

SPC + Authenticators

Two relevant properties of SPC

Privacy: No credential probing!

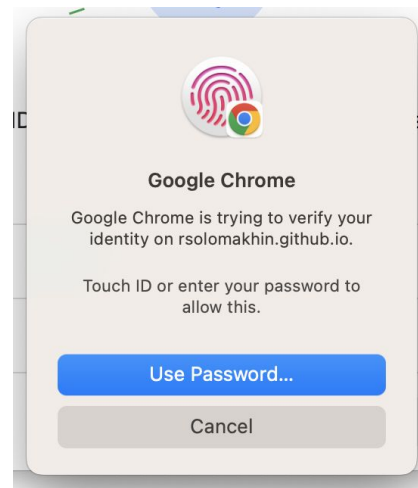
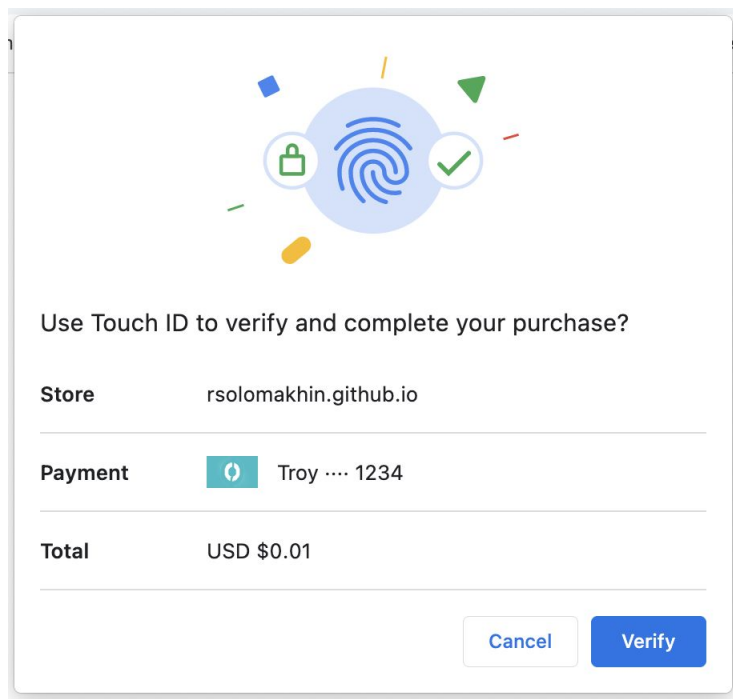
RP Security: 'Cross-origin' auth ceremony only with RP's permission!

Credential probing

- WebAuthn / web privacy requirement:
 - A website requires the users consent to know if a user **does or does not** have a matching credential available.
 - Both directions of this are important (i.e., knowing the absence of a credential is not allowed!)

Credential probing - positive affirmation

- Positive affirmation is easy:




Credential probing - negative affirmation

- Doesn't exist!
- We don't ask the user "are you ok with site X knowing that you don't have a credential for them" - it would just be confusing.
- Instead, both WebAuthn and SPC **combine output states** to make probing impossible:

User declines

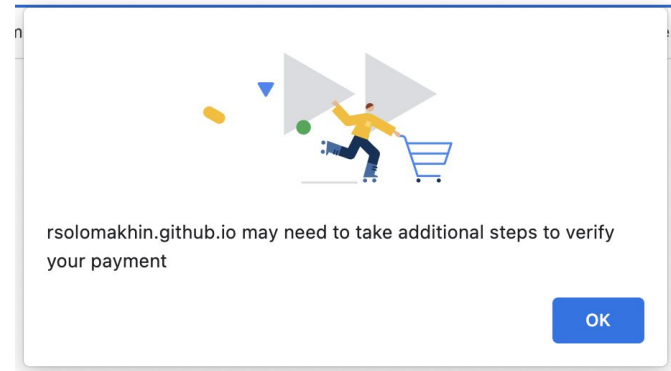
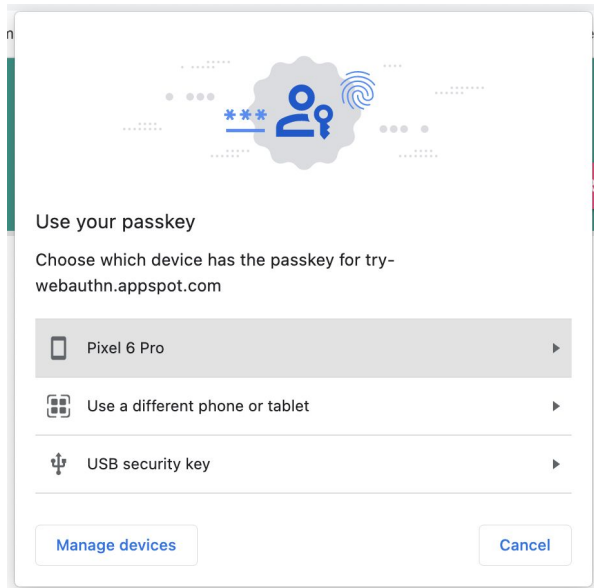
User has no credential



NotAllowedError: The operation either timed out or was not allowed. See: <https://www.w3.org/TR/webauthn-2/#sctn-privacy-considerations-client>.

Credential probing - timing attack

- To avoid a timing attack, both WebAuthn and SPC always have to show **some** UI, even if there are no matching credentials:



Credential probing - relation to authenticators

- Ok, so what does this have to do with authenticators?
- In order to know what UX to show, the browser has to be able to know if an authenticator device has credentials available.
- This is often called a credential listing API.

Credential listing API availability

- Android: ✓, but...
- Windows: ✓
- MacOS: ✗ (yet?)
- iOS: ✗
- Remote authenticators / Hybrid: ✗ (technically impossible if the device isn't 'connected' to the OS in some way)

- What do we do for SPC when this API isn't available? We cache credential existence in the browser itself... which has problems.
 - No longer cross-browser
 - Fails in bad ways if credential state changes underneath us

Ok, so you can at least use these APIs on
Android+Windows, right?

Ok, so you can at least use these APIs on
Android+Windows, right?

(Spoilers: No)

Remember the cross-origin opt-in requirement?

- Website merchant.com can only trigger SPC for credentials from bank.com if bank.com **opted-in** to this behavior at credential creation time!
- This is the 'thirdPartyPayment' bit now spec'd in FIDO, and also still part of the 'payment' extension in SPC (bit of a mess...)
- Not only does the browser need to be able to check credential availability, it also needs to be able to set and check for this bit.

thirdPartyPayment bit availability

- Android: ✓, but...
 - Windows: ✗
 - MacOS: ✗
 - iOS: ✗
 - Remote authenticators: ✗
-
- And what do we do for SPC when this bit isn't available? We cache the bit in the browser itself... which has problems.
 - No longer cross-browser
 - Fails in bad ways if credential state changes underneath us

Sigh.

The path forward

- Work with the remaining platform authenticators to support a listing credentials API.
 - MacOS is **possibly** going to have this - no promises/insider knowledge here, but hope.
- Work with the platform authenticators to support the thirdPartyPayment bit.
 - We should start on this yesterday - they don't tend to move super fast.
- Work with Android folks to address potential upcoming regressions for both of the above.
- Figure out a story for remote authenticators - some way for users to say 'hey I have a remote authenticator but its not plugged in yet'
- (Unrelated, but) fix the no-matching credentials UX to not be so terrible. It's a whole other deck...