



# Thinking differently about passkeys: New threats require a new threat model



## Dean H. Saxe, CIDPRO

Sr. Security Engineer, Amazon Web Services  
Co-Chair, FIDO Alliance Enterprise Deployment Working Group

# Passkeys >> Passwords

# Passkeys vary in their security properties

# What's a passkey?

- A passkey is **any** FIDO discoverable credential

# What's a passkey?

- A passkey is **any** FIDO discoverable credential
- Passkeys may be further differentiated

# What's a passkey?

- A passkey is **any** FIDO discoverable credential
- Passkeys may be further differentiated
  - Synced passkey

# What's a passkey?

- A passkey is **any** FIDO discoverable credential
- Passkeys may be further differentiated
  - Synced passkey
  - Device-bound passkey



**FIDO discoverable credentials**



# FIDO discoverable credentials

Synced  
passkey

Device-bound  
passkey

# FIDO discoverable credentials

Synced  
passkey

Cryptographic  
key pair

Device-bound  
passkey

# FIDO discoverable credentials

**Synced  
passkey**

**Device-bound  
passkey**

Cryptographic  
key pair

**Origin bound**

# FIDO discoverable credentials

**Synced  
passkey**

**Device-bound  
passkey**

Cryptographic  
key pair

Origin bound

**Highly phishing  
resistant**

# FIDO discoverable credentials

**Synced  
passkey**

**Device-bound  
passkey**

Cryptographic  
key pair

Origin bound

Highly phishing  
resistant

**Password  
replacement**

# FIDO discoverable credentials

**Synced  
passkey**

**Device-bound  
passkey**

Cryptographic  
key pair

Origin bound

Highly phishing  
resistant

Password  
replacement

**Second  
factor**

# FIDO discoverable credentials

**Synced  
passkey**

**Device-bound  
passkey**

Cryptographic  
key pair

Origin bound

Highly phishing  
resistant

**Non-exportable  
key material**

Password  
replacement

Second  
factor



# FIDO discoverable credentials

**Synced  
passkey**

**Exportable  
key material**

**Device-bound  
passkey**

Cryptographic  
key pair

Origin bound

Highly phishing  
resistant

Non-exportable  
key material

Password  
replacement

Second  
factor

# How does NIST classify passkeys?

- NIST SP 800-63B-4 (draft)

# How does NIST classify passkeys?

- NIST SP 800-63B-4 (draft)
  - Multi-factor cryptographic software authenticator → Synced passkey
    - Up to AAL2

# How does NIST classify passkeys?

- NIST SP 800-63B-4 (draft)
  - Multi-factor cryptographic software authenticator → Synced passkey
    - Up to AAL2
  - Multi-factor cryptographic device → Device-bound passkey
    - Up to AAL3

# FIDO discoverable credentials

## Synced passkey

Exportable key material

## Device-bound passkey

Non-exportable key material

Cryptographic key pair

Origin bound

Highly phishing resistant

Password replacement

Second factor

Unrecoverable if lost

# FIDO discoverable credentials

## Synced passkey

Exportable key material

## Device-bound passkey

Non-exportable key material

Cryptographic key pair

Origin bound

Highly phishing resistant

Password replacement

Second factor

Account recovery via RP

Unrecoverable if lost

# FIDO discoverable credentials

## Synced passkey

Exportable key material

Credential recovery via provider

## Device-bound passkey

Non-exportable key material

Unrecoverable if lost

Cryptographic key pair

Origin bound

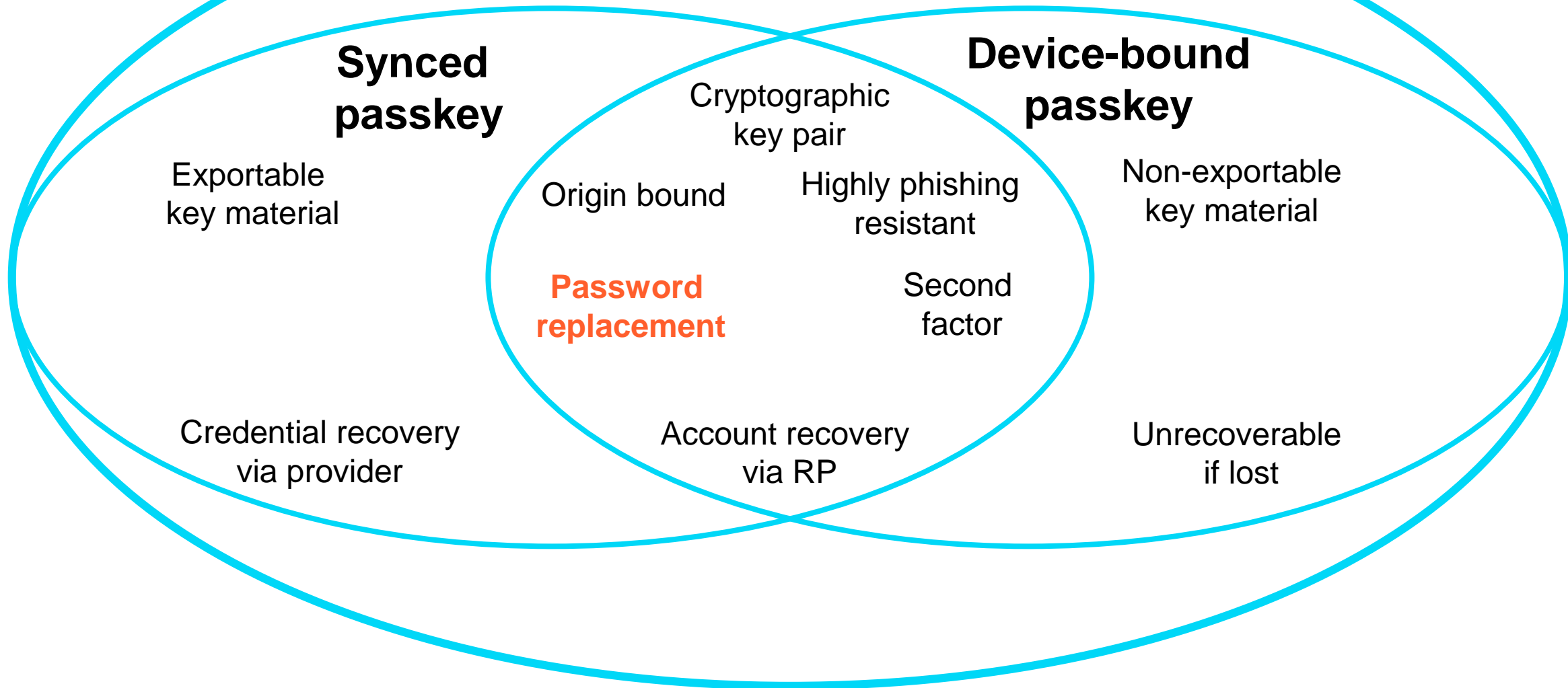
Highly phishing resistant

Password replacement

Second factor

Account recovery via RP

# FIDO discoverable credentials





# Increased credential cardinality

- To displace passwords, relying parties **may** support increased credential cardinality

# Increased credential cardinality

- To displace passwords, relying parties **may** support increased credential cardinality
  - Backup device-bound credentials (e.g., security keys)

# Increased credential cardinality

- To displace passwords, relying parties **may** support increased credential cardinality
  - Backup device-bound credentials (e.g., security keys)
  - Disconnected passkey provider ecosystems

# Increased credential cardinality

- To displace passwords, relying parties **may** support increased credential cardinality
  - Backup device-bound credentials (e.g., security keys)
  - Disconnected passkey provider ecosystems
  - User migration between ecosystems

# FIDO discoverable credentials

## Synced passkey

Exportable key material

Credential sharing

Credential recovery via provider

## Device-bound passkey

Non-exportable key material

Unrecoverable if lost

Cryptographic key pair

Origin bound

Highly phishing resistant

Password replacement

Second factor

Account recovery via RP

# Passkeys don't prevent credential sharing

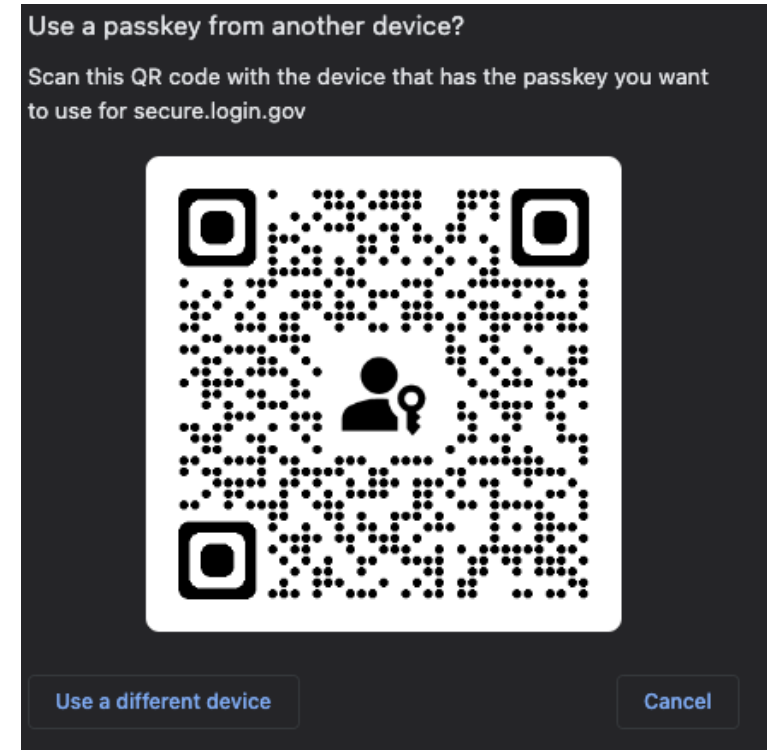
- Passkeys change the sharing model vs. passwords

# Passkeys don't prevent credential sharing

- Passkeys change the sharing model vs. passwords
- Apple AirDrop shares a **copy** of a credential

# Passkeys don't prevent credential sharing

- Passkeys change the sharing model vs. passwords
- Apple AirDrop shares a **copy** of a credential
- Cross-device authentication flow may be used to bootstrap a **new** credential





# **New rules: Managing multiple credentials**

- Notify user when new credentials are created in their account

# New rules: Managing multiple credentials

- Notify user when new credentials are created in their account
- Make credentials identifiable
  - Name
  - Creation metadata – date, browser, IP, GeoIP, etc.
  - Credential origin
  - Currently active sessions (if any)
  - Date of last use

# New rules: Managing multiple credentials

- Notify user when new credentials are created in their account
- Make credentials identifiable
  - Name
  - Creation metadata – date, browser, IP, GeoIP, etc.
  - Credential origin
  - Currently active sessions (if any)
  - Date of last use
- Nudge users to review/manage credentials – but don't annoy them!

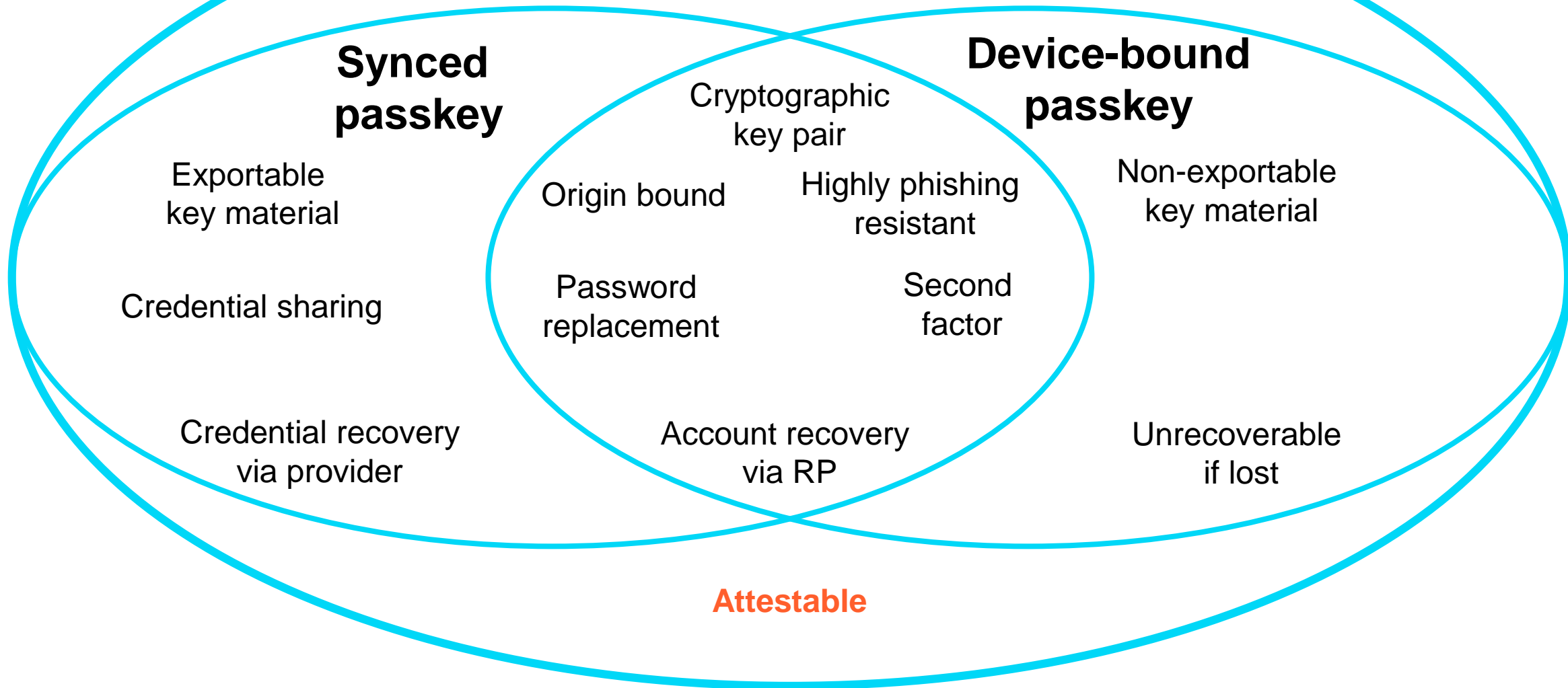
## New rules: Managing passkeys

- Deleting a passkey from your passkey provider prevents **you** from using the credential

## New rules: Managing passkeys

- Deleting a passkey from your passkey provider prevents **you** from using the credential
- Deleting a passkey from the RP prevents **anyone** from using the credential

# FIDO discoverable credentials



# Attestation

- Attestations are statements of fact about an authenticator that may be provided during credential creation events

# Attestation

- Attestations are statements of fact about an authenticator that may be provided during credential creation events
  - Attestations contain an Authenticator Attestation GUID (AAGUID)



# Attestation


- Attestations are statements of fact about an authenticator that may be provided during credential creation events
  - Attestations contain an Authenticator Attestation GUID (AAGUID)
- Metadata is made available by the FIDO Alliance Metadata Service (MDS)
  - <https://mds3.fidoalliance.org/>

```
attestationObject: {
  "fmt": "packed",
  "attStmt": {
    "alg": -7,
    "sig": Download "30440220568cce252007256d50933cc5143067ff8be8202cf3b6866c7f40477",
    "x5c": View Download PEM [
      "308202d9308201c1a003020102020900df92d9c4e2ed660a300d06092a864886f70d01010b050"
    ]
  },
  "authData": {
    "rpIdHash": "f95bc73828ee210f9fd3bbe72d97908013b0a3759e9aea3d0ae318766cd2e1ad",
    "flags": {
      "userPresent": true,
      "reserved1": false,
      "userVerified": false,
      "backupEligibility": false,
      "backupState": false,
      "reserved2": false,
      "attestedCredentialData": true,
      "extensionDataIncluded": false
    }
  },
  "signCount": 3,
  "attestedCredentialData": {
    "aaguid": "2fc0579f-8113-47ea-b116-bb5a8db9202a",
    "credentialId": "8e/datt1ece3638bc99/43333048/cet/0a40547c9cb57841f66fac07fa34",
    "credentialPublicKey": Download COSE Download JWK Download PEM {
      "kty": "EC",
      "alg": "ECDSA_w_SHA256",
      "crv": "P-256",
      "x": "VHGav1J+cr9Z6lkRa2IsM1MDeqfpDyGNPQVBvnqt14o=",
      "y": "+mkLrN6aSLiahptbi5xVP08CxwsY1Mzr8W3yFIaPQSE="
    }
  }
},
},
```

```
},  
"signCount": 3,  
"attestedCredentialData": {  
  "aaguid": "2fc0579f-8113-47ea-b116-bb5a8db9202a",  
  "credentialId": "8e/datt1ece3638bc99/43333048/cet/0a40547c9cb5784",  
  "credentialPublicKey": Download COSE Download WK Download PEM /
```

- **aaguid:** "2fc0579f-8113-47ea-b116-bb5a8db9202a" ←
- **metadataStatement:**
  - **legalHeader:** "Submission of this statement and retrieval of this statement is subject to the terms and conditions of the FIDO Alliance's FIDO Certified Product License Agreement."
  - **aaguid:** "2fc0579f-8113-47ea-b116-bb5a8db9202a"
  - **description:** "YubiKey 5 Series with NFC"
  - **authenticatorVersion:** 328706
  - **protocolFamily:** "fido2"

- **statusReports:**
  1.
    - **status:** "FIDO\_CERTIFIED\_L1"
    - **effectiveDate:** "2020-05-12"
    - **certificationDescriptor:** "YubiKey 5 NFC Series"
    - **certificateNumber:** "FIDO20020190826002"
    - **certificationPolicyVersion:** "1.1.1"
    - **certificationRequirementsVersion:** "1.3"
  2.
    - **status:** "FIDO\_CERTIFIED"
    - **effectiveDate:** "2020-05-12"
- **timeOfLastStatusChange:** "2020-05-12"

- **aaguid:** "2fc0579f-8113-47ea-b116-bb5a8db9202a"
- **metadataStatement:**
  - **legalHeader:** "Submission of this statement and retrieval of this statement is subject to the terms and conditions of the FIDO Alliance Certification Program."
  - **aaguid:** "2fc0579f-8113-47ea-b116-bb5a8db9202a"
  - **description:** "YubiKey 5 Series with NFC" 
  - **authenticatorVersion:** 328706
  - **protocolFamily:** "fido2"

- **statusReports:**
  1.
    - **status:** "FIDO\_CERTIFIED\_L1"
    - **effectiveDate:** "2020-05-12"
    - **certificationDescriptor:** "YubiKey 5 NFC Series"
    - **certificateNumber:** "FIDO20020190826002"
    - **certificationPolicyVersion:** "1.1.1"
    - **certificationRequirementsVersion:** "1.3"
  2.
    - **status:** "FIDO\_CERTIFIED"
    - **effectiveDate:** "2020-05-12"
- **timeOfLastStatusChange:** "2020-05-12"

- **aaguid:** "2fc0579f-8113-47ea-b116-bb5a8db9202a"
- **metadataStatement:**
  - **legalHeader:** "Submission of this statement and retrieval of this statement is subject to the terms and conditions of the FIDO Alliance Certification Program."
  - **aaguid:** "2fc0579f-8113-47ea-b116-bb5a8db9202a"
  - **description:** "YubiKey 5 Series with NFC"
  - **authenticatorVersion:** 328706
  - **protocolFamily:** "fido2"

- **statusReports:**
  1.
    - **status:** "FIDO\_CERTIFIED\_L1" ←
    - **effectiveDate:** "2020-05-12"
    - **certificationDescriptor:** "YubiKey 5 NFC Series"
    - **certificateNumber:** "FIDO20020190826002"
    - **certificationPolicyVersion:** "1.1.1"
    - **certificationRequirementsVersion:** "1.3"
  2.
    - **status:** "FIDO\_CERTIFIED" ←
    - **effectiveDate:** "2020-05-12"
- **timeOfLastStatusChange:** "2020-05-12"

o **attestationRootCertificates:**

1.

- **Subject:** "CN=Yubico U2F Root CA Serial 457200631"
- **Issuer:** "CN=Yubico U2F Root CA Serial 457200631"
- **Not Before:** "Fri, 01 Aug 2014 00:00:00 GMT"
- **Not After:** "Sun, 04 Sep 2050 00:00:00 GMT"
- **Serial Number:** "1b4053f7"
- **Public Key:**
  - **Algorithm:**
    - **name:** "RSASSA-PKCS1-v1\_5"
    - **publicExponent:** undefined
    - **modulusLength:** 2048
  - **Value:**  
30820122300d06092a864886f70d01010105000382010f003082010a0282010
- **Signature:**
  - **Algorithm:**
    - **name:** "RSASSA-PKCS1-v1\_5"
    - **hash:**
      - **name:** "SHA-256"
  - **Value:**  
8ef8ee38c0d26be2571422f204ab32717b41559b09e147b72db684b0f6383183

# Attestations are optional

- Relying parties **may** request attestations

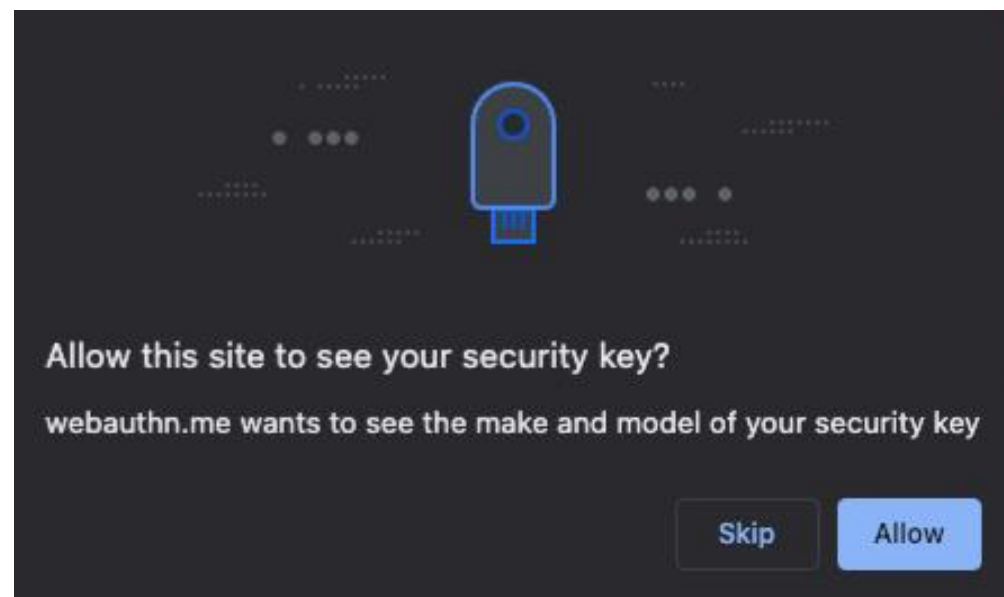


# Attestations are optional

- Relying parties **may** request attestations
- Authenticators **may** provide attestations

# Attestations are optional

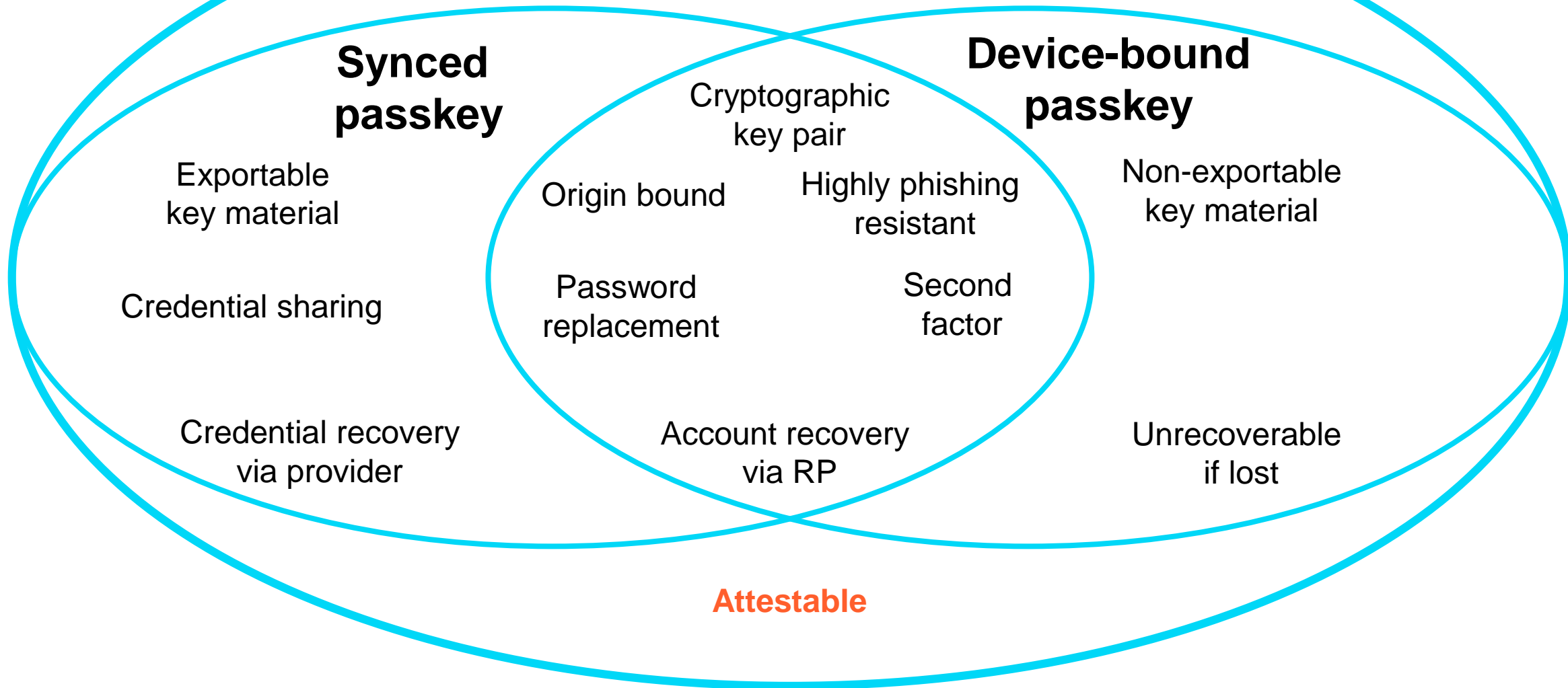
- Relying parties **may** request attestations
- Authenticators **may** provide attestations
- Users **may** block attestations





# **FIDO credentials without attestation **lack provable security properties****

# FIDO discoverable credentials



**Synced passkey**

Exportable key material

Credential sharing

Credential recovery via provider

Cryptographic key pair

Origin bound

Highly phishing resistant

Password replacement

Second factor

Account recovery via RP

**Device-bound passkey**

Non-exportable key material

Unrecoverable if lost

**Attestable**



**Passkey providers are part  
of your threat model**

# Passkey prognostication

**THANK YOU!**