Authenticators
Convergence of Technologies and Activities Across Use Cases

- Identity Proofing
- Compliance
- Online Fraud Detection
- User Authentication

Identity Corroboration
Scenario 1

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

Risk-based authentication analyzes:

Traditional Pattern

- User ID: Valid
- Password: Valid
- Device Fingerprint: Corporately issued computer, normally utilized by user
- Location: Location of company, from where user normally works
- Geo-velocity: No distance travelled, accepted geo-velocity range
- IP Address: Valid
- Login History: 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:

Traditional Pattern

- User ID: Valid
- Password: Valid
- Device Fingerprint: Recognized device associated with user
- Location: Not normal location, but near enough geographically
- Geo-velocity: Distance travelled inappropriate for user's last login time
- IP Address: Valid
- Login History: 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:

Traditional Pattern

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

FAIL
<table>
<thead>
<tr>
<th>Storage</th>
<th>Mobile</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mobile</strong></td>
<td>✓ (FIDO UAF, WebAuthN)</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Server</strong></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Shares (both mobile and server)</strong></td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
### IEEE 2410-2017 Platform Configuration Options (ISO 24745)

<table>
<thead>
<tr>
<th>Storage</th>
<th>Matching</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mobile</td>
</tr>
<tr>
<td>Mobile</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>(FIDO UAF, WebAuthN)</td>
</tr>
<tr>
<td>Server</td>
<td>✓</td>
</tr>
<tr>
<td>Shares (both mobile and server)</td>
<td>✓</td>
</tr>
</tbody>
</table>
### 2410-2017 platform configuration options (ISO 24745)

<table>
<thead>
<tr>
<th>Storage</th>
<th></th>
<th>Matching</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mobile</td>
<td>Server</td>
</tr>
<tr>
<td><strong>Mobile</strong></td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>(FIDO UAF, WebAuthN)</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Server</strong></td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Shares (both mobile and server)</strong></td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
Six Principles for Self-Sovereign Biometrics

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

1. DID (with VID address, uid & JWT encrypted with privkey & RP's pubkey)
2. DID
3. DID doc (with pubkey)
4. uid (decrypted with pubkey in DID doc and server privkey)
5. push notification
6. auth result
7. session

RP

DID

blockchain

Universal Resolver

© 2018 Veridium IP Ltd. All Rights Reserved.
Decentralized Identifiers
(Identifiers are owned by individuals)

Blockchains / DHTs
(Decentralized Ledger)
Veres One, Sovrin, Bitcoin, Ethereum, etc.