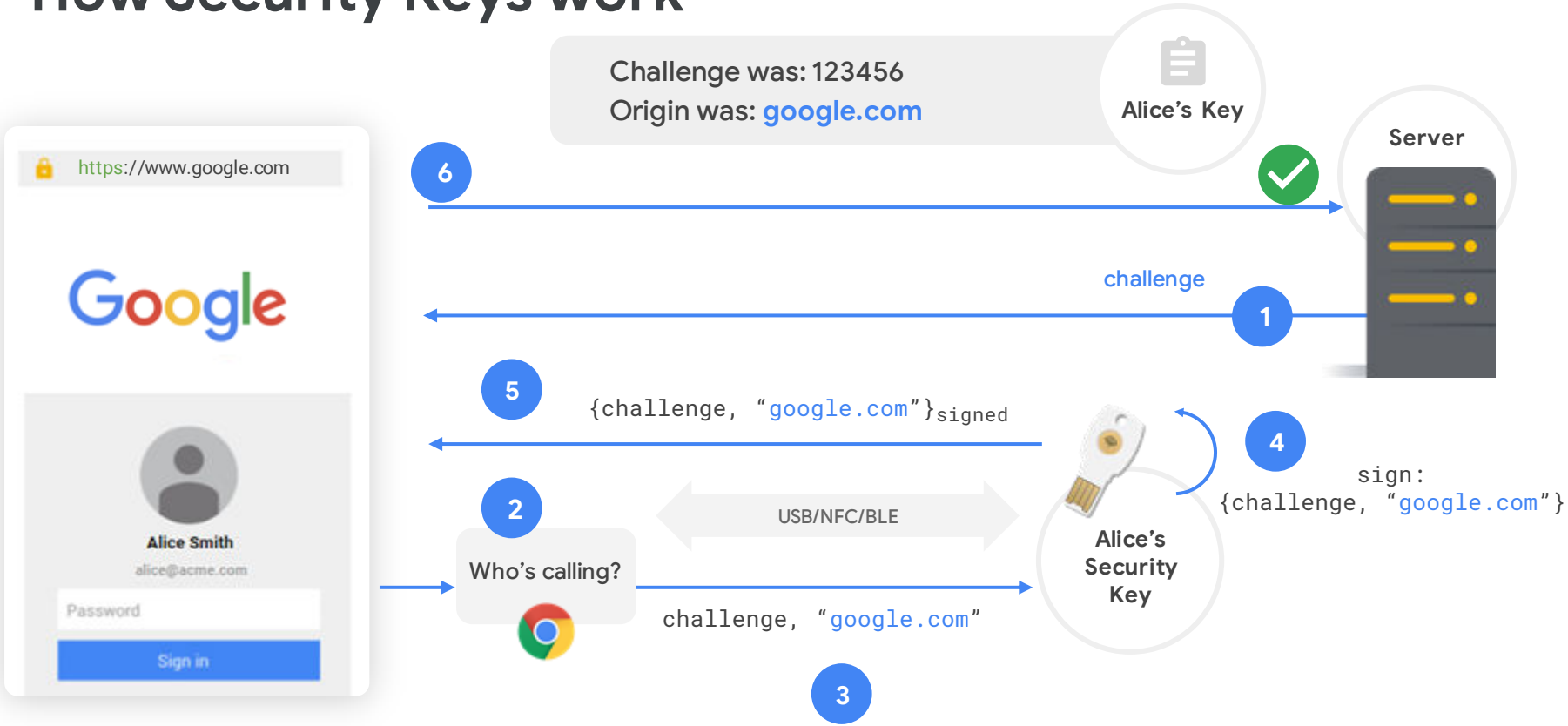
WebAuthn / CTAP

Modern Authentication

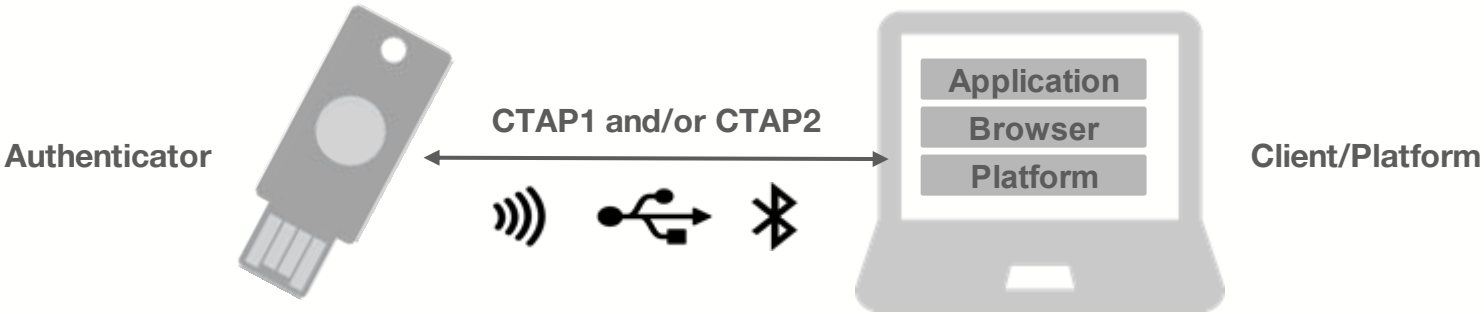
How Security Keys work



Registration Recap

1. **Relying Party generates challenge**
   - Prevents replay
2. **Client validates origin**
   - Prevents phishing
3. **Authenticator checks user presence and consent**
   - Prevents silent tracking
4. **Authenticator creates key pair**
   - No secret is shared with Relying Party
5. **Relying Party verifies attestation signature**
   - Prevents phishing
   - Proof that private key is safe

What is CTAP?

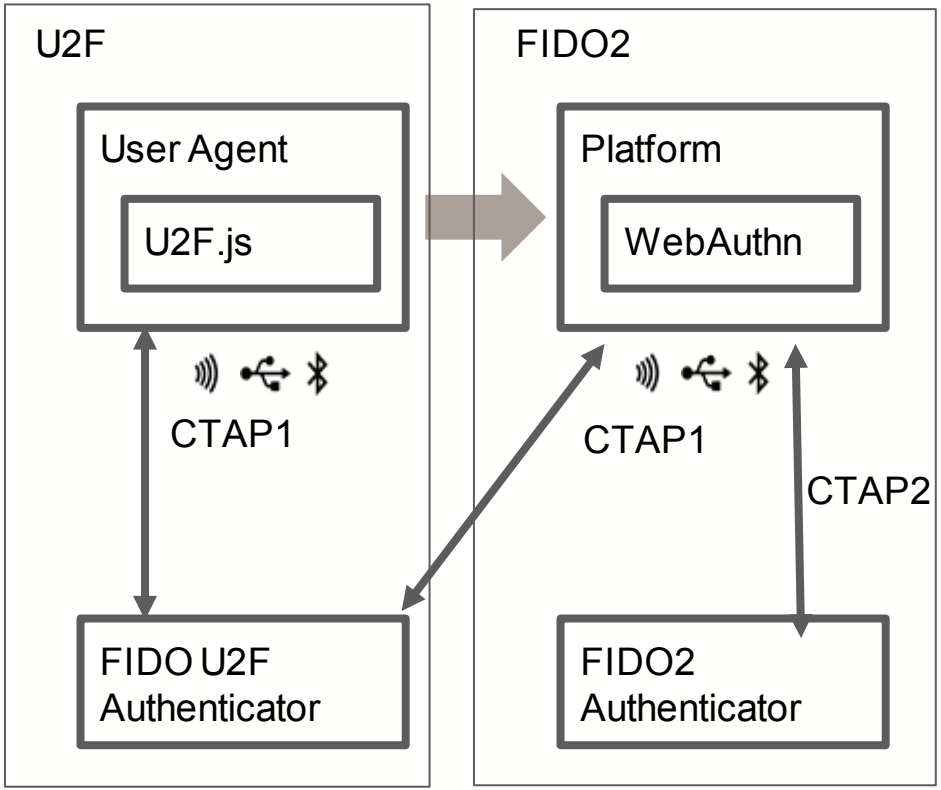


- Authenticator generates and securely stores credentials
- Communicates over USB, NFC, or Bluetooth
- Private keys, PINs, and biometric information never leave the authenticator
- CTAP2 Data format: Concise Binary Object Representation (CBOR)

What is WebAuthn?

- WebAuthn (JavaScript) API lets Browser, Client talk about external or platform (embedded) authenticators. **It is 2-party interaction.**
- Enables the creation and use of strong, attested, scoped, public key-based credentials for use by web applications.
- Strongly authenticates users.
- All major browsers are on track to implement full Web Authentication APIs. Chrome, Edge, Mozilla all support now.

Evolution of FIDO Authentication to FIDO2



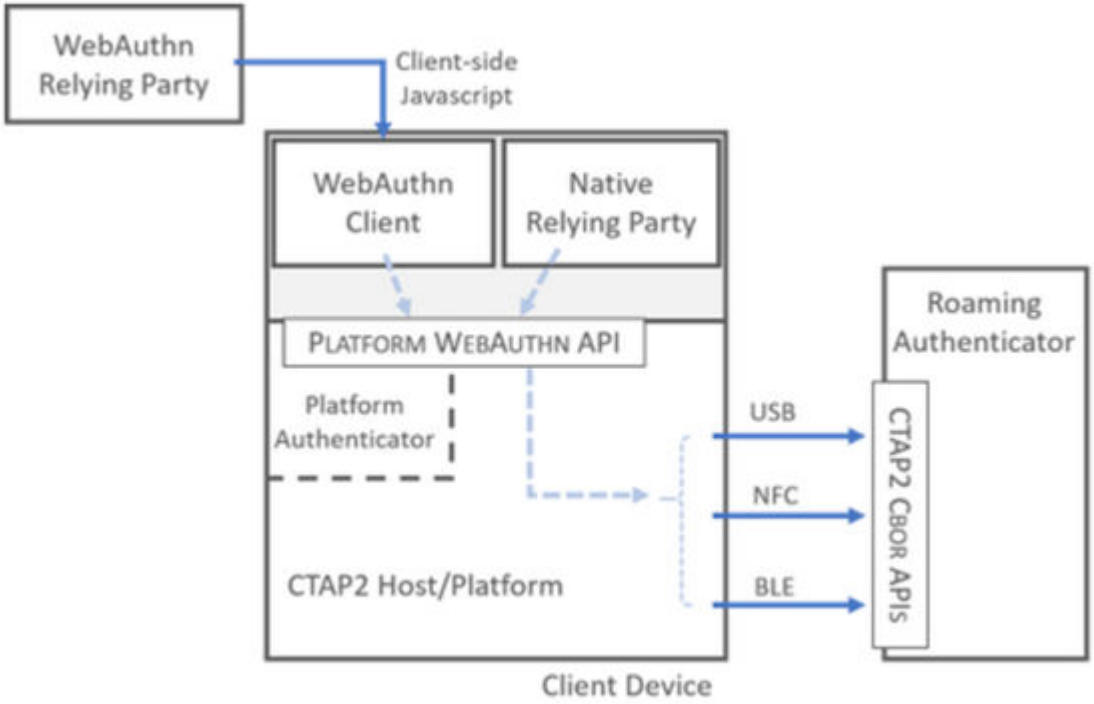
U2F

- Phishing resistant authentication with user intent
- Multi-Factor Authentication (MFA) Subset
  - Authenticator - something you have
  - Password - something you know

FIDO2

- True MFA
  - Authenticator - something you have
  - User verification - something you know (PIN) or are (Biometrics)

WebAuthn and CTAP2



State of state

- CTAP2 in final review at FIDO; standardization soon
- WebAuthn clearing up some issues for move to PR (resolution soon, PR early 2019?).
- New FIDO2 (CTAP2/WebAuthn) features:
  - Resident Keys provide first-factor, high assurance MFA, and enable passwordless authentication
  - HMAC support to enable offline authentication
- Migration path to WebAuthn exists for U2F devices, credentials
- FIDO UAF features, such as transactions, part of Level 2 W3C work

EAT

Entity Attestation Token
IETF Internet Draft

EAT (more)

- Web Authn WG looking at this in IETF
- Key use is with payment handlers that open a new window
- We don’t anticipate any extra work in CredMan
- Been seeking guidance via Mike West

FIDO and Authenticators

Dr. Rae Hayward
Certification Director
FIDO Alliance

BENEFITS TO CERTIFICATION

Validation

Interoperable

Rigorous testing

Trust

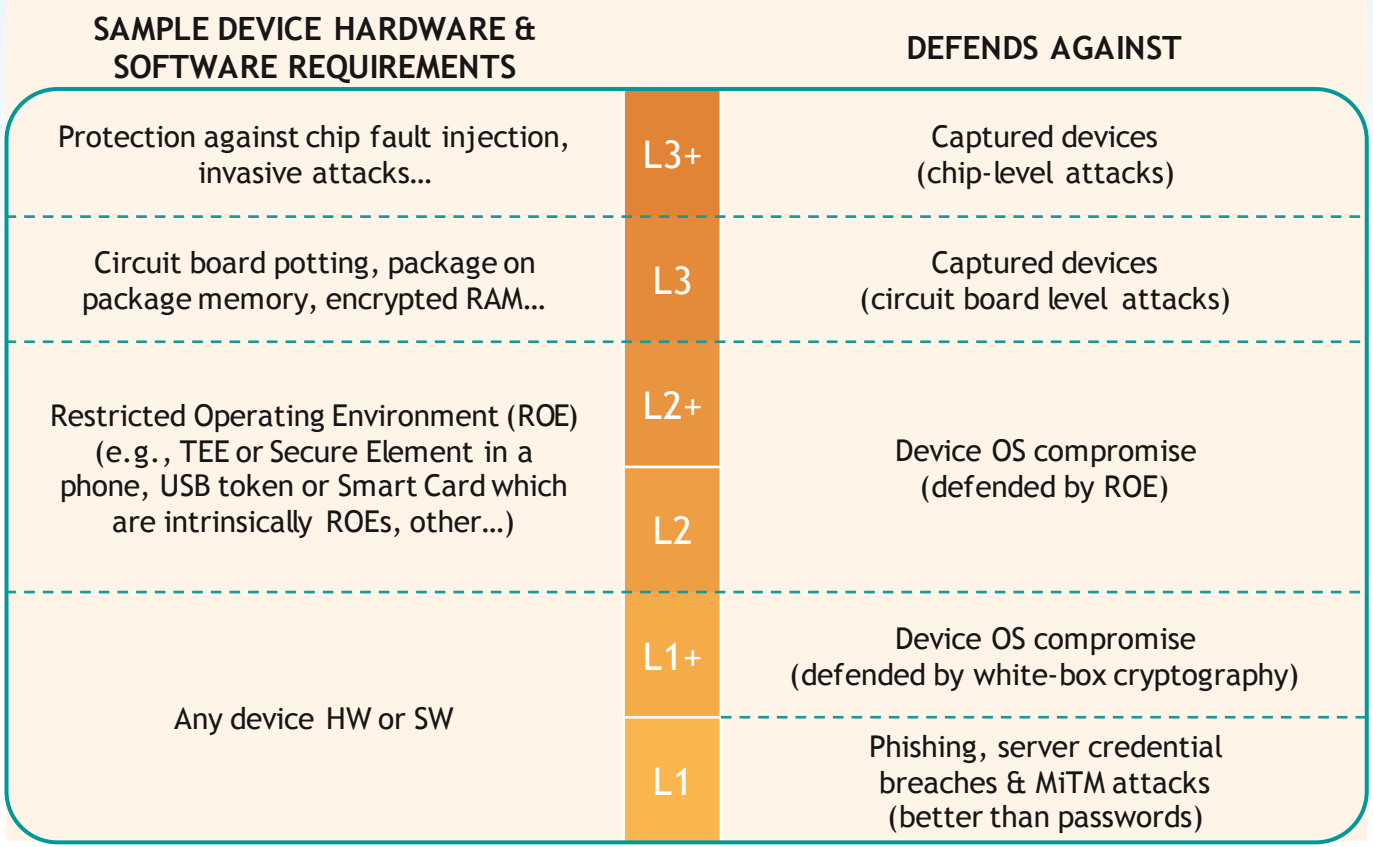
Competitive edge

Market expansion

FIDO AUTHENTICATOR CERTIFICATION

- Validates the security characteristics of **authenticator** implementations
- Functional is a prerequisite

A COMPREHENSIVE SET OF LEVELS FOR ALL USES CASES



LEVEL 1

- Better than passwords
  - FIDO is unfishable and biometrics are more convenient
- Keys and biometric templates are protected similar to passwords stored by a browser or password manager app
- Requires best facilities offered by hosting OS
- L1+ adds white-box cryptography (obfuscation and other techniques) to defend against compromise of hosting OS

Examples

- Android or IoS applications
- Platform built-in authenticators
- Level 2- or Level 3-capable authenticators not yet certified at Level 2 or Level 3

Certification Process
Vendor documents their design in detail
L1+ only: Evaluation by FIDO-accredited lab, penetration testing (L1+ program still in development)
Evaluation by FIDO Alliance Security Secretariat

LEVEL 2

In addition to L1

- A restricted operating environment like a TEE gives security even if OS is compromised.
- Separate USB, BLE and NFC authenticators are considered to use a restricted operating environment
- Gives defense against larger scale attacks
- Additional assurance at L2+

Examples

- Android apps using FIDO Level 2 certified phone (there aren't any yet)
- USB, BLE and NFC Security Keys
- Level 3-capable authenticators that haven't yet been certified at Level 3

Certification Process
Vendor documents their design in detail L2+ only: Vendor submits source code (L2+ program still in development)
Evaluation by a FIDO-accredited lab L2+ only: Attack potential calculation, pen testing

LEVEL 3

In addition to L2

- Defends against physically captured authenticators
- Defenses against disassembling, probing, glitch and other such physical attacks

- L3+ adds defense against chip-level physical attacks, such as decapping and probing the chip

Examples

- USB, BLE and NFC Security Keys using Secure Elements or other means of defending HW attacks
- In some case phone or platform authenticators may achieve L3, but is difficult

Certification Process

Vendor documents their design in detail
Vendor submits source code

Evaluation by a FIDO-accredited lab (l3, L3+)
Attack potential calculation and penetration testing
L3+ only: Higher attack potential requirements

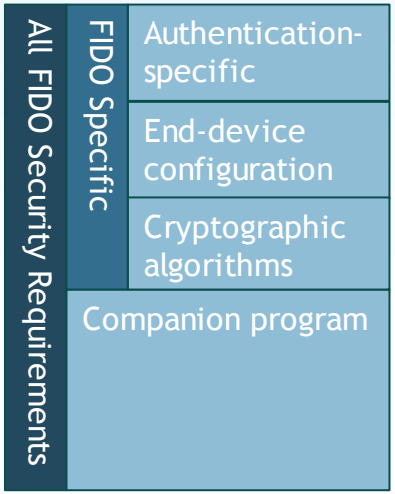
COMPANION PROGRAMS

Re use as much as possible from other programs like Common Criteria

- Reduces time, effort and cost of certification for authenticator vendors, sometimes by quite a lot

Companion programs never cover all FIDO requirements; they were not developed specifically for authenticators

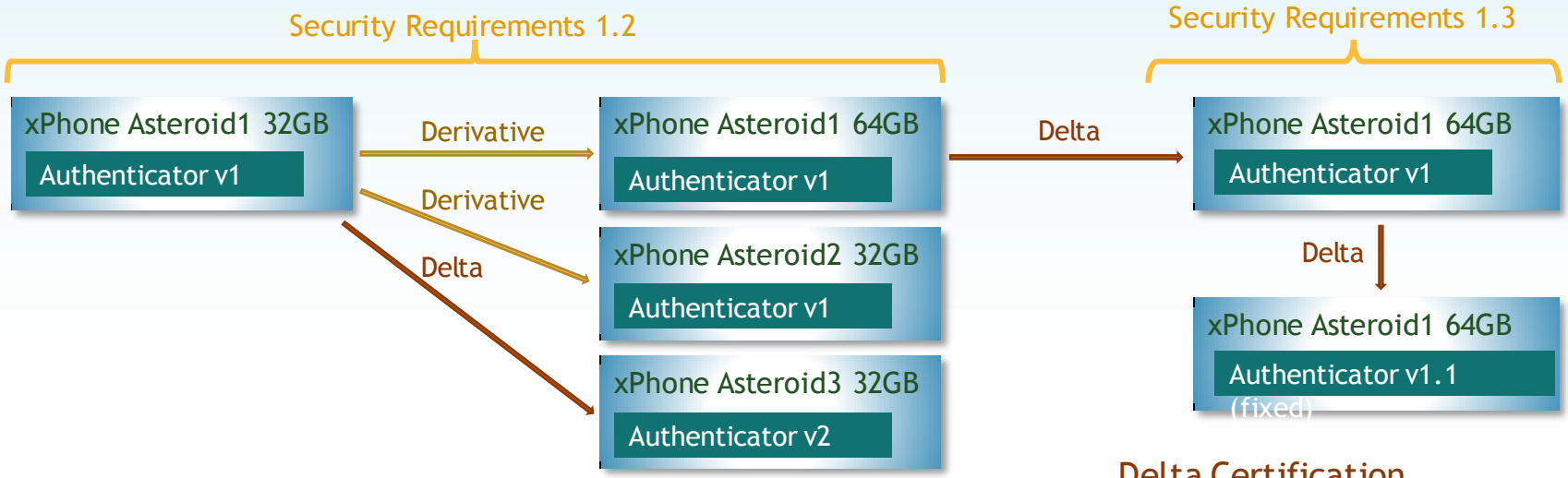
- Even with advanced companion programs, vendors will have to go through additional certification with the FIDO Alliance



Companion Program	FIDO Security Level	Program Status
Common Criteria AVA_VAN 3	L3	Operating
Common Criteria AVA_VAN 4	L3+	Operating
FIPS	L2+, L3	In development
Global Platform TEE Protection Profile	L2+	In development

FIDO ACCREDITED LABS

EXPIRATION, DERIVATIVE & DELTA CERTIFICATION



No Expiration

- Certification of a given product never expires
- Recertification against new versions of the requirements is optional

Derivative certification

- No change to FIDO functionality allowed
- Surrounding functionality may change
- Packaging & product name may change
- No re evaluation of security

Delta Certification

- When the FIDO functionality changes
- Recertification against new requirements
- After fix to close a vulnerability
- Reevaluation of security is required