AuthnTic

Ian Jacobs, May 2020

Problem Statement

- Payments systems want to recognize authorized parties. As part of risk assessment, systems such as 3DS ask the question “Is this the same browser as the last time someone used this card to pay?”
- Solutions today rely heavily on browser fingerprinting and persistent storage.
- Browsers are limiting third-party storage capabilities and fingerprinting. **These changes are happening now and will break deployed code.** This is driving us to explore new strategies to enable risk assessment.
- Note: this topic is also being discussed elsewhere at W3C such as in the Advertising Business Group.

Goal

- Use a payment app to demonstrate a cascade of authentication flows where flows are preferred in this cascade order:

  1.“minimal UI”

  2. Web Authentication from a payment app window

  3. Prompt user to return browser-stored password credentials (no retyping

  4. Prompt the user to enter name/password

Scope

- In scope:
  - Two flows: Account bootstrapping (first visit) and re-authentication (second visit)
  - (1) Minimal UI flow and (2) payment app can open a window for user interaction (e.g., for selection of an instrument).
  - The demo should show where a 3-D Secure flow could be invoked, without invoking it (to simplify the demo).
  - Experimentation with a new class of PaymentCredential (see idea) to store credential ID without cookie and prevent tracking.
- Out of scope:
  - Use of browser or platform profiles to firewall identities.
  - Payment app installation (e.g., just-in-time or manual)
  - Credential lifecycle management (e.g., lost my authenticator).
  - Shipping

Deliverables

- Demo showing different flows, depending on the user environment conditions
  - *Ideally the demo works on 2 browsers*
- Blog post describing the experiment (to be done after the code-a-thon)

User environment conditions

- Authenticators
  - User has a FIDO2 platform authenticator (can be a phone)
  - User has a FIDO2 roaming authenticator that is not a phone
  - User has no authenticator
- Browser support for APIs
  - Browser supports Web Authentication / does not
  - Browser supports Credential Management API / does not

Resources

- How to FIDO and decision tree
- Google documentation on auto-sign in with Credential Management API
- Idea for a CM API class of credential to replace cookies for username storage