Hands-On Perspectives: Deploying FIDO-Based Modern Authentication – The door to secure commerce

Abbie Barbir, Ph.D. November 2017

aetna® The next generation in identity and access validation

Agenda

- Problem Statement
  - Password
- Next Generation Authentication
  - Risk based authentication
    - FIDO based Solution
- Experience with Large deployment
- Online identity vetting
- Blockchain
  - Savrin
    - Decentralized Identity Descriptors
  - Next Steps
- Q&A

The trouble with passwords

Most people use less than 5

Reuse makes them easy

They are very

There are lots of places

- Over 3 billion user IDs and passwords were stolen in 2016
- When combined with other stolen identity attributes
  - Criminals use those credentials to take over accounts
  - Forgot password flow
  - Opening new account flow
    - KBA is not secure

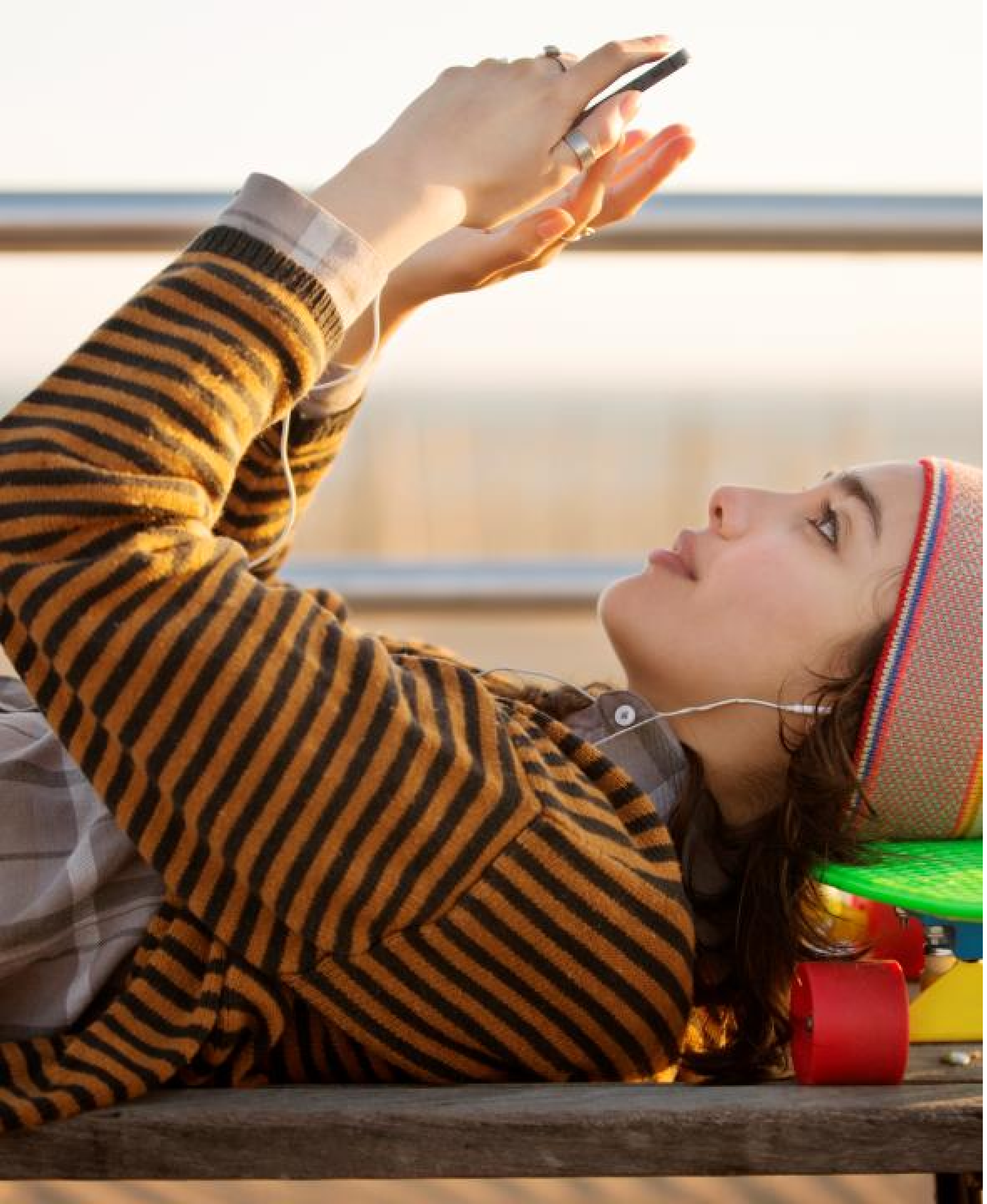
Sources: Pew research; Telesign research

It’s time for something better

A simpler and more secure experience

Aetna is leading the way in introducing advanced authentication methods into the health care sector.

- Our consumers no longer need to rely on traditional usernames and passwords when logging into Aetna applications
- Authentication, once a single event, is now integrated into the application transparently and continuously
- We’re adjusting controls and analytic capabilities to create friction for the threat adversaries while reducing friction for our users



It’s all about you

Passwords are impersonal

We give you other choices. Our advanced authentication methods are built around attributes unique to you such as:

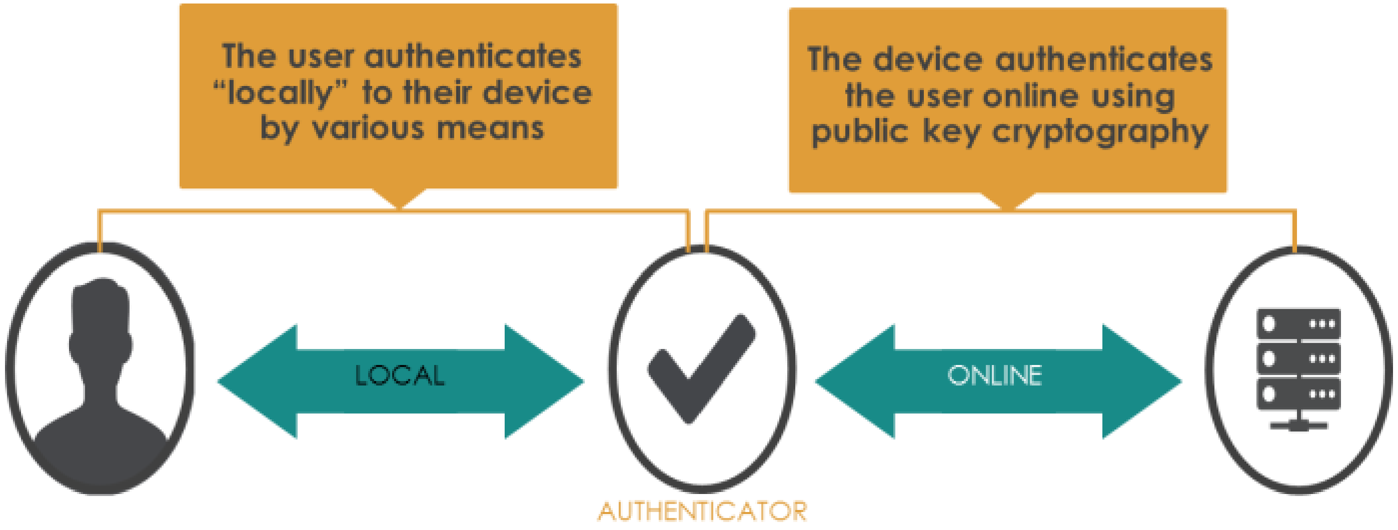
- Your physical location
- The time of access
- Your thumbprint
- How you hold your phone
- Your keystroke speed
- Your swipe gesture patterns
- How you walk

When combined, these attributes help us more accurately determine if you are who you say you are and how much access to provide.

NGA: Design principles

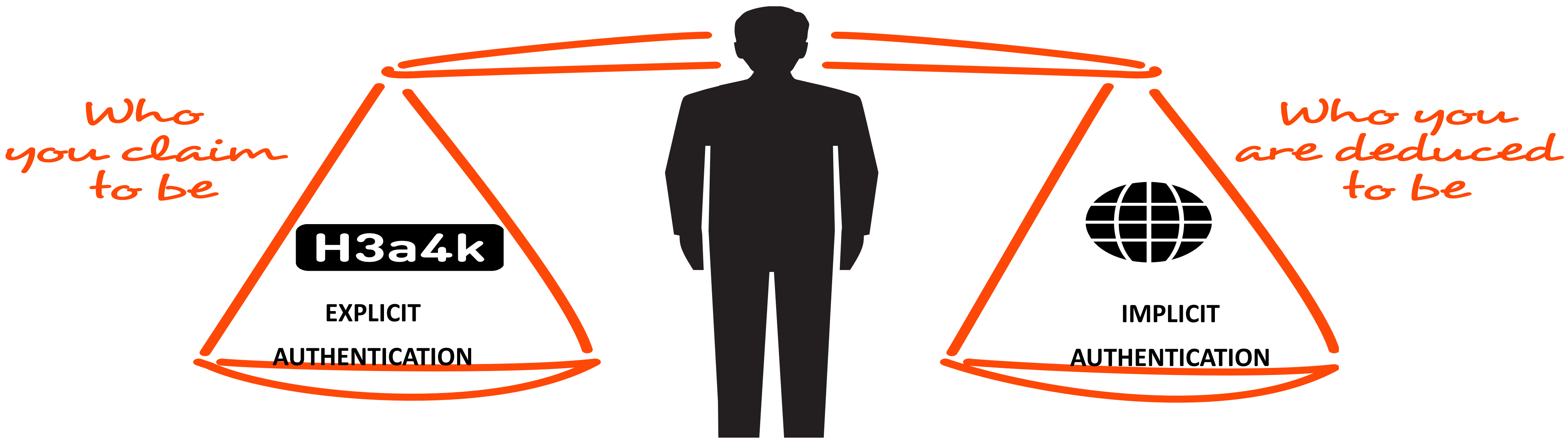
- Based on Open Specifications (i.e. FIDO)
- Easy SDK integration for web and mobile
- NGA's centralized authentication hub provides centralized analysis and decision making across all NGA applications
- API-based architecture
- Lightweight and efficient
- Device and platform portability
- Flows and interactions designed to reduce friction and improve user experience
- Eliminate fraud through increased friction for threat actor interactions
- Support for dynamic authentication through LOA

fido™ alliance


The user authenticates "locally" to their device by various means
The device authenticates the user online using public key cryptography
LOCAL
ONLINE
AUTHENTICATOR

aetna

Modern Authentication



Who you claim to be

H3a4k

EXPLICIT AUTHENTICATION

Who you are deduced to be

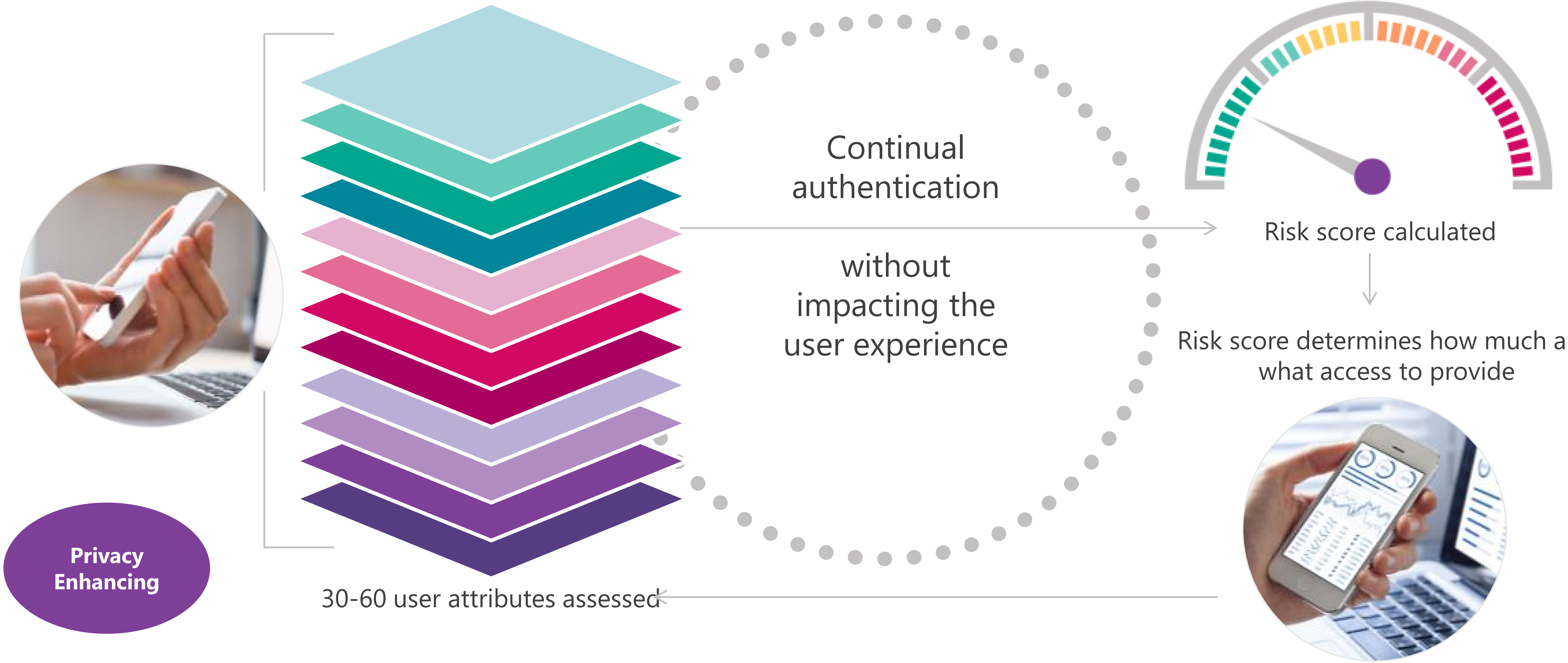
IMPLICIT AUTHENTICATION

- MUST eliminate symmetric shared secrets
- Address poor user experiences and friction
- **FIDO is a building block**
  - complements federation solutions

Impact

- **Identity binding is essential**
- **Strong identity proofing a must**

Continuous risk-based authentication



Continual authentication

without impacting the user experience

Risk score calculated

Risk score determines how much and what access to provide

30-60 user attributes assessed

Privacy Enhancing

Advanced authentication for mobile and web

Transparently and continuously authenticate the device and the user

Mobile

Biometric Integration

- Primary Login - Fingerprint
- Secondary Login – PIN
- FaceID in progress

Continuous Contextual Authentication (ex. geolocation)

Continuous Behavioral Authentication (ex. Keystroke)

Continuous Risk-based Consumer Authentication

Web

Browser and system fingerprinting

Device Binding

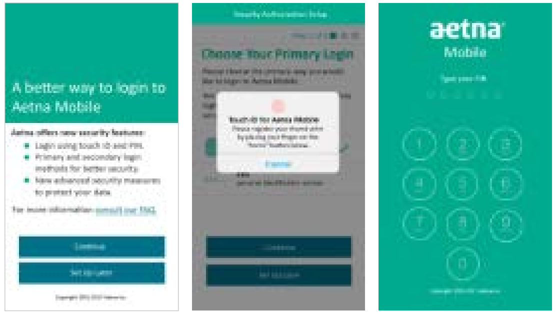
- Associate users and their devices

FIDO Standards assure that sensitive information never leaves your device

An evolution from binary to behavioral authentication

Today

- Username and password login


A better way to login to Aetna Mobile

Aetna offers new security features:

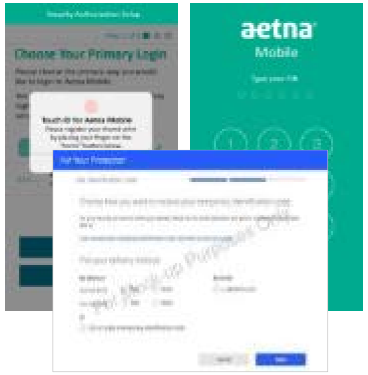
- Login using touch ID and PIN
- Primary and secondary login methods for better security
- New advanced security measures to protect your data

For more information consult our FAQ

Continue
Set Up Later
Security Authentication Setup
Choose Your Primary Login
Touch ID for Aetna Mobile
Cancel
aetna
Mobile
Type your PIN
1
2
3
4
5
6
7
8
9
0

Phase 1 - 2017

- Fingerprint and PIN login for mobile
- Introduction of risk-based authentication
- Enhanced security capabilities for mobile
- **Aetna Mobile**


Security Authentication Setup
Choose Your Primary Login
Touch ID for Aetna Mobile
aetna
Mobile
1
2
3

Phase 2 - 2017

- Browser fingerprinting for web
- Web & mobile risk based authentication
- **PayFlex Mobile**
- **PayFlex Web**
- **Aetna Navigator (TBD 2018)**

2018

- Behavioral-based authentication (mobile)
- Support for biometric authentication on web applications
- Cross platform authentication
- **Enterprise web & mobile applications**

NGA: Mobile offering

NGA's mobile integration capabilities provide a mechanism for implementing consumer accepted and expected authentication capabilities in a manner that:

- Transparently and continuously authenticates the device and user
- Improves security and reduces the risk of fraud
- Removes barriers to application access

*...while **improving** the user experience*

Reduced reliance on **passwords** through enhanced user & device authentication

Continuous Behavioral Authentication (i.e. swipe attributes)

Continuous Contextual Authentication (i.e. geolocation)

Biometric Integration

fido™ alliance

Designed in alignment with **FIDO Standards**

NGA: Web offering

NGA’s web integration capabilities provide a mechanism for implementing consumer accepted and expected authentication capabilities in a manner that:

- Improves member data security
- Reduces the risk of fraud

*…while **improving** the user experience*

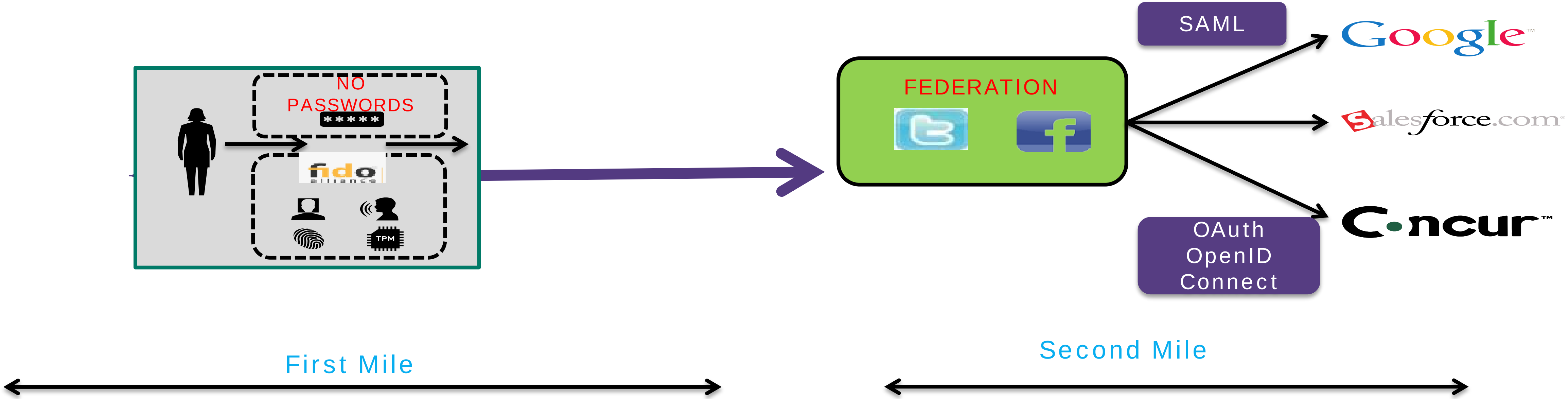
Reduced reliance on **passwords** through enhanced user & device authentication

Browser & System Fingerprinting for each session improves security & usability

Associate members & their devices through ***Device Binding*** to improve user experience & security

Eliminates risk of **impersonation**, account takeover, and registration **fraud**

Federation



- Standards are catching up on mile one
- Mile two is getting more mature
  - Federation need improvement
  - No prior relationship
    - SAML: Dynamic AuthN/Z
    - OAuth, OIDC dynamic end point
    - Blockchain Opportunity

- How about identity assurance?
  - Poorly deploying strong authentication is the same as weak authentication
- **FIDO solves the PW problem but mandates better identity binding at the relaying party**
- **Proper Identity vetting/proofing becomes essential**

Identity proofing and account recovery

Account Login Current Pain Points

- I forgot my password
- I cannot find/lost my phone
- I am locked out of my account

Account Recovery Options

- KBA (static and/or dynamic)
- Email account (compromised)
  - Password reset link
  - Or a new password
  - Enrolling back in FIDO

Identity Proofing

- Binding a FIDO authenticator to a user account on relying party requires performing an Identity vetting step
  - Trust anchor (aka Bootstrapping problem)
- Currently pre-established Authenticators are used as anchors of Trust (such as passwords)

Online identity proofing is challenging and still relies on something "you know"

Blockchain technology

- Blockchain – distributed data store
- Public Key Cryptography (PKI)
- Peer to peer connected nodes

- Consensus mechanism (PoS, PoW, etc)
- Smart contracts

Permisionless

- Proof of work (PoW)
- Open node participation
- Weak(er) governance
  - Role of determined entities
- Performance
  - Mileage may vary

Permissioned

- Controlled participation
  - Authorized entities
- Improved Governance
- Entities are vetted
- Potentially faster consensus

Blockchain: What is the opportunity

Motivation

- Improve on identity vetting, registration and verification
- Address open issues in our current solutions such as
  - Missing identity attributes
  - Identity bootstrapping
  - Compliance
  - initial identity proofing
  - Identity binding
  - Better user experience
- What we want to achieve is a reliable and scalable system for attributes verification, storage, access, revocation and update
- Privacy enabled architecture where multiple entities collaborate on identity attribute services per user consent

Blockchain can transform identity proofing, binding and recovery

Use Blockchain to implement a common identity trust fabric

Blockchain for identity vetting

U
S
E
R
I
N
V

- Blockchain does not hold individual identity
- Trusted Nodes (act like a Federation)
- Individual identity data is stored off chain
  - Avoid storing private attributes on a public ledger (even when encrypted)
  - Stores references to data
- Originators retain control of their data
- **For the client**

Looking Into

- **(DID) Decentralized identifiers**
- **Sovrin Blockchain**

IOT support

- Serve as Infrastructure for extra services including user wallets

- Client acquire policy
s to Application
enrol
step requires
ntity
ification
uivalent of
C
tion stage
asserted
ttestations on
hain
re importantly
h FIDO a
ding between a
ice and
ntity can be
erted

On Block : Going Forward

Investigate if a core consortium of trusted entities is possible

- Share individual identity data attributes that all parties agree on exchange mechanisms, data structure, semantics and the context under which it is shared based on relationship and purpose
- Enable large scale trust and federation without the need of one to one relationship
- Global Federation capabilities
  - Dynamic SAML and OAuth
  - Improved Security and No need for prior negotiation
- Enable interoperable system of data exchange of healthcare records

Lessons learned

- Implementing FIDO is easy at the technical level
- Hard lessons: Get Applications owners on-board
    - Set expectation up front
    - UI-free API for
        - enrolment/registration/authentication flows
        - Do not expect application owners to user your flows
        - You have to work with their flows
    - Manage expectations
        - Things get out of hand to support many use cases and scenarios
        - Not two applications are the same
        - Look and feel matter
            - stay out of it

- Build ID Proofing engine using OpenID Connect
    - Allows for multiple proofing solutions/providers
    - Develop an the Identity toolkit
- Protecting PII is resource intensive
- Remote ID proofing is Hard
    - High Assurance level is a must
- Need to design to reduce reliance on CSR

Questions?