



E-Authentication Guidance

*Jeanette Thornton,
Office of Management and Budget*



“Getting to Green with E-Authentication”

February 3, 2004

Executive Session

E-Authentication: What's IN, What's OUT

- ◆ The Federal Government going it alone: an authentication system and operating rules that are “agency-specific,” “State-unique,” etc.

OUT!

E-Authentication Bugle: What's IN, What's OUT

- ◆ Developing a partnership between Government, relying parties, IT vendors and advocacy groups –
collaboration!

IN!

E-Authentication Bugle: What's IN, What's OUT

- ◆ Developing Government-only, proprietary solutions, e.g. Gateways

OUT!

E-Authentication Bugle: What's IN, What's OUT

- ◆ Enabling interoperability between disparate systems.

IN!

E-Authentication Bugle: What's IN, What's OUT

- ◆ Being beholden to one particular approach.

OUT!

E-Authentication Bugle: What's IN, What's OUT

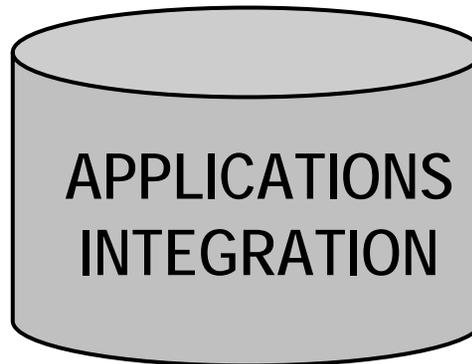
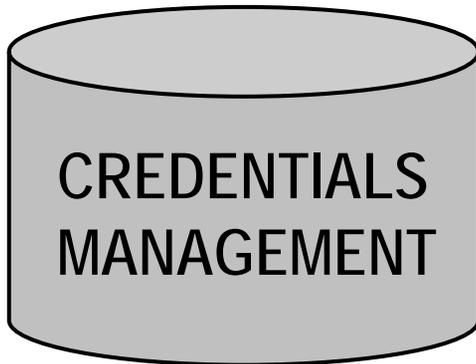
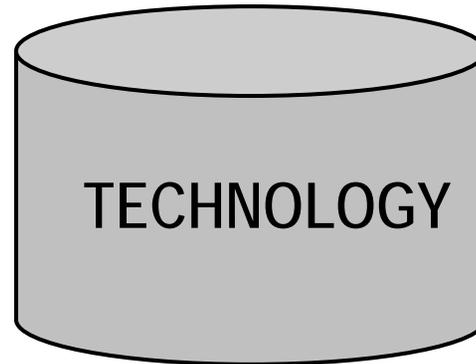
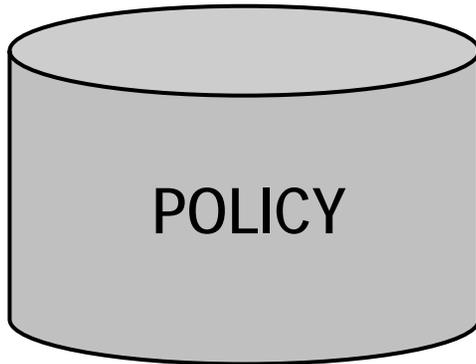
- ◆ Movement towards common standards that all interested parties can adopt.

IN!

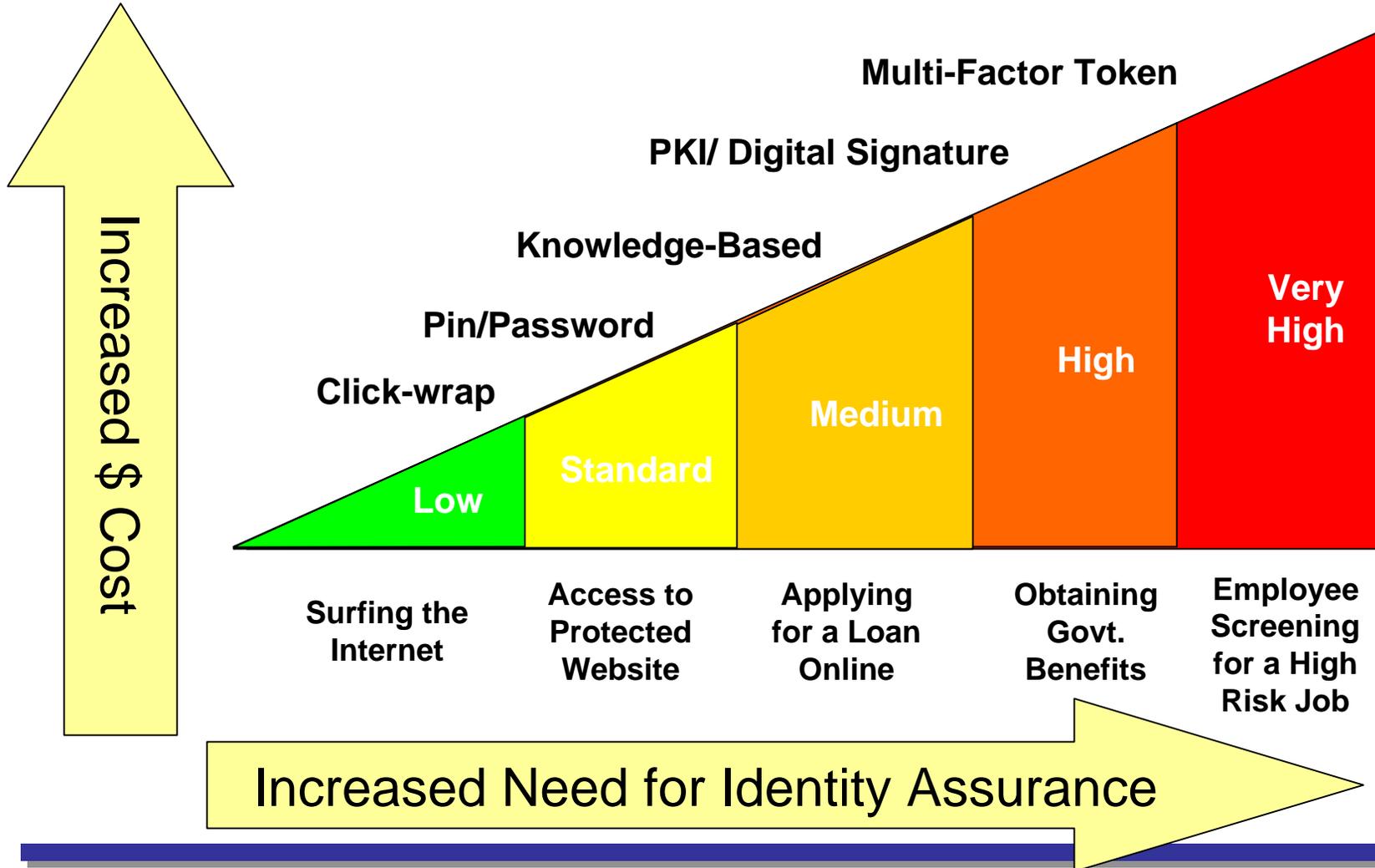
Policy + Technology + Credentials +
Agency Applications + Management &
Administration =

E-Authentication

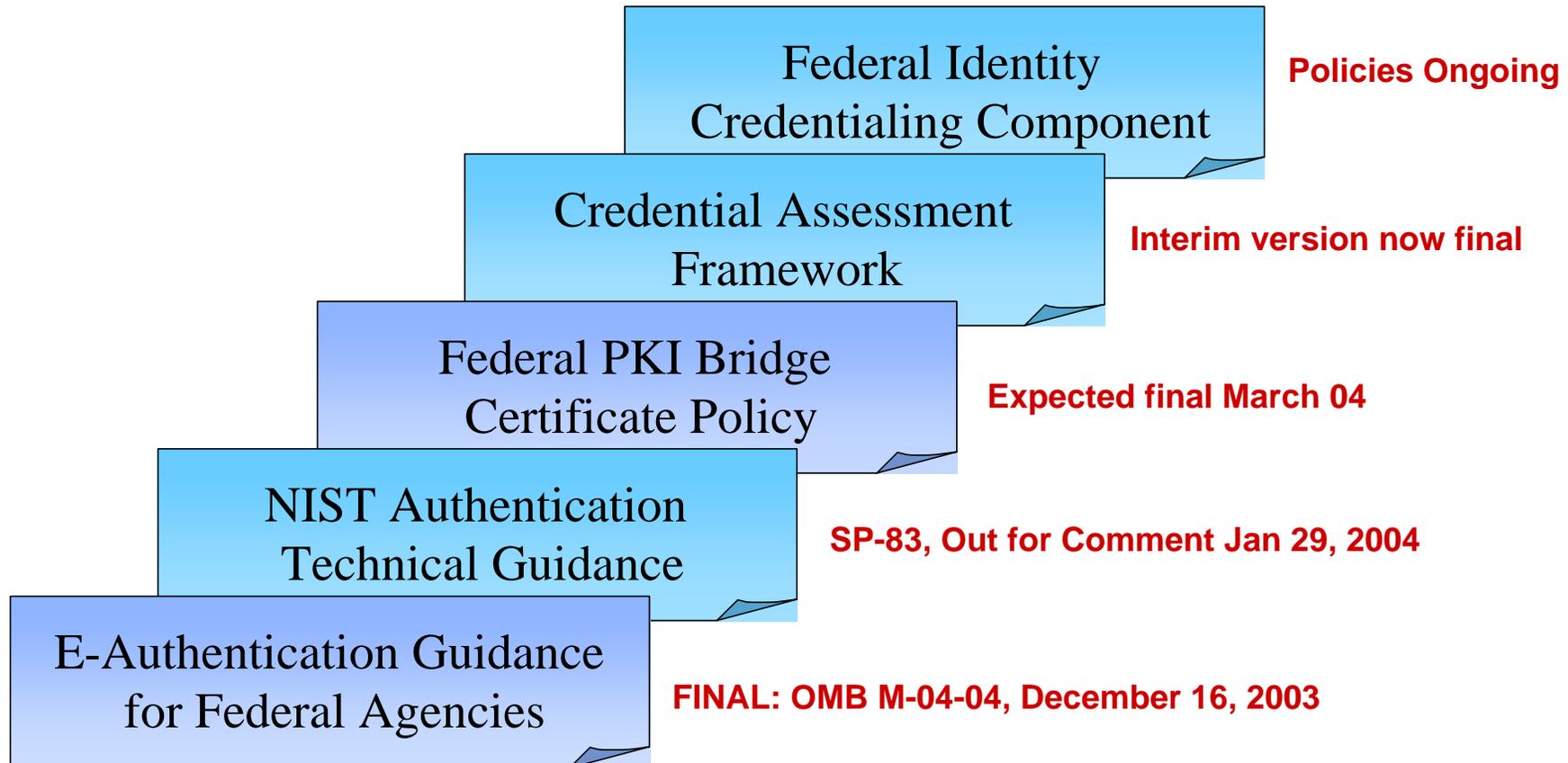
E-Authentication 5 Work Packages



Approaching Authentication...



Part of a Larger Policy Framework



Role of OMB

- ◆ Mandate implementation
 - FEA
 - Budget Authority
 - Policy Authority
- ◆ Issue Govt wide information policy
- ◆ Oversee and ensure success of Presidential E-Government Initiative.

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”

Result: A more consistent application of electronic authentication across the Federal Government

Assurance Levels

M-04-04:E-Authentication Guidance for Federal Agencies
 OMB Guidance establishes 4 authentication assurance levels

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

NIST SP-83 Electronic Authentication
 NIST technical guidance to match technology implementation to a level

Scope

Applies 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.

Risk Assessment Steps

1. Conduct a risk assessment of the e-government system.
2. Map identified risks to the applicable assurance level.
3. Select technology based on e-authentication technical guidance.
4. Validate that the implemented system has achieved the required assurance level.
5. Periodically reassess the system to determine technology refresh requirements.

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

Potential Impact Categories for Authentication Errors	Assurance Level Impact Profiles			
	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

NIST SP 83: Recommendation for Electronic Authentication

- ◆ Maps to OMB E-Authentication guidance
- ◆ Covers conventional token based remote authentication
 - May be additional guidance on “knowledge based authentication”
- ◆ Draft for comment at: <http://csrc.nist.gov/eauth>
- ◆ Comment period ends: March 15

NIST SP 83: Recommendation for Electronic Authentication

- ◆ What type of token should be used for each level?
 - Password?
 - PKI?
- ◆ What Protections required for each level?
- ◆ What type of ID proofing is required?
- ◆ How does it map to the Federal Bridge?

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.

Wrapping Up

- ◆ Questions?

Jeanette Thornton

202.395.3562