The Federation for Identity and
Cross-Credentialing Systems®

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

The Value of FiXs-- Interoperable Identity Management

The Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®) is a coalition of commercial companies, government contractors, and not-for-profit organizations whose mission is to establish and maintain a worldwide, interoperable identity and cross-credentialing network built on approved standards for trust, security, privacy, policy and operating rules. FiXs certifies and accredits products such as government approved Personal Identity Verification Interoperability (PIV-I) and authentication devices. FiXs provides granular personal identity data, certificate revocation management, and multiple levels of assurance and service across the FiXs Network. The FiXs Network is used today to verify and authenticate the identity for Business to Government/ Citizen to Government transactions. The FiXs governance model and resultant Network is extensible to any level of government and industry segment supporting physical and logical access control decisions.

Background

Founded in 2004 as a 501(c) 6 non-profit trade association based in Fairfax, Virginia, FiXs was formed to demonstrate a federated identity transaction model in collaboration with the U.S. Department of Defense (DoD). A long-standing affiliation with Federal credentialing programs has enabled government organizations and industry members to establish secure and interoperable identity verification and authentication for secure access.

The FiXs Network

FiXs provides a trusted mechanism for a federated identity infrastructure within and between public and private sector organizations with accuracy and trust through the application of a Federated Trust Model. The network capabilities can be accessed worldwide, in remote or fixed environments, wired or wirelessly, and in real- or near real-time. A key component of the Network's integrity is its strong authentication and revocation processes for both individuals and end point devices, as governed by the FiXs Operating Rules.

Functionally modeled after the widely accepted ATM (Automated Teller Machine) approach, the FiXs Network meets federally mandated requirements, to include: HSPD 12 and FIPS 201; supports physical and logical access applications; and integrates with an organization's existing personnel and other systems, while leveraging the network's economies of scale.

Privacy and Trust

A primary objective of FiXs is to protect personal identity information. Personal identity information is kept and maintained by the organizational sponsor of the individual – accessible for validation but not replicated throughout the Network via FiXs' architectural infrastructure commonly known as "federation". In most cases sponsorships is by the individual's public or private sector employer or their agent.

FiXs Federated Trust Model and Technology

The FiXs Network and certified applications using it, employ a sophisticated Federated Trust Model that allows disparate organizations to interoperate and authenticate identities, while allowing privileges to be managed locally by the facility, organization or system owner.

1

The key components of this Federated Trust Model are interdependent and require; 1) a trusted organization, which has been vetted; and, 2) a trusted individual identity within that organization, which has also been vetted. The two are linked through a "chain of trust" process (which includes identity documents and biometrics) that gives vetted and trusted organizations the ability to create and issue individual identity credentials that can be authenticated and managed over the trusted and secure network by other members and government users.

Once the identity credential is established, it can be used in workplace environments to assign privileges consistent with the objectives and unique requirements of each member organization. The FiXs role is limited to providing the trusted contract framework for identity <u>authentication</u>, which occurs prior to assignment of role or privilege designations (either physical or logical) by member organizations using the certified credentials.

The FiXs identity credentialing process and network currently is the <u>only</u> network certified to interoperate with the Defense Cross-Credentialing Identification System (DCCIS) infrastructure, the identity authentication network of the DoD.

It is important to note that FiXs does not grant or deny physical or logical access for any credential bearer. Rather, it delivers a trusted *infrastructure* that provides participating members with a high-assurance means to authenticate the actual identity of individuals presenting FiXs-certified credentials, and other approved PIV and PIV-I credentials, for access to facilities and systems. Through the FiXs Network authentication and verification process, facility and system managers independently determine whether they choose to grant or deny access or other privileges.

PIV-I

FiXs employs a set of Operating Rules consistent with the National Institute for Standards and Technology's FIPS 201 issued to implement Homeland Security Presidential Directive 12 (HSPD-12) for *a common policy for an interoperable identification standard for federal employees and their contractors.* Subsequent federal guidance directs the acceptance of non-government issued credentials that adhere to FIPS 201 FiXs provides the **only** non-federal secure certified network that meet FIPS 201 standards that meet or exceed the requirements and intent of Office of Management and Budget Memorandum M 11-11.

While only Federal government organizations can sponsor PIV credentials once cross-certified via the Federal Bridge Certificate Authority (FBCA) Non-Federal Issuers (NFI's) are trusted to issue PIV-I credentials that may be used across Federal, State, and Local government domains. Operational Research Consultants (ORC) has been approved as FiXs Certified PIV-I Credential issuer and is able to issue PIV-I credentials.

Who Participates

FiXs is an open membership organization that includes members from various communities of interest that promote improved workforce protection and systems security for critical infrastructure. Members include professional associations, not for profits, and commercial entities who contribute ideas, technologies, and best practices for implementing a secure identity cross-credentialing network based on open standards, sound business processes, and proven technologies.

For more information on FiXs membership, capabilities, and upcoming events, please visit www.fixs.org or call 703-591-3704.

For more information on obtaining FiXs Certified Credentials and network certified products, please go to www.dsainc.com, www.orc.com or www.sol-passs.com

Revised November 2016