Biometric Service Provider (BSP)

John “Jack” Callahan
Veridium
Knowledge  
Possession  
Biometric
Figure 4-1 (annotated) The Identity Proofing User Journey [source: NIST 800-63-3A]
Biometric ≠ Password

• Typically combined with liveness
  • “IAL3: Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained CSP representative”

• aka Presentation Attack Detection (PAD)

• NIST 800-63-3B Section 5.2.3
  • “Testing of presentation attack resistance SHALL be in accordance with Clause 12 of ISO/IEC 30107-3. The PAD decision MAY be made either locally on the claimant’s device or by a central verifier.”
  • “PAD is being considered as a mandatory requirement in future editions of this guideline”

• PAD can be performed remotely
  • IAL2 introduces the need for either remote or physically-present identity proofing. [NIST 800-63-3A Section 2.2]
Biometric Verifiable Credentials

Issuer

Holder

Verifier

Blockchain provenance & integrity information

Blockchain provenance & integrity verification
A Range of Biometric Use Cases

- Device unlocking
- Authentication
- Identification
- Identity Proofing
- Identity Verification
- Deduplication (on enrollment)
- Fraud prevention (on enrollment)
Initial & Candidate Biometric Vectors

Registration

IBV

Match?

CBV

Presentation
Some Simple Best Practices

• Protect biometric data ...
  • at collection (sensor safeguards)
  • at rest (special hardware, TPM/TEE, database encryption)
  • in transit (encrypted communications)
  • during match (volatile memory protections)

• Never log biometric data!

• Candidate Biometric Vector is ephemeral
Using Biometrics to Fight Credential Fraud
Daniel Hardman, Lovesh Harchandani, Asem Othman, Ph.D., John Callahan, Ph.D.

Abstract
Verifiable credentials are an exciting innovation in decentralized and self-sovereign identity. However, the ease of copying digital files and sharing cryptographic keys makes an old problem from physical credential space more pressing: How do we prevent a credential from being used by someone other than its legitimate holder? Biometrics provide an answer—but they also introduce some complexity and some trust and privacy concerns that need careful treatment. In this paper, we explore three patterns of biometric use with verifiable credentials, identify appropriate use cases for each, and recommend best practices that make the patterns trustworthy, robust, and interoperable.
<table>
<thead>
<tr>
<th>Where is IBV persisted?</th>
<th>Mobile</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:1 Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Unlocking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pocket Pattern</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:N Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deduplication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:1 Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity Verification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:N Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity Proofing</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Identity Proofing

- Know Your Customer (KYC)
- Anti-Money Laundering (AML)
- Required by most countries for banking
Biometric Verifiable Credentials

Issuer

Holder

Verifier

BOPS, ABIS, MOSIP Aadhaar
Biometric Verifiable Credentials

Issuer

BOPS, ABIS, MOSIP Aadhaar

Holder

Biometric Verifiable Credentials

Verifier

BOPS, ABIS, MOSIP Aadhaar
Biometric Verifiable Credentials

Issuer

Holder

Verifier

BOPS, ABIS, MOSIP Aadhaar
Biometric Verifiable Credentials

Issuer

Holder

Verifier

BOPS, ABIS, MOSIP, Aadhaar

BOPS, ABIS, MOSIP, Aadhaar
Biometric Service Provider (BSP)

- A protocol?
- Should define biometric verifiable credential schema(s)
  - Biometric modality agnostic
  - Accommodate Biometric shards
  - Integrate with Ursa crypto
  - Integrate with service endpoint model
- Allows Issuers, Verifiers, and Holder wallets & agents to invoke services like:
  - Registration
  - Matching
  - Deduplication
  - Verification
- Provides new services
  - Fuzzy matching
  - Shard management (for DKMS)
  - Holder-specific biometric matching “machine” (using ZK-STARKs)
- Compatible with trust relationships
  - Supports DID connections/Trust relationships (Holder ↔ BSP ↔ Verifier)
Biometric Verifiable Credentials

Issuer

Holder

Verifier

BOPS, ABIS, MOSIP, Aadhaar

BOPS, ABIS, MOSIP, Aadhaar

Biometric Verifiable Credentials

Agent/self-hosted?
Issuer
Verifier
Holder

Interpol, FBI, UK Border

Issuer-generated, Holder-specific ZK-STARK

BSP
Next Steps

• Feedback
• Draft RFC aligned with
  • Distributed Key Management RFC
  • Credential Fraud RFC (Threat model, Patterns & Anti-Patterns)
• BSP threat model?
• Prototype implementation(s)
• Relation to
  • IEEE 2410 (BOPS)
  • FIDO and new FIDO IDV