WebAuthn/FIDO2 deployment feedback R09

9/20/2019

Max Hata, Koichi Moriyama

NTT DOCOMO, INC.

Introduction

- Thanks to the contributors to WebAuthn WG @W3C and FIDO2 TWG @ FIDO Alliance for all their hard work, many products are becoming available for deployments to achieve simpler and stronger authentication.
- NTT and Japan Teams, through their activities of FIDO Japan WG and Consumer Deployment WG @FIDO Alliance, are gathering voices mainly from RPs who are engaged in WebAuthn/FIDO2 deployment to understand the users' needs and issues.
- Based on the initial attempts, we have feedback that includes some challenges for WebAuthn/FIDO2 deployments.
- They include various aspects.
- We would like to share some of the feedback that relates to WebAuthn WG.

Contributors

- FIDO Alliance WGs
  - FIDO Japan WG
  - FIDO Korea WG
  - FIDO Europe WG
  - Consumer Deployment WG
- Individual companies
  - LINE, Yahoo! JAPAN, NTT DOCOMO, ISR, KDDI, SoftBank, Thales

High Level Feedback

1. Uneven feature support by browsers / platforms as of today
2. End users want RPs to offer simple and frictionless user experiences (UXs)
3. Lack of best practices to develop successful password-less UXs

Additional Voices:

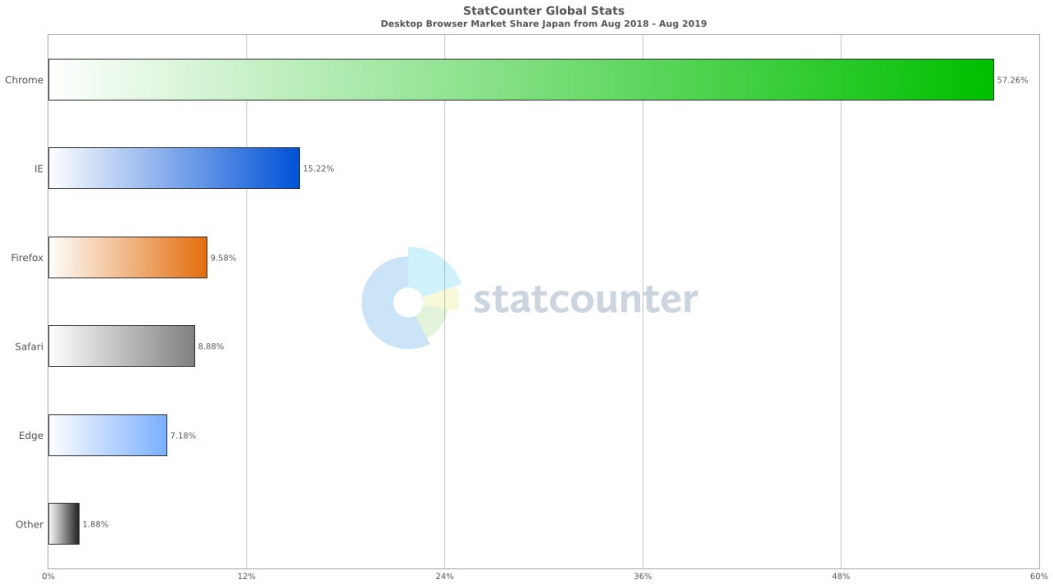
- Lack of browser support for WebAuthn extensions that would support various use cases

1. Uneven feature support by browsers / platforms as of today

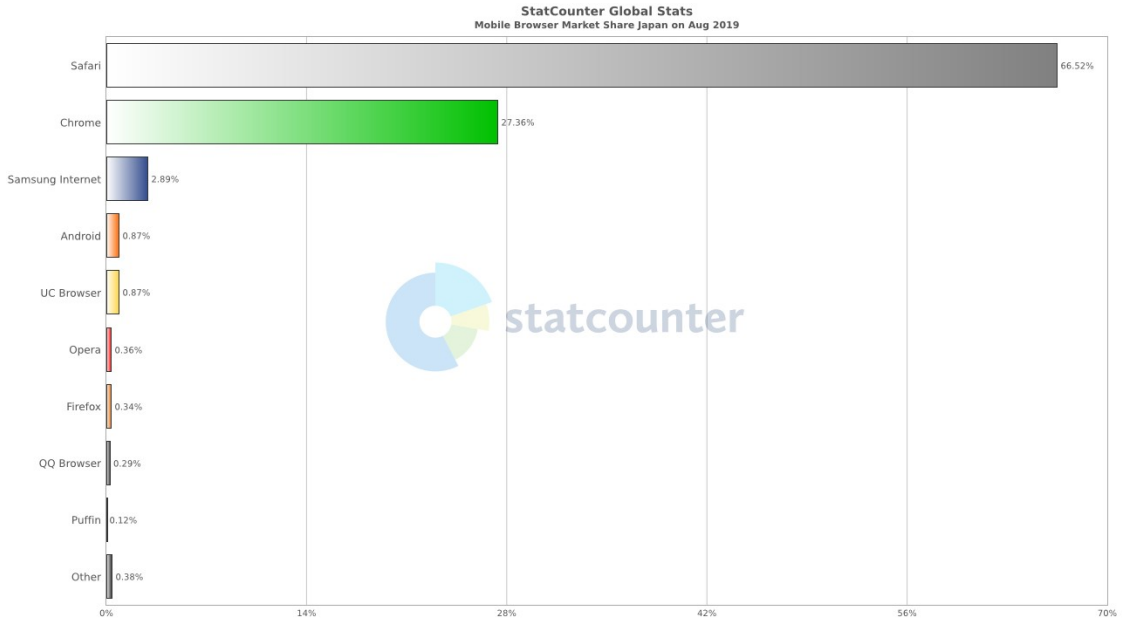
- WebAuthn feature support by major browsers is critical for deploying WebAuthn/FIDO2 commercially.
- They are making progress but there are still limitations.
- Safari/iOS coverage is an issue for wide range deployment of WebAuthn due to high Safari/iOS share for mobile in Japan.

- The accurate progress updates of implemented features of each client need to be clearly communicated to the ecosystem.

Browser market share in Japan (Aug. 2019)



Desktop



Mobile

Source: https://gs.statcounter.com

Example:
WebAuthn/FIDO2 feature implementation status (unofficial)

FIDO2 Implementation Status: July 2019											
		Chrome Desktop				Chrome Mobile		Windows 10 (May 2019 version)			
		Windows	MacOS	ChromeOS	Linux	Android	iOS	Old Edge	New Edge	Chrome	FireFox
U2F API		O	O	O	O	deprecated	O	----	O	O	O
WebAuthn API		O	O	O	O	O	O	O	O	O	O
CTAP1/U2F	USB	O	O	O	O	O	----	O	O	O	O
	NFC	O	----	----	----	O	----	O	O	O	O
	BLE	O	. . .	. . .	. . .	O	O	O	O	O	O
CTAP2 (Core)	USB	O	O	O	O	. . .	----	O	O	O	O
	NFC	O	----	----	----		----	O	O	O	O
	BLE	O	. . .	. . .	. . .	. . .	. . .	O	O	O	O
	Platform Authenticator	O	O	----	----	O	----	O	O	O	O
	caBLE client (to be signed into) - Next Version	O	O	O	----	----	O	----	O	O	----
	caBLE authenticator (can use to sign in with) - Next Version	----	----	----	----	O	. . .	----	O	O	----
	Resident Key (External) / Account selector / empty allowList	O	O	O	O	----	----	O	O	O	O
	Resident Key (Internal) / Account selector / empty allowList	O	O	O	O	----	----	O	O	O	O
	Client PIN (external UV)	O	O	O	O	----	----	O	O	O	O
	UVM Extension	----	----	----	----	O	----	----	----	----	----
Additional Features	isUVPAA()	O	O	O	O	O	----	O	O	O	O
	isUVPAA() only true for fingerprint (a temporary measure)	----	O	O	O	O	----	----	----	----	----
	getTransports() - Next Version	O	O	O	O	----	----	----	O	O	----
	Credential Management	O	. . .	. . .	...	----	----	O	O	O	O
	Biometric Enrollment	O	. . .	. . .	...	----	----	O	O	O	O
Other special cases tracked	UX & NotAllowedErrors for not-registered	O	O	O	O	----	----	O	O	O	O
	AbortController (RP can abort a request)	---	O	O	O	----	----	----	----	----	----
	Attestation prompt for AttestationConveyancePreference=Direct/Indirect	?				----	----	O	O	O	O

Source: FIDO Alliance preliminary strawman draft (as of July 2019).
This was created experimentally as a trial.

Voices

1. From the perspective of Service Providers, it is difficult to guide their customers in relation to Browsers being constantly evolving and changing its FIDO2 usages and functions.
   - We would like to request an official and real-time updates on such items by Browsers, along with hardware related functions, such as BLE.
2. We would like to have following items to be included on the FIDO Alliance website which indicates the adoption status of various platforms
   - Indicate versions of each supported features. For examples; USB (Support v70), NFC (No Support), BLE (Support v74)
   - Indicate W3C extensions for each supported features.

Source: FIDO Korea WG

2. End users want RPs to offer simple and frictionless user experiences (UXs)

- 2.1 Selecting User Verification Method
  - If an Authenticator supports more than one User Verification Method, there is no way to select the desired User Verification.

- 2.2 Selecting authenticator attachment
  - RPs know their consumer users and need to tailor UX to the customers' needs and preferences.

2.1 Selecting User Verification Method

- Multi-modal is already popular for authentication.
  - E.g., fingerprint and Iris
- Multi-modal supports users for their preference and their situations.

2.2 Selecting authenticator attachment

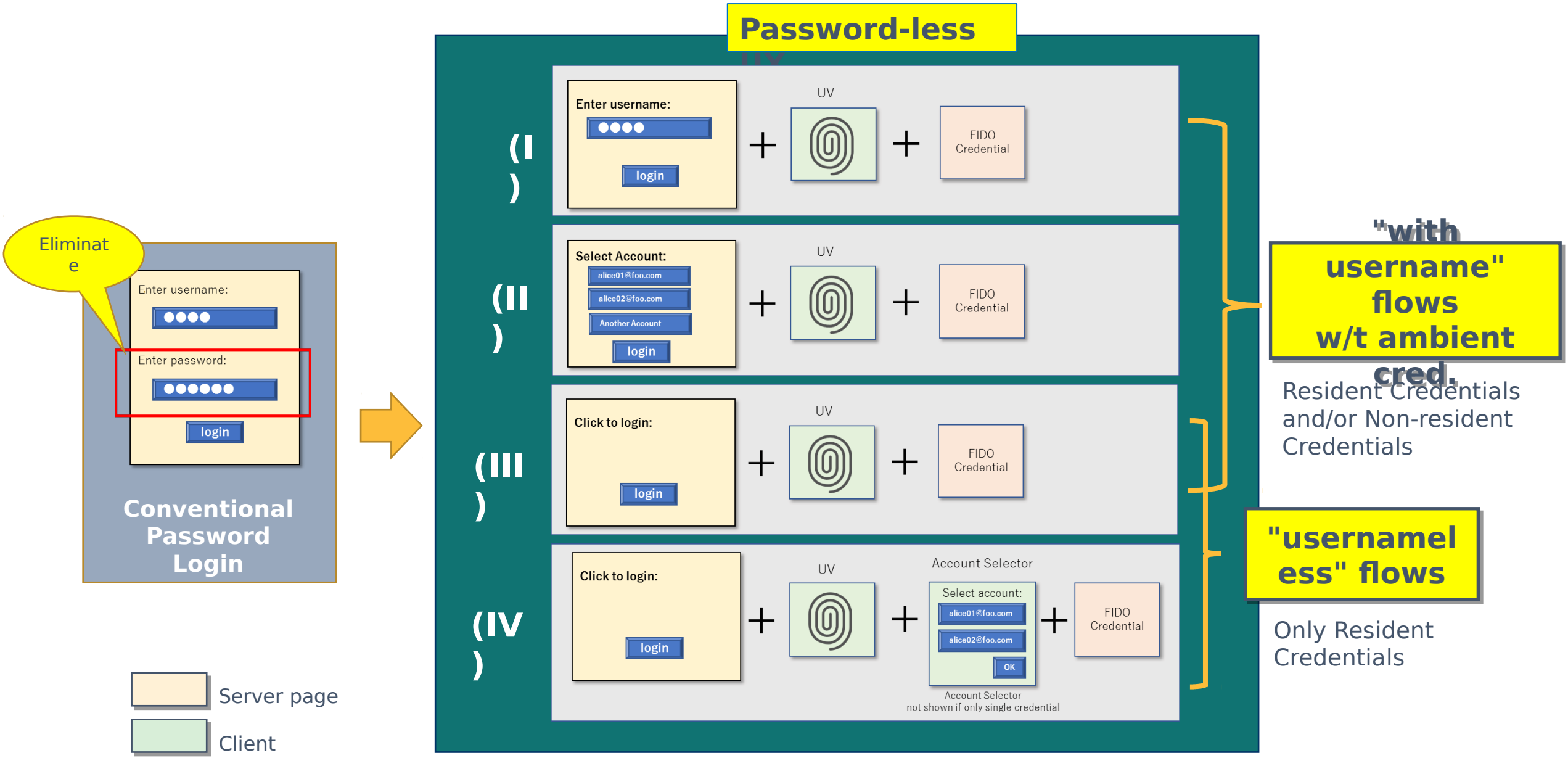
WebAuthn Operation		Selection attachment/transports	Note
Create()		Possible	
Get()	w/t credentialIDs	Possible	Do we have consistent behaviour among various browsers/platforms?
	empty	**Not possible**	https://github.com/w3c/webauthn/issues/1267

- RPs need to be able to select which attachment they want to invoke.
- Some RPs start deployment with platform authenticators only first, e.g., mobile phones. Showing cross-platform attachment not supported confuse many consumers who do not know the attachment.
- RPs need to be able to select attachment to ensure successful adoption by their targeted customers.

3. Lack of best practices to develop successful password-less UXs (1/2)

- WebAuthn/FIDO2 define generic building blocks. RPs need to pick up these blocks to build their services. It is not a turn-key solution.
- It is not straightforward for many RPs to select right ones to come up with simple and frictionless services for consumers:
  - Coverage of browsers and platforms
  - Features supported by each client
  - Selecting right features, e.g. resident/non-resident credentials
  - Browsers and/or native apps
  - Error handling for various cases that users may experience
    - RPs need to eliminate or minimize error cases that can be found only after user intervention.
    - Instead, they need to find it before user intervention, so that they can preemptively guide the users appropriately.

FIDO Password-less Login UX Variations (2FA)



3. Lack of best practices to develop successful password-less UXs (2/2)

Recommendations:

- WebAuthn spec. offers many options. But what are the recommended models for RPs to deploy are not clear. This is confusing RPs.
- Describe more deployment aspects in the WebAuthn specs, e.g., https://github.com/w3c/webauthn/pull/1300
- Develop white papers and blogs on best practices for deployment models.
  - including how various errors are handled to enable frictionless UX.

Additional Voices

Lack of browser support for WebAuthn extensions that would support various use cases

- RPs want to use extensions to address various use cases.
- Major extensions are defined by the spec., but they are optional for clients.
- No major browsers support extensions except for a limited one.
- Unless browsers support extensions, RPs cannot use them, or authenticator vendors will not implement extensions.

Priority extensions that need to be supported

txAuthSimple	Transaction Confirmation
txAuthGeneric	Transaction Confirmation
authnSel	For secure services, only the selected Authenticator shall be supported
exts	Default for extension
uvi	Users to be distinguished when multiple biometrics are registered
uvm	Default for uvi and authSel

Source: FIDO Korea WG

Transaction Confirmation (TC)-Voices

- The need for TCs (txAuthSimple and txAuthGeneric) is a regulatory one for financial transactions, PSD2.
- PSD2 mandates, in the Regulatory Technical Standards, that for remote commerce the authentication code (for FIDO that would be the signed response from the authenticator) should be “dynamically linked” to the transaction details.
- To use FIDO2 for e-commerce transactions, there is a need to support dynamic linking. As the browsers do not support the txAuthSimple or txAuthGeneric extensions, FIDO2 is seen as not compliant with PSD2.

Source: FIDO Europe WG