FIDO and Web Authentication

David Waite <dwaite@pingidentity.com>

Topics

What are FIDO, Web Authentication

How do they fit into the credentials ecosystem

How do the systems work

Current state and challenges

About Myself

- Work on various standards for Ping Identity
  - 20 years mostly in federated identity and MFA
  - Ping also has identity verification and decentralized identity products
- Participant in Web Authentication
- Vice-chair of the FIDO 2 Technical Working group
- Focus on privacy approaches and technologies

FIDO and Web Authentication

Web Authentication (WebAuthn)

- W3C Working group to standardize client-side API for interacting with strong authentication
  - Authentication provided by "authenticators" which can create and assert credentials in the form of public keys
  - Authenticators are expected to require user presence, no silent/machine authentication
- Supports primary and secondary authentication
- Can be backed by FIDO protocols, or a platform's own native functionality (e.g. Windows Hello, FaceID/TouchID)
- Describes message exchanges and cryptographically protected formats
- Extensible (with caveats)

Quick terminology

- **Discoverability** - can a relying party ask for a credential without knowing any information about the user
- Older U2F authenticators had no storage and only supported non-resident credentials; a list of handles corresponding to previous registrations by the user needed to be provided
- **User Presence** - always required, a gesture to show the user understands they are authenticating like a button press or tap of hardware against a NFC sensor
- **User Verification** - additional checks by authenticator that interactions are being performed by an authorized user - activation PIN check, biometric, etc.

FIDO Alliance

- The FIDO Alliance, established in 2013 as a way to promote stronger authentication and reduce the use of passwords
  - **UAF, U2F** : Independent initial protocols to support primary and second-factor authentication, respectively
  - **CTAP 2.x** : Technical specification underpinning the FIDO 2 efforts; describes operations and their transport over USB, NFC, Bluetooth and hybrid transports
  - **FIDO 2** : Umbrella term for CTAP 2.x and Web Authentication

Passkeys

- "A passkey is a better alternative to passwords"
- Not a technical term, rather a conceptual term to aid in consumer education/ adoption
- Maps to a broad category of "discoverable" credentials from a diverse set of authenticators
  - Platform Authenticators
  - Third-Party Software Authenticators
  - Hardware Authenticators in the form of key fobs or wearables

(Minimum Bar) security properties

- **Tracking resistance**: unique credentials are generated pairwise for relying parties, released only through consent
- **Breach resistance**: public key cryptography means reading credential database on the relying party does not provide for future exploits.
- **Strong phishing resistance**: cannot request credentials for a different relying party; relying party information baked into protocol response

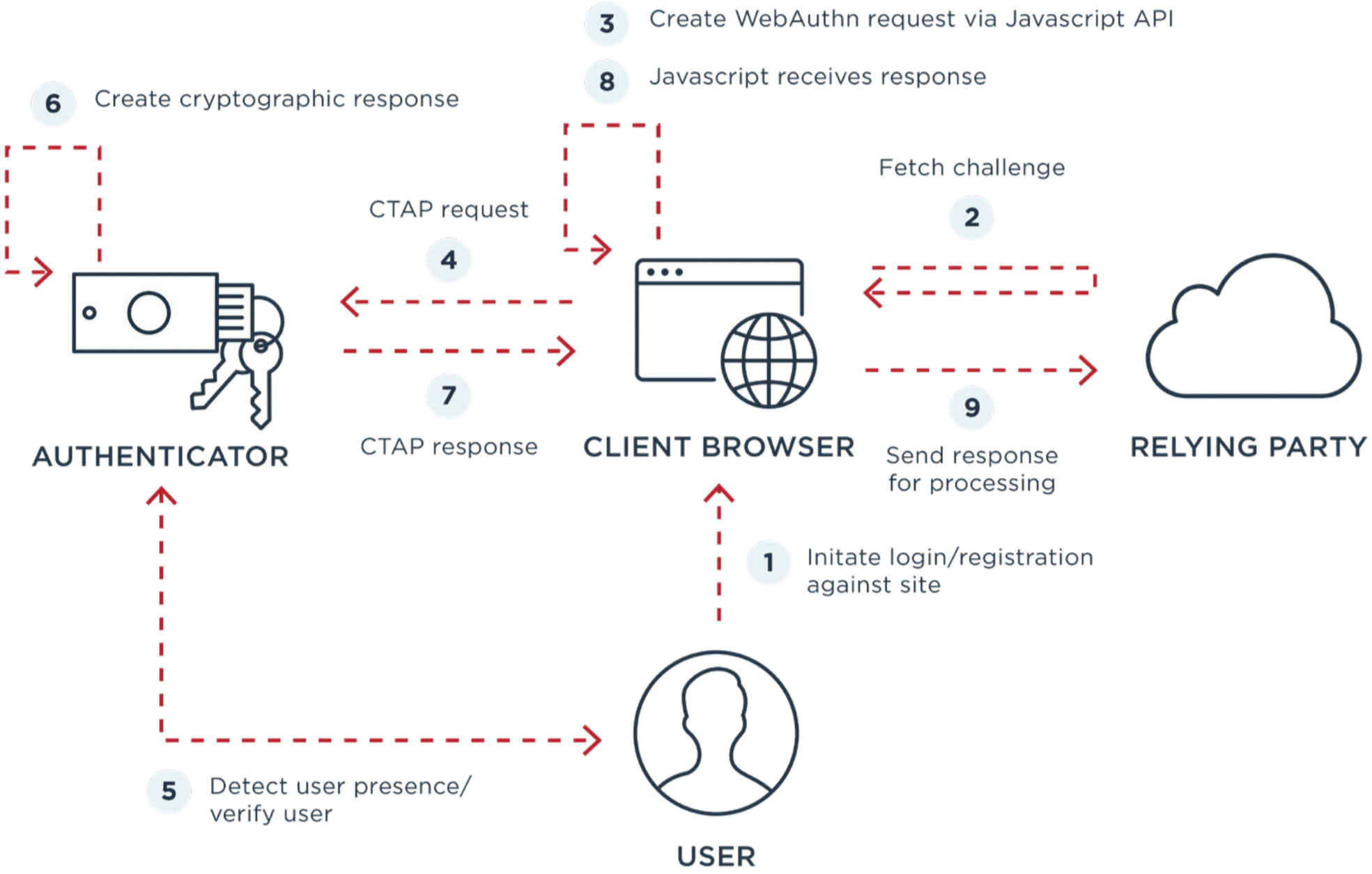
Place in Credential Ecosystem

Credential Capabilities

- Pairwise, NOT globally accepted
- NOT representing certifications, qualifications, or other identity attributes
- NOT representing authority or other authorizations
- Purely decentralized, created locally by authenticator

- Pure authentication, e.g. "proof this is the same party I saw previously"
  - Optional attestation, e.g. "how I verify the user and my security properties"
  - Optional data storage

How it works


3 Create WebAuthn request via Javascript API
8 Javascript receives response
6 Create cryptographic response
Fetch challenge
2
CTAP request
4
7
CTAP response
9
Send response for processing
AUTHENTICATOR
CLIENT BROWSER
RELYING PARTY
1 Initate login/registration against site
5 Detect user presence/ verify user
USER

Current State

Market Evolution

- All major browsers have had support for at least WebAuthn Level 1 for years
- Moving from a small number of hardware-based authenticators to ubiquitous platform-provided authenticators
  - Platform authenticators have different security properties (recoverability/ syncing), leading to a bit of growing pain for regulated industries
- Significant investment around consumer adoption; adoption of the passkey terminology, iterative UX refinement by platforms
- Platform support for software "passkey providers", such as consumer password managers

Market Evolution (continued)

- For consumers, passkey metaphor aligns with password manager adoption
  - Without asserted security properties, simply "a better alternative to passwords"
- Autofill behavior matching password managers reduces the need for the user to learn mechanics or terminology; reduces churn
- The hope is as uptake improves, relying parties do not feel the need to explain passkeys to users
  - …similar to how they do not explain passwords today

Standards-in-progress

- Web Authentication Level 3
  - Adds call-outs for conditionally mediated UI (form fill)
  - Synced credential information for sites
    (not for rejecting credentials - reporting recoverability burden on site)
  - Various quality-of-life improvements (JSON wire formats)
  - Many features already deployed by browsers
- CTAP 2.2
  - Supporting functionality for Level 3
  - Hybrid transport (cross-device/cross ecosystem)

Open World Model

- End user selects preferred authenticator
  - Relying party evaluates how well authenticator meets their requirements
  - Relying party lets user in or prompts for additional factors
- A private party (e.g. enterprise) may restrict to just authenticators they have issued
- Public-facing relying parties are expected to honor user choice
- Goal is to allows for a diverse ecosystem for authenticators

On Attestations

- Attestations and the open model have a complex relationship
  - Do not want sites to outright reject user choice in authenticators
  - Do not want to recreate user-agent problem, where new authenticators have to lie due to allow-lists
- Security Key Fobs, often purchased for the end-user for access to closed environments, have a motivation to provide attestations.
- Software-based authenticators wanting broad adoption have different motivations, and have been resistant to provide fingerprinting information
- Known gaps for regulated industries; active areas of research/development