
fido™
alliance
simpler
stronger
authentication

Goal: Simpler Stronger Authentication

INTERNET SERVICES	COMPONENT & DEVICE VENDORS	SOFTWARE & STACKS
BlackBerry	Synaptics	Chrome
DISCOVER	lenovo	Android
MasterCard	LG Electronics	Insyndia
Microsoft	Infineon	IT'S ME!
PayPal	NXP	Nok Nok Labs
RSA	yubico	CHECK PROTECT
	CrucialTec	Entersekt
	FingerQ	SECURE KEY
	BlackBerry	Ping Identity
		AGNITIO
		FINGERPRINTS

User Authentication Online

Do you want to login?

Do you want to transfer $100 to Joe?

Do you want to ship to a new address?

Do you want to delete all of your emails?

Do you want to share your dental record?

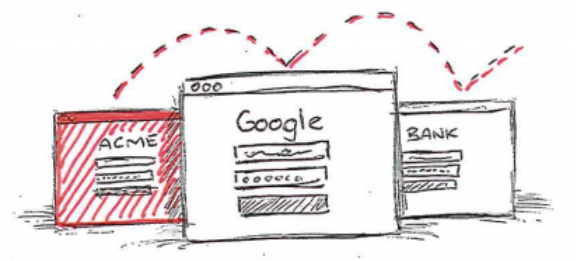
Authentication today:

Ask user for a password

(and perhaps a one time code)

Passwords

Too many to remember, difficult to type,
and not secure



REUSED

PHISHED

KEYLOGGED

One Time Codes

Improves security but not easy enough

SMS USABILITY

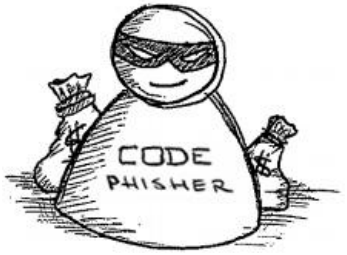
Coverage | Delay | Cost

DEVICE USABILITY

One per site | Fragile

USER EXPERIENCE

User confusion



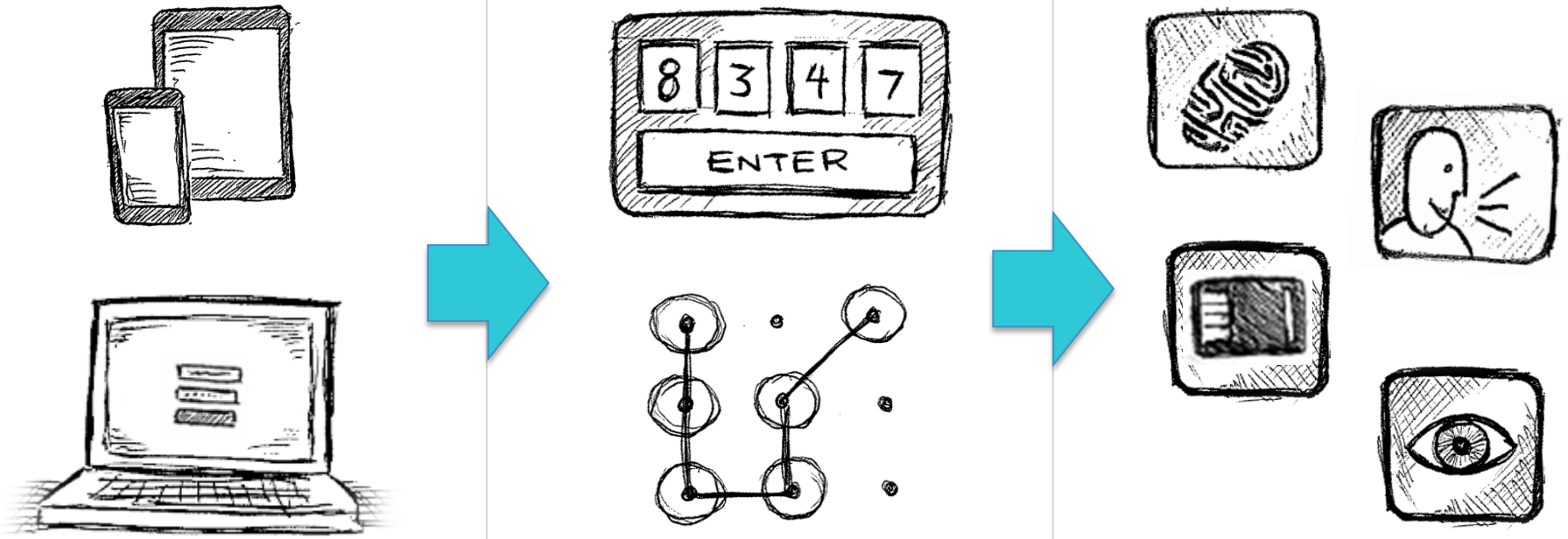
STILL PHISHABLE

Known attacks today

Megatrend

Simpler, Stronger Local Device Auth

PERSONAL DEVICES	LOCAL LOCKING	NEW WAVE: CONVENIENT SECURITY
Carry Personal Data	Pins & Patterns today	Simpler, Stronger local auth



Putting It Together

The problem:
Simpler, Stronger online authentication

The trend:
Simpler, Stronger local device authentication

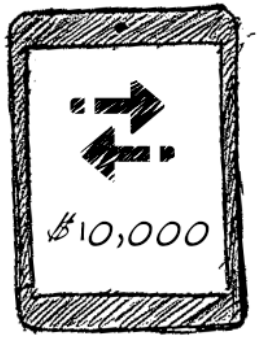
Why not:
Use local device auth for online authentication?

This is the core idea behind FIDO standards!

FIDO Experiences

ONLINE AUTH REQUEST	LOCAL DEVICE AUTH	SUCCESS

PASSWORDLESS EXPERIENCE (UAF standards)



Transaction Detail

Show a biometric

Done

SECOND FACTOR EXPERIENCE (U2F standards)

Login & Password

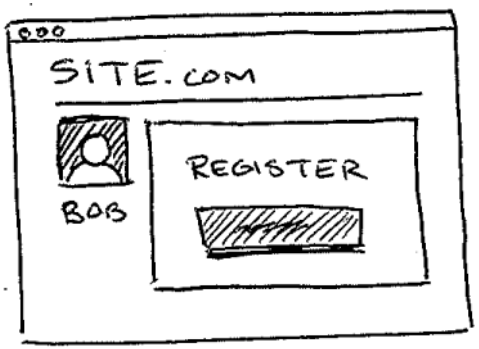
Insert Dongle, Press button

Done

FIDO Registration

1

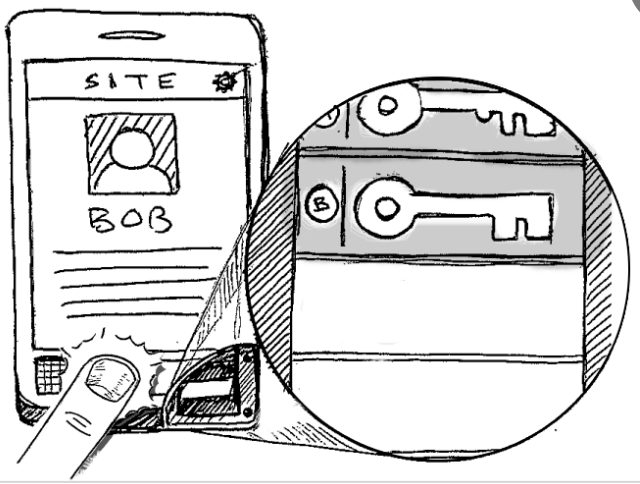
REGISTRATION BEGINS



USER APPROVAL

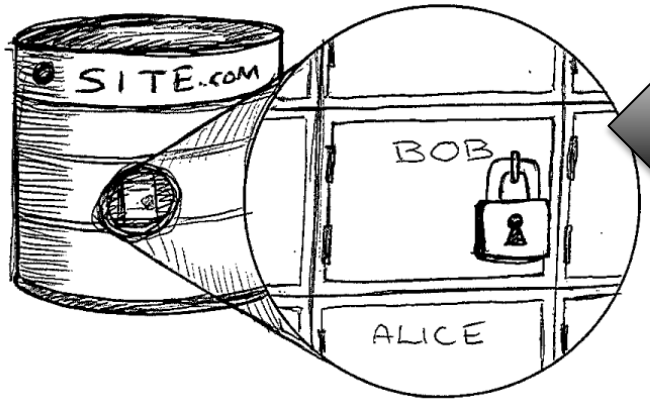
USER APPROVAL

2



4

REGISTRATION COMPLETE

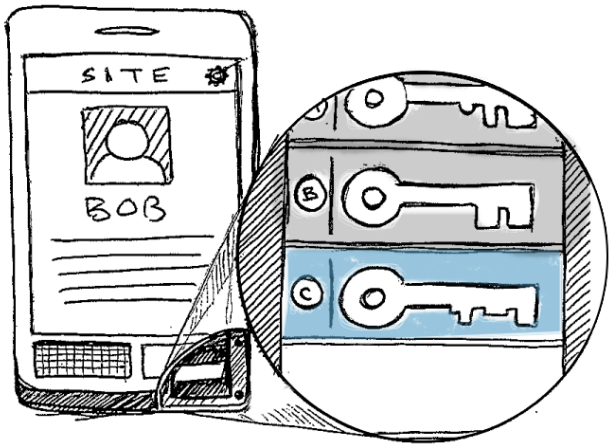


KEY REGISTERED

Using Public key Cryptography

NEW KEY CREATED

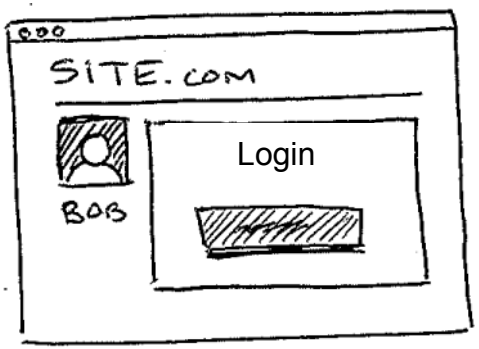
3



FIDO Login

1

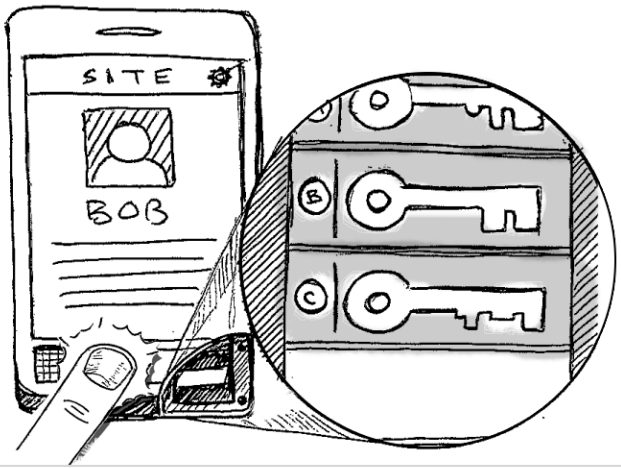
LOGIN



LOGIN CHALLENGE

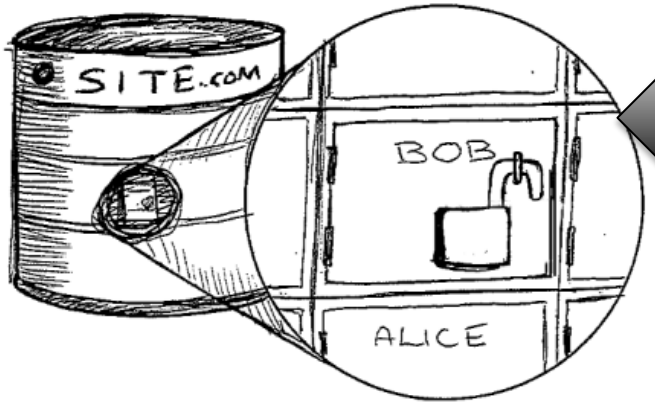
USER APPROVAL

2



4

LOGIN COMPLETE

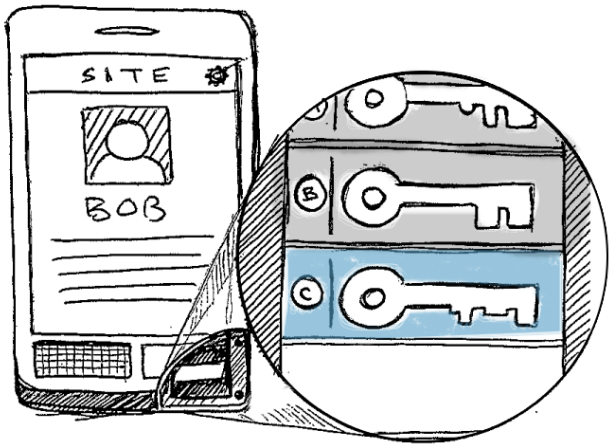


LOGIN RESPONSE

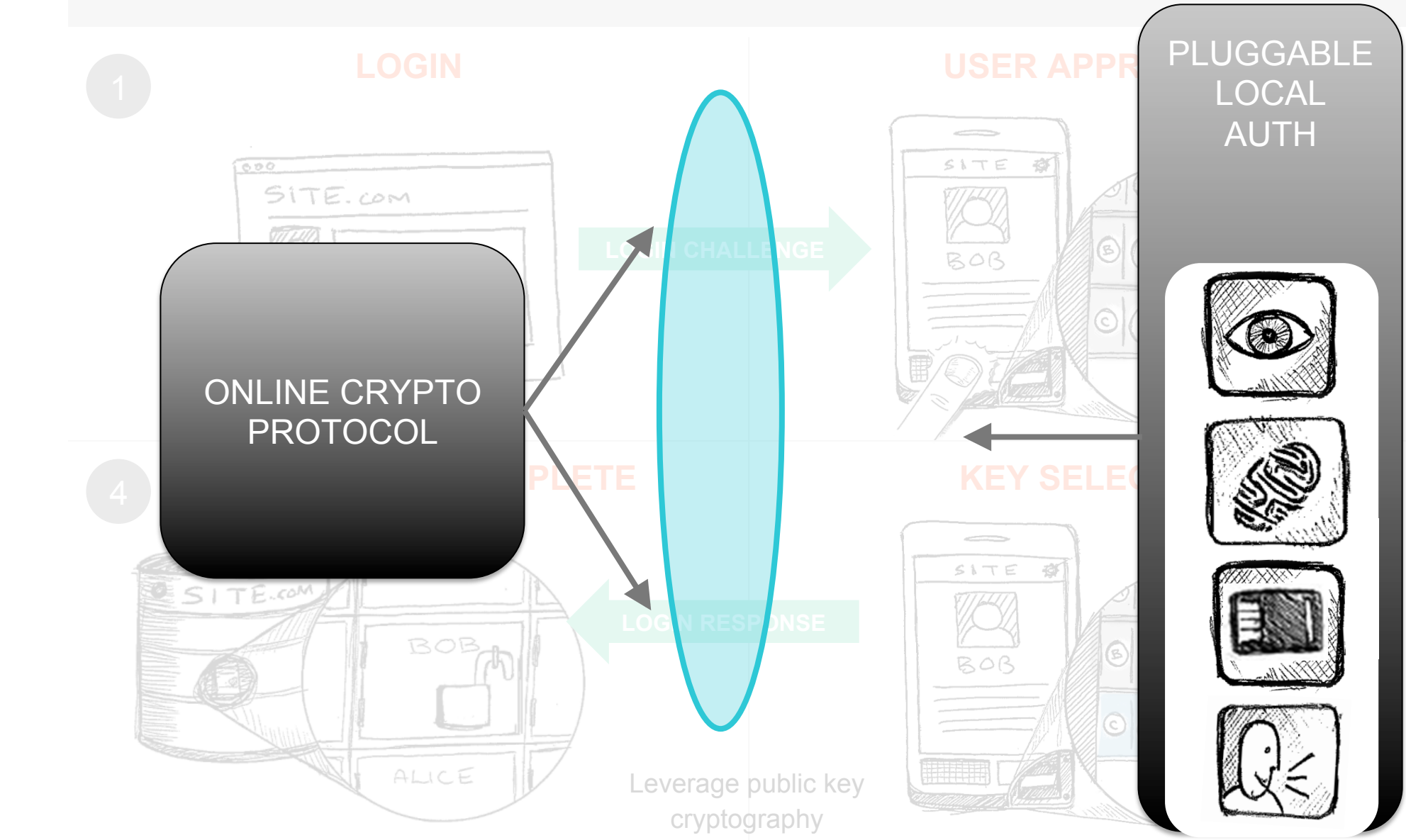
Using Public key Cryptography

KEY SELECTED

3



FIDO Standardization



Options for Internet Services

Passwordless UX = UAF:
Universal Auth Framework

- User carries client device with UAF stack installed
- User presents a local biometric or PIN
- Website can choose whether to retain password

Second Factor UX = U2F:
Universal Second Factor

- User carries U2F device with built-in support in web browsers
- User presents U2F device
- Website can simplify password (e.g, 4 digit PIN)

Simpler Stronger Authentication

What's the Benefit?

For Users

- Easy to use
- No more worrying about passwords
- Be safer on the Internet

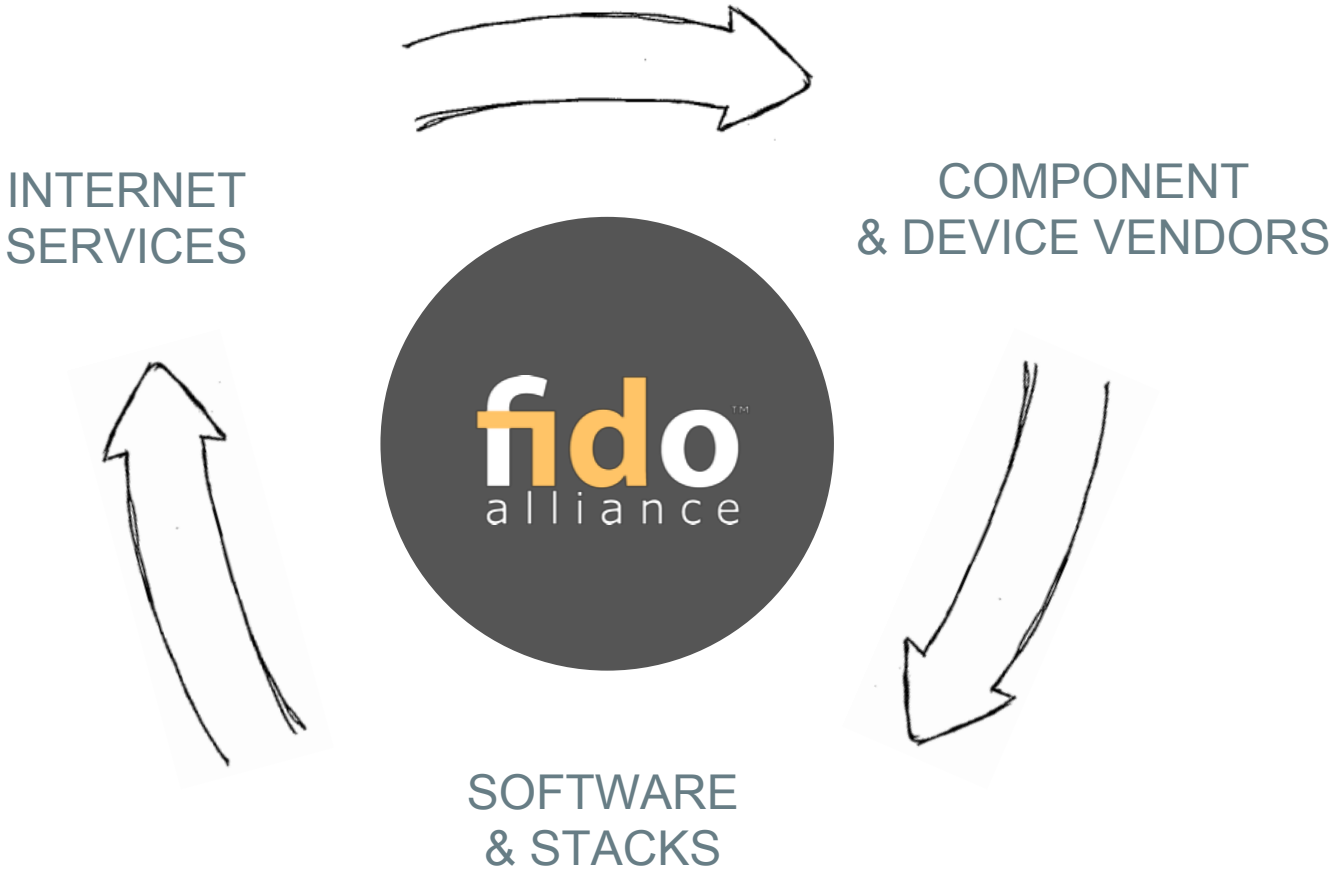
For Internet Services

- Greatly improved public key cryptography based security
- Increased user engagement
- User brings own device
- Build server once: Leverage any auth method

For Vendors

- Standardization ignites market
- Move past fragmented custom solutions

The Ecosystem



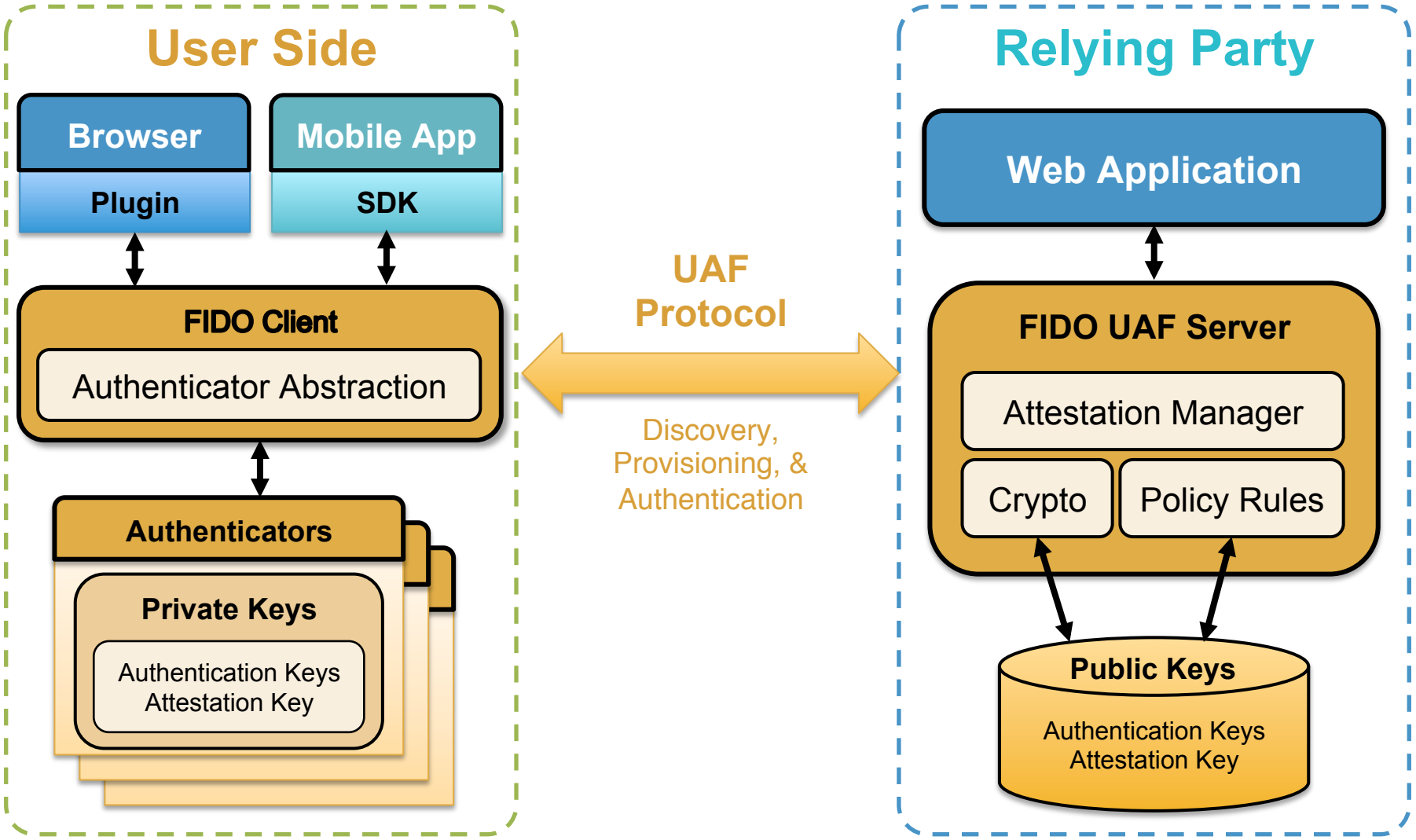
FIDO Today

- **Technical Working Groups active**
  - Public Spec Drafts early 2014
  - FIDO Ready Products available
  - Complement to existing standards & efforts
    - e.g., Federation, OpenID, SAML etc
- **Actively adding to FIDO membership**
  - Targeting Internet Services, Client Platform Owners, Device & Component Vendors, System Integrators

fido™ alliance | simpler stronger authentication

JOIN US! info@fidoalliance.org

UAF Flow Diagram



U2F Flow Diagram