authenticate 2024

THE FIDO CONFERENCE

# Shift into high gear: Answering common questions to help you get off the starting line


Karen Larson
Sr. Director, Uniken

Matthew Miller
Technical Lead, Cisco Duo


Signature Sponsors:

cisco | Microsoft | yubico | Google

authenticatecon.com

# Agenda

- **WebAuthn** and **passkeys**
- Acronyms galore: **UP** vs **UV** vs **BE** vs **BS** vs **PIN…**
- **To attest** or **not to attest**
- What can I do with **attestation**?
  - Regulation compliance
  - Reporting
  - Nicknaming
- Benefitting from the **FIDO Convenience Metadata Service**
- Recap
- Q & A

# WebAuthn and passkeys

## WebAuthn

- A **browser API** for Relying Parties to deliver secure, user-friendly authentication using public-key cryptography
- One half of **FIDO2** along with CTAP
- WebAuthn registration creates a public-key **credential**
- An open standard worked on in the W3C's **Web Authentication Working Group** (WAWG)

## Passkeys

- Still just WebAuthn!
- A **discoverable** credential that may be used across devices (**"multi-device"**), or only from a single authenticator (**"single-device"**)
- A **consumer-friendly term** to help communicate them as an alternative to "passwords"

# Acronyms Galore - Flags to be aware of for RPs

| | |
|---|---|
| UP | User Presence |
| BS | Backup State |
| UV | User Verification |
| AT | Attested Credential Data |
| BE | Backup Eligibility |
| ED | Extension Data |

# Flags Example - Registered passkey with Mac

## Attestation object:

```
"authenticatorData": {
    "rpIdHash": "f95...",
    "flags": {
      "userPresent": true,
      "reserved1": false,
      "userVerified": true,
      "backupEligibility": true,
      "backupState": true,
      "reserved2": false,
      "attestedCredentialData": true,
      "extensionDataIncluded": false
    },
...
```

## What this means

**User presence (UP) check passed**
*Typically touching or interacting with the authenticator*

**User verification (UV) completed**
*User supplied an accepted gesture to verify their identity like a PIN or biometric*

**Credential source CAN be backed up (BE)**
*Credential has been saved where it can be backed up*

**Credential source IS being backed up (BS)**
*Credential is currently being backed up*

# Flags Example - Registered passkey with YubiKey

## Attestation object:

```
"authenticatorData": {
    "rpIdHash": "f95...",
    "flags": {
      "userPresent": true,
      "reserved1": false,
      "userVerified": true,
      "backupEligibility": false,
      "backupState": false,
      "reserved2": false,
      "attestedCredentialData": true,
      "extensionDataIncluded": false
    },
...
```

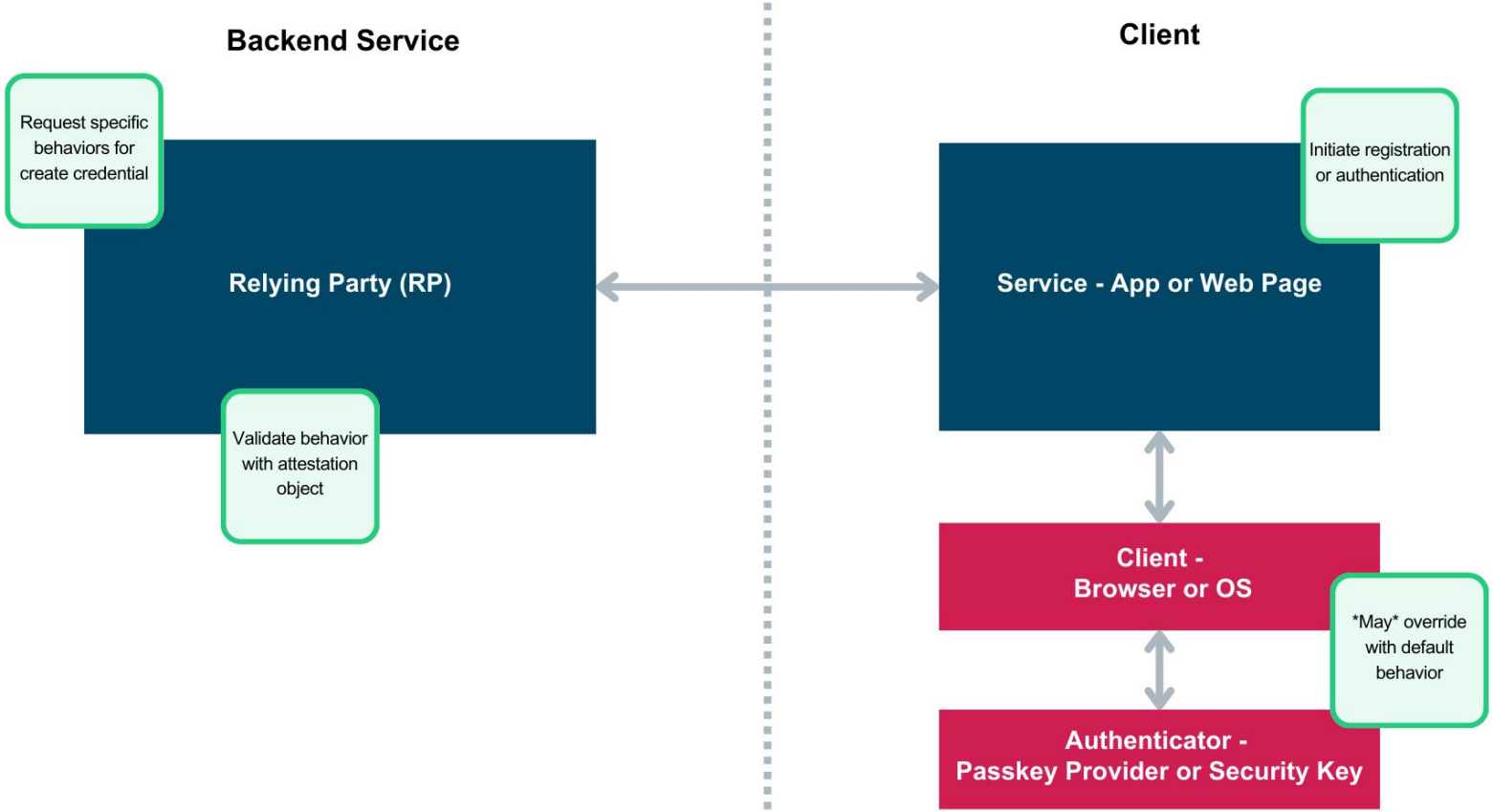
## What this means

**User presence (UP) check passed**
*Typically touching or interacting with the authenticator*

**User verification (UV) check passed**
*User supplied an accepted gesture to verify identity like a PIN or biometric*

**Credential source is NOT back up eligible (BE)**
*Credential has been saved where it can't be backed up*

**Credential source is NOT backed up (BS)**
*Credential isn't being backed up*



# To attest or not to attest…that is the question

## What is the attestation object?

Attestation object contains information about the authenticator AND attestation statement

Data includes things like:

- Flags (UV, UP, BE, BS)
- AAGUID
- Unique credential ID
- Attestation certificate

## Why this is important?

Supports use cases like allowing or denying authenticators by AAGUID

Allows the RP to see how and where the credential was registered *before* enabling the credential on an account

Helps with reporting on things like what types of authenticators are being registered

May *not* be needed in many cases

# Relating Attestation to FIDO Metadata Service (MDS)

## Attestation object

```
...
"attestedCredentialData": {
  "aaguid": "fbfc3007-154e-4ecc-8c0b-6e020557d7bd",
  "credentialId": "ad3f3763..",
  "credentialPublicKey": {
      "kty": "EC",
      "alg": "ECDSA_w_SHA256",
      "crv": "P-256",
      "x": "KOial5..",
      "y": "UYY2t.."
  }
}...
```

## MDS

MDS v3 provides a blob of JSON data in a JWT that provides information about the authenticators

Can be used to validate AAGUIDs, attestation certificates

Look-up authenticator properties

# FIDO Convenience Metadata Service (MDS)

- A new service alongside the **FIDO Metadata Service** (MDS)
- Contains **a subset of MDS info** to help RPs consistently name credentials and show appropriate iconography
- Metadata includes:
  - Localized names (RFC5646 + ISO3166)
  - Provider logos (`data:` URLs)
  - Authenticator icons (`data:` URLs)
- Available "Soon" (TBD)

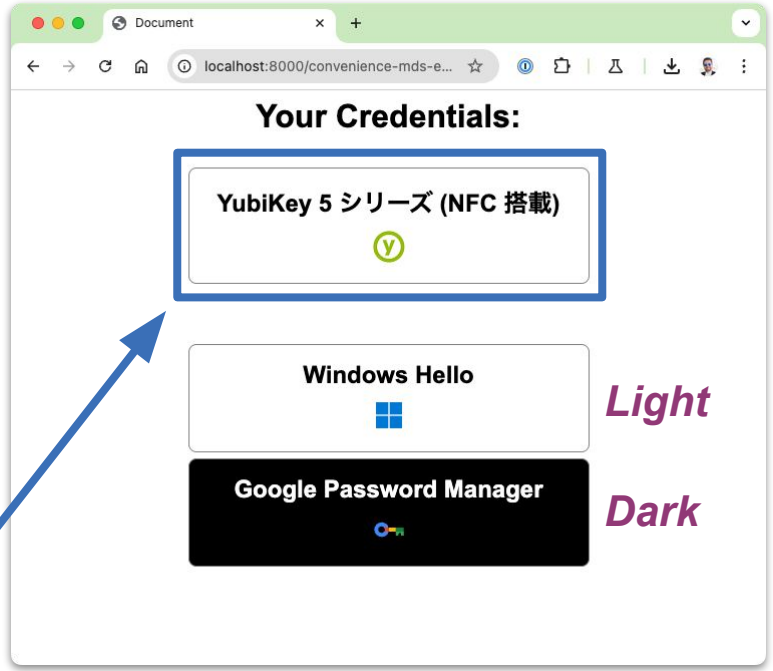
```
{
  "6028b017-b1d4-4c02-b4b3-afcdafc96bb2": {
    "friendlyNames": {
      "en-US": "Windows Hello"
    },
    "providerLogoDark": "...",
    "providerLogoLight": "..."
  },
  "a25342c0-3cdc-4414-8e46-f4807fca511c": {
    "friendlyNames": {
      "en-US": "YubiKey 5 Series with NFC",
      "ja-Hani-JP": "YubiKey 5 シリーズ (NFC 搭載)"
    },
    "icon": "..."
  }
}
```

# Benefitting from FIDO Convenience MDS

- Get AAGUID from registration (unattested or attested)
- Look up metadata by AAGUID
- Use localized **names**, and dark and light **icons** and **logos** to stylize credential presentation

```
{
  authData: {
    // ...
    aaguid: "a25342c0-3cdc-4414-8e46-f4807fca511c"
  }
}
```

```
"a25342c0-3cdc-4414-8e46-f4807fca511c" {
  "friendlyNames": {
    "en-US": "YubiKey 5 Series with NFC"
    "ja-Hani-JP": "YubiKey 5 シリーズ (NFC 搭載)"
  },
  "icon": "..."
}
```



# Q & A

authenticate 2024

THE FIDO CONFERENCE

# Thank you

Signature Sponsors:

cisco | Microsoft | yubico | Google

authenticatecon.com