Securing Web and Mobile Payments with FIDO Authentication

Brett McDowell, Executive Director, FIDO Alliance
The Problem
The Solution
The Alliance
Case Studies
Data Breaches...

781 data breaches in 2015

170M records since 2015 (up 50%)

$3.8 million/breach (up 23% f/2013)
“A look through the details of these incidents shows a common sequence of

phish customer ≥
get credentials ≥
abuse web application ≥
empty bank/bitcoin account.”

2015 Data Breach Investigations Report
The world has a **PASSWORD PROBLEM**
ONE-TIME PASSCODES

Improve security but aren’t easy enough to use

- SMS Reliability
- Token Necklace
- User Confusion
- Still Phishable
WE NEED A NEW MODEL
WE CALL OUR NEW MODEL Fast IDentity Online

online authentication using public key cryptography
The Problem
The Solution
The Alliance
Case Studies
THE OLD PARADIGM

SECURITY  USABILITY
THE FIDO PARADIGM

SECURITY

Poor

Easy

USABILITY

Strong

Weak

FIDO alliance
The user authenticates themselves online by presenting a human-readable secret.
HOW FIDO AUTHN WORKS

The user authenticates “locally” to their device by various means

The device authenticates the user online using public key cryptography
FIDO Registration

1. User is in a Session
   Or
   New Account Flow

   Invitation Sent

2. User Approval

3. New Keys Created

4. Public Key Registered
   With Online Server

Registration Complete
FIDO Authentication

1. FIDO Challenge
   - User needs to login or authorize a transaction

2. User Approval
   - Signed Response verified using Public Key Cryptography

3. Key Selected & Signs

4. Login Complete
   - Confidential
ATTESTATION & METADATA

FIDO Authenticator

Signed Attestation Object

FIDO Server

Verify Trust Anchor (Available from Metadata Service or Other Source)

Metadata

Understand Authenticator Characteristic (Using Info From Metadata or Other Source)
Passwordless Experience

1. Authentication Challenge
2. Biometric Verification*
3. Authenticated Online

Second Factor Experience

1. Second Factor Challenge
2. Insert Dongle* / Press Button
3. Authenticated Online

*There are other types of authenticators
FIDO WITH USER VERIFICATION

Same User as enrolled before?

Same Authenticator as registered before?

USER VERIFICATION

FIDO AUTHENTICATION

AUTHENTICATOR
STEP 1
STEP 2

Log in to your account with your fingerprint.
STEP 3
STEP 4

Payment complete!

Return to the merchant's web site to continue shopping

Return to the merchant
FIDO AS 2\textsuperscript{ND} FACTOR

- Is a user present?

- USER PRESENCE

- FIDO AUTHENTICATION

- Authenticator

- Same authenticator as registered before?

- Happens after 1\textsuperscript{st} factor challenge
Step 1

Email
Password
Sign in
Stay signed in
Need help?
Step 2

Email

Password

Sign In

Stay signed in

Need help?
Step 3

2-Step Verification

Tip: You may need to tap or re-insert your security key.

Confirm using your security key

Use a verification code instead

☑ Don't ask for my security key again on this computer
Step 4
USABILITY, SECURITY and PRIVACY
No 3rd Party in the Protocol

No Secrets on the Server Side

Biometric Data (if used) Never Leaves Device

No Link-ability Between Services

No Link-ability Between Accounts
Better security for online services
Reduced cost for the enterprise
Simpler and safer for consumers
The Problem
The Solution
The Alliance
Case Studies
FIDO Alliance Mission

1. Develop Specifications
2. Operate Adoption Programs
3. Pursue Formal Standardization
Liaison Partners
2014 FIDO ADOPTION

“Secure Consumer Payments Enabled for Alipay Customers with Easy-to-Use Fingerprint Sensors on Recently-Launched Samsung Galaxy S5”
September 17, 2014

“PayPal and Samsung Enable Consumer Payments with Fingerprint Authentication on New Samsung Galaxy S5”
Feb 24, 2014

“Google Launches Security Key, World’s First Deployment of Fast Identity Online Universal Second Factor (FIDO U2F) Authentication”
October 21, 2014
2015 FIDO ADOPTION

“Microsoft Announces FIDO Support Coming to Windows 10”
Feb 23, 2015

“Microsoft launches Snapdragon fingerprint scanning technology”
March 2, 2015

“Google for Work announced Enterprise admin support for FIDO® U2F 'Security Key’”
April 21, 2015

“Largest mobile network in Japan becomes first wireless carrier to enhance customer experience with natural, simple and strong ways to authenticate to DOCOMO’s services using FIDO standards.”
May 26, 2015

“[T]he technology supporting fingerprint sign-in was built according to FIDO (Fast IDentity Online) standards.”
September 15, 2015

“Today, we're adding Universal 2nd Factor (U2F) security keys as an additional method for two-step verification, giving you stronger authentication protection.”
August 12, 2015

“GitHub says it will now handle what is called the FIDO Universal 2nd Factor, or U2F, specification.”
October 1, 2015

All Rights Reserved, FIDO Alliance. Copyright 2016.
2016 FIDO ADOPTION

“FIDO Universal 2nd Factor (U2F) authentication is now being used to allow all UK citizens to easily and securely access GOV.UK Verify digital public services. Mar 23, 2016

“BC Card provides Token and FIDO services to strengthen security and safety of Samsung Pay” March 1, 2016

“KEB Hana’s new solution is notably FIDO Certified.” February 3, 2016

“NTT DOCOMO is now offering FIDO-enabled biometric authentication for customers using Apple iOS devices” Mar 7, 2016
Deployments are enabled by FIDO Certified™ products available today
Available to anyone
✓ Ensures interoperability
✓ Promotes the FIDO ecosystem

Steps to certification:
1. Conformance Self-Validation
2. Interoperability Testing
3. Certification Request
4. Trademark License (optional)

fidoalliance.org/certification
The Problem
The Solution
The Alliance
Case Studies
Case Study: BC Card’s FIDO Services

Jaemoon Yoo
Overview of BC Card

BC Card, established in 1982, provides the core services in acquiring and issuing on behalf of 29 member banks and clients with its expertise and excellence.

Our Member Banks & Clients

29 Member Banks/Clients of BC Card

2.8 Mil. Active Merchants

Our Services

Acquiring Processing
(Switching/Authorization/Settlement)

316 Mil. Transactions per month (’15)

Merchant Networking

2.8 Mil. Active Merchants

Issuing Processing

Card Issuing BPO
25 M. Cards per year (’15)
Biometrics Authentication (FIDO)

To ensure security of the payment solutions, BC Card developed a FIDO Server and Biometrics Authentication Applications.

**BC Card’s FIDO Service Overview**

<table>
<thead>
<tr>
<th>Biometric Method</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Fingerprint**  | Fingerprint Recognition for Samsung Pay  
• Applied BC Card owned FIDO Server to SAMSUNG Pay fingerprints authentication |
| **Voice**        | Voice Recognition to apply for BC Pay  
• Self Authentication and Payment through Voice (Apr. 2016) |
| **Face**         | Face Recognition for Simple Payment  
• Self authentication and payment by Face recognition (3Q 2016)  
• Distinguishes twins and pictures |
| **Iris**         | Offline Payment by Iris Recognition  
• You can pay just by scanning your eyes at the camera at the store |

“The First Asian Financial Institution to be approved as FIDO Board member”

BC Card established FIDO Server, which strengthens convenience and security.

<table>
<thead>
<tr>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completed</td>
</tr>
<tr>
<td>Work in Progress</td>
</tr>
</tbody>
</table>
[Case] BC Pay Voice Authentication

BC Card adopted voice authentication technology to BC Pay (mISP) services successfully.

### Key Features and Performances

**Application of Voice Authentication to On/Offline Payments**
- Replace PIN
- FIDO based safe payment at offline store by my voice
- Launched Voice Authentication service at April 2016 BC Pay and mISP

**FRR\(^1\) 4\%, FAR\(^2\) 0.05\%**
- Elimination of Noise and Channel bias
- Adaption Algorithm good for microphone and Environment variables
- Accommodation for Voice change as time passes
- Recording Distinction Algorithm
- Learning and User friendly UI

---

(please say the above sentence)
Case Study: Ledger, FIDO & Blockchain

Nicolas Bacca
FIDO and Blockchain: a good match

**FIDO**: Better *identity*, using strong cryptography

**Blockchain**: Better *trust*, using strong cryptography

Foundations of innovative privacy aware, user centric applications relying on strong cryptography
FIDO U2F provides a secure authentication framework to sensitive Bitcoin applications, such as currency exchanges.

Bitcoin key derivation and backup standards (Hierarchical Deterministic Wallets and mnemonics) improve U2F user experience if a token is lost.
Building the user keyring

One master key, the user digital identity

Derived for specific applications

FIDO being several of them

Smart, secure hardware enforcing permissions
JOIN THE FIDO ECOSYSTEM