Identity Authentication
using the
PIV Token

Sarbari Gupta
sarbari@electrosoft-inc.com
October 6, 2004
Identity Authentication

• **Definition**
  - The process of establishing confidence in the identity of a User presenting a PIV Token

• **Purpose**
  - Allow an Agency to make access decision (to controlled Federal Resources) based on authenticated identity of the User and the Agency's own access control policy
Authentication Assurance Levels

- Resource Owner determines level of assurance required for authentication
- PIV Token Authentication Assurance Levels

<table>
<thead>
<tr>
<th>Authentication Assurance Level</th>
<th>Resistance to Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOW</td>
<td>Forgery (limited), Illegitimate Use (limited)</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>Forgery, Illegitimate Use (limited)</td>
</tr>
<tr>
<td>HIGH</td>
<td>Forgery, Illegitimate Use, Interposition</td>
</tr>
</tbody>
</table>

NOTE: Residual Access threat can be countered through use of backend systems and processes at any of the above levels

- PIV Token Use Threats
  - Forgery: Token cloning, tampering, bogus Token
  - Illegitimate Use: Use of valid Token by non-Owner
  - Interposition: Man-in-the-Middle Attacks on Protocol
  - Residual Access: Use of token beyond period of validity
Token Verification Infrastructure

- Token Status Service
  - LDAP Service
  - Provides status of PIV Token

- PKI Repository
  - LDAP Repository
  - Provides public key certificates and Certificate Revocation Lists (CRLs)

- OCSP Responder
  - OCSP Protocol
  - Provides Status of Certificate
PIV Token Authentication Environments

- **Visual Authentication**
  - No token reader
  - Human Intervention

- **Contactless Authentication**
  - Contactless Token Reader
  - No PIN Pad or Biometric Reader

- **Contact-based Authentication**
  - Contact Token Reader
  - PIN Pad
  - Biometric Reader

<table>
<thead>
<tr>
<th>Authentication Environment</th>
<th>Suitable for Access Control to …</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visual</td>
<td>Physical Resources</td>
</tr>
<tr>
<td>Contactless</td>
<td>Physical Resources</td>
</tr>
<tr>
<td>Contact</td>
<td>Logical Resources, Physical Resources</td>
</tr>
</tbody>
</table>
Visual Authentication

Physical Facility Entry Point

Access Authorized

Token Status Service

Visual comparison of Token holder and picture on Token followed by online status check of Token ID
Visual Authentication Assurance Levels

- **Low**
  - Guard inspects PIV Token for
    - Physical Integrity
    - Match of picture to Token Holder

- **Medium**
  - Guard inspects PIV Token for
    - Physical Integrity
    - Match of picture to Token Holder
  - Guard inspects Second Picture ID
    - Match name and picture on both PIV Token and Second ID
Contactless Authentication

Access Authorized

Contactless Token Reader
Control Panel

Token Status Service

Physical Facility Entry Point
Contactless Authentication

Assurance Levels

- **Low**
  - PACS LOW Scheme
    - Open read of FASC-N (Electronic Token Holder ID)
    - Match of FASC-N to “Authorized FASC-N List”

- **Medium**
  - PACS Medium Scheme
    - Open read of FASC-N and Token Unique ID
    - Computation of Unique Authorization String
    - Compare to list of “Authorized Strings”
Contact Reader Authentication

- Contact Token Reader
- PIN Pad
- Biometric Reader

Token Status Service
PKI Repository
OCSP Responder

Access Authorized
Contact Token Authentication

Assurance Levels

• Low (1)
  - PACS LOW Scheme
    • Open read of FASC-N
    • Match of Token ID to “Authorized List”

• Low (2)
  - Biometric Match-off-Card
    • Open read of Biometric Template from Token
    • No signature check on biometric template
    • Compare Token Holder’s biometric to template from Token
Contact Token Authentication

Assurance Levels (contd.)

• Medium
  • PACS Medium Scheme
    • Open read of FASC-N and Token Unique ID
    • Compute Unique Authorization String
    • Compare to list of “Authorized Strings”
Contact Token Authentication

Assurance Levels (contd.)

• High (1)
  o PACS High Scheme with PIN
    • Open read of FASC-N and Token Unique ID
    • Collect Token Holder PIN
    • Conduct Challenge-Response between Token Reader and Token
    • Compare Token Response to expected value (computed with collected and local info)

• High (2)
  o Biometric Match-off-Card with Signature Check
    • Open read of Signed Biometric Template from Token
    • Signature check on biometric template
    • Compare Token Holder’s biometric to template from Token
Contact Token Authentication

Assurance Levels (contd.)

• High (3)
  o Invoke Challenge-Response using Token Private Key
    • Issue Asymmetric Key Challenge to Token
    • Collect Token Holder PIN/Biometric and pass to Token
    • Receive Response to Challenge from Token
    • Verify digital signature on Response
    • Verify Token Holder’s Certificate chain
## PIV Token Authentication Summary

<table>
<thead>
<tr>
<th>Authentication Mechanism</th>
<th>Assurance Level</th>
<th>Resource Suitability</th>
<th>Shorthand</th>
<th>Network Connectivity</th>
<th>User Processing Volume</th>
<th>No Card Reader</th>
<th>Contactless Environment</th>
<th>Contact-Based Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visual</td>
<td>Low</td>
<td>Physical</td>
<td>VIS</td>
<td>No Connectivity</td>
<td>High User Volume</td>
<td>VIS</td>
<td>PACS-L</td>
<td>PACS-H</td>
</tr>
<tr>
<td>Visual+2nd Picture ID</td>
<td>Medium</td>
<td>Physical</td>
<td>VIS-ID</td>
<td>No Connectivity</td>
<td>Low User Volume</td>
<td>VIS-ID</td>
<td>PACS-L</td>
<td>PACS-M</td>
</tr>
<tr>
<td>Biometric Match</td>
<td>Low</td>
<td>Physical</td>
<td>BIO</td>
<td>Network Connectivity</td>
<td>High User Volume</td>
<td>VIS/SC</td>
<td>PACS-L/SC</td>
<td>PACS-H/SC</td>
</tr>
<tr>
<td>Biometric Match+Dig Sig Verification</td>
<td>High</td>
<td>Physical, Logical</td>
<td>BIO-S</td>
<td>Network Connectivity</td>
<td>Low User Volume</td>
<td>VIS-ID/SC</td>
<td>PACS-L/SC</td>
<td>PKI/SC</td>
</tr>
<tr>
<td>PACS Low</td>
<td>Low</td>
<td>Physical</td>
<td>PACS-L</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PACS Medium</td>
<td>Medium</td>
<td>Physical</td>
<td>PACS-M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PACS High</td>
<td>High</td>
<td>Physical, Logical</td>
<td>PACS-H</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PKI Challenge Response</td>
<td>High</td>
<td>Physical, Logical</td>
<td>PKI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NOTE: SC implies the use of online status check for PIV token or its resident credentials
Questions??