E-Authentication Guidance

NIST KBA Symposium
February 9, 2004
Jeanette Thornton
E-Authentication Goals

– Build and enable mutual trust needed to support wide spread use of electronic interactions between the public and Government, and across Governments

– Minimize the burden on public when obtaining trusted electronic services from the Government, and across the governments

– Deliver common interoperable authentication solutions, appropriately matching the levels of risk and business needs
Areas of Focus

- Policy
- Technology: Architecture/Requirements
- Applications (bringing Applications on to a shared service): Conducting a pilot
- Credential Providers (accrediting electronic credential providers to they could be used across govt.)
- FICC: Smart Cards/IDs for Federal Employees
The President’s E-Government Initiatives

Part of a Larger Policy Framework

- Community Specific Policies
- Federal Identity Credentialing Component
- Credential Assessment Framework
- Federal PKI Bridge Certificate Policy
- NIST Authentication Technical Guidance
- E-Authentication Guidance for Federal Agencies

- FINAL: OMB M-04-04, December 16, 2003
- SP-800-63, Out for Comment Jan 29, 2004
- Expected final March 04
- Policies Ongoing
- Interim version now final
- FINAL: OMB M-04-04, December 16, 2003
Approaching Authentication…

- Surfing the Internet: Low
- Access to Protected Website: Standard
- Applying for a Loan Online: Medium
- Obtaining Govt. Benefits: High
- Employee Screening for a High Risk Job: Very High

Increased $ Cost

Increased Need for Identity Assurance

PKI/ Digital Signature
Knowledge-Based
Pin/Password
Click-wrap

Multi-Factor Token
OMB Authentication Guidance

- M-04-04 Signed by OMB Director on 12/16/2003
- Supplements OMB Guidance on implementation of GPEA
- Establishes 4 identity authentication assurance levels
- Requires agencies to conduct “e-authentication risk assessments”
- Planned result is a more consistent application of electronic authentication across the Federal Government
Applyes To:
- Remote authentication of human users of Federal agency IT systems for e-government.
- Identification and analysis of the risks associated with each step of the authentication process

Does Not Apply To:
- Authentication of servers, or other machines and network components.
- Authorization -- the actions permitted of an identity after authentication has taken place.
- Issues associated with “intent to sign,” or agency use of authentication credentials as electronic signatures.
- Identifying which technologies should be implemented.
Definitions

- **Authentication**—process of establishing confidence in user identities electronically presented to an information system.

- **Identity authentication**—confirming a person’s unique identity.

- **Authorization**—identifying the person’s user permissions.

- **Attribute authentication**—confirming that the person belongs to a particular group (such as military veterans or U.S. citizens).
1. Conduct a risk assessment of the e-government system.

2. Map identified risks to the applicable assurance level.


4. Validate that the implemented system has achieved the required assurance level.

5. Periodically reassess the system to determine technology refresh requirements.
### M-04-04: E-Authentication Guidance for Federal Agencies

OMB Guidance establishes 4 authentication assurance levels:

<table>
<thead>
<tr>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Little or no confidence in asserted identity (e.g. self identified user/password)</td>
<td>Some confidence in asserted identity (e.g. PIN/Password)</td>
<td>High confidence in asserted identity (e.g. digital cert)</td>
<td>Very high confidence in the asserted identity (e.g. Smart Card)</td>
</tr>
</tbody>
</table>

### NIST SP800-63 Electronic Authentication

NIST technical guidance to match technology implementation to a level.
Categories of Harm and Impact

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or agency liability
- Harm to agency programs or public interests
- Unauthorized release of sensitive information
- Personal safety
- Civil or criminal violations.
## Maximum Potential Impacts

<table>
<thead>
<tr>
<th>Potential Impact Categories for Authentication Errors</th>
<th>Assurance Level Impact Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Inconvenience, distress or damage to standing or reputation</td>
<td>Low</td>
</tr>
<tr>
<td>Financial loss or agency liability</td>
<td>Low</td>
</tr>
<tr>
<td>Harm to agency programs or public interests</td>
<td>N/A</td>
</tr>
<tr>
<td>Unauthorized release of sensitive information</td>
<td>N/A</td>
</tr>
<tr>
<td>Personal Safety</td>
<td>N/A</td>
</tr>
<tr>
<td>Civil or criminal violations</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Other items covered

- Examples for each level
- Use of anonymous credentials
- Impact of the authentication process
- Considering costs and benefits
Effective Dates

– 90 days from completion of the final NIST E-Authentication Technical Guidance—New authentication systems should begin to be categorized, as part of the system design.

– **December 15, 2004**—Systems classified as “major” should be categorized.

– **September 15, 2005**—All other existing systems requiring user authentication should be categorized.
What’s missing?

– Attribute authentication
– Knowledge based authentication