Why do we need workload authentication levels?

• All workloads authenticate...
  • ..., but not all authentication is created equal

• There are frameworks for user authentication levels
  • Something you have, something you are, something you know
  • NIST Authentication Assurance Levels

• How they help
  • Establish a benchmarks and classification systems
  • Guide “expertise elsewhere” decision makers
  • Surfaces risk and allow for systemic and industry level mitigation
Authenticator Assurance Level

**AAL1:** AAL1 provides some assurance that the claimant controls an authenticator registered to the subscriber. AAL1 requires single-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator(s) through a secure authentication protocol.

**AAL2:** AAL2 provides high confidence that the claimant controls authenticator(s) registered to the subscriber. Proof of possession and control of two different authentication factors is required through a secure authentication protocol. Approved cryptographic techniques are required at AAL2 and above.

**AAL3:** AAL3 provides very high confidence that the claimant controls authenticator(s) registered to the subscriber. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 is like AAL2 but also requires a “hard” cryptographic authenticator that provides verifier impersonation resistance.
## What might that look like for Workloads

<table>
<thead>
<tr>
<th>Level 0: No Authentication</th>
<th>Level 1: Deploy Time Shared-Secret Based Authentication</th>
<th>Level 2: Deploy-Time Credential Based Authentication</th>
<th>Level 3: Automated Authentication with Static Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong>: No authentication mechanisms are in place.</td>
<td><strong>Description</strong>: Manual deploy time of simple passwords, shared secrets and API keys without lifecycle management</td>
<td><strong>Description</strong>: Static asymmetric key-based authentication and symmetric credential management systems that are deployed during setup.</td>
<td><strong>Description</strong>: Automated authentication using static credentials and improved logging.</td>
</tr>
</tbody>
</table>
What Next?

• Is this needed?
• Is this something for the IETF or WIMSE?
• What criteria to consider?
  • Granularity – how many levels?
  • Additional Metadata – Runtime information for threat detection
  • Time Variance – How to allow for evolution over time
  • Adoption – Making it easy for “expertise elsewhere”