

Charter for the Federal Identity Credentialing Committee

Purpose

The FICC provides a focal point for implementation of a Government-wide identity credentialing capability as required by Homeland Security Presidential Directive (HSPD) 12: *Policy for a Common Identification Standard for Federal Employees and Contractors*, and defined in Federal Information Processing Standard (FIPS) 201: *Personal Identity Verification of Federal Employees and Contractors*. Members of the FICC are expected to both participate in the implementation of FIPS 201 and champion these activities at the agencies they represent.

Background

In order for the Federal government fully to realize the benefits of electronic government, it must have a ubiquitous and consistent method of providing identity credentials, for both logical and physical access, within the Federal sector. As the Federal government modernizes internal processes to reduce costs for agency administration and moves to cross agency applications that are available to all Federal employees, a common, trusted basis for authentication is needed. In recognition of this need, the President signed HSPD 12, which provides the requirements and expectations for these credentials. With the issuance of FIPS 201 and its related Special Publications, the National Institute of Standards and Technology set in motion the timeline for implementation of HSPD 12. According to this Directive, the Executive Departments and Agencies must begin implementing standard compliant identity credentialing by October 2005 and issuing personal identity verification credential in October of 2006.

Scope

The Federal Identity Credentialing Committee provides recommendations for the development of an interoperable identity management infrastructure for Federal organizations in accordance with HSPD 12 that utilizes commercial-off-the-shelf, standards-based products and services. The FICC will provide recommendations to identify and resolve Federal Identity Credentialing technical and business issues and, when necessary, provide a coordination point for resolving policy issues.

The Federal Identity Credentialing Committee provides a focal point for the Agencies to share design and development plans, lessons learned, and develop solutions to common problems as they are identified during the implementation of HSPD 12.

The Committee:

- Recommends procedures and strategies to support implementation of HSPD 12;
- Provides a forum for attaining technical assistance for Federal organizations engaged in implementing HSPD 12;
- Provides assistance to Federal organizations on the requirements for identity assurance;
- Establishes work groups for tackling the issues surrounding the interoperability and security requirements for interagency exchange of Federal Identity credentials.
- Assists GSA in ensuring a strong evaluation program and maintaining “approved products” lists.
- Evaluates commercially available digital certificate services and maintains a list of approved PKI Shared Service Providers

- Develops agreed upon processes for dealing with cross-cutting issues, including but not limited to Training, Partnerships and Sponsorship activities.
- Facilitates sharing “best of breed” solutions for all aspects of implementation.

Membership

Membership is open to all executive Departments and Federal agencies. Members should have expertise in at least one of the following areas: IT Security, IT Architecture, IT Policy, Smart Card Implementation, Human Resources, Physical Security, or Personnel Security. Agencies are encouraged to ensure the voting member and alternate are from different disciplines within the agency.

- Each Federal CIO Council Agency shall designate one voting member and an alternate to the Federal Identity Credentialing Committee.
- The voting member should have responsibility for implementing HSPD 12 within his or her agency,
- Exclusive of Agency membership, OMB shall designate the Chair, Federal Identity Credentialing Committee
- In addition, the OMB E-Authentication Portfolio Manager, the NIST Computer Security Division, the Interagency Security Committee, the Federal PKI Policy Authority, the Smart Card Interagency Advisory Board, and the GSA Authentication Services Program Office, will participate as ex-officio, non-voting members.
- Industry participation is provided through the use of cooperative agreements and participation/contributions to the Government Smart Card Interagency Advisory Board and the Federal PKI Technical Working Group.
- The Small Agency Council is encouraged to provide a representative.

Responsibilities

The FICC Chair:

- 1) Represents the Committee at meetings of other committees and councils both within and outside the Federal community.
- 2) Promotes collaboration and consensus-building among the membership.
- 3) Coordinates the activities of the Federal Identity Credentialing Committee with the Federal Public Key Infrastructure (PKI) Policy Authority, the Federal PKI Operational Authority (to include the Federal Bridge Certification Authority), Interagency Security Committee, and the Smart Card Interagency Advisory Board, to ensure cooperation, information sharing, and avoidance of redundant activities.

Federal Agencies:

- 1) Designate Agency voting member and alternate to the FICC
- 2) Provide support and feedback on proposed approaches and solutions

Each FICC voting member and alternate:

- 1) Attends each meeting of the FICC, designating an alternate when necessary.
- 2) Provides Agency input, makes commitments on behalf of the Agency (this may require coordination), and votes on behalf of the Agency.
- 3) Communicates and coordinates best practices from and within the member Agency in order to ensure alignment of the Agency and Federal Identity Credentialing.

- 4) Ensures member Agency participation in activities and solutions recommended and deployed by the FICC.

NIST:

- 1) Acts as the Office of Primary Responsibility for development, maintenance, and interpretation of the Standard.
- 2) Provides expert technical advice to the FICC in development of recommendations and solutions.

OMB:

- 1) Acts as the primary policy office for interpreting HSPD-12
- 2) Provides a participant for FICC meetings
- 3) Accepts requests for policy clarification from the FICC

Logistics

- 1) The FICC will meet at least monthly, with additional meetings as called by the FICC chair.
- 2) Attendance at FICC meetings is restricted to Federal Employees, unless otherwise designated by the Chair.
- 3) Working group meetings are held as needed.
- 4) Membership and attendance at working groups is unrestricted.
- 5) The FICC will vote on key issues related to the Federal Identity Credentialing as follows:
 - a) A vote on any issue may be called by the Chair or by any voting Member of the FICC.
 - b) There will be one vote per Agency with a simple majority rule. Voting members are designated by their respective Agencies.
 - c) Minority reports may be submitted to the record on any actions made by the FICC or its subordinate working groups
- 6) Additional procedures may be proposed by the Chair or any member and adopted with the concurrence of the members
- 7) There are eight related committees and working groups that collaborate with the FICC:
 - a) Smart Card Managers Interagency Advisory Board
 - b) Federal PKI Policy Authority
 - c) Federal PKI Shared Services Providers Working Group
 - d) FIPS 201 Sponsorship Working Group
 - e) HR Issues Working Group
 - f) Physical Security Issues Working Group
 - g) Logical Security Issues Working Group
 - h) Partnership Working GroupAdditional groups and ad hoc working groups may be formed as need arises with concurrence of FICC membership.

Approval