



The Federation for Identity and
Cross-Credentialing Systems

President/CEO
Mike Mestrovich

Vice President
Rob Brandewie

Secretary
Bob Martin

Treasurer
Rob Russell

Committees

Federation Strategy, Business and Finance
Gary Glickman
Kent Schneider

Implementation Guidelines
Nabil Azar
Tom Connell

Infrastructure and Network Operations
Lew Henderson
Marty Wargon

International
Rob Brandewie
Jack Radzikowski

Logical Operating Rules
Dan Turissini

Marketing and Membership
Warren Blosjo

Policy and Rules
David Braswell

Privacy and Legal
Eugene Costa
Bob Martin

Security
Danny Michael

January 23, 2008

Mr. Mark Breckenridge
Deputy Director
Defense Manpower Data Center
DoD Center
400 Gigling Road
Seaside, CA 93955

Subject: Terms of Use Agreement

Reference 1: Memorandum of Understanding (MOU) between the Defense Manpower Data Center and the Federation for Identity and Cross-Credentialing Systems, Inc. (FiXs) dated 10 January, 2006

Reference 2: DMDC letter to FiXs dated 11 December 2007 pertaining to the sharing of software and related documentation

Mr. Breckenridge,

DMDC and FiXs entered into the referenced Memorandum of Understanding (MOU) which provides the terms and conditions under which the parties' will collaborate on the usage and development of a suite of systems that the parties will use to form the nexus of a federated inter-operable identity network. The purpose of this network is to verify the identity of people seeking to enter military installations or government-controlled areas, and FiXs commercial facilities.

Included in this MOU are provisions requiring the protection and security of information to be shared between the parties. Under Reference 2 above DMDC versions of such information have been shared and will continue to be shared consistent with the terms of the MOU.

Accordingly, the following measures will be, or in some cases have been, implemented to ensure that the proper protections and safeguards are in place to protect the unauthorized disclosure of sensitive information and data, to include versions of software and related documentation, being provided to FiXs by the Defense Manpower Data Center (DMDC).

These FiXs measures are:

1. All such software, documentation, data and other artifacts (DMDC-provided assets or assets) will be secured in a physically secure and controlled access area (i.e. a lab).
2. One copy of all such assets will be stored at a secure remote facility.
3. Logical access controls will be implemented to such assets where applicable.
4. Access to all of the DMDC-provided assets will be authorized on a case-by-case basis. This authorization must be provided by at least 2 FiXs representatives, either 2 FiXs officers or a FiXs officer and the FiXs technical architect.
5. The DMDC-provided assets will not be made available over an external network nor be transmitted over any such network.



The Federation for Identity and
Cross-Credentialing Systems

6. Any and all access to the DMDC-provided assets will be documented.
7. Access will only be granted on a need-to-know basis for bona fide business purposes as described in the DMDC-FiXS Memorandum of Understanding (MOU).
8. Access will only be granted to those specific DMDC-provided assets actually needed for purposes of storing, developing, operating or deploying components or all of the FiXS Network.
Access will only be provided to those assets actually needed, not the entire suite of assets.
9. Assets will only be allowed to be duplicated or modified for use in the needed environments - production; pre-production test; test; development, operations or deployment.
10. Any modifications, alterations etc. will be solely and exclusively the intellectual property of FiXS.
11. Any party having access to such assets will be required to agree in writing to the flow down terms of the MOU flowing down the applicable terms of the DMDC-FiXS MOU to such party.
12. FiXS will have the contractual authority to revoke such access and to demand the return or destruction of any such intellectual property at its' sole discretion.
13. Any party receiving such assets will sign a Terms of Use Agreement acknowledging and agreeing to these provisions as well as agree to strictly adhere to the FiXS Intellectual Property Policy.
14. The Terms of Use Agreement will include a provision to authorize injunctive relief for violations of these provisions.

The Federation understands the need for properly securing such assets and is committed to making sure that these needs are satisfied to the full satisfaction of DMDC.

Sincerely,

The Federation for Identity and Cross-Credentialing Systems, Inc. ®

A handwritten signature in black ink, appearing to read 'Michael J. Mestrovich', is written over a horizontal line.

Michael J. Mestrovich, PhD
Chairman, Board of Directors
President



DEPARTMENT OF DEFENSE
HUMAN RESOURCES ACTIVITY
DEFENSE MANPOWER DATA CENTER
1600 WILSON BOULEVARD SUITE 400
ARLINGTON VA 22209-2593

11 DEC 2007

Michael J. Mestrovich, PhD
President and CEO
The Federation for Identity and Cross Credentialing Systems (FiXs)
10400 Eaton Place
Suite 500A
Fairfax, VA 22030-2208

Dear Dr. Mestrovich:

Over the past four years the Defense Manpower Data Center (DMDC) and The Federation for Identity and Cross Credentialing Systems (FiXs), a not-for-profit 501 (c) 6 trade association, have collaborated in establishing the first secure interoperable cross-credentialing infrastructure/network for the exchange, verification and authentication of identity credentials between the Federal government and Industry.

We need to continue to maintain the joint architecture in both the DMDC and FiXs development environments. With the DCCIS to FiXs interface finalized, and the system in production (see enclosed IOC letter, dated July 16, 2007), and in accordance with our existing MOU dated January 16, 2006, we are transmitting to you a copy of the DCCIS and DMVC software and associated sub-files and documentation for use in the FiXs development lab. In return, we ask that you provide DMDC with current versions of the FiXs TGB, authentication station software, and all associated documentation for use in the DMDC development lab.

We envision continued evolution of this important interoperable cross-credentialing infrastructure, with industry, thru the FiXs Federation, and we look forward to our continuing collaboration.

Sincerely,

Mary Snavelly-Dixon
Director

Enclosure:
As stated



DEPARTMENT OF DEFENSE
HUMAN RESOURCES ACTIVITY
DEFENSE MANPOWER DATA CENTER
1600 WILSON BOULEVARD SUITE 400
ARLINGTON VA 22209-2593

**MEMORANDUM OF UNDERSTANDING
BETWEEN
The Federation for Identity and Cross Credentialing Systems
AND
DEFENSE MANPOWER DATA CENTER**

1. **PURPOSE.** This Memorandum of Understanding (MOU) is made, and entered into, by and between the Federation for Identity and Cross-Credentialing Systems, Inc. (FiXs) (a not-for-profit organization in the Commonwealth of Virginia) and the Defense Manpower Data Center (DMDC). The purpose of this MOU is to establish terms and conditions under which FiXs and DMDC will use the below-listed DMDC and FiXs systems as part(s) of an identity suite of systems. This set of systems is designed to easily interoperate between the DoD and the commercial FiXs Network to verify the identity of personnel seeking to enter military installations or government-controlled areas, and FiXs commercial facilities. These systems use currently available identity credential technology, in conjunction with biometric identification. The systems being offered by DMDC, and accepted by FiXs, and those being offered by FiXs, and being accepted by DMDC, are selected below, and will form the nexus of a federated, interoperable identity network between the parties.

- Defense Biometric Identification System (DBIDS) (to include EBIDS)
- Defense National Visitors Center (DNVC)
- Defense Cross-Credentialing Identification System (DCCIS)
- FiXs Network, infrastructure and affiliated identity credentials
- DoD Sensitive and Classified Visit Request System (under development by DMDC)

2. **AUTHORITY.**

- A. DoD Instruction 1000.25, 19 July 2004, DoD Personnel Identity Protection (PIP) Program
- B. DoD Instruction 1000.13, 5 December 1997, Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals
- C. DoD Instruction 4000.19, 9 August 1995, Interservice and Intergovernmental Support
- D. DoD Directive 8500.1, 24 October 2002, Information Assurance (IA)
- E. DoD Instruction 8500.2, 6 February 2003, Information Assurance (IA) Implementation
- F. Defense Biometric Identification System (DBIDS), System Notice S322.70, 18 Nov 04
- G. Public Law 93-579, Disclosure of Social Security Number
- H. Privacy Act of 1974, 5 USC 552a
- I. FiXs Bylaws (as amended), January 1, 2006

3. **EFFECTIVE PERIOD and MODIFICATIONS.** The provisions of this MOU will commence on the date of mutual acceptance as indicated by the latest signature date contained in this MOU and will remain in effect indefinitely or until terminated upon 90 day advance notice in writing to the other party. This MOU may be modified by written amendment signed by both parties. Minor modifications, such as Points of Contact (POCs), may be updated by the exchange of dated revisions to the appropriate attachment. More substantive changes shall be reflected in a rewritten, dated Appendix. Such changes shall not affect the base agreements governed by this MOU.

4. **RESOURCES.** Each party to this agreement is expected to provide appropriate and adequate resources for their portion of the federated network and its affiliated infrastructure, in order to operate and maintain interoperability between DMDC and FiXs. *This section is intended to assist in configuration control between the parties, however, it is recognized that changes to the operational infrastructure side may be influenced by national security requirements that are outside the control of the parties to this agreement and thus the timing stipulations agreed to may not be met in such circumstances.* For the FiXs portion of the federated network and infrastructure, funding and resources for policy/process changes, equipment, software, licenses, maintenance and user support will be provided by FiXs, and its members, during the duration of this MOU. For the DMDC portion of the network and infrastructure, funding and resources for policy/process changes, equipment, software, licenses, maintenance, and user support will be provided by DMDC during the duration of this MOU. The parties agree to share information about any current and projected out-year requirements, for their portion of the network **which will affect the other party**, for the purposes of joint planning. Those requirements, **affecting the other party**, will detail any changes to the policies, processes, equipment, software, security or interfaces affecting the following MOU calendar year. Notification of projected changes, as noted in this section, and projected impact on resources or funding, for each party, will be jointly provided at least 120 days prior to any requirements driven changes that impact joint interoperability. Resource requirements/projections for each organization, to support the federated network operations or modifications, will be jointly shared, so as to coincide with the term of service for the operation of the federated identity network in order to preclude network interruptions. The operational year of the network will run from 1 October through 30 September each year, to coincide with the DoD Fiscal Year.

5. **CONCEPT OF OPERATIONS.** The provisions of this MOU are designed to support the operational framework for interoperability of DMDC and FiXs in establishing effective DBIDS, DNVC, DCCIS and other DMDC and FiXs system(s) as selected above.

6. **OPERATIONAL RESPONSIBILITIES.** Operational responsibilities for the interoperable, federated, identity network that apply to both DMDC and FiXs are considered joint. In addition to joint responsibilities, each party has individual responsibilities. System-specific responsibilities are listed in the appropriate documentation for each system selected. Responsibilities for all DMDC and FiXs systems addressed by this Memorandum of Understanding are listed below.
 - A. Joint Operational Responsibilities. Both DMDC and FiXs will:
 - (1) Notify POC opposites, or their replacements, of any planned changes to data requirements or data formats at least 60 days in advance of any system/requirement changes. This notice allows the affected party to assess impact and to plan, resource and implement changes. All changes will be documented in the appropriate document for each project. *It is recognized that the 60 day notification requirement will change to, **as soon as possible**, when modifications by the government are necessitated due to urgent information security or national security requirements.*
 - (2) Notify POC opposites, or their replacements, no less than 60 days in advance of any deliverable on system upgrades or issues that could impact system availability, and provide updated status on implementation activities.
 - (3) Transfer data securely using an encrypted, authenticated transmission mechanism.

- (4) Give written notification to POC opposites of any material change in the POC roster for selected systems (POC roster(s) will be attached to any system documentation).
- (5) Abide by all applicable DoD and FiXs security rules, regulations, policies, and guidance governing Certification and Accreditation, and security management, relating to the exchange of data, including:
 - (a) DOD Instruction 5200.40, 30 December 1997, "DOD Information Technology Security Certification and Accreditation Process (DITSCAP)"
 - (b) DoD Instruction 8510.1-M, 31 July 2000, Information Technology Security Certification and Accreditation Process (DITSCAP) Application Document.
 - (c) CJCSI 6212.01B, 8 May 2000, "Interoperability and Supportability of National Security Systems, and Information Technology Systems"
 - (d) ASD (C3I) Memorandum, 20 March 1997, "Secret and Below Interoperability (SABI)"
 - (e) FIPS 140-1, FIPS 140-2, 25 May 2001, "Security Requirements for Cryptographic Modules"
 - (f) DoD 5200.2, 9 April 1999 or latest release, "Personnel Security Program"
 - (g) FiXs Security Guidelines , September 22, 2005
 - (h) FiXs Trust Model, September 22, 2005
 - (i) FiXs Operating Rules, September 22, 2005
 - (j) FiXs Technical Specifications (as amended, February, 2006)
 - (k) DCCIS and FiXs Interface Specification (as amended, February, 2006)
- (6) Assure compliance with the Privacy Act, as well as all applicable laws, regulations, policies and guidance governing records management and the release of personal information, including:
 - (a) Section 552a of title 5, United State Code, Privacy Act of 1974
 - (b) Office of Management and Budget, Circular No. A-130, "Management of Federal Information Resources" July 2, 1993 with revisions
 - (c) DoD 5400.7-R, September 1998, "Freedom of Information Act of National Security Systems, and Information Technology Systems"
 - (d) DoD 5400.11-R, 13 December 1999, "Department of Defense Privacy Program"
 - (e) FiXs Policy, September 22, 2005
- (7) Abide by all applicable DoD security rules, regulations, policies, and guidance governing Personnel identity protection, including:
 - (a) DoD Directive 1000.25, July 19, 2004, "DoD Personnel Identity Protection Program"

B. DMDC Operational Responsibilities:

- (1) Provide a POC for governance activities (see Section 7) to provide liaison with FiXs regarding policies, procedures, business rules, hardware, software, security, scheduling and other matters affecting the interoperability of the agreed to federated network.
- (2) Provide data in a consistent, and mutually agreed, format/means to ensure successful technical interoperability with FiXs.
- (3) Support ongoing operations with FiXs in conformance with applicable DoD policy.
It is recognized that changes to the operational infrastructure due to information assurance or national security requirements are outside the control of the parties to this agreement.

- (4) Continue support throughout the operational process.
- (5) Provide training, or technical guidance, for modifications (if required).
- (6) Ensure DMDC's stated responsibilities for the Automated Data Processing Environment for each system selected is fulfilled.
- (7) Provide system software changes (if required) and interface updates as they become applicable to FiXs.
- (8) Upon receipt of agreed to joint funding profiles, of each organization, take all required actions to accomplish modifications (if required) according to the joint schedule supported by the funding profiles.

C. FiXs Operational Responsibilities:

- (1) Appoint a single POC to provide liaison with DMDC regarding policies, procedures, business rules, hardware requirements, and scheduling.
- (2) Notify DMDC immediately of changes/developments that could affect the current operational/deployment timeline. Share future changes in a timely manner, if they will affect joint operations or interoperability.
- (3) Support ongoing operations with DMDC and DCCIS, technical interoperability, and trusted exchange of credentials between trusted FiXs partners and DoD.
- (4) Use data/hardware in a manner consistent with uses identified in each system description.
- (5) Prevent unauthorized personnel from obtaining physical access to system equipment.
- (6) Provide a safe and appropriate physical location for the installation, of all equipment required to support the interoperable network that is as free as possible from all environmental hazards including undue heat, cold, moisture, contamination, shock, or vibration.
- (7) Ensure FiXs member's stated responsibilities for all requirements of this MOU are carried out within their own organizations. This includes individual facilities that are identified as a FiXs node or end user site, of the interoperable federated identity network between DMDC and FiXs. To that end, each FiXs user member will sign a separate MOU with FiXs reflecting the specifics of this MOU between DMDC and FiXs. These individual FiXs member MOU's will provide for assessments and certifications of adherence to all rules and policies of this agreement either by FiXs or DMDC.
- (8) FiXs (The Federation) will conduct periodic random assessments and certifications that FiXs members are in compliance with the terms and conditions in this agreement and transferred to its membership that use the interoperable federated network and its products and services. Copies of these assessments will be made available to DMDC. If deemed appropriate DMDC may conduct its own independent assessments, with seven days prior notification to the FiXs Executive Committee.

D. Joint Responsibilities:

- (1) Develop a technical specification describing the technological interface between DMDC and FiXs.
- (2) In capacity of FiXs Government Advisor, DMDC will provide support to the ongoing collaboration, development and evolution of the technological interface between DMDC and FiXs.
- (3) Take newly released documents and standards, such as PIV & FIPS-201, as well as federated identity management standards, such as SAML and Liberty Alliance, under consideration for inclusion in future releases. These future interfaces could include but are not restricted to such systems as: JPAS; EBIDS and CAC web based enrollment via DCCIS and FiXs; and web based visitor request systems.
- (4) DMDC and FiXs will develop and execute the appropriate public affairs materials, briefings, white papers, etc. required to provide the appropriate information to users, or potential users, of the federated, interoperable identity network.

7. **GOVERNANCE.** This MOU and it's agreed to responsibilities, will be governed by existing forums within the DoD and FiXs. FiXs will provide appropriate liaison membership for DMDC assigned POC(s) to its Board of Directors, Executive Committee, Operations and Security Committees and all other committees and sub-committees established in accordance with the FiXs Bylaws and permitted by Federal statute. DMDC will provide for FiXs representation on/at management and oversight forums or meetings, for the purposes of: operating oversight; process changes; security requirements; developing, modifying and maintaining the interoperable federated network between FiXs and DMDC; or other policy, development or operational issues affecting the relationships established in this MOU.

8. **UNAUTHORIZED DISCLOSURE.** In the event DMDC determines that FiXs, or one of its members, has made an unauthorized disclosure of the data provided by DMDC, DMDC may:
1. Request a formal inquiry into an allegation of an unauthorized disclosure or, depending on severity, refer the issue to DoD and Federal law enforcement.
 2. Take appropriate action on 1 above, where an authorized release has been determined to have occurred, proceed with action required by law enforcement/general counsel. Require the submission of a corrective action plan formulated to implement steps to be taken to alleviate the possibility of any future unauthorized disclosure.
 3. Require the return of the data.
 4. Sanction against the further release of DMDC data to FiXs or its member users.

Additionally, FiXs acknowledges that criminal penalties under the Privacy Act (5 USC 552a (1) (3)) may apply if it is determined that FiXs, or any individual employed or affiliated therewith, knowingly and willfully obtained the file(s) under false pretenses. DMDC acknowledges that reciprocal actions (Items 1-4 above) apply to DMDC in the event of unauthorized disclosure of the data provided by FiXs to DMDC.

9. **ACCEPTANCE AND RATIFICATION.** The provisions of this MOU become effective upon signature and date as indicated below.

For: Defense Manpower Data Center

For: Federation for Identity and Cross-Credentialing Systems, Inc.

Mary Snavelly-Dixon

Michael J. Mestrovich

Mary Snavelly-Dixon
Deputy Director
Defense Manpower Data Center

Michael J. Mestrovich, PhD
Chairman
FiXs, Board of Directors

Jan 10, 2006

JANUARY 10, 2006

Date: January 10, 2006

Date: January 10, 2006