Helping Meet the OMB 11-11 Directive

March 2018

Implementing federated identity management
OMB Memo 11-11
Meeting FICAM Objectives

Figure 1: ICAM Conceptual Diagram
FICAM Targets

Figure 11: Federal Enterprise Target Conceptual Diagram

Figure 12: Federal Enterprise Target Conceptual Diagram: Cross-Agency Access
The Problem Defined

- **Identity Assurance is a critical foundational element of information sharing and access decisions**
- **Federal, State, Local Governments and their commercial partners have no interoperable and integrated means of trusting identity credentials issued externally.**

**Results:**
- Less efficient, less effective information sharing/authentication
- Increased costs
  - Redundant credential issuance, background check, identity management operations
- Limited situational/resource awareness in all response and operational scenarios including cloud and mobile environments
  - Inefficient deployment of resources
  - Confusion on what is acceptable solution
The Federated Identity Solution

An identity framework and network leveraging a common trust model, issuance, governance, revocation, and operational policies:

- **Solves problems raised across disparate organizations by providing a strong, biometrically enabled identity credential that can be validated at any logical/physical access point**

- **Allows a decision maker or trusted application to make a locally-specific privilege and/or authorized ACCESS decision confident that:**
  - the identity of the person can be electronically verified
  - the organization the person represents was properly vetted
  - the individual possesses attributes he or she claims to possess
  - the organization and the individual have a legal relationship to do business with the federal government or organization; and,
  - that the individual has been issued a credential, in person and has undergone a background investigation consistent with DoD, Federal, State or Local Agency defined criteria.
FiXs is a Not for Profit 501-c(6) trade organization formed in 2004, that focuses on Governance, Standards, and Interoperability while providing:

- Complete contractual framework for member organizations, including a trust model, operating rules, audit criteria, a FISMA aligned C&A program, risk and liability criteria and flow down agreements signed by the member organization’s legal representatives.
- C&A program for hardware, applications and infrastructure focused on issuing and electronically authenticating federated identity credentials, while securing personal identifying information.
- A secure network Trust Broker (smart router(s)) through which transactions can be passed for PACS and LACS applications (including secure information sharing).
- Technical specifications for interfacing with the network trust broker(s) via authentication stations or via certified software for interoperability of applications.
- Access (over a digital certificate authenticated secure network) to certified service providers and sponsors of individuals holding certified credentials for additional data and criteria for services such as revocation and privilege management.
- Clearinghouse for objective consideration of technologies, business processes, rules and requirements between organizations across government and Industry.
FiXs is an end to end federated solution

The FiXs Federated identity solution solves problems raised across disparate organizations by providing a strong, biometrically enabled identity credential, that can be validated at any logical/physical access point - allowing the decision maker or trusted application to make a local specific privilege and/or authorized ACCESS decision confident that:

• the identity of the person can be electronically verified, including biometrics

• the organization the person represents was properly vetted

• the organization and the individual have a contractual relationship to do business with the federal government or organization; and,

• that the individual has been issued a credential, in person, and has undergone a background investigation consistent with DoD or Federal Agency defined criteria, including examinations of: breeder documents; security status; contract requirements; legal status & attributes.
FiXs Certified and Accredited Subsystems

FiXs Network –
The Defense Cross Credentialing Identification System (DCCIS) infrastructure and its interface to the FiXs Network are now fully operational for worldwide use in support of identity authentication purposes and applications. The architecture is in place today to inter-operate similarly with non-DoD organizations in a secure manner. Identity services are available to support users.

Credential Issuers (CI) –
Each CI undergoes an extensive and complete review in accordance with the highest industry standards and cover all requirements of the solution proposed in the solution. This is documented in detailed Certification and Accreditation (C&A) reports.

Authentication Stations/Devices –
FiXs certified authentication stations/devices enable FiXs PIV-I and Department of Defense (DoD) CAC PIV credentials to be verified and accepted for physical access authentication purposes by implementing the cross-credentialing services supported by this combined network. Final decisions on physical access privileges, whether at a government or vendor site, are local decisions. These solutions are enabled to work in other PIV and PIV-I environments.
Policy and Operational Timeline for Federated Solution

PIP Establishes Standard Systems to be used: DBIDs; DNVC, DCCIS

2004

2005

DoDI 3020.41 requires “Central Database for contractor info.” SPOT is designated by OSD

ARMY Vice Chair Letters directs ARMY Organizations to Follow Pip

FiXS created as Not for Profit Organization

2006

2007

DMDC issues IOC for DCCIS/FiXS Network

HSPD-12 and FIPS 201 standards and criteria issued

First DMDC-FiXS MOU lays the groundwork for DCCIS-FiXS Interoperability

2009

2010

USNORTHCOM message authorizes acceptance of FiXS credentials

DoDI 8520.03 Identity Authentication for Information Systems issued and FiXS PIV-I certified credentials available

Army Provost Marshall accepts FiXS credentials and OMB 11-11 issued

2nd DMDC-FiXS MOU signed focusing on identity credentials for physical and logical

SPOT FiXS Pilot at Ft. Belvoir outcomes endorsed by USD/AT&L

2011

2012

FiXS PIV-I certification for NFI’s begins

FiXS created as Not for Profit Organization
DoD’s DCCIS/FiXs Policy on Operations and Usage

2004 – PIP Standard Systems to be used: DCCIS/DBIDS/DNVC

“4.3. The PIP Program shall use emerging technologies to support the protection of individual identity and to safeguard DoD physical assets and logical systems from unauthorized access based on fraudulent or fraudulently obtained credentials. Further, identification credentials shall be authenticated to ensure that they are currently valid and issued to the individuals presenting them, whenever possible. “


“FiXs credentials that include PKI certificates issued from DoD ECA vendors are acceptable for use by DoD web based systems

2010 – USNORTHCOM Issues message on acceptance of FiXs certified credentials for physical access decisions

“FiXS CREDENTIALS ARE CERTIFIED AND ARE NOT FRAUDULENT ID CARDS. THESE CARDS ARE INDUSTRY CORPORATE IDENTIFICATION CREDENTIALS AND PRIVATE PROPERTY OF THE HOLDER. --- DOD’S DMDC WHICH IS RESPONSIBLE FOR PRODUCING THE CAC AND THE DBIDS, HAS BEEN WORKING WITH THE FiXS FEDERATION AND HAS RECOGNIZED THE FiXS CARD FOR IDENTITY AUTHENTICATION, BUT NOT FOR PHYSICAL ACCESS CONTROL – UNLESS ACCEPTED BY THE INSTALLATION OR FACILITY COMMANDER”

2011 – DoD CIO issues DoDI 8520.03 Identity Authentication for Information Systems
Identity Federation between DCCIS/DBIDS/DNVC and FiXs

Users: Member company employees w/ their credentials or CAC holders

DoD/DMDC

DCCIS Network

FiXs Network

Member Companies

Federation

DoD/DMDC Issuance System

DoD Facilities & Networks

Member Issuers / Subscribers

Member Relying Parties

Users: Member company employees w/ their credentials or CAC holders
All certificates on a FiXs credential include an Organizational Unit that identifies the FiXs assurance level as follows:

- ou=FiXs4, for FiXs credentials asserting FiXs equivalent “High”
- ou=FiXs3, for FiXs credentials asserting FiXs equivalent “Medium High”
- ou=FiXs2, for FiXs credentials asserting FiXs equivalent “Medium”
- ou=FiXs1, for FiXs credentials asserting FiXs equivalent “Low” (not recommended)
“Hardware tokens [FiXs] & associated certificates issued by the ECA providers have the same assurance level as a Common Access Card (CAC).” – EPMA

Note: Access privileges are granted under the purview of the Facility / Application owner
FiXs Chain of Trust – See FIPS 201

1. The sponsoring party (organization) asserts need for credentials and attests to the identity of the individual to receive credential.

2. The appropriate and necessary background verification is performed on both the sponsoring company and the individual.

3. Individuals are “enrolled” and issued credentials.

4. A single credential can be “linked” to multiple entities, precluding the need for multiple credentials (badges).

Chain of Trust

Credential holder may then use their credential for identity authentication purposes and have it validated across FiXs Network.
ICAM Compliant Credential Management

FIPS 201 compliant lifecycle management of users, their identity devices, & associated credentials…

… with the strength of DoD Medium Hardware Assurance
Robust Validation Infrastructure

FiXs Validation Service (Site 1)

CRL Update Path (ldap/ldaps http/https)

FiXs Validation Service (Site N)

Alternative Validation Paths (OCSP)

50 plus FiXs Compliant CRLs

20 plus FiXs Compliant PKI Directories

Local Area Network

Application Servers

https

Client/WS

Inside and/or Outside the LAN

OCSP Repeater

Client/WS

Client/WS
Robust revocation processes

Credentials issuers are required to maintain FiXs enrollment, control, administrative, REVOCATION, & audit information.

Maintenance & updating of the revocation information is the joint responsibility of the sponsoring organization & the Credential issuer.

Card & Certificate Revocation Lists issued immediately upon revocation.

“A revocation process must exist such that an expired or invalidated credential is swiftly revoked.”
FiXs Provides

• Vetting of organizations
• Vetting of organization’s legal representatives
• Provision of unique organization code
• Vetting of employee, including JPAS verification (at level 4)
• 4 levels of credentials – to include biometrics and nationality assertion
• Electronic authentication of CACs and FiXs credentials
• 3 hour revocation policy
• Secure information sharing environment
• PKI CRL & OCSP/SCVP services
• Audit services
• Test Lab services
• Interoperable and Secure Network services
• FISMA aligned C&A program
• Compliance w/ FIPS 201 and PIV-I tech specifications
• Formal MOU with DMDC covering all above
Enabling Solutions for Identity Assurance and Critical Infrastructure Protection

How do we protect our Identity Assurance goals and critical infrastructure resources, balanced with ease of use? ---Let’s start by:

• Providing easy and secure access for those who belong
• Simplifying identification verification and authorizations of visitors and network users by using federated solutions

Identity assurance (IA) and Identity management (IM) programs for contractors and suppliers must use certified and accredited solutions and:

• Incorporate strong vetting for those that require network or installation and facility access and authorizations
• Follow established and emerging DoD and Federal guidelines and consensus built standards on interoperability and secure information sharing

Access decisions must become automated, reliable & trusted.

Installation and Facility Owners/ Security Managers/Network and Application Owners are ultimately responsible, so let’s help to:

• Improve decision making capability
• Make it more secure, smarter and cost efficient with available IM and IA tools and solutions
Established Governance Structure

• Defined Trust Model
• Legal foundation
• Operating Rules
• Security Guidelines
• Policy Standards
• Privacy Act compliance
• Technical Architecture Specs and Standards
• Implementation Guidelines
• Certification and Accreditation Program
Identity assurance policy and standards have been developed for federated use. Vetting and security is in place for PIV, FiXs PIV-I, DoD/ECA, and for the requirements, intents, and expectations of HSPD-12 and FIPS 201.

- All are secure identities
- All can be used for access decisions
- All provisioned for 3 factor authentication

*It's been done, decided, now let's use it.*
Value Proposition and ROI

- Easy business decision for CIO and Security officer---”identity as a service”
- Leverages existing organizational infrastructures
- Fully operational TODAY for both LACS and PACS
- Achieves enterprise-wide capability and best practices
- Security and Privacy of staff, systems, and facilities
- Provides method for data security in compliance with latest identity authentication processes
- Comply with FAR contract requirements
- Supports the FICAM Roadmap and Implementation Guidance
- Demonstrates leadership in a large and developing market on a matter that is of major national importance
Visit the FiXs website

www.fixs.org

Contact FiXs at
703-591-3704