

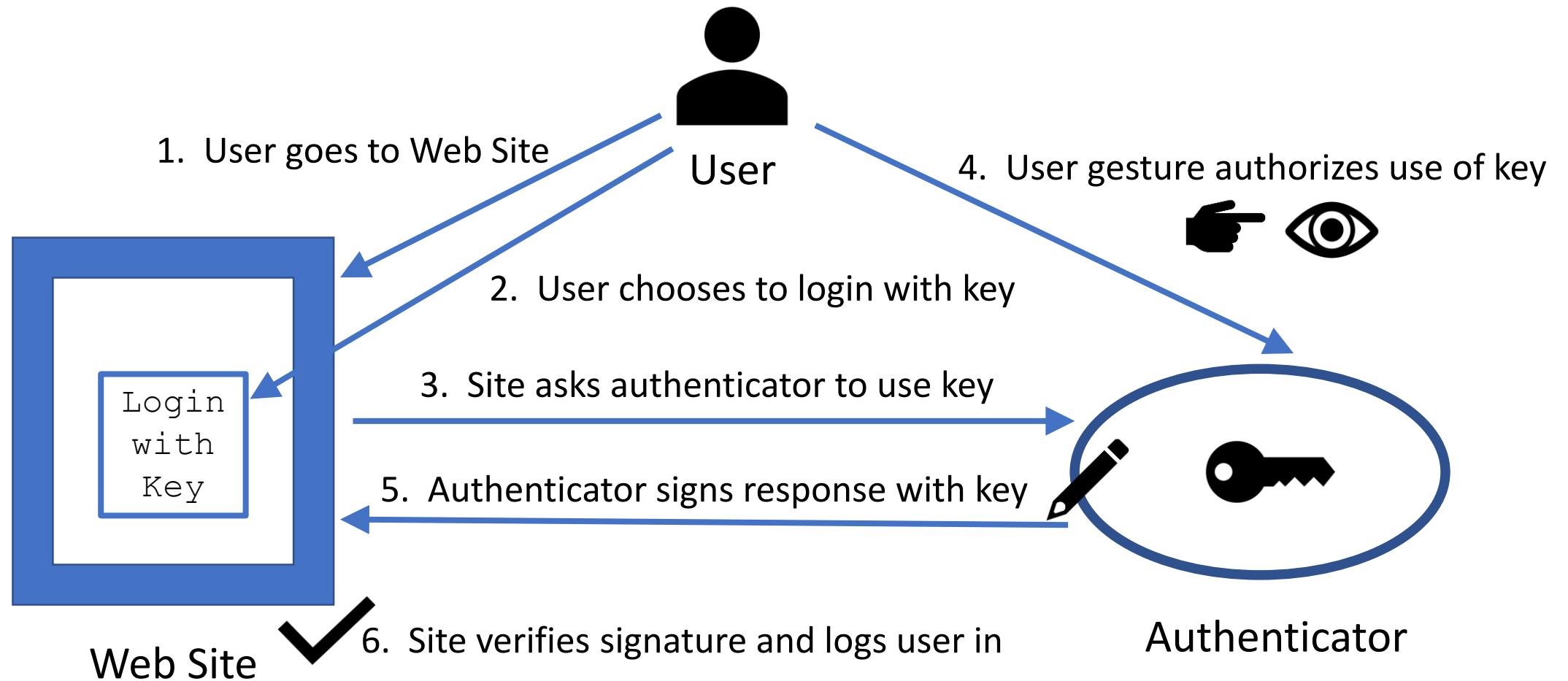
Strong Authentication using Asymmetric Keys on Devices Controlled by You

Dr. Michael B. Jones

Identity Standards Architect, Microsoft

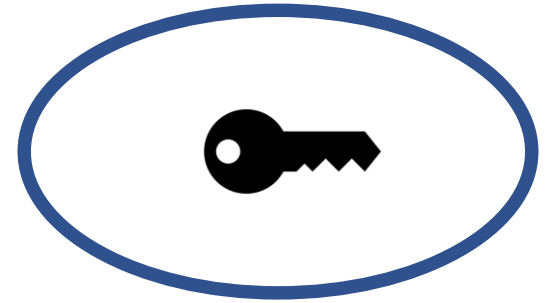
May 10, 2017

Web Authentication using Asymmetric Keys



What's an Authenticator?

- An Authenticator is an abstraction that
 - Can securely use private keys for authentication
 - Will only use those keys when prompted by a user gesture
- What kinds of places might keys for an authenticator be?
 - TPM on laptop
 - Secure element on phone
 - Storage on connected authenticator device
 - Encrypted by the authenticator and held elsewhere for it
- What kinds of user gestures might prompt user of keys?
 - Biometric
 - PIN
 - Touch



What's Strong about using an Authenticator?

- Authenticators
 - don't expose any secrets like passwords that can be stolen or guessed
 - keep a private key private and sign with it – providing proof of possession
 - only use the key when authorized by a user gesture

The Standards Making it Possible

- W3C Web Authentication (WebAuthn)
 - Enables sign-in with methods stronger than passwords
 - with authenticators using securely held private keys
 - that use the private key only with user permission
 - which is given to the authenticator with a user gesture
 - such as a biometric or PIN.
- FIDO 2.0 Client to Authenticator Protocol (CTAP)
 - Can be used with WebAuthn
 - to enable use of remote authenticators
 - such as those on mobile phones or connected devices
 - to be used when signing in.

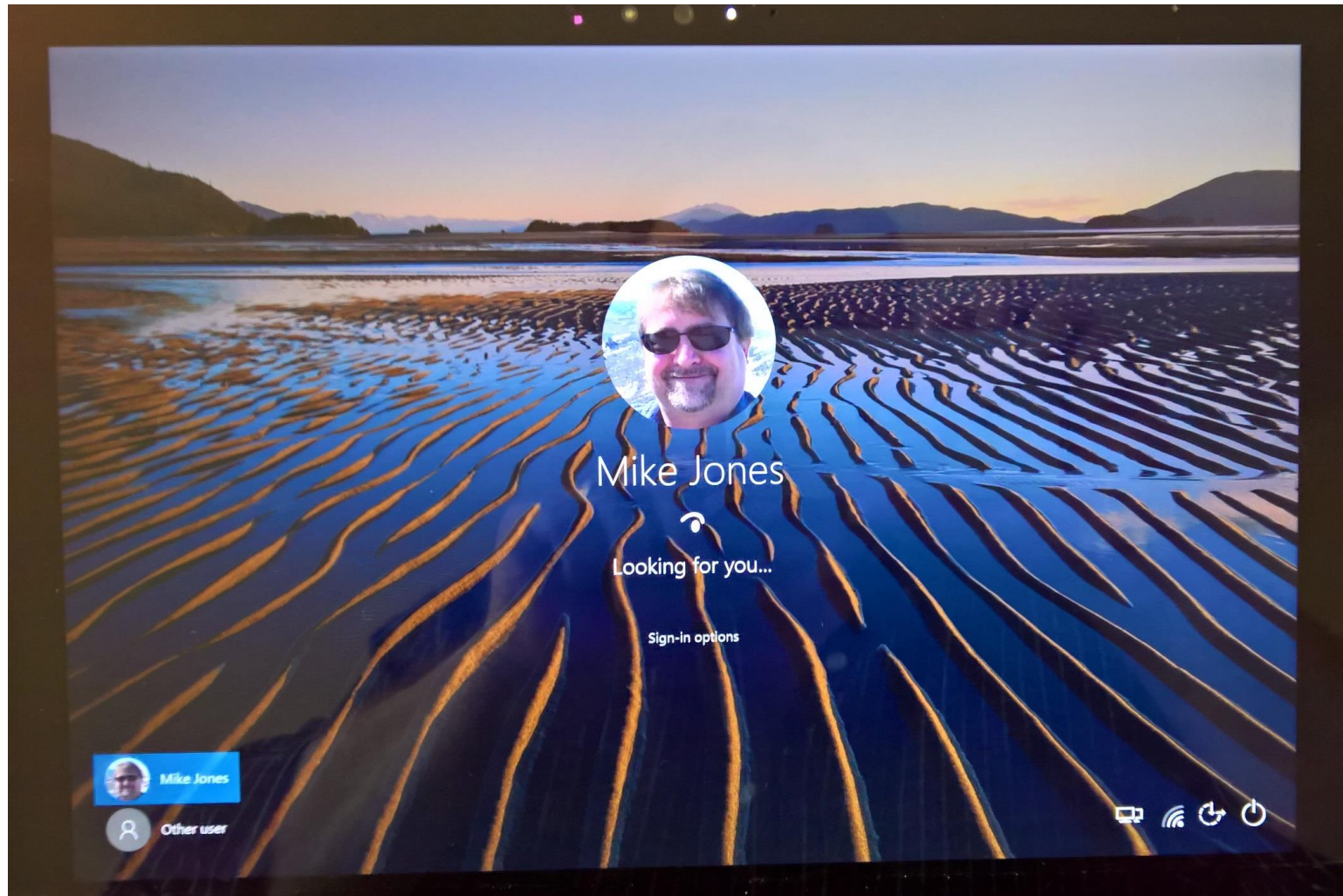
Is WebAuthn for the first or second factor?

- It is for both use cases
- When first factor, user is logged in directly using authenticator
 - Requires that the user gesture be specific to the user
- When second factor, authenticator augments first factor
 - The first factor is often a traditional username/password
 - The second factor tests user presence, but need not be user-specific
 - This is the way that existing U2F devices are used

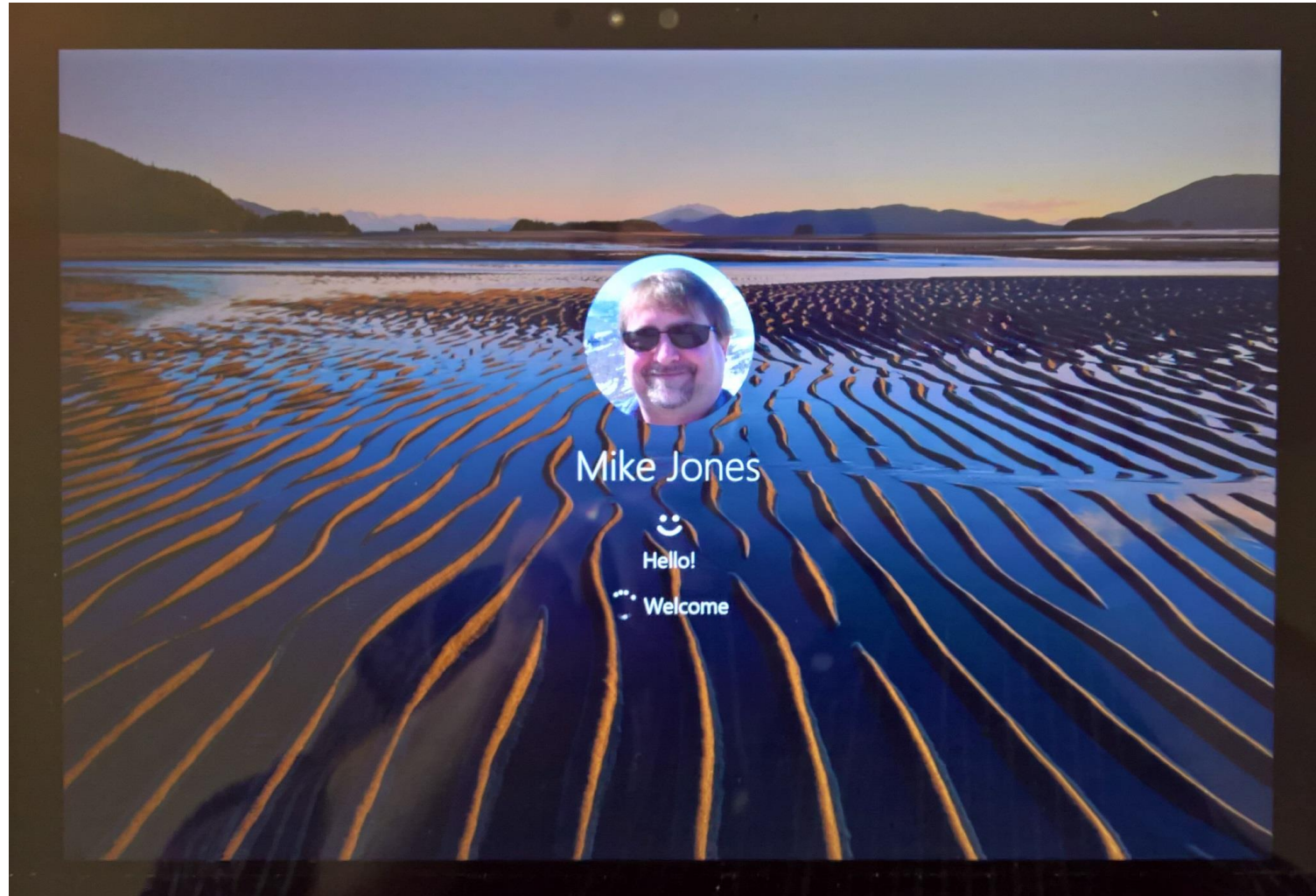
Example first factor user experience

- Using Windows Hello to log into my Surface 4
 - This is using a Microsoft-developed protocol predating WebAuthn
 - (Microsoft donated this protocol to the FIDO Alliance to use as they saw fit)
- Windows 10 implements the authenticator and stores the key
- The user gesture used is facial recognition
 - Could also be a fingerprint or PIN

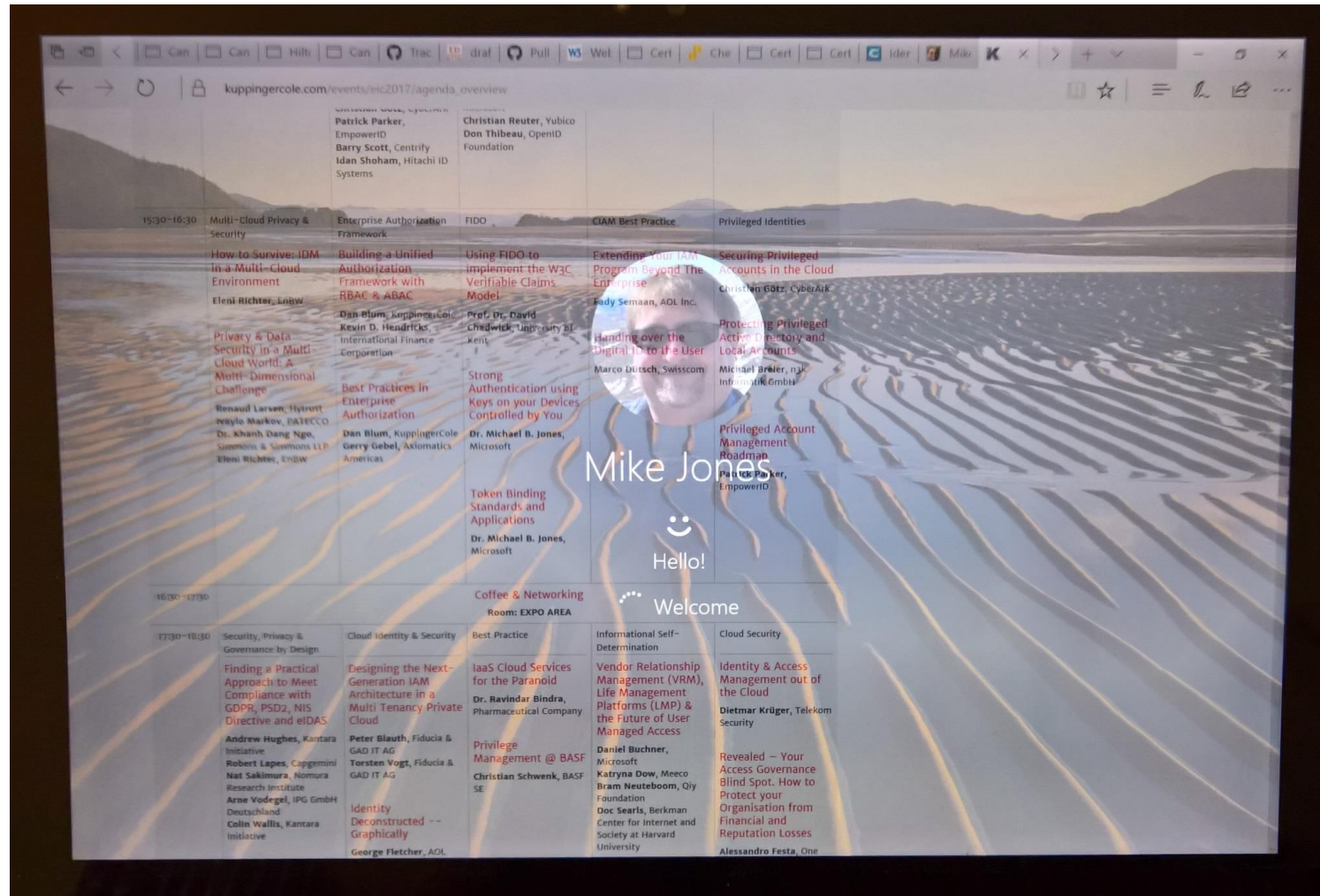
Looking for you... (camera on)



Hello Welcome... (camera off)



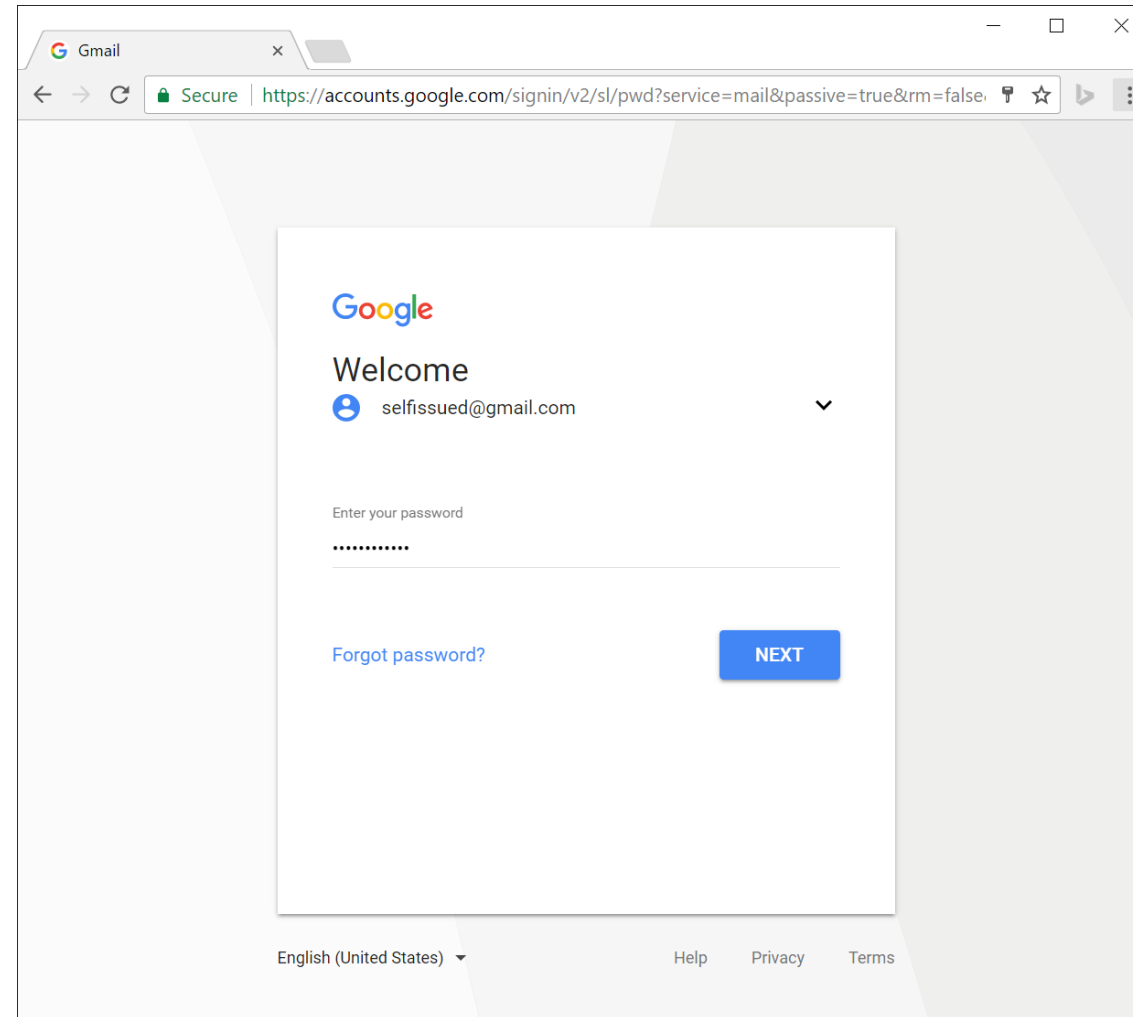
Signed in and transitioning to desktop



Example second factor user experience

- Using Yubico YubiKey as second factor for a Google account
 - This is using the FIDO U2F protocol predating WebAuthn and FIDO 2.0
- The authenticator is attached by a USB port
- The user gesture is touching a capacitive touch sensor
 - Note that this is not user-specific, since anyone could successfully touch it

Prompt for first factor (password)



A screenshot of a web browser window displaying the Google sign-in page. The browser's address bar shows the URL `https://accounts.google.com/signin/v2/sl/pwd?service=mail&passive=true&rm=false`. The page features the Google logo at the top, followed by the word "Welcome" and the email address "selfissued@gmail.com". Below this, there is a prompt "Enter your password" with a text input field containing masked characters. A blue button labeled "NEXT" is positioned to the right of the input field. A link for "Forgot password?" is located below the input field. At the bottom of the page, there is a language selector set to "English (United States)" and links for "Help", "Privacy", and "Terms".

Google

Welcome

selfissued@gmail.com

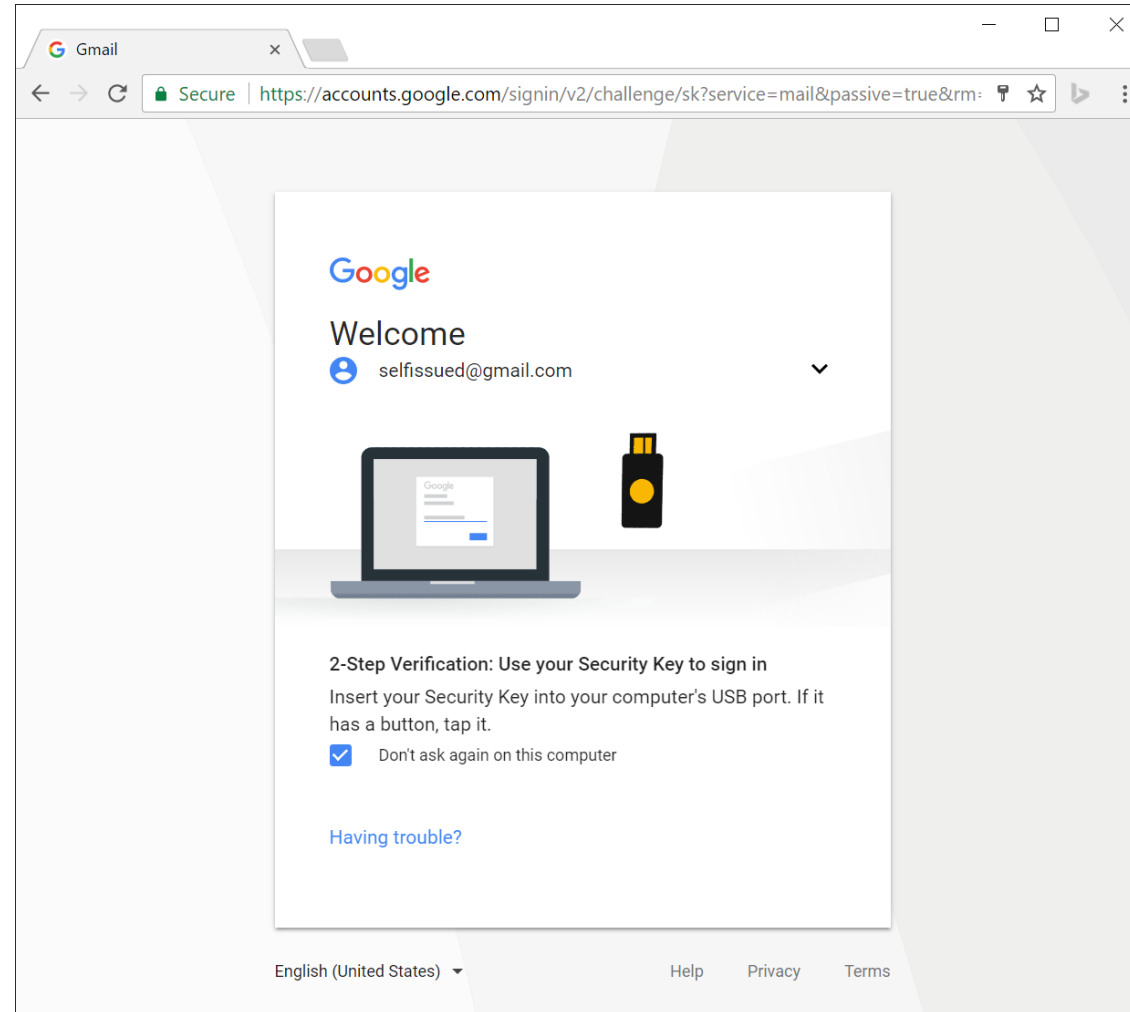
Enter your password

.....

[Forgot password?](#) [NEXT](#)

English (United States) [Help](#) [Privacy](#) [Terms](#)

Prompt for second factor (authenticator)



User touches authenticator to authorize
release of cryptographic second factor



Standards Status

- On May 5, 2017, W3C WebAuthn published WD-05
 - <http://www.w3.org/TR/2017/WD-webauthn-20170505/>
 - Several browsers plan to update their implementations to this version
- FIDO 2.0 Client to Authenticator Protocol (CTAP) progressing in parallel
 - Current drafts available to FIDO Alliance members
 - Public drafts will be published by FIDO when deemed ready

Preview of Coming Attractions

- Browsers implementing WebAuthn and CTAP drafts
- Experimental applications using these browsers with authenticators
- Interop testing of implementations
- Continuing refinements of WebAuthn and CTAP specifications
- *Enablement of commonplace strong authentication on the Web!*

Where can I participate & learn more?

- W3C Web Authentication working group
 - <https://www.w3.org/Webauthn/>
- FIDO 2.0 working group
 - <https://fidoalliance.org/>
- My blog
 - <http://self-issued.info/>
- E-mail me
 - mbj@microsoft.com