertion” Design Questions

1.	Who owns it?	*Issuer in the original SPC proposal, but can it also be merchants or scheme per “delegated authentication”?* *What does “ownership” mean if the public key is shared between issuers and merchants?*
2.	How does it look like?	*Signature + what metadata? Is it a payment instrument or a user (i.e. cardinality)?*
3.	How to create it?	*Just-in-time during a checkout? Out-of-band in an online banking portal?* *FIDO only or can it also be backed by a Possession Credential?* *Does it have to be created on the Relying Party origin? In a cross-origin iframe?*
4.	How to exercise it?	*Can a non-“owner” request the browser to create the assertion? With what input data?* *What kind of UX, one-click or “frictionless”? How does the payer bank get the assertion?*
5.	How to manage it?	*Can a FIDO credential created for this purpose also be reused for login or vice versa?* *Can a credential be reused between web and native apps? Can it be deleted / updated?*


Payer bank
Payment network
Assertion data model
Acquirer / processor
Network Protocol
Device
Browser
Web API (Creation)
Web Platform implementation
Web API (Exercise)
User
UX
"Authenticator Backend"
Merchant
FIDO authenticator
[Future?] Client-side credentials
[Future?] payment apps
User Domain
Interoperability Domain
Merchant Domain

Design Space



Assertion Data Model

UX

One-click

Zero-click

Authenticator Backend

FIDO

Payment Apps

“Possession Credential”

Network Protocol

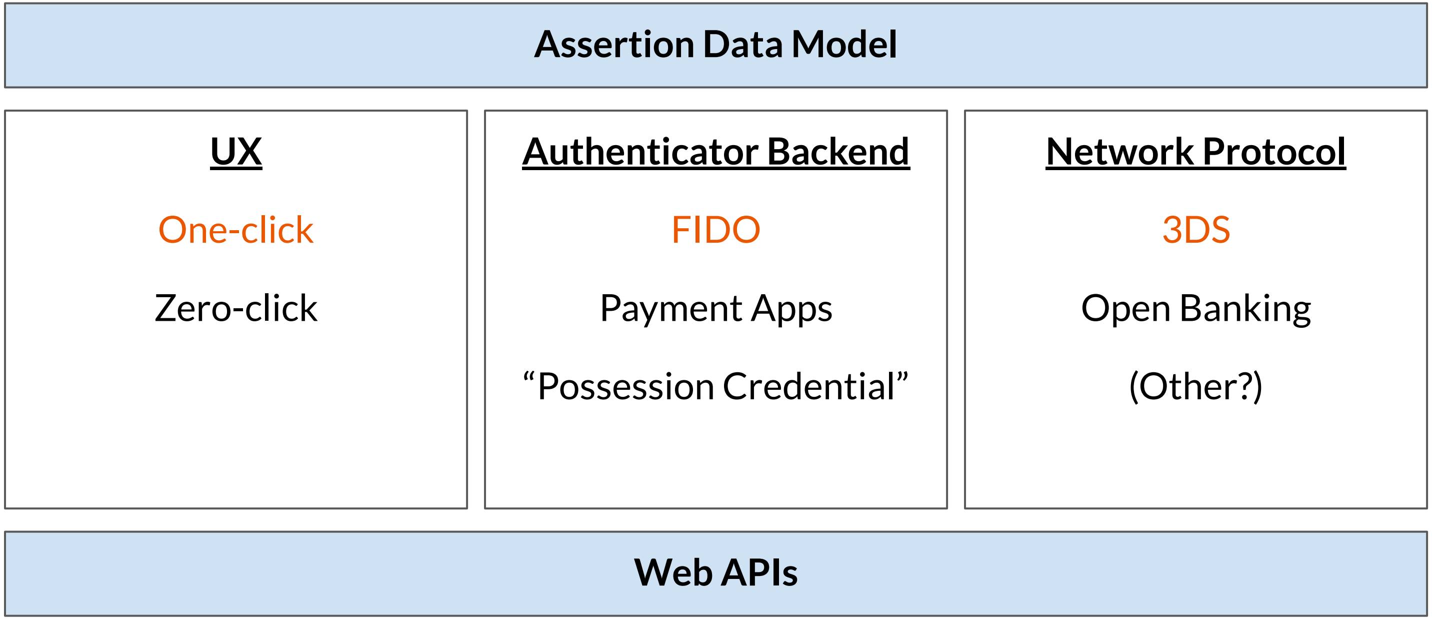
3DS

Open Banking

(Other?)

Web APIs

Stripe + Chrome Pilot (#1)



Assertion Data Model

UX

One-click

Zero-click

Authenticator Backend

FIDO

Payment Apps

“Possession Credential”

Network Protocol

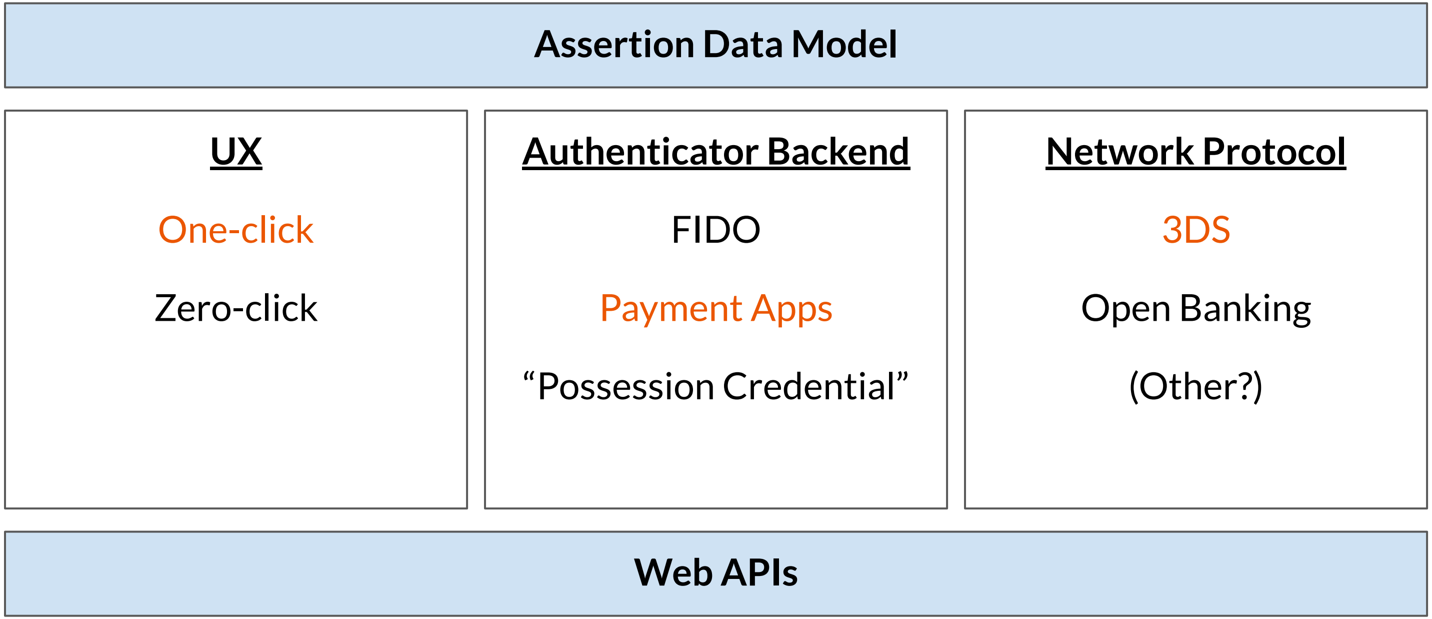
3DS

Open Banking

(Other?)

Web APIs

Might this be SRC? (#2)



Assertion Data Model

UX

One-click

Zero-click

Authenticator Backend

FIDO

Payment Apps

“Possession Credential”

Network Protocol

3DS

Open Banking

(Other?)

Web APIs

Work Streams

1. **Assertion Data Model**
   Who owns it? How does it look like?

2. **Use cases** (UX × Authenticator Backend × Network Protocol)
   Which use cases do we want to support eventually? How to sequence them?
   How do creation and exercise UX look like in each case?
   What needs to be added to the relevant network protocol to support each case?

3. **Web API specification**
   Just writing things down

Design Space: 3DS

No.	UX	Authenticator Backend	Network Protocol	Interested Developers
1	One-click	FIDO	3DS	Stripe, Nok Nok
2	One-click	Payment app	3DS	SRC?
3	One-click	“Possession Credential”	3DS	Entersekt
4	Zero-click	FIDO	3DS	
5	Zero-click	Payment app	3DS	
6	Zero-click	“Possession Credential”	3DS	

Design Space: Open Banking

No.	UX	Authenticator Backend	Network Protocol	Interested Developers
7	One-click	FIDO	Open Banking	
8	One-click	Payment app	Open Banking	
9	One-click	“Possession Credential”	Open Banking	
10	Zero-click	FIDO	Open Banking	
11	Zero-click	Payment app	Open Banking	
12	Zero-click	“Possession Credential”	Open Banking	

Design Discussion

Design Principles

In alignment with the Web Payments WG context (Adrian Hope-Bailie, Mar 29), our design principles are:

- **Low Friction**
  fewer clicks, swipes, taps, no typing
- **High Security**
  cryptographic certainty, risk-based policies, two-factor authentication
- **Strong Privacy**
  only share data as required, always with consent

Seed Questions

- Assertion Data Model
- 3DS Support
- Possession Credential
- FIDO as authenticator backend
- Payment app support

Assertion Data Model

- Who owns the credential, issuer, network or merchant?
- One credential per instrument or one credential per user?
- What other data would issuer want to see besides challenge and signature?
- What kind of management options should the user have?

```
{
  "requestId": "3183fbc3-fbbe-43b2-938e-a289af16af66",
  "methodName": "secure-payment-confirmation",
  "details": {
    "challenge":
"{\"merchantData\":{\"merchantOrigin\":\"https://fancyb
ank.com\",\"total\":{\"currency\":\"USD\",\"value\":\"0
.01\"}},\"networkData\":\"bmV0d29ya19kYXRh\"}",
    "signature":
"MEUCIAuUeARWZRB8yu9yCqN3cZp4k1UOWCY8hulJN2SZYcChAiEAmG
aofxIUVPpBPqmKoR6IujAWeWa+aeK7SVMX6JWCmvk=",
  },
}
```

3DS Support

- What is the best path to support in future versions of 3DS?
- Is 3RI the best path for 3DS 2.2?
- What about earlier versions of 3DS2 and 3DS1?

Possession Credential

Explainer

- What if FIDO backend can be made such that only the browser prompt click is needed?

FIDO

- Should roaming authenticators be supported?
- Should Discoverable Credential be supported?

Payment App Support

- What should be the role of the payment app when creating a credential? When exercising a credential?
- If multiple payment apps exist, what options should be given to the user?
- When does it make sense to show browser UI? When does it make sense to show payment app (i.e. web or native) UI?

Open Banking Support

Chris Wood, Mar 30

Next Steps

SPC Task Force

- Meet regularly to flesh out all design questions
- Coordinate with the network working groups (e.g. 3DS WG) on assertion data model and network protocol design
- Publish a Public Working Draft through WPWG

Starter team:

Benjamin Tidor (Stripe)
Rolf Lindemann (Nok Nok Labs)
Gerhard Oosthuizen (Entersekt)
Adrian Hope-Bailie (Coil)
Marcos Caceres (W3C)
Stephen McGruer (Google)

Please contact ij@w3.org if you're interested in joining.