GSA

U.S. General Services Administration

Office of Governmentwide Policy

Identity Management Services Industry Day

Topic: E-Authentication: Where do we go from here?

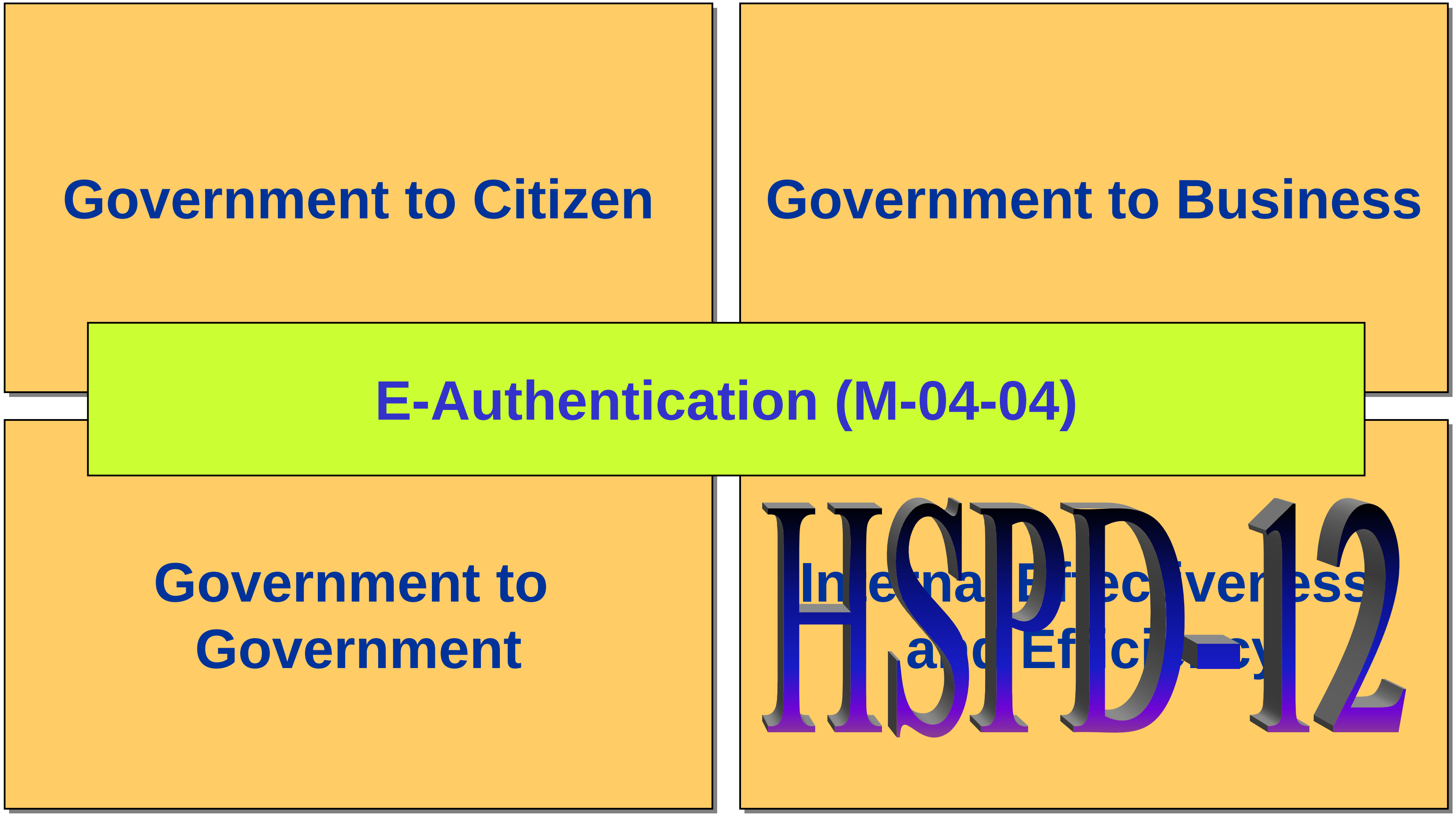
November 5, 2008

Judy Spencer
Chair, Federal Identity
Credentialing Committee
judith.spencer@gsa.gov

Point One: E-Authentication Is NOT Going Away

- *E-Authentication Guidance for Federal Agencies*, issued by the Office of Management & Budget, Dec. 16, 2003
  - http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
  - About identity authentication, not authorization or access control
  - Incorporates Standards for Security Categorization of Federal Information and Information Systems (FIPS-199)
- NIST SP800-63: *Recommendation for Electronic Authentication*
  - Companion to OMB e-Authentication guidance
  - http://csrc.nist.gov/eauth
  - Covers conventional token based remote authentication

4 Sectors for Government Interaction



Government to Citizen

Government to Business

E-Authentication (M-04-04)

Government to Government

Internal Effectiveness and Efficiency

HSPD-12

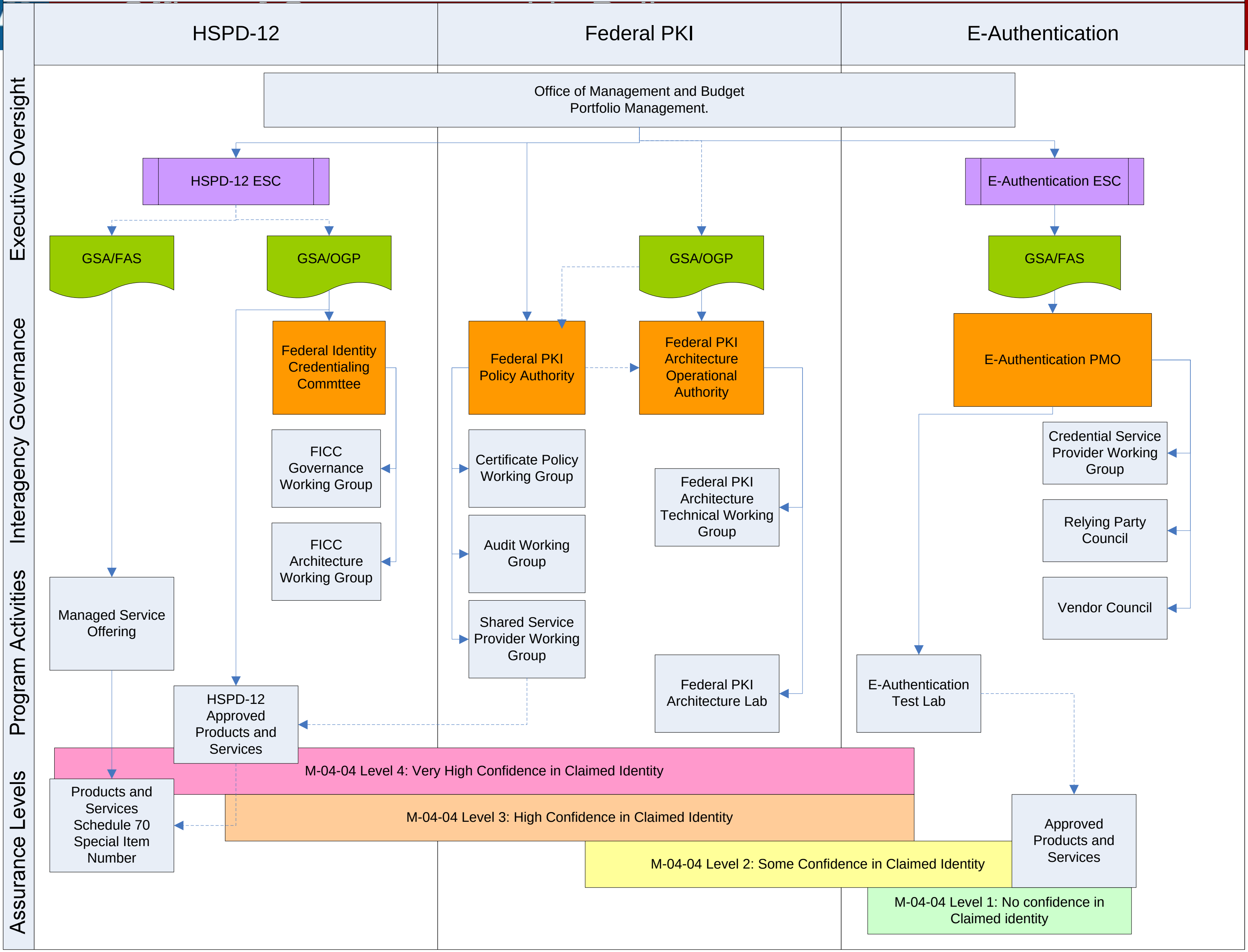
GSA OGP Responsibilities

- Governance – M-04-04 take-up
  - Credential Assessment Framework
  - Approved Products List
  - Guidance/Best Practices to Agencies
- Architecture
  - On-going management
  - Industry alignment
- Lab Activities
  - Test Environment
  - CSP Applicant Testing
  - Next Generation Testing
- Interagency Collaboration
  - Federal Identity Credentialing Committee
- Industry Collaboration
  - Liberty Alliance
  - Finding Natural Affinities (InCommon)

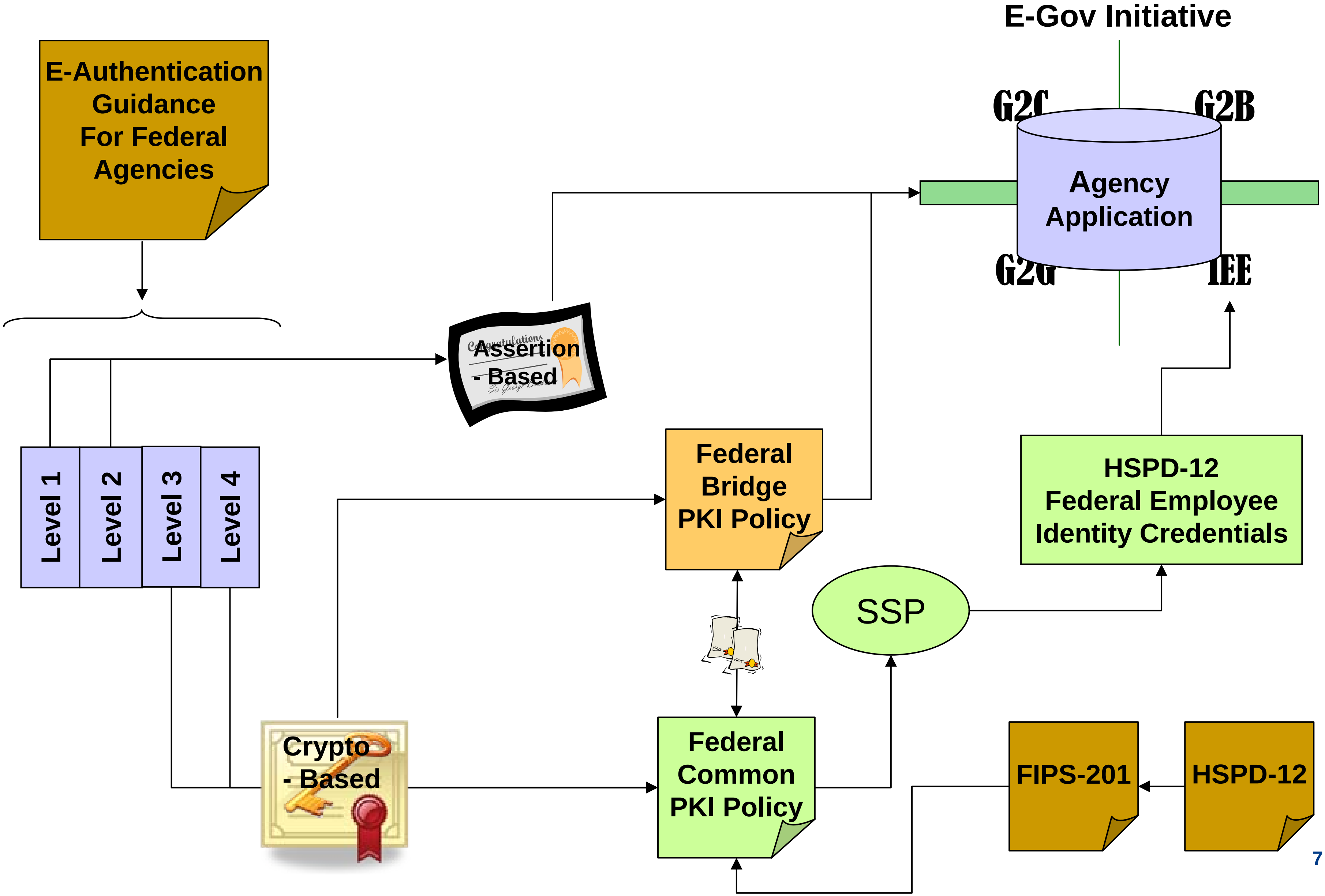
Increasing the Trusted Credential Community

- Federal Bridge will continue to play a role at Levels 3 & 4
  - External Shared Service Providers
  - Bridge relationships (Certipath & SAFE-BioPharma)
- Expanding our use of Assertion-based solutions (Levels 1 & 2)
  - Partnering with Liberty Alliance
  - Stronger industry alignment for trust and technology standards
  - Architecture Refresh (SAML 2.0/WS*)
- Outreach to communities of interest
  - InCommon – Post-secondary education community
  - Explore natural affinities

Current State



HSPD-12
Federal PKI
E-Authentication
Executive Oversight
Interagency Governance
Program Activities
Assurance Levels
Office of Management and Budget
Portfolio Management.
HSPD-12 ESC
E-Authentication ESC
GSA/FAS
GSA/OGP
GSA/OGP
GSA/FAS
Federal Identity Credentialing Commttee
Federal PKI Policy Authority
Federal PKI Architecture Operational Authority
E-Authentication PMO
FICC Governance Working Group
FICC Architecture Working Group
Certificate Policy Working Group
Audit Working Group
Shared Service Provider Working Group
Federal PKI Architecture Technical Working Group
Credential Service Provider Working Group
Relying Party Council
Vendor Council
Managed Service Offering
HSPD-12 Approved Products and Services
Federal PKI Architecture Lab
E-Authentication Test Lab
M-04-04 Level 4: Very High Confidence in Claimed Identity
M-04-04 Level 3: High Confidence in Claimed Identity
M-04-04 Level 2: Some Confidence in Claimed Identity
M-04-04 Level 1: No confidence in Claimed identity
Products and Services Schedule 70 Special Item Number
Approved Products and Services



E-Gov Initiative

G2C

G2B

G2G

IEE

Agency Application

E-Authentication Guidance For Federal Agencies

Level 1

Level 2

Level 3

Level 4

Assertion - Based

Crypto - Based

Federal Bridge PKI Policy

Federal Common PKI Policy

SSP

HSPD-12 Federal Employee Identity Credentials

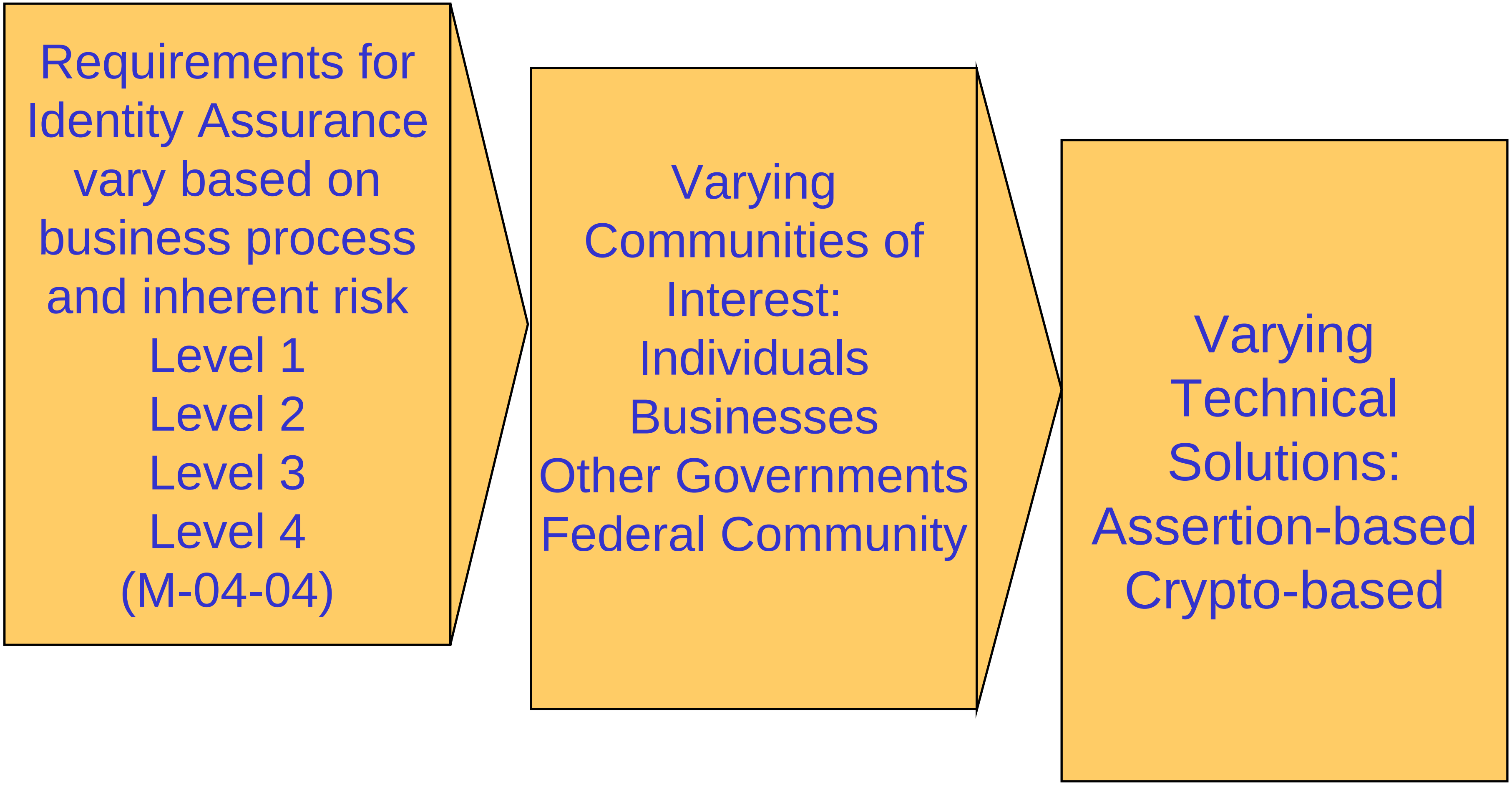
FIPS-201

HSPD-12

Consolidation of Identity Management

- National Science and Technology Council (NSTC) Identity Management Task Force Report
- CIO Council – Security and Identity Management Committee
- New Emphasis on Federal Identity, Credential, and Access Management
- Encompass E-Authentication, Federal PKI, and HSPD-12

3 Primary Considerations



Requirements for Identity Assurance vary based on business process and inherent risk
Level 1
Level 2
Level 3
Level 4
(M-04-04)

Varying Communities of Interest:
Individuals
Businesses
Other Governments
Federal Community

Varying Technical Solutions:
Assertion-based
Crypto-based

Looking Forward

OGP will spearhead the integration of the three current IDM activities:

- Better alignment with industry partners
- Focus on communities of interest
- Streamlined processes
- Open up the architecture
- Capitalize on existing investments
  - 80+ applications in E-Authentication
  - 23 departments and agencies
  - 1M transactions a year
- Review/revise existing documentation

For More Information:

www.idmanagement.gov