FICC Shared Service Provider Industry Day

March 11, 2004

Federal Identity Credentialing Committee

Agenda

Welcome and Introduction	Judith Spencer
The Shared Service Provider Initiative	Fred Catoe
The Shared Service Provider Roadmap	Tim Polk
Break	
Questions and Answers	FICC team

Federal Identity Credentialing Committee

Guidance for E-Authentication

- OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, Dec. 16, 2003
  - http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
  - About identity authentication, not authorization or access control

Guidance for E-Authentication, cont'd

- NIST SP800-63: *Recommendation for Electronic Authentication*
  - Companion to OMB e-Authentication guidance
  - Draft for comment at: http://csrc.nist.gov/eauth
  - Comment period ends: March 15
  - Covers conventional, token-based remote authentication
    - Does not cover Identity Based Authentication

Federal Identity Credentialing Committee

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)

Federal Identity Credentialing Committee

FICC Overview

- **Vision**: A common, ubiquitous, interoperable, Federal identity credential that facilitates trusted physical and logical access to buildings and services across the Federal sector while preserving the unique requirements of individual Federal organizations
- FICC addresses the needs of U.S. Federal Entities providing employee identity credentials

Federal Identity Credentialing Committee

Goals

- Simplify and unify identity authentication for Federal employees
- Create requirements for physical credentials, electronic credentials, and issuance
- Develop the Federal Identity Credentialing Component of the Federal Enterprise Architecture

Federal Employee Credentials

- Employees, contractors, and affiliates
- Primarily levels 3 and 4
  - Most will eventually be hard token (CAC card)
  - Near term, many will be soft token

Federal Employee Credentials, cont'd

- PKI based
  - New agency PKIs will use shared service provider CAs
    - Common certificate policy framework
  - Legacy agency-operated PKIs will continue to operate
  - Bridge CA will remain for policy mapping
    - Legacy agency-operated PKIs
    - States and local government, business, foreign, etc.
    - Commerce and citizen class

Federal Identity Credentialing Committee

Important Note

The Shared Service Provider Qualified Bidder List applies ONLY to the issuance of PKI certificates to Federal employees, contractors and other affiliates "behind the firewall".

E-Gov's 4th Sector – Internal Efficiencies and Effectiveness

Federal Identity Credentialing Committee

Two-Step Approach

- Step 1: Invite Service Providers to join the Qualified Bidders List
- Step 2: Provide the members of the Qualified Bidders List with the opportunity to attain a GSA Schedule 70

We will not be addressing Step 2 today. Please hold questions concerning the Schedule 70 for future discussions.

The E-Authentication Connection

- FICC meets the needs of the 4th Sector: Internal Effectiveness and Efficiency
- It provides Federal employees the means to perform their official and personal business using their Federally-issued logical identity credential.
- The FICC Common PKI Certificate Policy meets Assurance Level 3 of the *E-Authentication Guidance for Federal Agencies*
- E-Authentication Architecture includes interface with Common Policy Server and Federal Bridge Certification Authority (FBCA)

Federal Identity Credentialing Committee

End Results

- This approach will:
  - End the proliferation of stove-pipes
  - Drive standards adoption
  - Simplify interoperability across the Federal enterprise
- The resulting infrastructure will enable the implementation of diverse capabilities that take advantage of standardized identity credentials and enhance security across and between Federal entities

Shared Service Provider: The Federal Intent and Overview

Federal Identity Credentialing Committee

Purpose for Industry Day

- Set stage for industry partners
- Explain the landscape
- Define the process
- Define the timeline
- Answer questions

What is a Shared Services Provider?

- Properly qualified provider of PKI services for the government
- Governed by Authentication and Identity Policy Framework
  - Federal Common Certificate Policy
  - Federal Smart Card Policy
  - Federal Identity Assurance Policy

Federal Identity Credentialing Committee

Opportunity

- Each federal government entity that desires to stand up a PKI required to do so under the Federal .gov root CA
  - Certain existing systems exempt, most existing systems have sunset date after which they must transition to SSP
- Migration to smart card based Identification Cards – token solution already in place
- Repeatable “approved” solution approach

Centralized Trust Anchor

- GSA will establish the .gov root CA
- SSPs will operate as subordinate CAs under the .gov root CA
- The .gov root CA will be cross certified with FBCA – interoperability
- Operate under Common Certificate Policy
- Certificate Practice Statement (CPS) /Registration Practice Statement (RPS) approved by PA

Organization Specific Tailoring

- Each agency/administration has capability to customize implementations
  - Within the Common Certificate Policy and Policy Authority (PA) approved CPS/RPS
  - Certificate profiles
  - Technology implementations

Federal Identity Credentialing Committee

Why an SSP?

- Centralized trust – driving toward cross credentialing and trust models
- Leverage industry expertise and experience
- Reduction of Total Cost of Ownership

Federal Identity Credentialing Committee

Intentions

- Industry day
- Qualified participants
  - Non-compliant vendors vetted early so limit expended time on both industry and Government
- Operational Capabilities Demonstration (OCD)
- Approval and placement on “qualified” list
- Tim Polk will discuss roadmap in greater detail
- Available to all government organizations via GSA Schedule 70

Federal Identity Credentialing Committee

Timeline

- Conduct Industry Day – March 11, 2004
- Start Evaluations – Receive Initial Response by April 15, 2004
- Post Qualified Bidders – June 30, 2004

Available Documentation

- X.509 Certificate Policy for Common Policy Framework
- X.509 Certificate and CRL extensions profile for the CP
- Registration Authority requirements
- CPS Evaluation Matrix
- SSP Repository Service requirements
- Archive requirements for shared services providers
- FICC audit standards for PKI SSP entities
- Shared Service Providers Roadmap
- Operational Capabilities Demonstration Criteria for SSP
- SSP Notice of Intent to establish qualified bidders list

NOTE: Documents are subject to versioning, and are under document control

Shared Service Provider Roadmap

Navigating the Process to Acceptance

Goal

- Assist Vendors in understanding the process for becoming *qualified* to sell PKI services to the government under the Shared Services Provider program
- Enable Federal agencies to deploy PKI meeting the Common Certificate Policy using managed services

Federal Identity Credentialing Committee

Overview

- Shared Service Provider Components
  - Division of responsibilities between the vendor and Agency
- Shared Service Provider Requirements
  - What a vendor should know before applying
- Application and Acceptance Process
  - Gaining acceptance *efficiently*
- Post-Acceptance Process
  - Post-award vendor responsibilities

Shared Service Provider Components

- Certification Authority
  - Generates X.509 certificates and CRLs
- Repository
  - Distributes X.509 certificates and CRLs via *both* LDAP and HTTP
- Archive
  - Stores and manages physical and electronic logs
- Registration Authority
  - Performs identity proofing

Division of Responsibilities Between Vendor and Agency

- Vendor Responsibilities
  - Provides CA, Repository, and Archive services
  - Provides a baseline RA capability
  - Audits vendor-supplied services and components
- Agency Responsibilities
  - Operates/manages the RA component
  - Audits agency-supplied services and components

Shared Service Provider Requirements

- PKI and Smart Card Specifications
- Certification and Accreditation
- Vendor CPS and Compliance Audits

Federal Identity Credentialing Committee

Core Specifications

- Primary sources
  - Common Policy Framework for PKI requirements
  - Smart Card Policy for smart card requirements
- Common Certificate Policy is directly referenced
- Smart Card Policy is the indirect source for smart card requirements

Federal Identity Credentialing Committee

Supplemental PKI Specifications

- Additional PKI Policy Requirements
  - Certificate and CRL Profile describes contents of certificates and CRLs
  - Repository Profile provides details on HTTP and LDAP distribution requirements
  - Archive Specification provides details on archiving

Supplemental Smart Card Requirements

- GSC-IS V2.1 (NISTIR 6887)

Federal Identity Credentialing Committee

CPS and Compliance Audits

- Vendor must have a documented CPS
  - Need not be a single document
- Compliance Audits
  - CPS Analysis Matrix developed by SSP Subcommittee to achieve consistency in third-party audits

Certification & Accreditation

- Source
  - Requirement imposed by Federal Information Security Management Act (FISMA) and OMB A-130
- Relevant Documents
  - FIPS Publication 199
  - NIST SP 800-37 (draft)
  - NIST SP-800-53 (draft)

Federal Identity Credentialing Committee

Application and Acceptance Process

- Step 1: Submit Initial Application
- Three parallel steps:
  - Step 2: Operational Capability Demonstration
  - Step 3: Compliance Audit
  - Step 4: Certification and Accreditation
- After *successful* completion of all four steps, the vendor is added to the Qualified Bidders List

Federal Identity Credentialing Committee

Step 1: Initial Application

- Package MUST include:
  - A narrative description of the components
  - A letter from the compliance auditor indicating that the vendor CPS is in compliance with the CCP, with all of the following:
    - Vendor CPS
    - Completed CPS Analysis Matrix
    - Credentials of the compliance auditor

Step 2: Operational Capability Demonstration (OCD)

- The OCD validates the ability of an SSP candidate to operate a PKI environment that is compliant with the Common Certificate Policy and the supplemental documents
- The “Operational Capabilities Demonstration Criteria for Shared Service Provider Candidates” specifies the functionality to be demonstrated during the OCD

Step 2: Operational Capability Demonstration (OCD), cont'd

- The OCD will be performed in Washington, DC at a government location
- The Government will provide:
  - Internet connections (Ethernet)
  - Phone lines
  - Electrical power

Step 2: Operational Capability Demonstration (OCD), cont'd

- Vendor needs to bring RA/client configuration to perform basic operations specified in OCD
- CA, Repository, and Archive components may be housed at Vendor facility and accessed via Internet

Step 2: Operational Capability Demonstration (OCD), cont'd

- SSP Subcommittee determination
  - OCD was successful if all OCD criteria were successfully demonstrated
  - OCD was unsuccessful but issues are minor
    - Vendor may submit written attestation that all issues have been corrected
  - OCD was unsuccessful, major issues
    - Vendor is required to repeat OCD

Federal Identity Credentialing Committee

Step 3: Compliance Audit

- In addition to Initial package, Vendor submits a letter from the compliance auditor indicating that the vendor PKI is operated in compliance with the CPS
- SSP Subcommittee will review compliance audit materials and make a recommendation

Step 4: Certification and Accreditation

- Vendor submits a System Certification and Accreditation package for review and approval by the Authorizing Official
  - Package must cover both the SSP-operated components and the SSP-supplied RA hardware and software
  - C&A performed using 800-37, 800-53 for FIPS 199 Moderate Impact Level

Federal Identity Credentialing Committee

Step 4: Certification and Accreditation, cont'd

- The authorizing official may
  - fully authorize the system to process government data,
  - grant interim approval to process government data, OR
  - deny authorization to operate.
- Full authorization or Interim Approval constitutes successful completion of this step!

Federal Identity Credentialing Committee

Post-Acceptance Process

- Government will add successful Vendor to the Qualified Bidders List
- Vendors are encouraged to establish a contracting vehicle
  - May optionally join a Schedule 70
  - May use existing GWAC or other GSA schedule contracts

Federal Identity Credentialing Committee

Post-Acceptance Process, cont'd

- Vendors are encouraged to offer related services
  - Custom integration activities to support:
    - Integrating the SSP with agency owned equipment
    - PKI-enabling agency applications
  - RA and end-user training
  - Policy development services for agencies that maintain an agency-specific Registration Practices Statement (RPS)

Federal Identity Credentialing Committee

Post-Acceptance Process, cont'd

- To maintain qualifications, vendors MUST do both:
  - Submit yearly compliance audits
  - Repeat C&A process every three years AND upon major system changes

Break

Please hand question cards to FICC members

Questions and Answers

Thank you!

Please refer to the website for questions and answers from this session