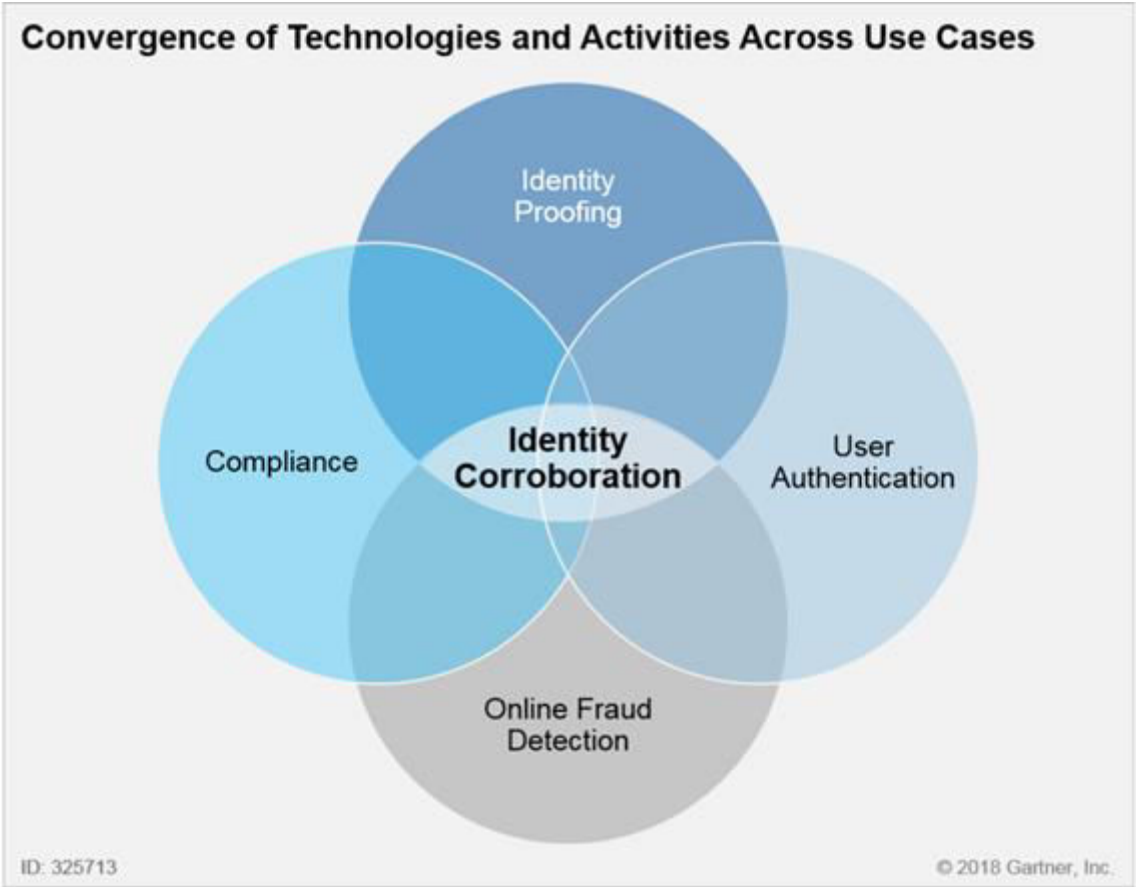
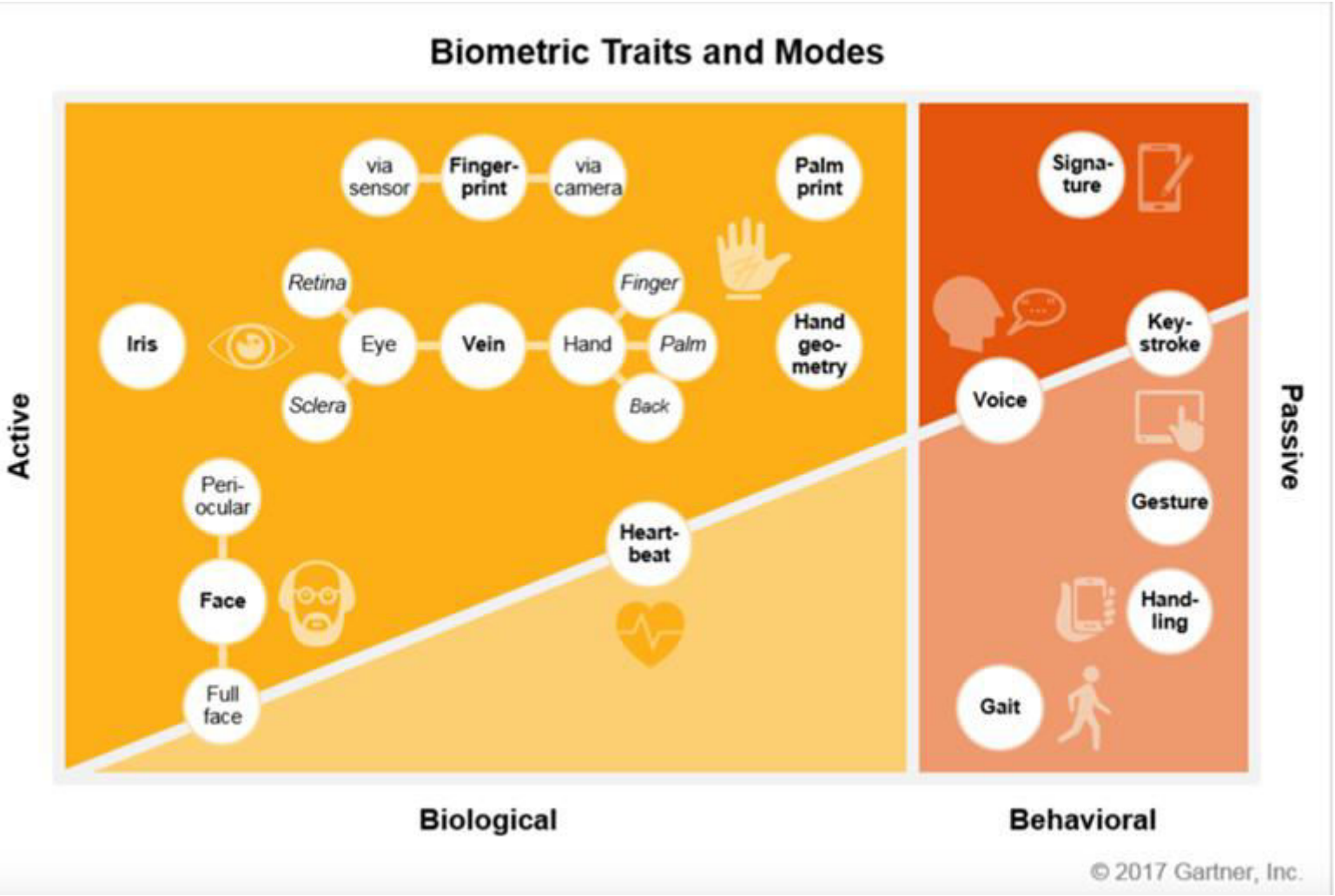

# Authenticators

# Convergence




Biometric Traits and Modes
Active
Passive
Biological
Behavioral
via sensor
Finger-print
via camera
Palm print
Retina
Finger
Iris
Eye
Vein
Hand
Palm
Hand geo-metry
Sclera
Back
Peri-ocular
Face
Full face
Heart-beat
Signa-ture
Key-stroke
Voice
Gesture
Hand-ling
Gait
© 2017 Gartner, Inc.

## Scenario 1

Legitimate employee attempts to log in to access corporate data from office in Southern California using work desktop at 9:00 a.m. PST

**Risk-based authentication analyzes:**

| User ID | Password | Device Fingerprint | Location | Geo-velocity | IP Address | Login History |
|---|---|---|---|---|---|---|
| **Traditional Pattern** | | | | | | |
| Valid | Valid | Corporate-issued computer, normally utilized by user | Location of company, from where user normally works | No distance traveled, accepted geo-velocity range | Valid | During normal working hours |

**PASS**

## Scenario 2

Legitimate employee attempts to log into corporate email in San Francisco on smartphone at 8:30 p.m. PST

**Risk-based authentication analyzes:**

| User ID | Password | Device Fingerprint | Location | Geo-velocity | IP Address | Login History |
|---|---|---|---|---|---|---|
| **Traditional Pattern** | | | | | | |
| Valid | Valid | Recognized device associated with user | Not normal location, but near enough geographically | Distance traveled appropriate for user's last login time | Valid | During abnormal working hours |

**PASS**

## Scenario 3

Attacker attempts to log in to access corporate data from the UK using a personal computer at 2:30 a.m. PST

**Risk-based authentication analyzes:**

| User ID | Password | Device Fingerprint | Location | Geo-velocity | IP Address | Login History |
|---|---|---|---|---|---|---|
| **Traditional Pattern** | | | | | | |
| Valid | Valid | Unknown device, no association to user | Abnormal Location and not near to standard location | Distance travel inappropriate for user's last login time | Valid | During very abnormal working hours |

**FAIL**

Source: StorageCraft

# IEEE 2410-2017 platform configuration options (ISO 24745)

| Storage | Matching | |
|---|---|---|
| | Mobile | Server |
| Mobile | ? (FIDO UAF, WebAuthN) | ? |
| Server | ? | ? |
| Shares (both mobile and server) | ? | ? |

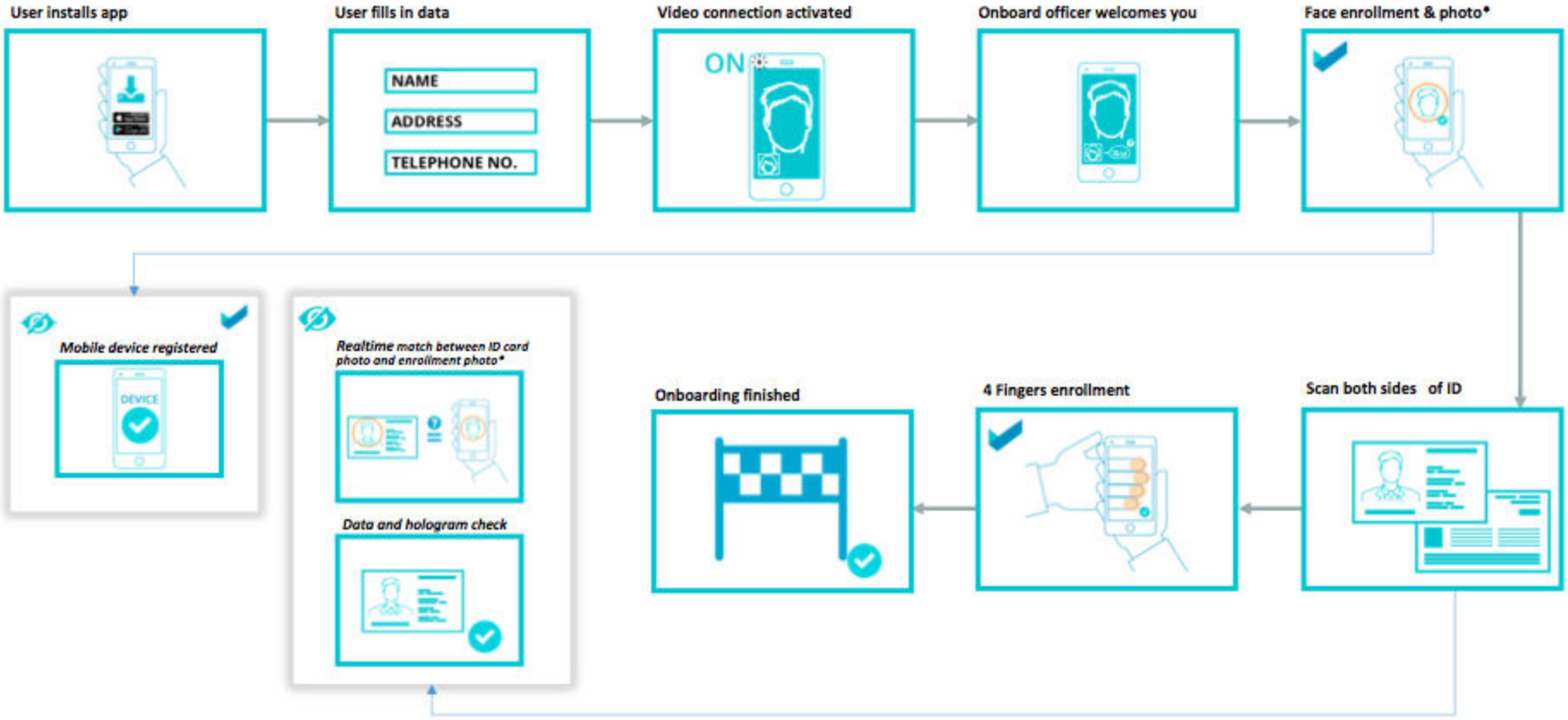
# IEEE 2410-2017 platform configuration options (ISO 24745)

| Storage | Matching | |
|---|---|---|
| | Mobile | Server |
| Mobile | ? (FIDO UAF, WebAuthN) | ? |
| Server | ? | ? |
| Shares (both mobile and server) | ? | ? |

# IEEE 2410-2017 platform configuration options (ISO 24745)

| Storage | Matching | |
|---|---|---|
| | Mobile | Server |
| Mobile | ? (FIDO UAF, WebAuthN) | ? |
| Server | ? | ? |
| Shares (both mobile and server) | ? | ? |

# INITIAL ONBOARDING & ENROLLMENT



# Six Principles for Self-Sovereign Biometrics

Contributors: John Callahan (JC), Heather Vescent (HV), Kaliya Young (KY), Darrell Duane (DD), Shannon Appelcline (SA), Asem Othman (AO), Adrian Gropper (AG)

Reviewers: Joe Andrieu, Manu Sporny, Kim Hamilton Duffy, Christopher Allen, Christian Lundkvist, Drummond Reed, Kyle Den Hartog, Markus Sabadello, Vishal Gupta

ABSTRACT

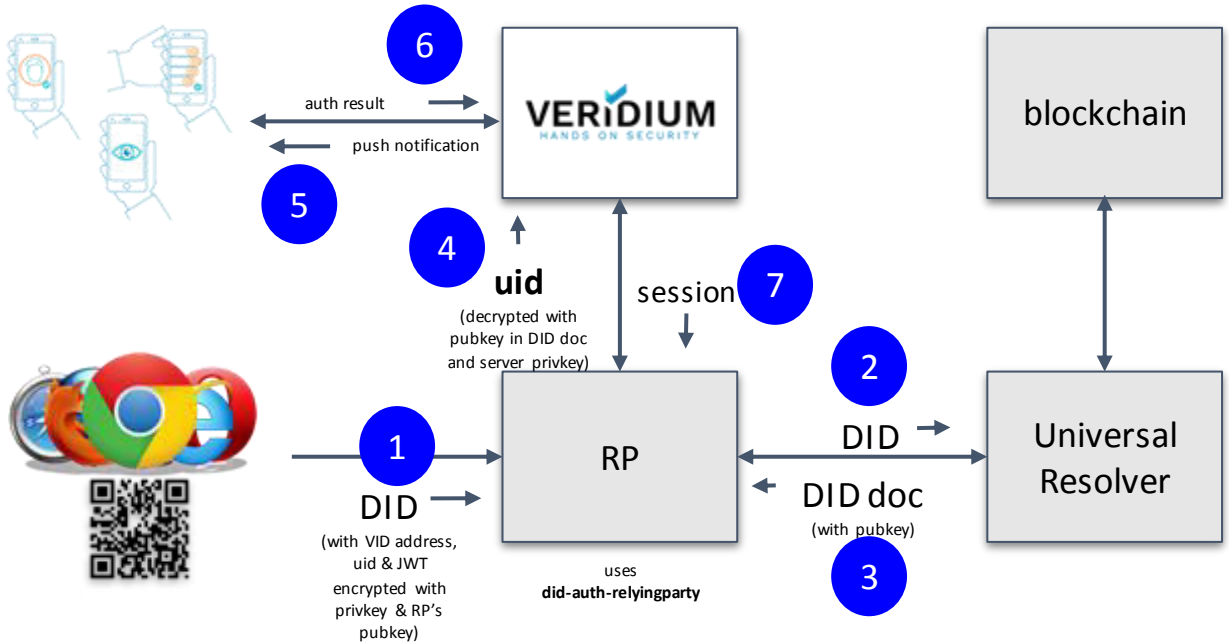
Biometrics are widely used for identity proofing, identity verification and authentication, but many implementations are vulnerable to breaches and exploitation. For example, centralized repo
biometric data, c
of privacy and c
blockchains that
This paper descr

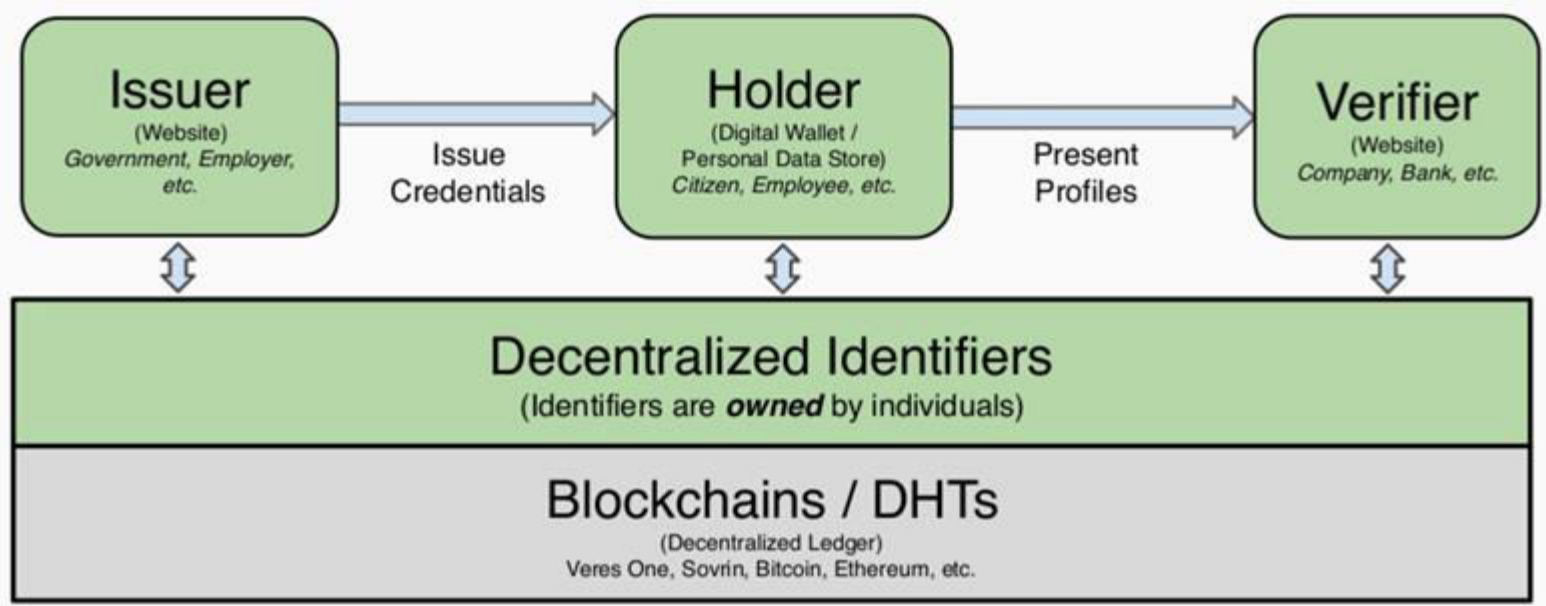
**Biometric DID Auth Flow A: mobile store and mobile match**

In this flow, the IBV is stored on the mobile device, typically with the assistance of a TPM, such as iOS Secure Enclave. This is a typical flow for hardware-specific biometrics, like TouchId and FaceID on iOS devices, where biometric data is never transmitted. This configuration is supported by IEEE 2410 and FIDO UAF. The mobile-mobile configuration corresponds to DID Architecture 1 and DID Architecture 2 ^19. In both architectures, the AuthN Materials (i.e., the private key) are protected by

1. **Biometrics Should Be Stored at the Edge**
2. **Biometrics Should Never Be Stored on a Blockchain**
3. **Biometrics Can Be Accessed *Via* a Blockchain**
4. **Biometrics Should Be Under A User's Control**
5. **Biometrics Traits Should Be Reliable**
6. **Biometrics Are Part of an Ecosystem**

# Biometric DID Authentication with IEEE 2410-2017






DIF W3C VERIDIUM HANDS ON SECURITY sovrin Homeland Security Science and Technology