
HIMSS18
The leading health information and technology conference
WHERE THE WORLD CONNECTS FOR HEALTH
Conference & Exhibition | March 5–9, 2018
Las Vegas | Venetian – Palazzo – Sands Expo Center
Next Gen Security Technologies for Healthcare Authentication
Session 261, March 8, 2018
Abbie Barbir, Senior Security Adviser, Aetna
Brett McDowell, Executive Director, FIDO Alliance
COMMITMENT
www.himssconference.org
#HIMSS18
fido ALLIANCE
aetna
DISCLAIMER: The views and opinions expressed in this presentation are those of the author and do not necessarily represent official policy or position of HIMSS.

Conflict of Interest

Abbie Barbir and Brett McDowell have no real or apparent conflicts of interest to report.

Agenda

- The Problem: Authentication in Healthcare
- Old Authentication vs. FIDO Authentication
- Advanced Authentication in Healthcare
- Aetna's Case Study
- Lessons Learned
- Q&A

Learning Objectives

- Examine the problems created by weak, password-based authentication, and how these credentials can be stolen and re-used
- Analyze the changes taking place in identity management and the patient's use of different devices and channels, and the problems this creates in managing the patient/provider/payer relationship
- Explain how new authentication standards from the FIDO (Fast IDentity Online) Alliance and behavioral authentication techniques enable a provider to protect against myriad attacks while ensuring a simple user experience

Learning Objectives

- Define the key capabilities required in a next-generation identity management and authentication healthcare solution
- Demonstrate and explain the architecture and advantages of a next-generation authentication solution for managing and deepening payer/provider/patient relationships across more personal devices, including wearable fitness or medical devices, and across multiple channels

Over 3 billion user IDs and passwords were stolen in 2016

Source: Shape Security

Criminals Use Those Credentials to Take Over Your Accounts

In 2016, data breaches increased by

40%

51%

of consumers suffered some kind of security incident in 2016, including a stolen password or breached account

81%

of hacking related breaches leveraged stolen or weak passwords

Sources: 2017 Verizon DBIR Report; Identity Theft Resource Center (ITRC) and CyberScout

The Trouble with Passwords

Most people use less than 5 passwords for all accounts

50%

of those haven't changed their password in the last 5 years

Reuse makes them easy to compromise

39%

of adults use the same password for many of their online accounts

They are very difficult to remember

25%

of adults admit to using less secure passwords, because they are easier to remember

There are lots of places to steal them from

49%

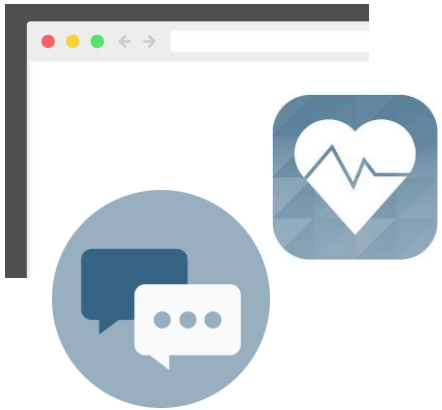
of adults write their passwords down on paper

Sources: Pew research; Telesign research

Modern Authentication Creates Opportunity

New channels and devices can enable simple and consistent user experiences

New Channels



How do we manage patient identity, patient use of devices, and the patient/provider/payer relationship?

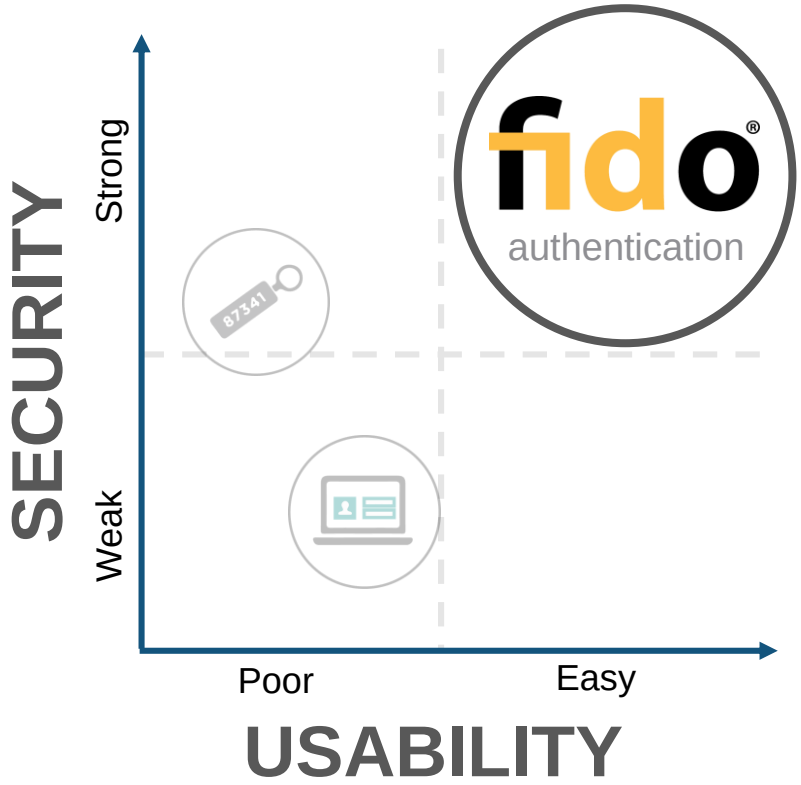
New Devices

250+ Organizations Solving the Problem Together

+ SPONSOR MEMBERS + ASSOCIATE MEMBERS + LIAISON MEMBERS

#HIMSS18

The Mission: Simpler & Stronger Authentication



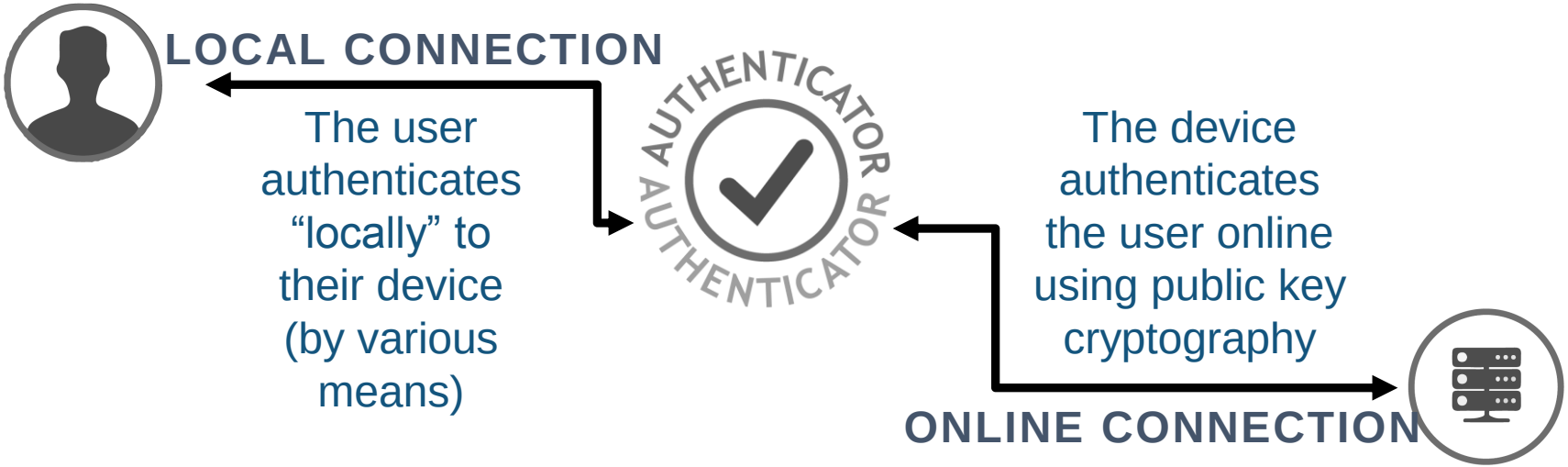
=

open standards for simpler, stronger authentication using **public key cryptography**

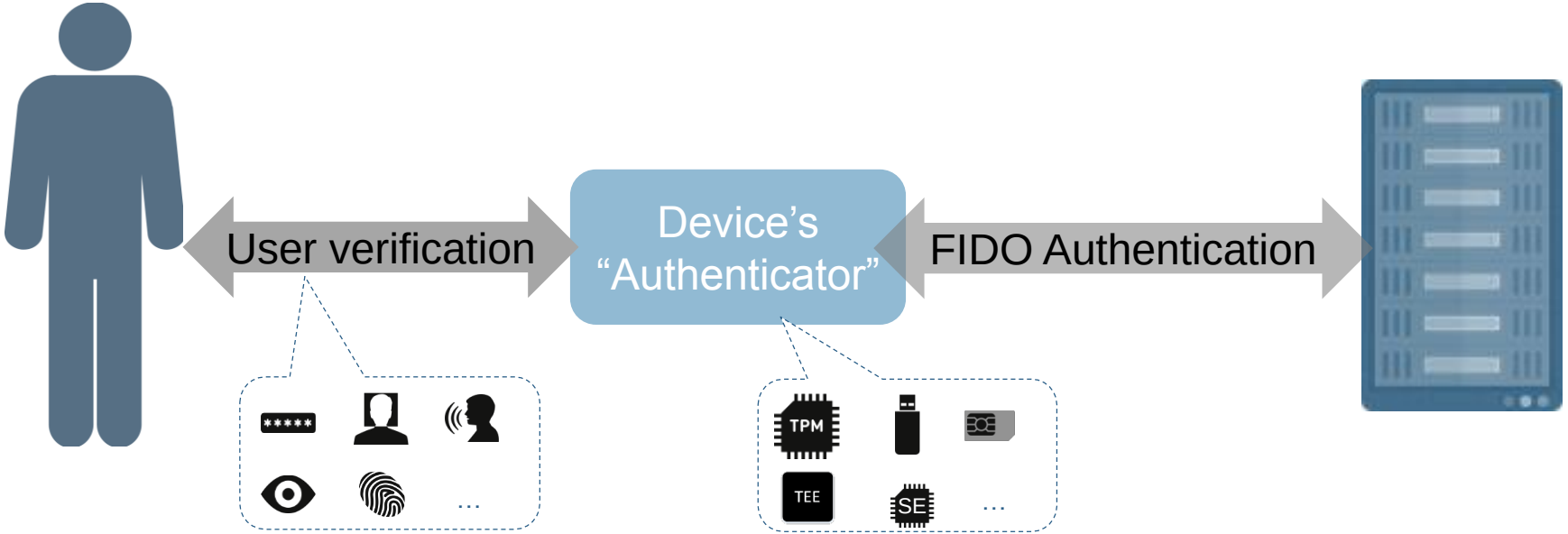
How Old Authentication Works

The user authenticates themselves online by presenting a human-readable “shared secret”

How FIDO Authentication Works



How Industry Enables FIDO Use Cases



Experiences Address an Array of Use Cases

FIDO standards provide support for user-friendly, privacy-aware user experiences across platforms to meet varying requirements

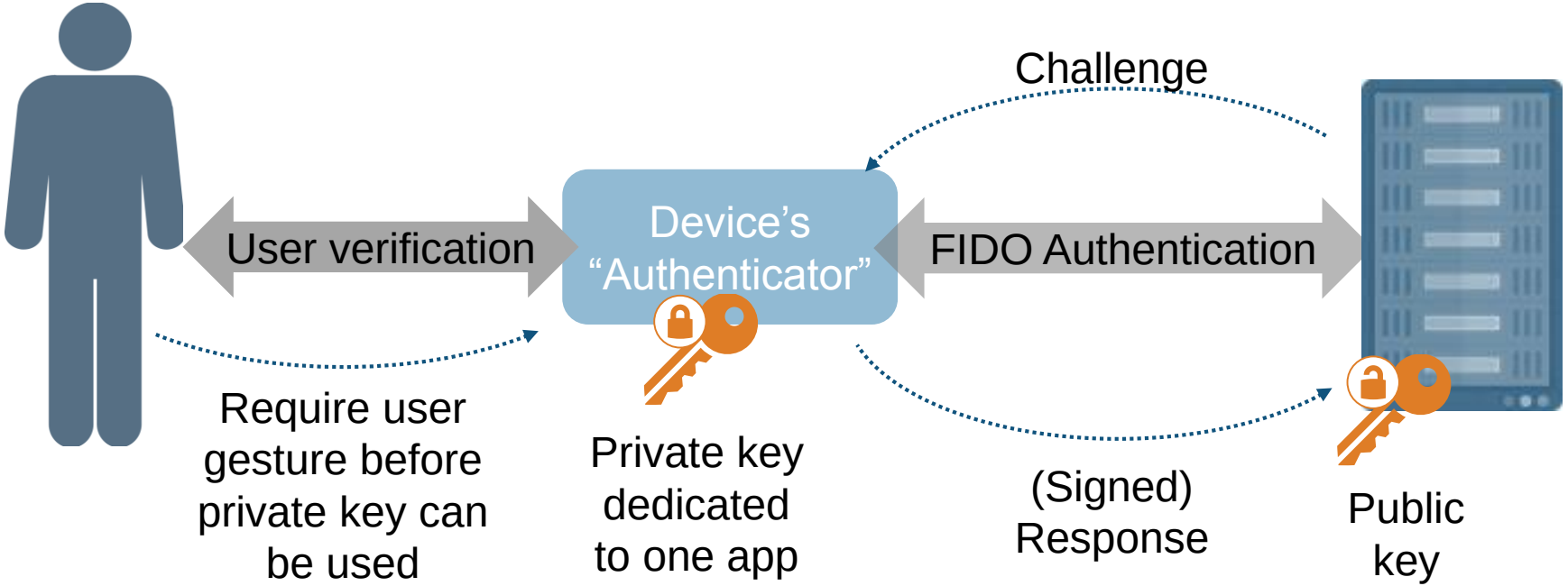
PASSWORDLESS EXPERIENCES

- Biometrics authn via mobile device
- Biometric authn via PC
- Biometrics authn to PC via mobile device

SECOND FACTOR EXPERIENCES

- External token to PC (USB, BLE)
- External token to mobile device (NFC/BLE)
- Embedded second factor on PC

How FIDO Authentication Works



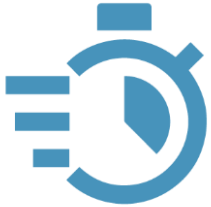
Simpler?

Reduces reliance on complex passwords

Single gesture to log on

Works with commonly used devices

Same authentication on multiple devices



Fast and convenient

Stronger?

Based on public key cryptography

No link-ability between services or accounts

Keys stay on device

Biometrics, if used, never leave device

No server-side shared secrets

No 3rd party in the

Sample: FIDO-enabled Services

Google

facebook.

salesforce

aetna®

Available to Protect

3.5 BILLION

Accounts Worldwide

Dropbox

ebay

Bank of America

PayPal

Advanced Authentication in Healthcare

Aetna is leading the way in introducing advanced authentication methods into the healthcare sector using FIDO standards and continual authentication.

Hands-On Perspectives: Deploying FIDO-Based Modern Authentication

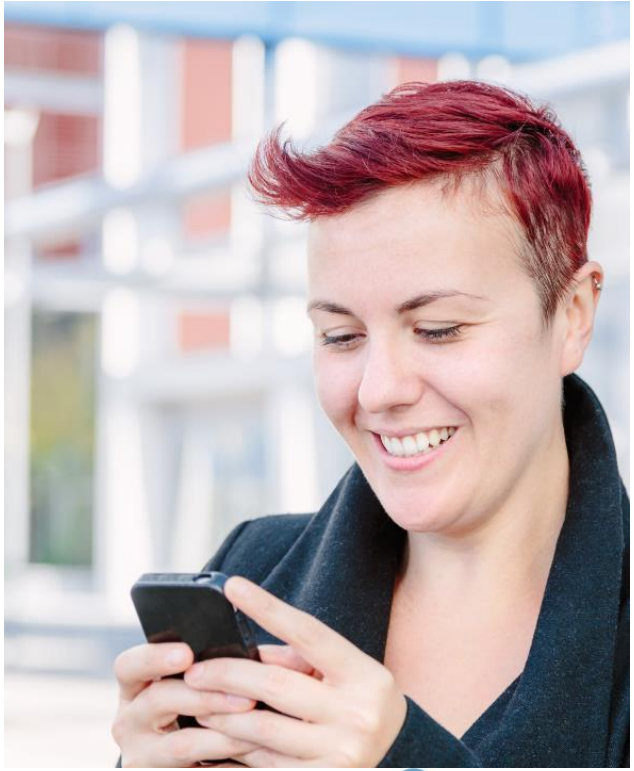
Aetna's Case Study

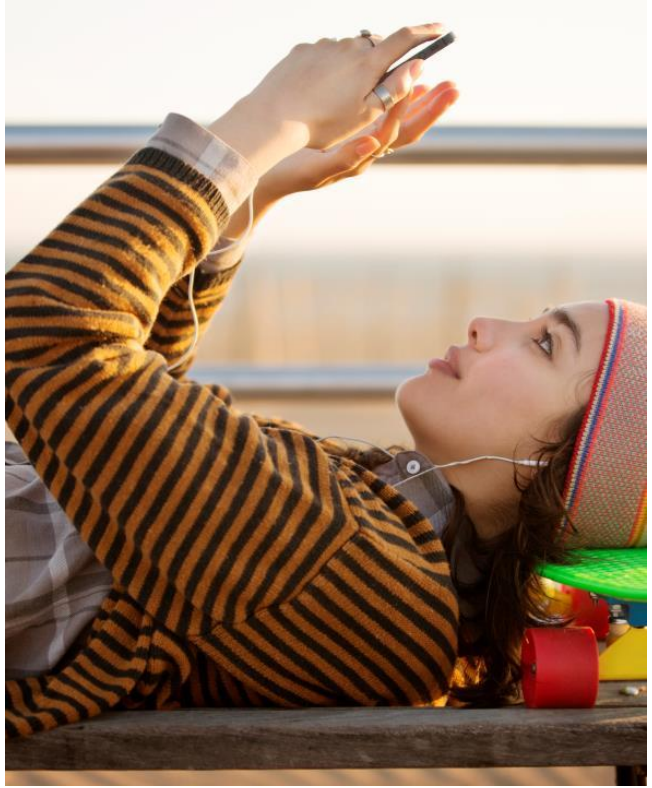
#HIMSS18

We Needed a Simpler and More Secure Experience

>>Next Generation Authentication (NGA) program

- 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





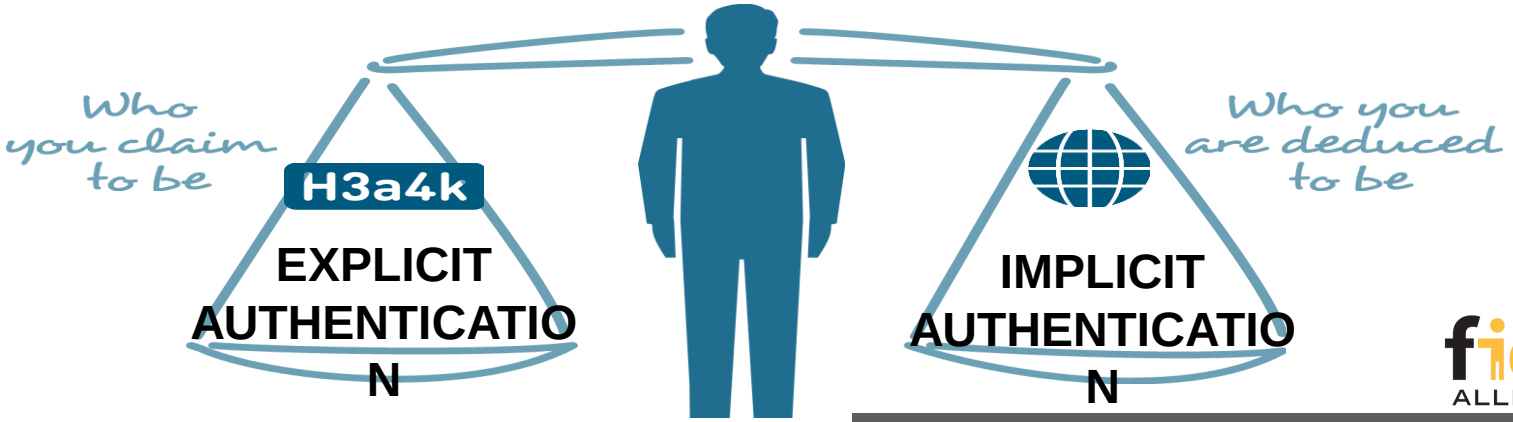
Attributes Identify You

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.

Modern 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

Privacy Enhancing

30-60 user attributes assessed

Continual authentication

without impacting the user experience

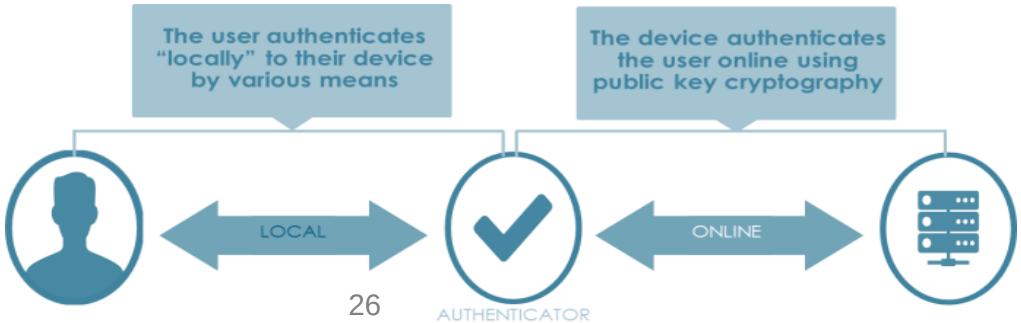
Risk score calculated

Risk score determines how much and what 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



Why Standards?

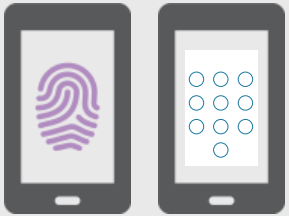
We chose to use the FIDO standard for the following reasons:

1. Local biometric capabilities are evolving rapidly and we wanted to enable the consumer with choices while following a standard to feed behavioral data into our NGA risk engine
2. The different capabilities for biometrics is dependent on carrier choices, manufacturer choices and software choices all beyond an enterprise's control and influence so adopting a standard like FIDO gives the enterprise a standard interface while providing the consumer with choices
3. Standards based architectures cost less to operate vs. non-standards based architectures

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

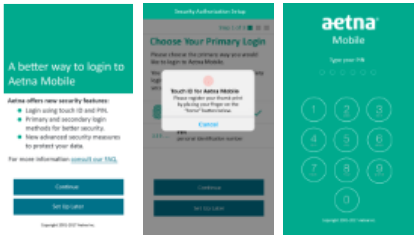
Browser and system fingerprinting

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

Phase 1 - 2017

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

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 and Mobile

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**

#HIMSS18

NGA and Web

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*

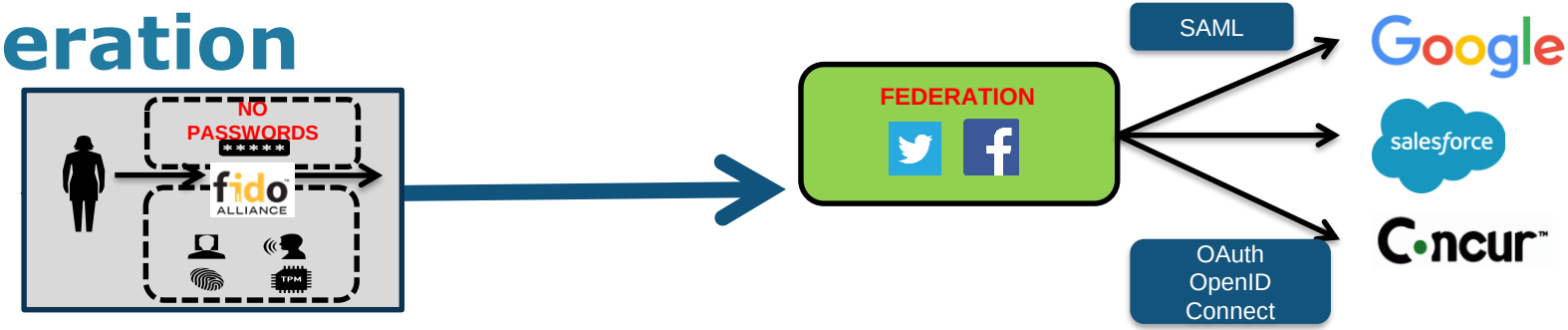
Reduced reliance on **passwords** through enhanced user & device authentication

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



First Mile

- 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

Second Mile

- 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

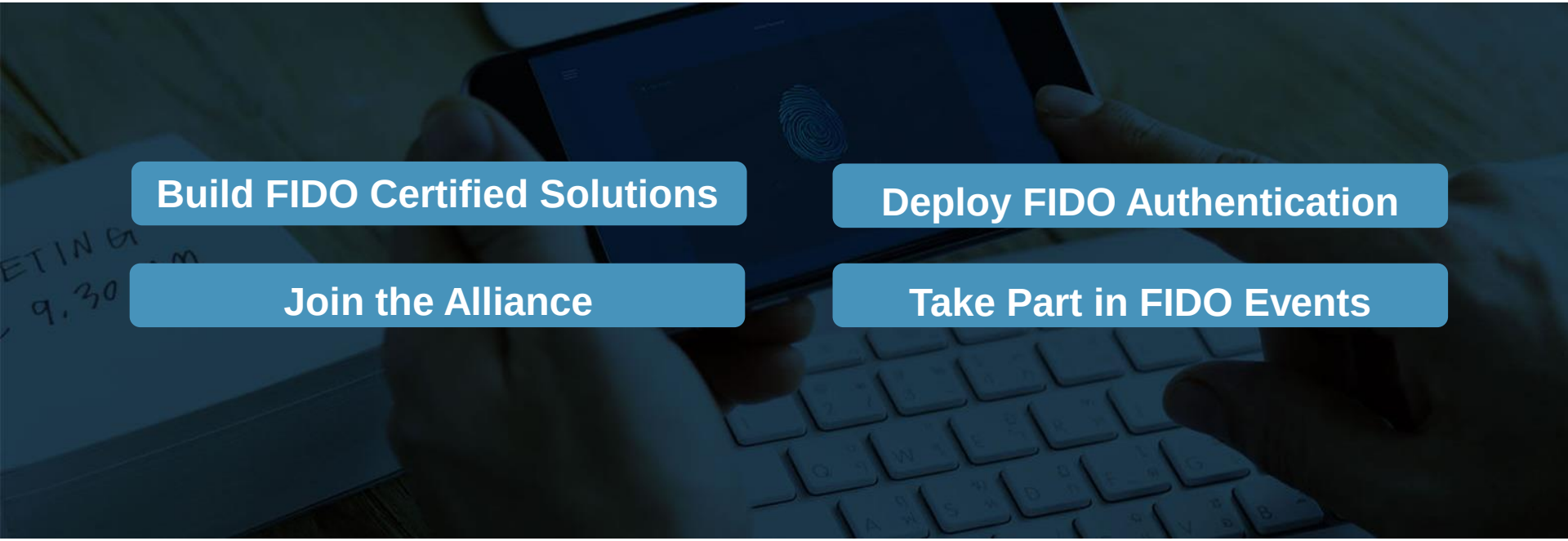
- **Identity Proofing**
- Binding a FIDO authenticator to a user account on relying party requires performing an Identity vetting step
  - Trust anchor (aka Bootstrapping problem)
- Currently pre-established Authenticators are used as anchors of Trust (such as passwords)

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

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

How to Get Involved



- Build FIDO Certified Solutions
- Deploy FIDO Authentication
- Join the Alliance
- Take Part in FIDO Events

Questions?

Abbie Barbir
BarbirA@aetna.com
@Aetna

Brett McDowell
brett@fidoalliance.org
@FIDOAlliance

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

- 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
- Permission based system

For the client

- No data about me without me
- N
- W
- C
- U

- Se

Looking Into

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

- Client acquire policy
- Client goes to Application
  ite to enrol
  ment step requires
  - Identity
  - Verification
  - Equivalent of KYC

  istration stage
  ty is asserted
  ugh Attestations on
  ockchain
  - More importantly with FIDO a binding between a device and identity can be asserted