Secure Payment Confirmation

smcgruer@google.com (he/him) & the Chrome Web Payments Team

June 2021

Problem

Card fraud is costly

Credit card fraud costs businesses $25 billion globally in 2018 or $7.37 per $100 revenue.[1]

User verification adds friction

Explicit flows for payment authentication (e.g. 3D Secure) are high friction and cause significant user drop off.[2]

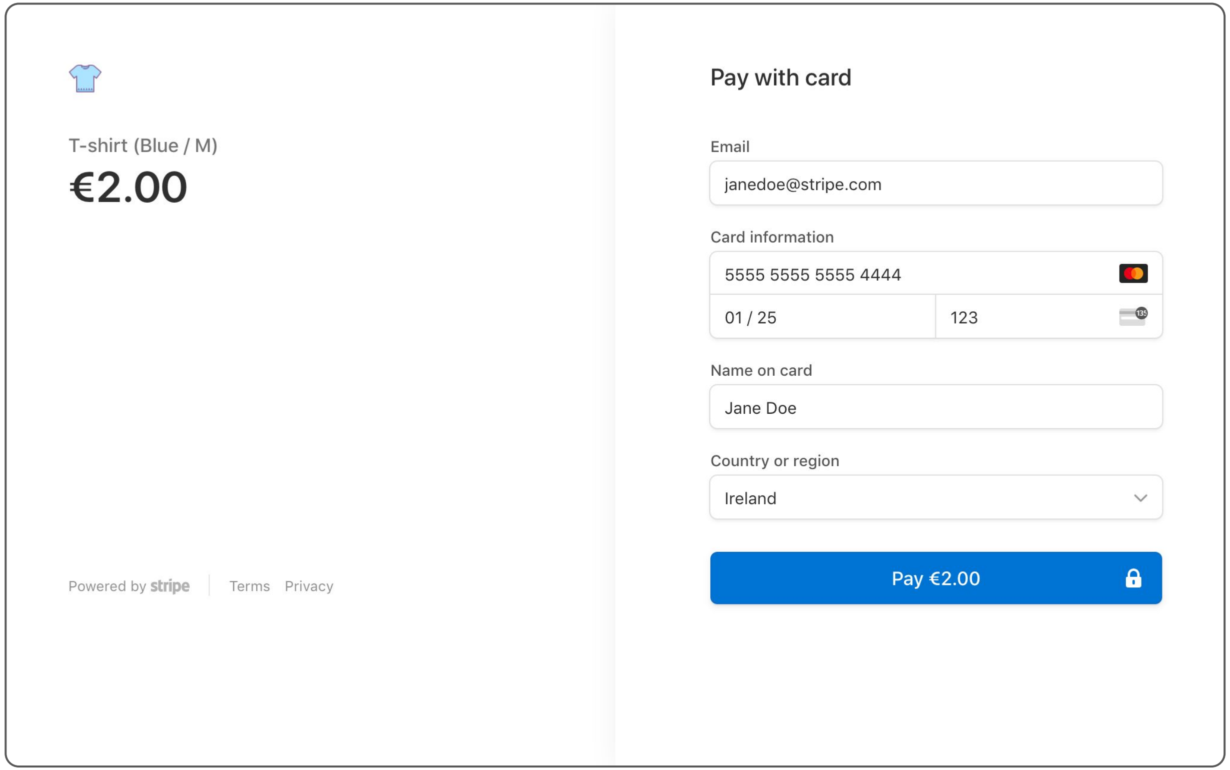
Starting Jan 1, 2021, Strong Customer Authentication (SCA) in Europe & UK requires explicit verification on more transactions.[3]

Today's frictionless flows are not privacy preserving

Fingerprinting and silent risk profiles based on 3P cookies are used today to reduce friction by avoiding explicit authentication.

But they do not give user control of their privacy and may break as privacy norms change on the web.

Buying a t-shirt on the web (today).



T-shirt (Blue / M)

€2.00

Powered by stripe | Terms Privacy

Pay with card

Email
janedoe@stripe.com

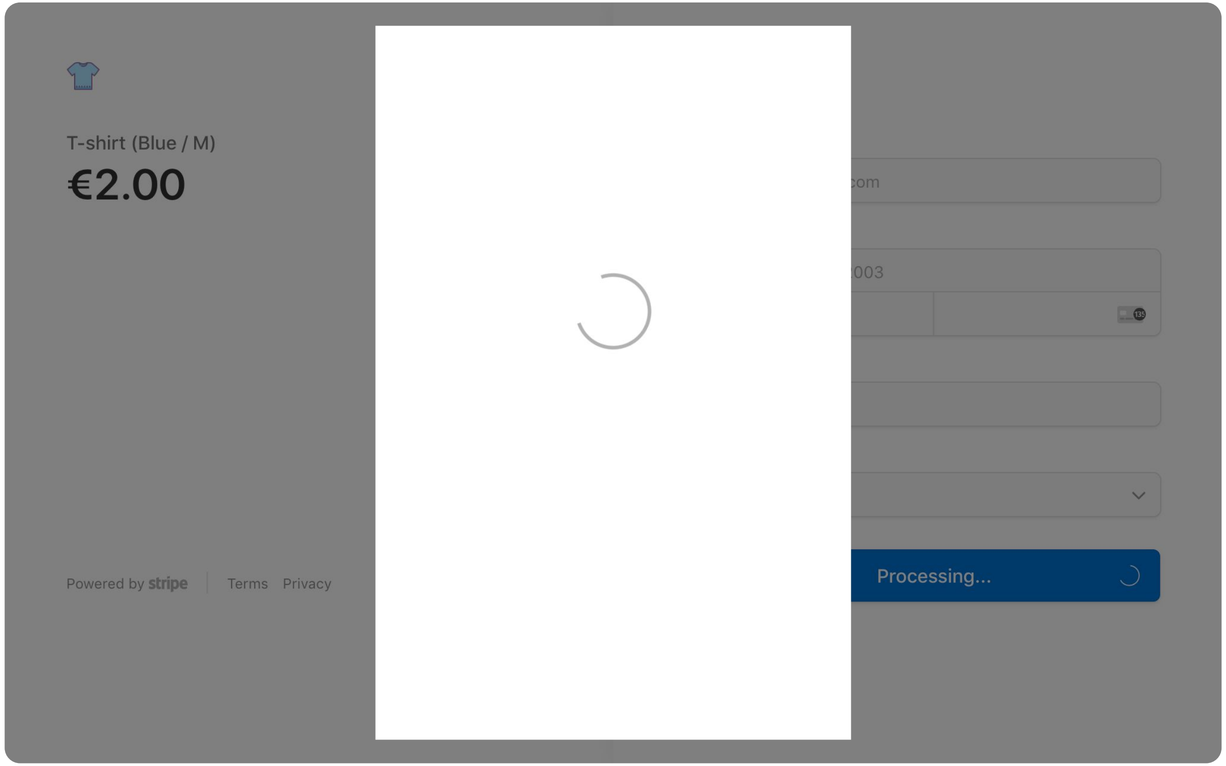
Card information
5555 5555 5555 4444
01 / 25
123

Name on card
Jane Doe

Country or region
Ireland

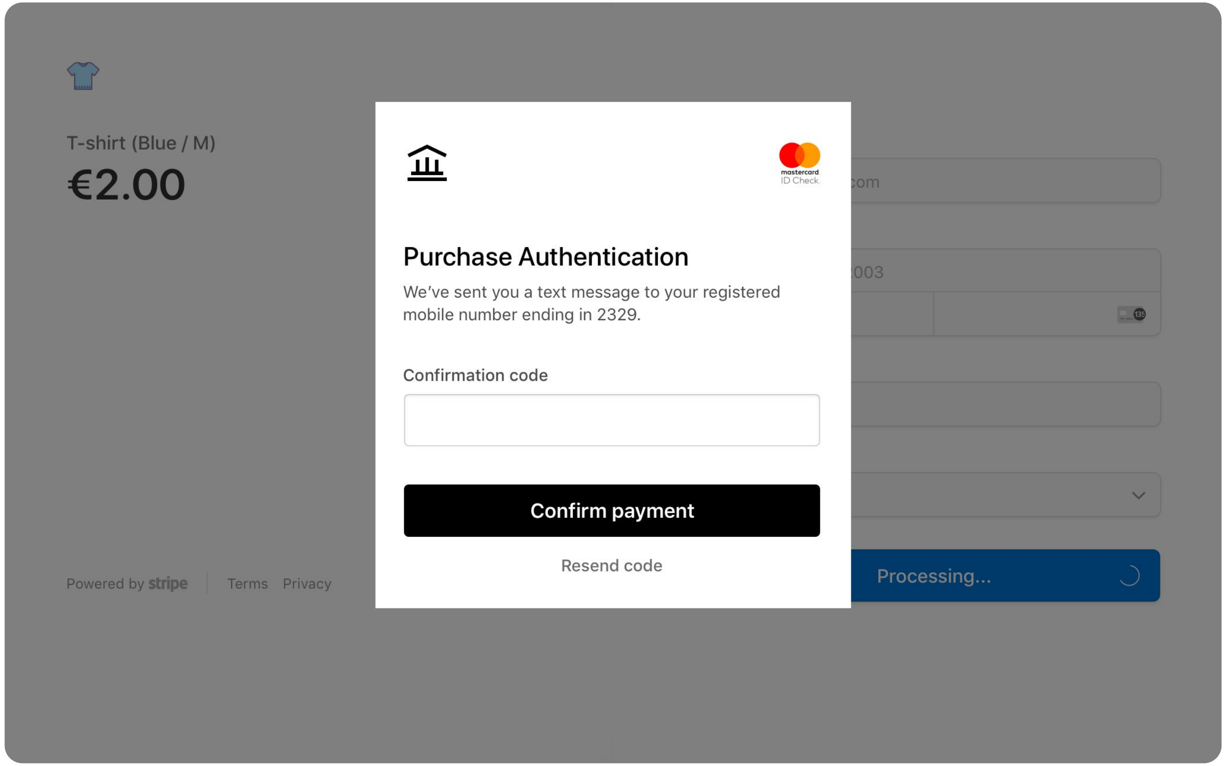
User enters card details

Buying a t-shirt on the web (today).



Bank (issuer) assesses the transaction...

Buying a t-shirt on the web (today).



T-shirt (Blue / M)

€2.00

Powered by stripe | Terms Privacy

Purchase Authentication

We've sent you a text message to your registered mobile number ending in 2329.

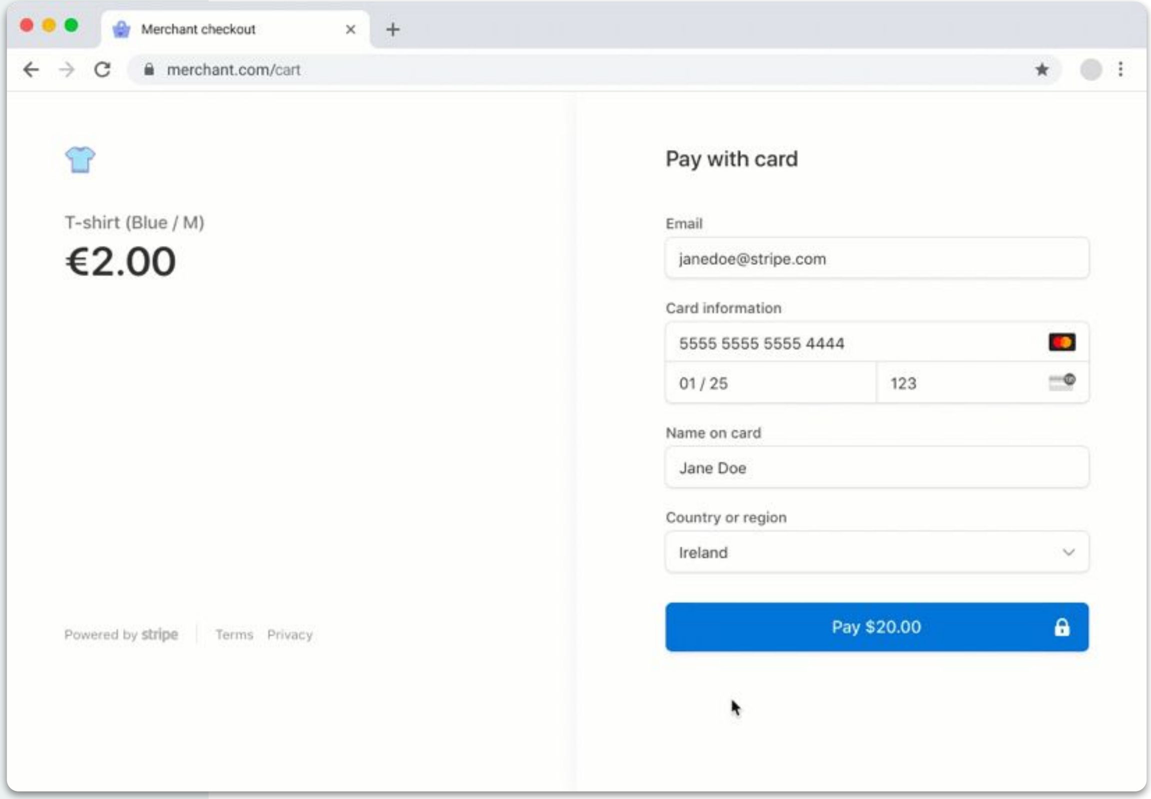
Confirmation code

Bank requests user to complete a step-up authentication.

Can we do better?

Seamless, WebAuthn-based user verification for all payment methods and all merchants.

Register once, authenticate across the web.



T-shirt (Blue / M)
€2.00

Pay with card

Email: janedoe@stripe.com

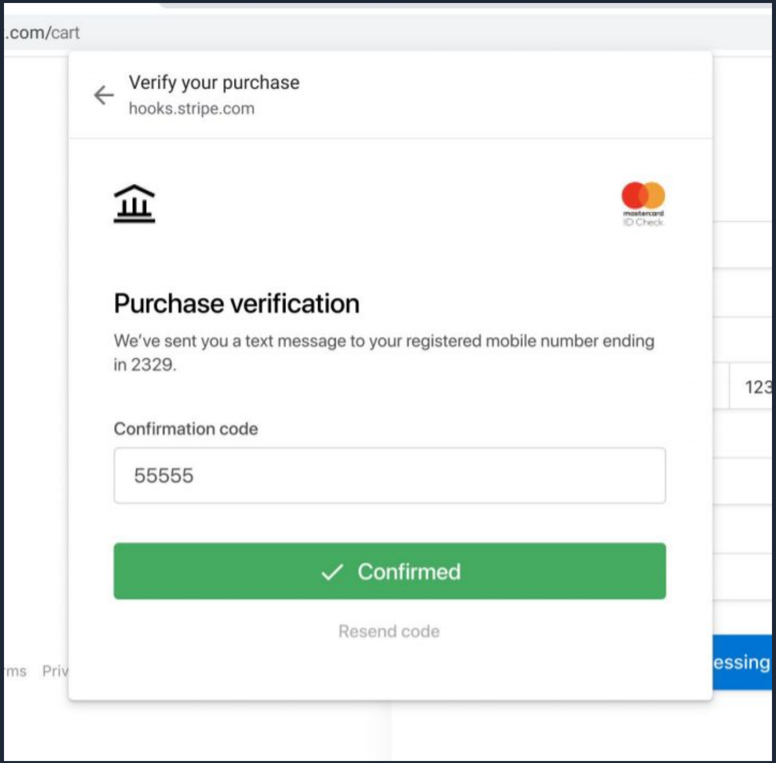
Card information: 5555 5555 5555 4444, 01 / 25, 123

Name on card: Jane Doe

Country or region: Ireland

Registration

1. During a transaction, user ID&Vs via a traditional method (e.g. OTP challenge), in a bank iframe.



.com/cart

Verify your purchase
hooks.stripe.com

Purchase verification

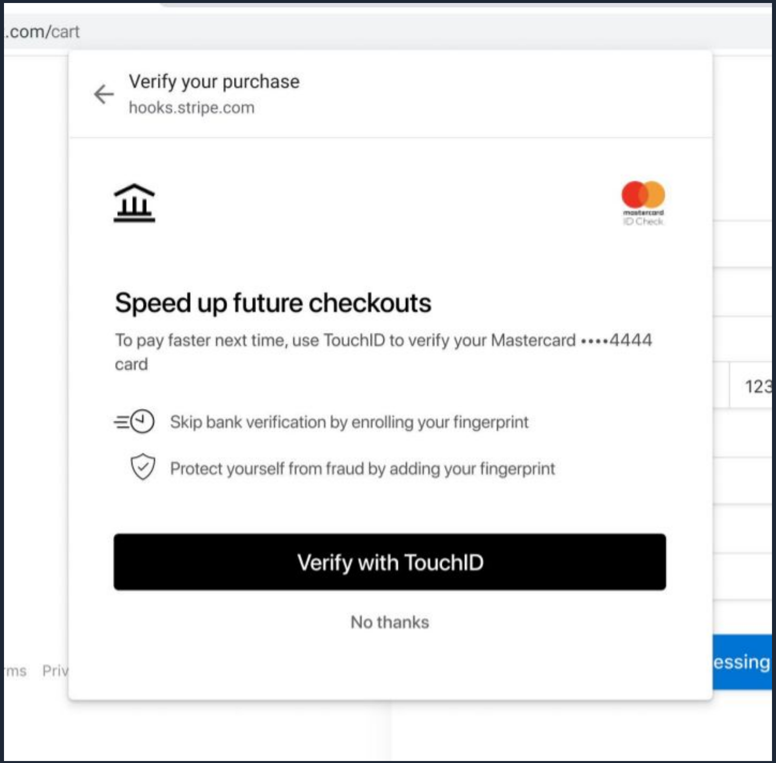
We've sent you a text message to your registered mobile number ending in 2329.

Confirmation code

55555

Registration

1. During a transaction, user ID&Vs via a traditional method (e.g. OTP challenge), in a bank iframe.
2. Bank offers user the chance to register this device for future checkouts.


.com/cart

Verify your purchase
hooks.stripe.com

Speed up future checkouts

To pay faster next time, use TouchID to verify your Mastercard ••••4444 card

Skip bank verification by enrolling your fingerprint

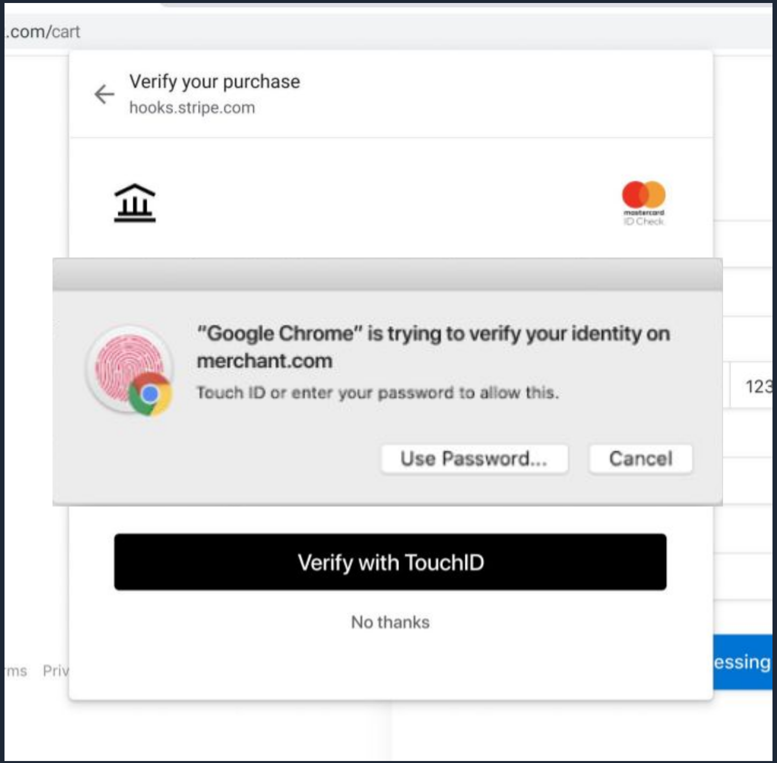
Protect yourself from fraud by adding your fingerprint

Registration

1. During a transaction, user ID&Vs via a traditional method (e.g. OTP challenge), in a bank iframe.

2. Bank offers user the chance to register this device for future checkouts.

3. Issuing bank invokes Credential Management API, with a 'payment' extension. Extension allows creation in cross-origin iframe.


.com/cart

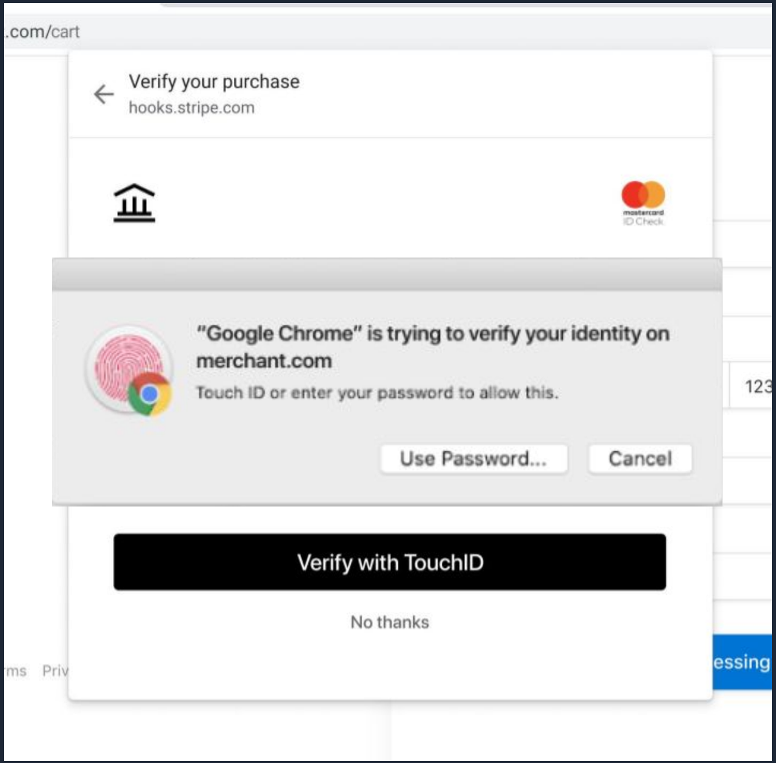
Verify your purchase
hooks.stripe.com

"Google Chrome" is trying to verify your identity on merchant.com

Touch ID or enter your password to allow this.

Registration

1. During a transaction, user ID&Vs via a traditional method (e.g. OTP challenge), in a bank iframe.
2. Bank offers user the chance to register this device for future checkouts.
3. Issuing bank invokes Credential Management API, with a 'payment' extension. Extension allows creation in cross-origin iframe.
4. After user authenticates, browser returns credential to the issuing bank iframe.
5. The issuing bank, acting as the Relying Party, registers the public key and instrument ID in their backend.


.com/cart

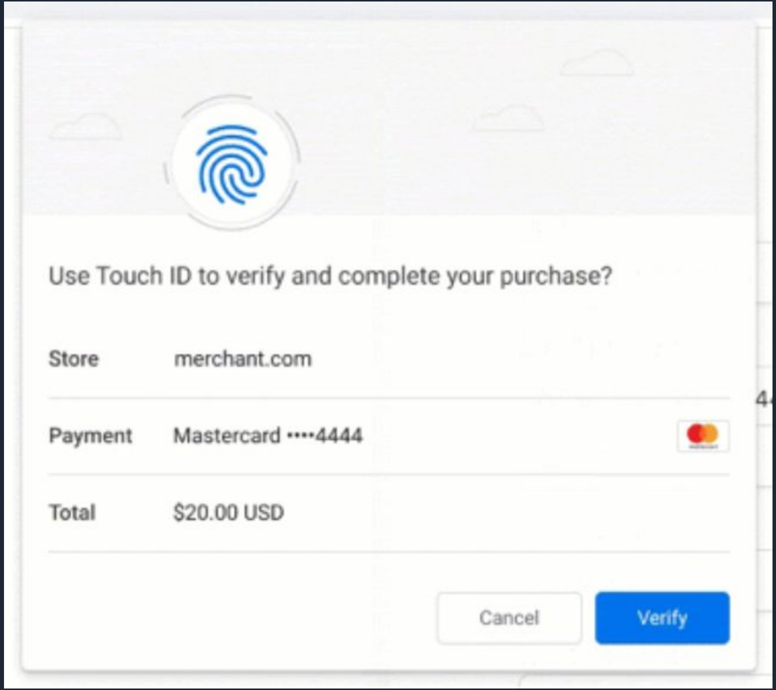
Verify your purchase
hooks.stripe.com

"Google Chrome" is trying to verify your identity on merchant.com

Touch ID or enter your password to allow this.

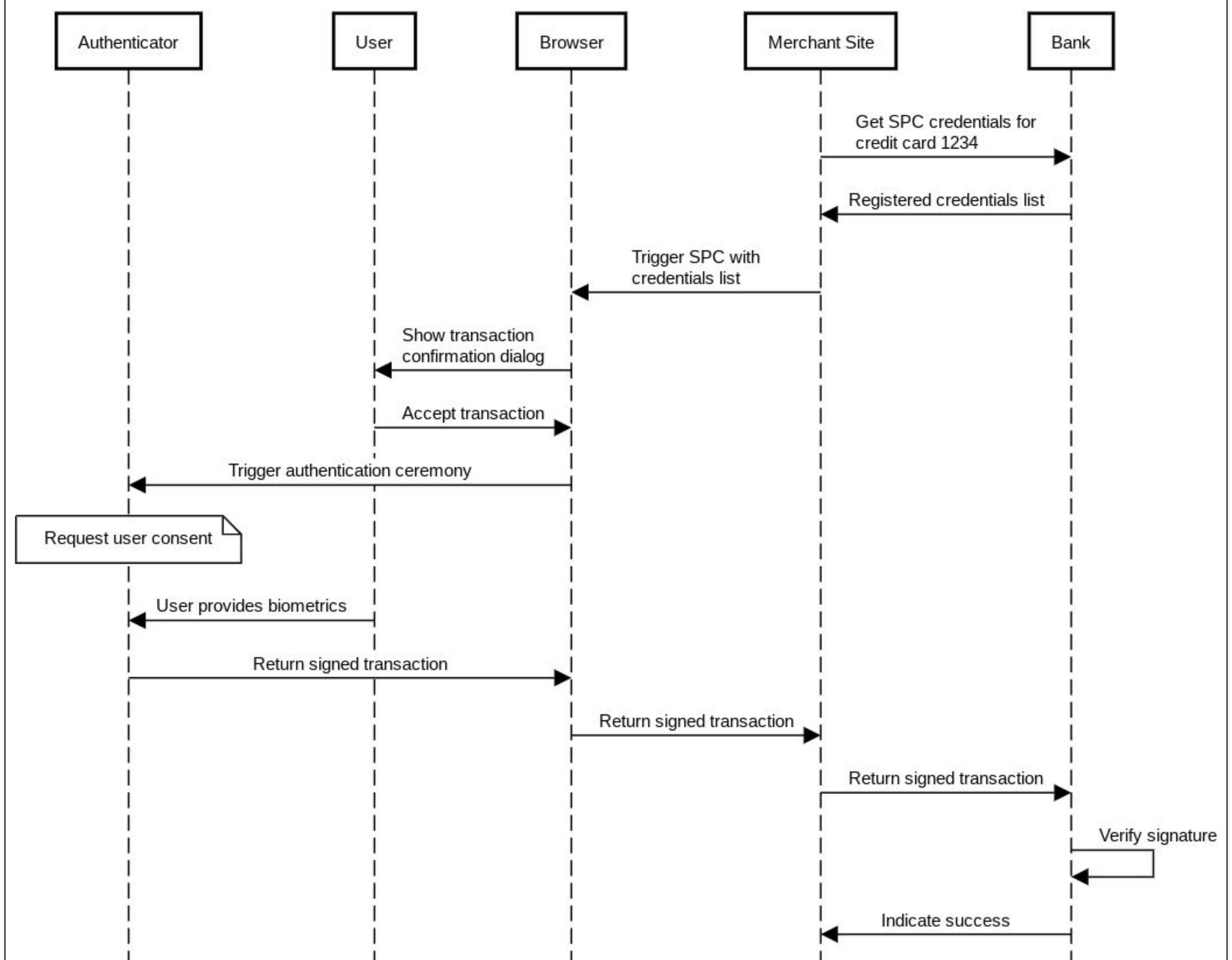
Authentication

1. Merchant requests a list of credential IDs from issuing bank via backend protocol (e.g. 3D Secure)
2. Merchant invokes Payment Request API **on their origin** with credential IDs and transaction details
3. Browser displays transaction details to user, collects biometric confirmation
4. Browser **binds transaction details into Web Authentication clientDataJSON** and returns signed assertion (Web Payment Cryptogram) to merchant.
5. Merchant submits Web Payment Cryptogram to issuer via backend protocol.
6. Issuer independently verifies the signature.


Use Touch ID to verify and complete your purchase?

Store	merchant.com
Payment	Mastercard ••••4444
Total	$20.00 USD

Authentication


Authenticator
User
Browser
Merchant Site
Bank
Get SPC credentials for credit card 1234
Registered credentials list
Trigger SPC with credentials list
Show transaction confirmation dialog
Accept transaction
Trigger authentication ceremony
Request user consent
User provides biometrics
Return signed transaction
Return signed transaction
Return signed transaction
Verify signature
Indicate success

Discussion Topics

1. Credential creation in cross-origin iframe
2. Cross-origin authentication ceremony
3. Payment-specific data in CollectedClientData
4. [Your questions/comments here!]