Does FIDO really usher in the Death of Passwords?

Salah Machani
Senior Technologist, Office of the CTO, RSA

Kayvan Alikhani
Senior Director of Technology, RSA
Agenda

- Introduction: Why FIDO?
- FIDO Architecture, Security & Privacy
- FIDO Adoption Challenges
- Summary and Recommendations
Disclaimer

* The views expressed here are our own and not necessarily those of our company or FIDO Alliance
Why Fast IDentity Online?
Password Problems

TOO MANY TO REMEMBER, DIFFICULT TO TYPE, AND TOO VULNERABLE
Today’s Solution

One Time Passcodes (SMS or Device)

IMPROVE SECURITY BUT AREN’T EASY ENOUGH

DEVICE COST

SMS USABILITY

PROVISIONING

STILL PHISHABLE

CODE PHISHER
FIDO Solution

- Second Factor Experience
- Passwordless Experience
Second Factor Experience

ONLINE AUTH REQUEST
Login ID & Password

LOCAL DEVICE AUTH
Insert Dongle & Press button

SUCCESS
Done
Passwordless Experience

ONLINE AUTH REQUEST
Transaction Detail

LOCAL DEVICE AUTH
Show a Biometric

SUCCESS
Done
FIDO Primary Goals

- Standardize strong multi-factor authentication
- Preserve end-user privacy
- Unify end-user experience
FIDO in Identity & Access Management (IAM)

- Single Sign-On
- Federation
- Authentication
- User Management
- Physical-to-digital identity

MODERN AUTHENTICATION

Passwords
- Strong
- Risk-Based
FIDO Authentication Frameworks

- **FIDO 1.0**
  - Universal Second Factor (U2F) → Second Factor Experience
  - Universal Authentication Framework (UAF) → Passwordless Experience
  - Specs available to the public

- **FIDO 2.0**
  - Second Factor and Passwordless Experiences
  - New technical working group
  - Mission: Future requirements and widespread interoperability
Common Design Considerations

- Decouple User Verification from Authentication Protocol
- Accept Different Kinds of Authenticators
- Use Asymmetric Key Cryptography
FIDO U2F Components and Protocols

User Computing Environment

- U2F Authenticator
  - User Presence Sensor
  - U2F Secure Element
  - Connectors: USB, NFC, Bluetooth

- Browser
  - U2F JavaScript API
  - U2F APDU
    - USB API
    - NFC API
    - Bluetooth API

Relying Party

- Web Application
- U2F Server
  - User Public Keys & Handles

Registration ➔ Authentication

FIDO UAF Components an Protocols

User Computing Environment
- User Agent (Mobile App, Browser)
- FIDO Client
  - Windows, Mac, IOS, Android
  - Authenticator Abstraction
- FIDO Authenticators

Relying Party
- Web Application
- FIDO Server
  - OS /Server Security Components
  - Risk & Identity Systems

FIDO UAF Components
- Registration
- Authentication
- Confirmation
- Deregistration

FIDO UAF Protocols
- UAF Components
- UAF Protocols
FIDO Protocol Flows

1. Setup

2. Processing

3. Verification

- FIDO Client
- FIDO Server
- Relying Party

UAF & U2F
- Registration
- Authentication

UAF-only
- Transaction
- Confirmation
- Deregistration*

FIDO Authenticator
FIDO Registration

1. Registration Begins
   - REGISTRATION BEGINS
   - Site registration process

2. User Approval
   - USER APPROVAL
   - User approval of registration

3. New Key Pair Created
   - NEW KEY PAIR CREATED
   - Key pair created
   - Public key registered
   - Using Public key Cryptography

4. Registration Complete
   - REGISTRATION COMPLETE
   - Registration complete
FIDO Login

1. LOGIN
   - Login using Public key Cryptography

2. USER APPROVAL/VERIFICATION
   - Login Challenge

3. KEY SELECTED
   - Login Response
   - Using Public Key Cryptography

4. LOGIN COMPLETE
FIDO as part of a complete IAM solution

1. User Agent
   - FIDO Client
   - FIDO Authenticator
     - Local Verification
     - Private Key

2. Relying Party
   - Identity Provider
     - SAML, OAuth2, OpenID connect, etc
   - FIDO Server
     - Public Keys
   - FIDO Meta-data Service

3. Relying Party
Security

- No Phishing
- No Man-In-The-Middle (MITM)
- No Secrets/Private Keys on Server
Privacy

- No link-ability
  - Relying party and account specific-keys
  - No unique ID per-device
- No Biometric data on server
- User Consent/Approval for all actions
Trust

- Verify Device Vendor
- Verify Device Security Characteristics
  - User Verification Methods
  - Key Protection Methods
  - Display Capabilities
  - Cryptography Algorithms, etc.
- Device certification program
FIDO Implementation Challenges
Interoperability

- UAF and U2F
- Further potential fragmentation with FIDO 2.0
New Infrastructure Investments

- Invest in new FIDO servers & (optional) Metadata services
- Changes to your web/mobile applications
  - Enrollment & Login workflow
  - Dependency on OS, Browser and device types/versions
- Last mile: Integrate with existing security IAM infrastructure
- Different laws and regulations in different regions
Enterprise Adoption Challenges

- Change tied to IT ‘refresh’ cycles (2-4 years) for such solutions
  - Look for similar adoption cycles within the enterprise
- Support integration with enterprise security IAM infrastructure
  - Authorization & Federation services
  - Blend-in as part of existing multi-factor framework/as part of assurance policies
  - User, Device and Application Provisioning & Management process
  - Integrate with IWA (Active Directory, existing identity stores)
Security threats

- Many things are **out of scope for FIDO** but important to your infrastructure security
  - Primary authentication (threat to Client, Server & RP)
  - Recovery (threat to RP)
  - Private Key protection (threat to Client)
  - Credential/Biometric data protection (threat to Client)
  - FIDO biometric authenticator “Strength”
User experience

- New experience: Registration, verification and recovery processes
- Necklace problem still exists
  - Various RPs may restrict support for specific authenticators
    - Fragmentation, Various Acceptance Criteria & Assurance levels

![Diagram showing differences between Relying Party 1 and Relying Party 2 acceptance of user's device]
Customer Support

- Help desk retraining
- Authenticators life-cycle management issues
- Expected increase in support calls
- Evaluate authenticators assurance levels (e.g., biometrics)
- Multi-authenticator support calls
  - Authenticators can not be uniquely identified (by-design)
  - How to decommission a specific authenticator
**Added Cost**

**User:** Smartphone/tablet should be FIDO-equipped/certified

**RP / Enterprise:** Add FIDO server, Metadata server, and integration into existing IAM
We’re not there ‘yet’

- **Utopia**
  - Devices: All have well designed, easy to use FIDO authenticators
  - Enterprise: All apps support FIDO authentication
  - Hackers: Leave device-side biometric authentication “alone”

- **Reality (for the next ~3-5 years)**
  - Devices: Growing mix of different capabilities, makes & models
  - Enterprise: Hodgepodge of Auth protocols and standards
  - Hackers: Can’t wait…
There’s some convincing to do…

- Adoption
  - As more companies deploy FIDO enabled solutions with positive feedback: Deployment & Usage

- Security
  - Assurance: As FIDO authenticators provide meta-data to clearly ‘grade’ each authenticator’s Assurance Level

- Certification
  - Rely on FIDO certification of larger number of authentication vendors
Recommendations
Recommendations for FIDO-aware solutions

- Take close attention to FIDO technical working groups
- Don’t put all your eggs in one basket, throw a wider net
  - Design around solutions that take advantage of the evolving mobile auth methods
  - **Avoid** solely relying on a single
    - FIDO Factor/Method
    - FIDO supported Platform/OS
  - Look for broad support and compliance
- Determine Risk
  - Take advantage of solutions that include “**User behavioral data**” to make better decisions
    - User location, network, device registration, usage and activity pattern
Recommendations for FIDO-aware solutions

- Survey your users with simple PoCs to see what FIDO method ‘works’ for them
- Remember: Combining auth methods lowers the risk of each method:
  - Improves chance of information being accessed by the right person
- It’s a Balancing Act
  - Blend FIDO with other auth methods based on user “role” & “action
Questions?