Identity Standards and Certification

Presentation to W3C Anti-Fraud Community Group

April 1, 2022

Jeremy Grant
Advisor
FIDO Alliance
jeremy.grant@venable.com

fido™ ALLIANCE

What's FIDO?

The FIDO Alliance is an open industry association with a focused mission:

Develop authentication standards, certification and market adoption programs to help reduce the world's over-reliance on passwords.

An industry movement

+ Sponsor members

+ Associate members

+ Liaison members

Government members

NIST National Institute of Standards and Technology U.S. Department of Commerce

GSA

Cabinet Office

National Cyber Security Centre

Australian Government Digital Transformation Office

Australian Government Australian Signals Directorate

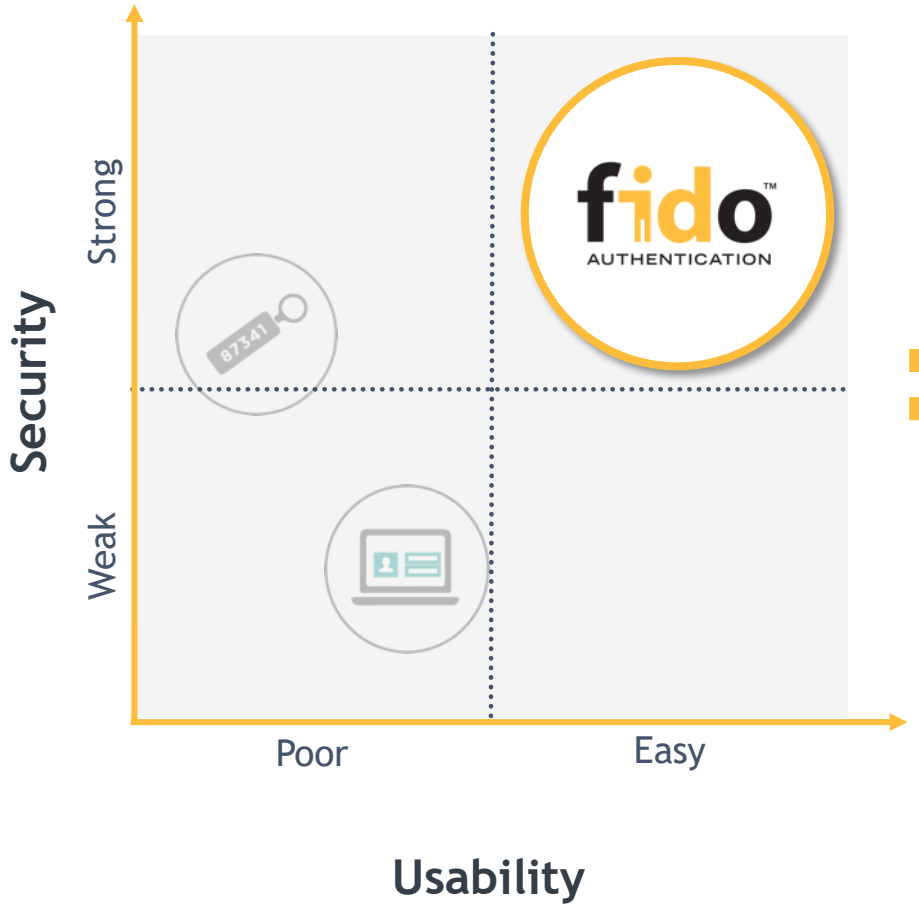
ACSC Australian Cyber Security Centre

Federal Office for Information Security

中華民國內政部 MINISTRY OF THE INTERIOR, R.O.C. (TAIWAN)

TTA 한국정보통신기술협회 Telecommunications Technology Association

Industry imperative: Simpler and stronger

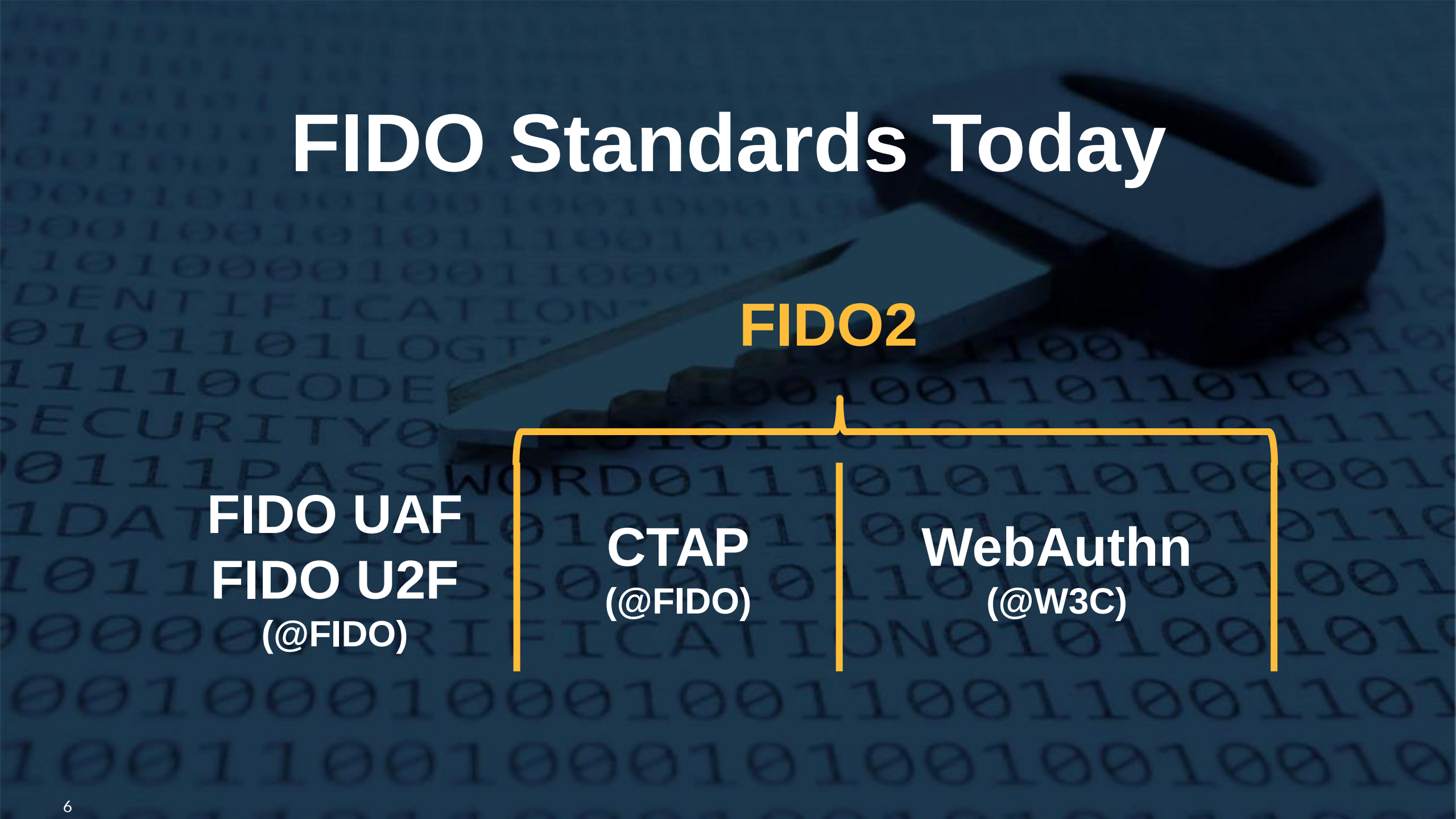


=

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

Single Gesture
Possession-based Authentication

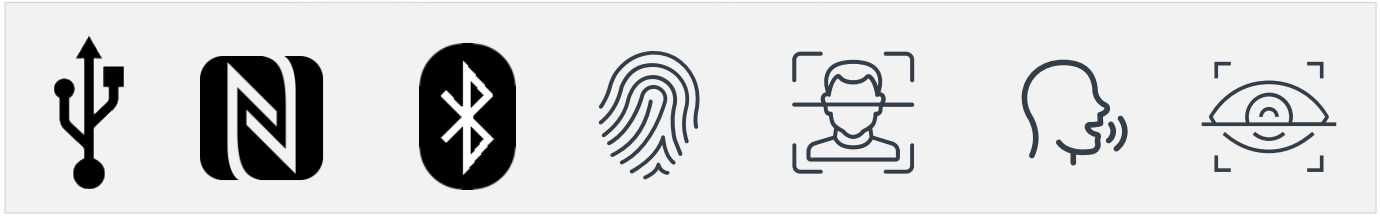
FIDO Standards Today

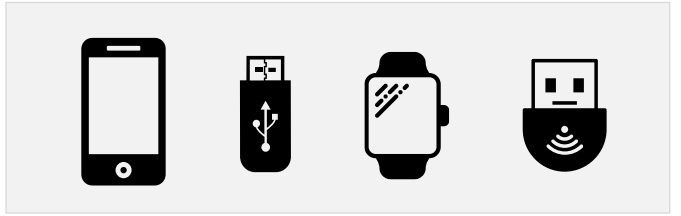


Global market validation

State of the Market: 2022

FIDO as a standard feature across browsers, platforms & devices





Backed by certification – 850+ products!

Functional Certification (End-to-End):

- Conformance Testing
- Interoperability Testing
- Universal Server

Security Certification Levels

- How well do you protect the private key?
- 3rd-party laboratory verification

Biometric Certification Program

- Empirically validate biometrics through third-party labs
- Assure that they correctly identify users regardless of biometric modality on all FIDO implementation types

The “gold standard” of MFA

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

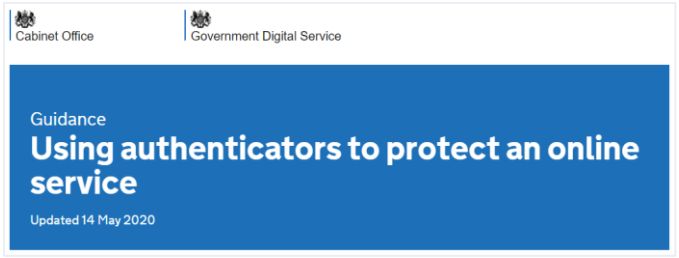
How Do I Enable MFA?

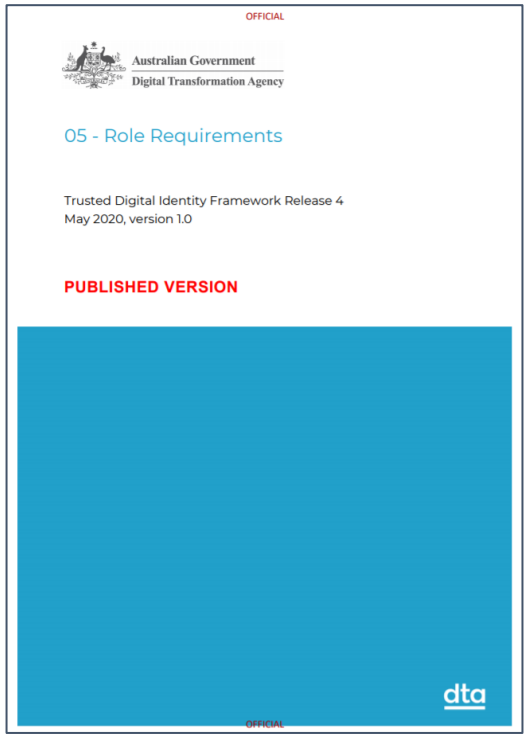
Start by looking at the security settings on your most-used accounts. You may see options to enable MFA listed as “Two Factor Authentication,” “Multi-Factor Authentication,” or “Two Step Factor Authentication.”

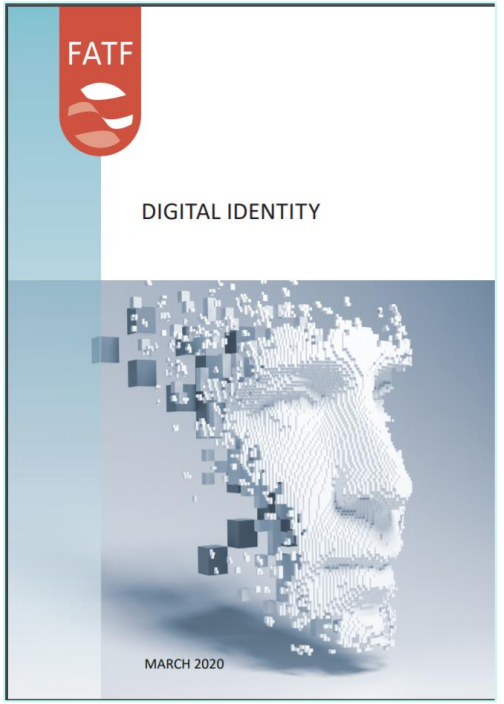
There are many ways you may be asked to provide a second form of authentication:

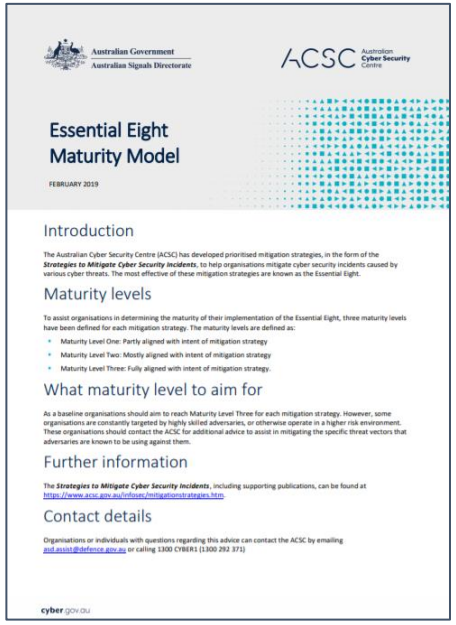
- Text Message (SMS) or Email: Every time you login to an account, you’ll be asked to provide a code sent to you by text message or email. Of note, this is actually the weakest form of MFA and you should only use it if none of the other options is available.
- Authenticator App: An authenticator app is an app thatgenerates MFA login codes on your phone. Whenprompted for your MFA code, you launch the app and read the applicable number. These codes often expire every 30 or 60 seconds.
- Push notification: Instead of using a numeric code, the service “pushes” a request to your phone to ask if it should let you in. You see a pop-up and can confirm the login request, or deny it if you were not initiating the authentication request.
- FIDO Key: FIDO stands for "Fast IDentity Online" and is considered the gold standard of multi-factor authentication. The FIDO protocol is built into all major browsers and phones. It can use secure biometric authentication mechanisms – like facial recognition, a fingerprint, or voice recognition – and is built on a foundation of strong cryptography. Often it uses a physical device – a key – essentially an encrypted version of a key to your house.
- More information on FIDO keys is available from the FIDO Alliance.

Part of a broader trend of government recognition of FIDO



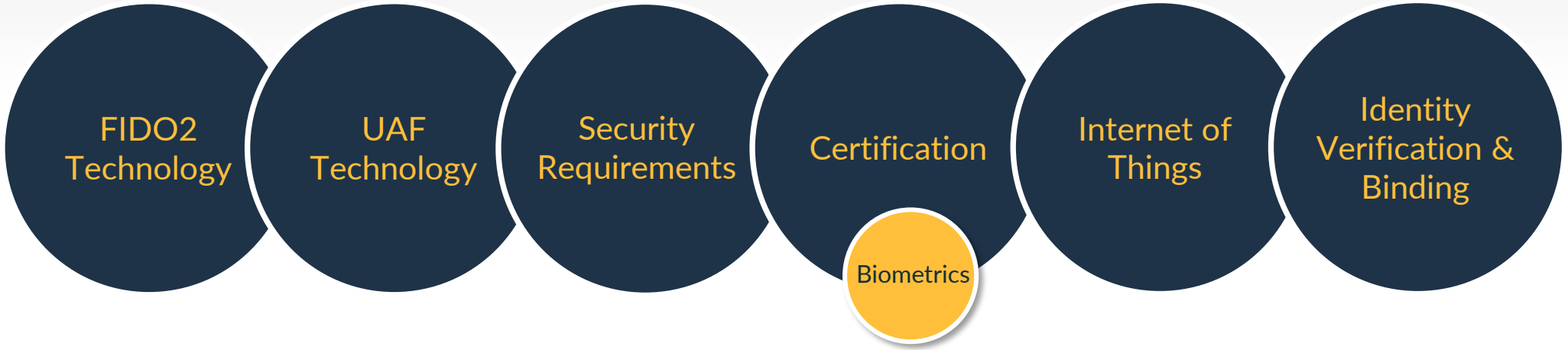






Getting involved in the Alliance

Technical Working Groups



Adoption Working Groups

Thank you!

@FIDOALLIANCE
WWW.FIDOALLIANCE.ORG

Jeremy Grant
jeremy.grant@venable.com