Improving SPC fallback UX
Background Considerations

- Due to Web Authentication privacy requirements:
  - Do not want to reveal that user has no matching credentials.
  - Want “cancel” and “no matching credentials” to look the same from API perspective
  - Need some UX when no matching credentials; otherwise detectable through timing attack
- Do not want to provide link from transaction dialog to fallback experience (rationale: no links to arbitrary pages from secure UX)
- Merchant, not browser, in best position to present authentication options
Today

Matching credentials

No matching credentials
API Behavior

• Matching Credentials
  • Verify => Invoke FIDO
  • Cancel => Error “XYZ”

• No Matching Credentials
  • Ok => Error “XYZ”
New idea

Matching credentials

No matching credentials
API Behavior

• Matching Credentials
  • Verify => Invoke FIDO
  • Authenticate a different way => Error “ABC”
  • Cancel => Error “XYZ”

• No Matching Credentials
  • Confirm => Error “ABC”
  • Cancel => Error “XYZ”
Benefits

• No leakage that there are no matching credentials
• New signal available to caller about user intention: “confirm” v. “cancel”
• Easier to understand user experience (to be confirmed by UX teams)
More ideas

Matching credentials

To confirm purchase, review details then verify with TouchID (or another way).

Store: rsolomakhin.github.io
Payment: 0 Troy ₳ 1234
Total: USD $0.01
Verify with TouchID  Verify another way
Cancel transaction

No matching credentials

To confirm purchase, review details then proceed to verification step.

Store: rsolomakhin.github.io
Payment: 0 Troy ₳ 1234
Total: USD $0.01
Cancel to Verification
Even More Ideas

• Matching Credentials
  • Verify => Invoke FIDO
    • Good FIDO authentication => Assertion
    • Bad FIDO authentication (cancel / error / timeout) => Error “ABC”
  • Authenticate a different way => Error “ABC”
  • Cancel => Error “XYZ”

• No Matching Credentials
  • Confirm => Error “ABC”
  • Cancel => Error “XYZ”
  • Timeout to close dialog => Error “ABC” /* Assume user still wants to do transaction so give PSP another auth opportunity */