

Federated Identity & Access Control

Presented at:

Public Meeting about ANPR DFAR 252.204-7000

Presented by:

Daniel Turissini, CEO

Operational Research Consultants, Inc. (ORC)

Board Member, Federation for Identity and Cross-Credentialing Systems (FiXs)

<http://www.ORB.com>

<http://www.FiXs.org>

April 22, 2010

Overview - Today's Enterprise Access Problem

- No uniform compliance
- Vulnerability
- Lack of vision
 - *Who's on - Who's off*
- No threat flexibility
 - *DHS NIMS code deployment plan*
 - *PX & commissary services*
 - *Suppliers to docks*
 - *Maintenance and repair access to grounds*

Overview - Issues with base security

- **How do we protect our National Security resources, balanced with ease of use?**
 - *Easy, secure access for those who belong*
 - *Simple identification verification of visitors*
- **Identity assurance for contractors & suppliers must:**
 - *Incorporate strong vetting for those that require base access*
 - *Follow DoD & Federal guidelines*
- **Access decisions must be automated & reliable:**
- **The Base Commander is ultimately responsible, so how do we help:**
 - *Improve decisions*
 - *Make it more secure, smarter & cost efficient*

Overview - Federated Identity Solution

- Federated identity solves problems raised by DoD IG by providing a strong, biometrically enabled electronic identity credential, that can be readily electronically validated by any Federal logical/physical access point that allows the decision maker or databases to make a local specific privilege and/or authorized ACCESS decision confident in:
 - the identity of the person attempting access;
 - the identity of vetted organization that they represent;
 - that the organization and the individual have a legal relationship to do business with the federal government; and,
 - that the individual has been vetted in person and has undergone a background investigation consistent with the DoD defined levels.

***Credential assures you are who you say you are,
Commander's confirm what holder is permitted to access!***

Overview - DoD Certified Federation

- The Federation for Identity & Cross-Credentialing Systems (FiXs) certified credential is currently approved for use by contractors for DoD Logical & Physical identity authentication & transactions; equivalent to the CAC.
- The credentials are approved under DoD rules required by the Defense Cross Credentialing Identification System (DCCIS), the Defense National Visitor Center (DNVC) System, and the Defense Biometric Identification System (DBIDS), DoD PKI infrastructures.
- The credentials are also fully compliant with FIPS-201 Personal Identity Verification (PIV), Part 1 and the Federal Bridge Certificate Authority (FBCA).

Tested and Proven

- Successful assessment of the feasibility to utilize commercially - issued credentials in “feeding” the SPOT database – that adhere to FiXs-certified standards
- Credentials authenticated across secure network against federated data stores (including DEERS)
- Included “cleared” personnel, non-cleared personnel, first responders, other entities that interact with Army Material Command
- Monitor utilization, increases in productivity, & security profile
- Provided strategic assessment for future activities

Federation for Identity & Cross-Credentialing Systems Scales Across Federal Enterprise

- A 501(c)6 not-for-profit trade association formed in 2004 in collaboration with the DoD to provide secure and interoperable use of identity credentials between and among government entities & industry
- A coalition of diverse companies/organizations supporting development & implementation of interoperable identity cross-credentialing standards and systems
- Members include: government contractors, technology companies, major financial firms, not-for-profit organizations, DoD, GSA, state governments, etc.

Existing Infrastructure - Foundation

- FiXs entered into formal Memorandum of Understanding (MOU) with the DoD that established terms & conditions under which FiXs & DoD will use their respective systems as part of an identity suite of systems in January 2006, updated February 2009:
 - <https://www.dmdc.osd.mil/dmdcomn/owa/DMDC.FEDPIIPS>
- The terms and conditions include:
 - Operational framework for inter-operability between DoD & FiXs
 - Specific operational responsibilities
 - Governance structure
- Interim Authority To Operate (IATO) Granted by DMDC in July 2007

Existing Infrastructure - Proven Benefits and Responsibilities

- Benefits
 - Federated Solution
 - Trusted authentication at FiXs recognized locations and systems
 - Syndicated Investment
 - Syndicated Risk
 - Branded Transaction
 - Certified & Accredited Products/Services
- Responsibilities
 - Warrant Trustworthiness of Employees
 - Comply with Operating Rules

Existing Infrastructure - Governance Structure

- Defined Trust Model
- Operating Rules
- Security Guidelines
- Policy Standards, including Privacy Act compliance
- Technical Architecture Specifications & Standards
- Implementation Guidelines

Documentation available online at: <http://www.fixs.org/library>

Existing Infrastructure – Currently in Full Operations

- Individual personal identifying information [biometrics, ssn, and other unique personal identifying information] captured once and accessed for identity verification
- Information is maintained in a federated manner
 - No single database of every person’s identifying information
 - Maintained in a distributed manner under the authority and control of the organization who “sponsors” the individual holding the credential
- Queries of this information “logged” to support privacy and protection [as in knowing when someone accesses your credit report]

Existing Infrastructure – Consistent with DoD Objectives

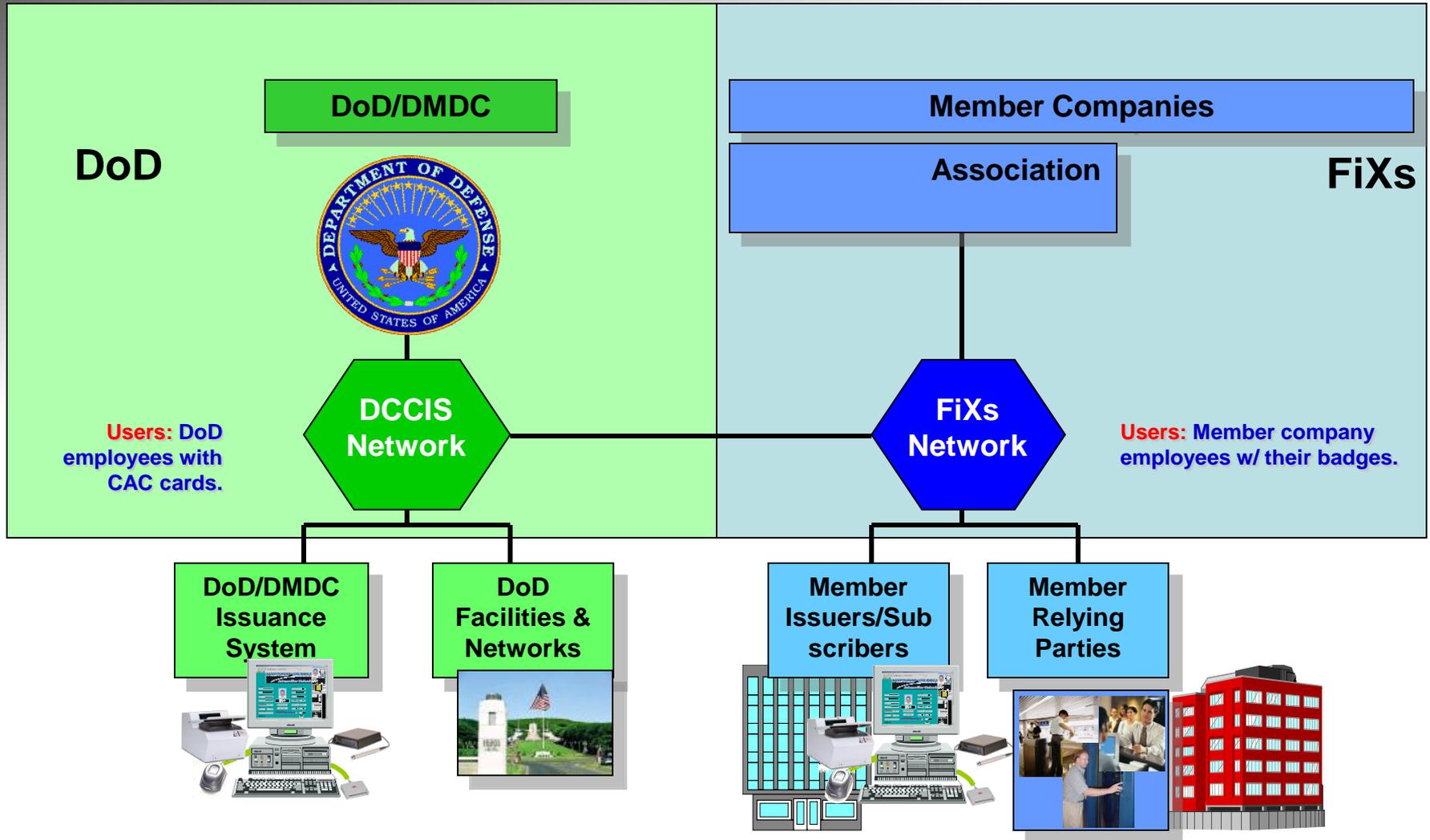
- Credentials that can be trusted with confidence
 - “FiXs network fully operational for worldwide use in support of identity authentication purposes & applications” -- DMDC 16JUL07
 - “The DoD shall establish & maintain the ECA program to support the issuance of DoD-approved certificates to industry partners & other external entities & organizations.” -- DoDI 8520
- Short term return on investment (ROI)
 - Existing, highly available architectures for identity deployment and revocation information -- immediate cost avoidance of CAC issuance “outside of the fence” and reliance on low value credentials

Minimal Installation Investments

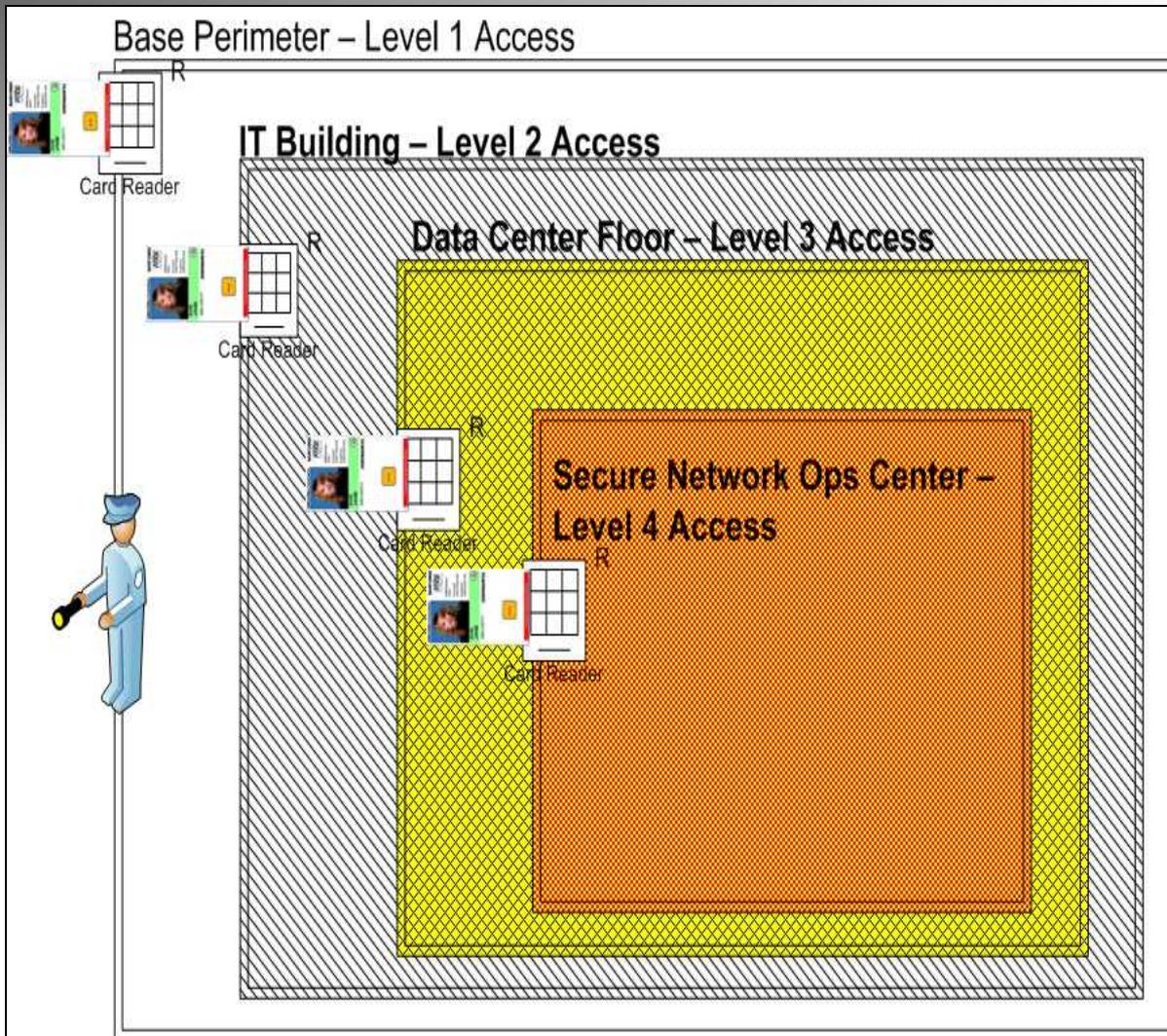
- Assurance of interoperability and convergence
 - DoD PKI Medium Hardware Assurance (CAC)
 - ECA Medium Hardware Assurance
 - Defense Cross Credentialing Identification System (DCCIS)
 - FiXs Initial Operating Capability (IOC)
- Distributed trust model DoD-wide
 - DoD PKI/ ECA Root distribution
 - Global Directory System (GDS)/ Credential Validation
 - FiXs Operating Rules - HSPD-12 compliant
 - **Defense National Visitor Center (DNVC) System**
 - **Defense Biometric Identification System (DBIDS)**
- CAC, PIV, & FiXs all read with the same existing equipment (contact or contactless readers)

Directly supports DoD mission of providing a safe, secure operating environment overseas & stateside

Currently Connected to DCCIS Network



Multi-level Vetting



- All certificates on a FiXs credential include an Organizational Unit that identifies the FiXs assurance level as follows:
 - FiXs4, for FiXs credentials asserting FiXs equivalent “High”
 - FiXs3, for FiXs credentials asserting FiXs equivalent “Medium High”
 - FiXs2, for FiXs credentials asserting FiXs equivalent “Medium”
 - FiXs1, for FiXs credentials asserting FiXs equivalent “Low”

Inline with Federal Acquisition Regulations

4.1301 Contract clause.

The contracting officer shall insert the clause at 52.204-9, Personal Identity Verification of Contractor Personnel, in solicitations and contracts when contract performance requires contractors to have physical access to a federally controlled facility or access to a Federal information system.

52.204-9 Personal Identity Verification of Contractor Personnel.

(a) The Contractor shall comply with agency personnel identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24, and Federal Information Processing Standards Publication (FIPS PUB) Number 201.

(b) The Contractor shall insert this clause in all subcontracts when the subcontractor is required to have physical access to a federally-controlled facility or access to a Federal information system.

Value Proposition & ROI

- Easy business decision for Provost and CIO
- Leverages existing DoD Infrastructure
- Fully operational TODAY
- Achieved enterprise-wide capability and best practices
- Security & Privacy of staff, systems, and facilities
- Provides method for data security in compliance with latest identity authentication processes
- Comply with FAR contract requirements
- Supports HSPD – 12 and DoD PIP instructions
- Leadership in a large and developing market on an matter that is of major national importance

The acceptance of Federated credential across DoD (and across the Federal government) is the most effective and efficient way to mitigate the risks associated with the important security problems associated with the issuance of Federal employee credentials to non-Federal employees.

Let's not reinvent ... !

Contact Information

Dan Turissini - FiXs Board Member

turissd@orc.com

703 246 8550

Robert Martin - FiXs FiXs Secretary

Robert.Martin@AmericanSystems.com

703 327 8916

Dr. Michael Mestrovich, FiXs President

Michael.Mestrovich@fixs.org

703 928 3157