



The Federation for Identity and
Cross-Credentialing Systems®

FIXS[®] OPERATING RULES
Version 3.2
November 13, 2008

www.fixs.org

Copyright 2005 by the Federation for Identity and Cross-Credentialing Systems, Inc.

All Rights Reserved

Printed in the United States of America

10400 Eaton Place, Suite 500A

Fairfax, VA 22030

(703) 591-9255

Table of Contents

| | | |
|------------|--|-----------|
| 1 | GENERAL REQUIREMENTS AND DEFINITIONS..... | 7 |
| 1.1 | Personnel Definitions and Requirements..... | 10 |
| 1.1.1 | Program Manager | 10 |
| 1.1.2 | Enrollment Personnel Requirements | 11 |
| 1.1.3 | Authentication Personnel Requirements | 12 |
| 1.2 | Systems Facility Definitions and Requirements..... | 13 |
| 1.2.1 | FiXs Trust Broker Interface Requirements | 13 |
| 1.2.2 | System Assessment | 14 |
| 1.2.3 | Credential Issuer Operational Requirements..... | 14 |
| 1.2.4 | FiXs Domain System Requirements..... | 16 |
| 1.2.5 | Relying Party Operational Requirements | 17 |
| 1.2.6 | Member Service Provider Requirements..... | 19 |
| 1.2.7 | Records/Files Maintenance Requirements..... | 20 |
| 2 | CREDENTIAL ISSUER RESPONSIBILITIES..... | 21 |
| 2.1 | Credential Issuance | 22 |
| 2.1.1 | Validate Applicant's need for FiXs Credentials..... | 22 |
| 2.1.2 | Verify Applicant Identification (Vetting/Identity Proofing)..... | 22 |
| 2.1.3 | Verification Process Requirements..... | 22 |
| 2.1.4 | Enroll Applicant Into FiXs System..... | 24 |
| 2.1.5 | Issue Participant Valid FiXs Identifier | 25 |
| 2.1.6 | Appeals Process | 26 |
| 2.2 | Transaction Request Processing | 26 |
| 2.2.1 | Processing Authentication Inquiries..... | 26 |
| 2.2.2 | Initiating Authentication Responses..... | 26 |
| 3 | SPONSORS..... | 26 |
| 3.1 | Vetting | 26 |
| 3.2 | Sponsorship of Employees..... | 27 |
| 3.3 | Adhere to FiXs Foundational Documents..... | 27 |
| 4 | RELYING PARTY RESPONSIBILITIES..... | 28 |
| 4.1 | Visitor Transaction Processing | 28 |
| 4.1.1 | Credential validation and TTransaction Routing..... | 28 |
| 4.1.2 | Processing Authentication Responses | 29 |
| 4.2 | Exception Processing..... | 30 |
| 4.2.1 | Badge/Token-Not-Present | 30 |

| | | |
|------------|---|-----------|
| 4.2.2 | Other Exceptions..... | 30 |
| 5 | FIXS TRUST BROKER RESPONSIBILITIES..... | 31 |
| 5.1 | System Administration Requirements..... | 31 |
| 5.1.1 | Designate FiXs TRUST BROKER System Administrator..... | 31 |
| 5.1.2 | Member Interface Management..... | 31 |
| 5.1.3 | Maintenance of Control Data..... | 31 |
| 5.1.4 | Activation and De-Activation of FiXs Domains..... | 31 |
| 5.1.5 | System Performance Requirements..... | 33 |
| 5.2 | Transaction Processing and Routing..... | 33 |
| 5.2.1 | Authentication Inquiries..... | 33 |
| 5.2.2 | Authentication Responses..... | 33 |
| 5.2.3 | Audit Control Data Transactions..... | 33 |
| 6 | SECURITY REQUIREMENTS..... | 33 |
| 6.1 | General Security Requirements..... | 33 |
| 6.2 | Infrastructure Requirements..... | 34 |
| 6.3 | Audit Requirements..... | 34 |
| 6.4 | Security Authorizations..... | 34 |
| 6.4.1 | General..... | 34 |
| 6.4.2 | Domain Technical Administrator..... | 34 |
| 6.4.3 | Domain Functional Administrator..... | 34 |
| 6.4.4 | Facility Domain Administrators..... | 35 |
| 6.4.5 | Facility Administrative Enroller..... | 35 |
| 7 | LIABILITIES AND INDEMNIFICATION..... | 35 |
| 7.1 | Liability under these Rules..... | 35 |
| 7.2 | Liability to Members and Participants..... | 35 |
| 8 | PRIVACY..... | 35 |
| 8.1 | Privacy..... | 35 |
| 9 | FIXS GOVERNANCE..... | 35 |
| 9.1 | FiXs Business Requirements..... | 36 |
| 9.1.1 | Establish FiXs Member Partnership Agreement(s)..... | 36 |
| 9.1.2 | Effect of Rules..... | 36 |
| 9.2 | Public Statements..... | 36 |

| | | |
|-----------|--|-----------|
| 10 | MEMBERSHIP APPROVAL, AUTHORIZATION TO OPERATE AND COMPLIANCE MONITORING | 36 |
| 10.1 | Summary | 36 |
| 10.2 | Vetting Requirements for Member Organizations | 40 |
| 10.2.1 | Application for membership | 40 |
| 10.2.2 | Membership Review and Approval Process | 40 |
| 10.2.3 | Certification of Authorization to Operate | 41 |
| 11 | MISCELLANEOUS | 42 |
| 11.1 | Voluntary Termination of Members..... | 42 |
| 11.2 | Amendment to These Rules..... | 42 |
| 12 | DEFINITIONS | 43 |
| 13 | REFERENCES | 50 |
| 14 | REVISION HISTORY | 51 |
| 15 | APPENDIX FiXs Logical Operating Rules Version 1.0 | 51 |

FIXS OPERATING RULES

Background

The Federation for Identity and Cross-Credentialing Systems® (FiXs®) is a not-for-profit 501 c (6) trade association comprised of a coalition of industry and public sector organizations whose objective is to support efforts to develop standards supporting the creation and deployment of a secure interoperable identity cross-credentialing network. These Operating Rules define the rights, responsibilities and liabilities of FiXs Member Organizations and those parties using FiXs-certified credentials or supporting components of the FiXs Network. The Rules are a part of a larger package of documents that lay the foundation for “trust” in the FiXs Network. The other documents, known as the FiXs Foundational Documents, include:

- The Trust Model;
- FiXs Policy;
- Implementation Guidelines;
- The Technical Architecture and Specifications; and
- Security Guidelines.

The FiXs Network provides a highly-scalable, secure, auditable solution set, whereby FiXs Member Organizations and relying parties can authenticate FiXs-certified Credentials (also known as FiXs-Credentials) issued to users from other participating organizations, or “Subscribers”. FiXs relies on a Federated Model of Trust, which is discussed more fully in the FiXs Trust Model. The federated identity model establishes trust between member organizations through the use of agreements, standards and technologies that make identity portable across the organizations.

Initially, FiXs established a trusted relationship between FiXs Member Organizations and the Department of Defense’ Defense Cross-Credentialing Identification System (DCCIS). Initially, the federation enabled participating Department of Defense (DoD) and industry facilities to achieve strong, and interoperable, identity verification and authentication of participating contractor/private sector personnel who present a company-issued trusted credential. Similarly, participating industry locations also recognize a DoD-issued Common Access Card (CAC) and the Defense Biometric Identity System (DBIDS) credential, which required no modifications in order to operate with FiXs and DCCIS.

FiXs, which is the only organization established to inter-operate a cross-credentialing system with DoD, can use its federated system to enable other government agencies, first responders, and industry partners to verify the identity of individuals who seek access to their physical or logical assets in either the government or commercial environment.

In a federated system each subscribing or participating organization maintains or controls its own data store of enrolled member data (“participants”) that the organization has sponsored. Privacy and security are maintained because no identity information is held centrally or maintained in the infrastructure except in the employee’s host organization domain server.

At the present time the Federal Government has defined four recognized levels of credentials and/or trust. It is generally accepted that each level is defined by two distinct processes; one that defines the vetting process that is accomplished prior to a credential being issued; and the second defines the standards for the data, and its placement on the credential, and the standards and specifications for the credential/card itself. FiXs has chosen to use a FIPS 201 compliant smart card specifications for all Levels of Trust. Thus, the main differentiation between the levels is primarily with the vetting process, documentation/verification, and biometric data collected, verified and maintained in the federated data model. FiXs certified credentials will also contain the appropriate data designating under which Level of Trust the credential was issued and classified.

The current Government sanctioned nomenclature for “Levels” is numerical (i.e. 4, 3, 2, 1) and described below. FiXs attempts to define these levels with a verbal designation of Trust Levels which offers its customers a descriptive context associated by level. Therefore, the remainder of this document and the accompanying Guidelines document will offer a corollary verbal description of levels to equate to the numerical levels:

“High Trust” = 4; “Medium High Trust” = 3; “Medium Trust” = 2”; and “Low Trust” = 1”

The highest trust level, Level 4, (FiXs equivalent “High”) is aligned with Homeland Security Presidential Directive 12 (HSPD 12). HSPD 12, dated August 27, 2004, entitled “Policy for a Common Identification Standard for Federal Employees and Contractors” directed promulgation of a Federal standard for secure and reliable forms of identification for Federal employees and contractors. In March 2006 the National Institutes of Standards and Technology issued Federal Information Processing Standards 201 for Personal Identity Verification (PIV) of Federal Employees and Contractors. The PIV standards consist of two parts – PIV-I and PIV-II. PIV-I satisfies control objectives, including enrollment requirements, of HSPD 12. PIV-II specifies implementation, including physical card characteristics, and use of identity credentials on integrated circuit cards for a Federal personal identity verification system.

The next level, Level 3, (FiXs equivalent “Medium High”) has not been defined, at this time, by a Federal Directive or Policy. FiXs members, however, have a requirement for this level of credential and thus FiXs has written a set of Guidelines to accommodate this requirement and will offer these Guidelines to the Federal government for consideration and adoption. FiXs Credentials certified at Level 3 are aligned with PIV II, but will differ from PIV I provisions relating to the enrollment process.

Level 2 (FiXs equivalent “Medium”) is defined in the FiXs Implementation Guidelines.

Level 1 (FiXs equivalent “Low”) if required. This level is considered a non-acceptable level of trust for the Federal government. FiXs “Certified Credentials” will at a future date assess the validity, requirements and resources required for this level. The level presently will not be used.

The FiXs Implementation Guidelines document provides the specific requirements for the vetting of sponsored individuals requesting credentials at levels 1-3, and in specific market/functional venues. The accompanying CHUID section of the Guidelines deals with the specifics of the data and specifications of the card. Thus, these Operating Rules and the Guidelines must be read in tandem to execute FiXs cross-credentialing services.

Historically, FiXs has borrowed many of its concepts from the electronic payments industry. In the electronic payments industry, specific operating rules provide a uniform business and legal framework, as well as standard formats, for the exchange of financial payments. To rely on the principles already established for the payments industry, NACHA – The Electronic Payments Association assisted with its knowledge and experience in development of the FiXs and DCCIS Operating Rules.

Since processing an employee's credentials is analogous to processing a payment, the FiXs Operating Rules for cross-credentialing, encourage maximum participation among participating members that would otherwise use differing internal practices and platforms. The objective is to establish a secure and interoperable "Chain of Trust" for all members (including contractors, delivery and repair personnel, transport workers, law enforcement, first responders and others, needing access to facilities).

1 GENERAL REQUIREMENTS AND DEFINITIONS

This Section defines the requirements that need to be met for performing FiXs operations. It describes the general requirements associated with FiXs Member Organizations as well as administrative and system requirements in their roles as Credential Issuers, Primary Trusted Organizations (PTOs) and Relying Parties. A **FiXs Member** or **Member Organization** is a company, agency, or organization that has submitted a Membership Application with the Federation for Identity and Cross-Credentialing Systems, Inc. to join FiXs in a membership category, and has been approved by the FiXs Board of Directors, in accordance with Section 9. **The Federation for Identity and Cross-Credentialing Systems, Inc. (FiXs)** is the legal entity that manages membership and maintains the FiXs Foundational Documents. (See Definitions for the precise meaning of all capitalized terms.)

The role of major governed by these Rules is described below. There are two processes that are fundamental to the issuance of FiXs-Certified Credentials. The first process requires that an organization sponsor an individual Participant into the FiXs Network and the second process involves issuing the Participant a FiXs-Certified Credential and processing Authentication Inquiries from Relying Parties. In the case of an Issuer Sponsor, described below, both of these roles are performed by the same FiXs Member Organization.

- A **Participant** refers to the individual employee or subcontractor of a Member Organization that qualifies to participate in the FiXs System.
- A **Credential Issuer** is a FiXs Member that issues a FiXs-Compliant Credential to FiXs Participants and processes and responds to Authentication Inquiries. A Credential Issuer is not responsible for the acts and omissions of the Participants to whom it issues Credentials.
- A **Sponsor** is an organization that uses the services of an Issuer Sponsor to host its FiXs operations and that sponsors Participants into the FiXs Network. A sponsor is responsible for the acts and omission of the Participants that it sponsors. There are two kinds of Sponsors – Member Organizations and Non-Member Organizations. In this case, the Issuer Sponsor hosts the Sponsor's FDS and processes its FiXs authentication transactions.

- An **Issuer Sponsor** is a Credential Issuer that also sponsors Participants to whom it issues FiXs-Certified Credentials. This means that an Issuer Sponsor is a Member Organization that is both a Credential Issuer and a Primary Trusted Organization.
- A **Relying Party** relies on the FiXs credential to authenticate the identity of a Participant and/or initiates authentication inquiries to the Credential Issuer and processes the responses in accordance with FiXs Operating Rules.
- A **Primary Trusted Organization (PTO) or Subscriber** is a member organization that sponsors individual employees or contractual agents of the PTO/Subscriber who are to be issued a FiXs-certified Credential in accordance with all FiXs processes, and policies and that agrees to be responsible for the acts and omissions of employees or Contractual Agents. These organizations must agree to and execute the current FiXs Terms of Use Agreement for use of such credentials.
- **The FiXs Trust Broker** is the operational intermediary between Credential Issuers and Relying Parties that serves as the “switch” by processing Authentication Inquiries from Relying Parties to Credential Issuers and Authentication Responses from Credential Issuers to Relying Parties via the FiXs Trust Broker.

Under the Federated Model of Trust XML messages and a system of servers are designed so that the Trust Brokers see *only* the data that they need. To ensure that is the case, the payload data of all XML transaction messages are encrypted, using the PKI certificates of the trusted end-point destination and the source domain servers. A trust broker serves as a single, centralized, and authoritative holder for the list of sites that are considered to be “trusted” FiXs members.

Organizations are likely to join FiXs for various reasons. Some organizations will join with the sole intent of using the FiXs infrastructure for *internal* purposes. For example, a company may have a large number of employees scattered in field offices around a large geographic area, and it may have a well-established internal networking infrastructure already in place. However, this particular company may not have a need to authenticate employees from other FiXs member company sites. In this situation, this particular company would not be listed in the FiXs Trust Broker, because they have no need to interact with other FiXs Members.

A Member only becomes a “trusted” organization when its unique identifying number, known as its Organizational Code, appears in the FiXs Trust Broker. If a Member uses the FiXs Network strictly for internal purposes, its Organizational Code will not appear in the Broker server’s trust list, and all transactions for the member will be rejected by that Trust Broker. Member companies become “trusted” by joining FiXs and expressing their desire to interact with other FiXs “trusted” members. A Member Organization is deactivated by removing its Organization code from the FiXs Trust Broker registry.

Let’s now consider the second case, where FiXs Member Organizations *are* interested in interacting with other FiXs Member Organizations. This illustrates a scenario where employees have frequent interactions with other FiXs member organizations, and there is a requirement for a high level of trust and assurance in the credentials and identities that are being presented. In this situation, these companies *would* be listed in the FiXs Trust Broker.

Finally, the third scenario is a complete and full trust by both FiXs and an entity, such as the Department of Defense (DoD), which has a separate Trust Broker. In this scenario companies require a high level of trust, assurance, confidence and interaction with other FiXs Member Organizations as well as with the DoD. Conversely, since this is a two-way trust, this scenario also implies that members of the DoD (CAC holders) will be able interact with these trusted FiXs member companies in a highly trustworthy manner. In this case, these member company sites will be listed in *both* trust lists of the FiXs Trust Broker *and* the DoD TGB. Again, it is important to note that DoD (and FiXs, for that matter) still retains the ability to individually single out a particular member for exclusion from its trust list. It is the sole decision and discretion of DoD to allow or deny electronic interchange of FiXs or DoD credentials with specific FiXs member companies.

The agreements process that binds FiXs Member Organizations to one another is depicted in Figure 1.1, while the transaction flow process is depicted in Figure 1.2.

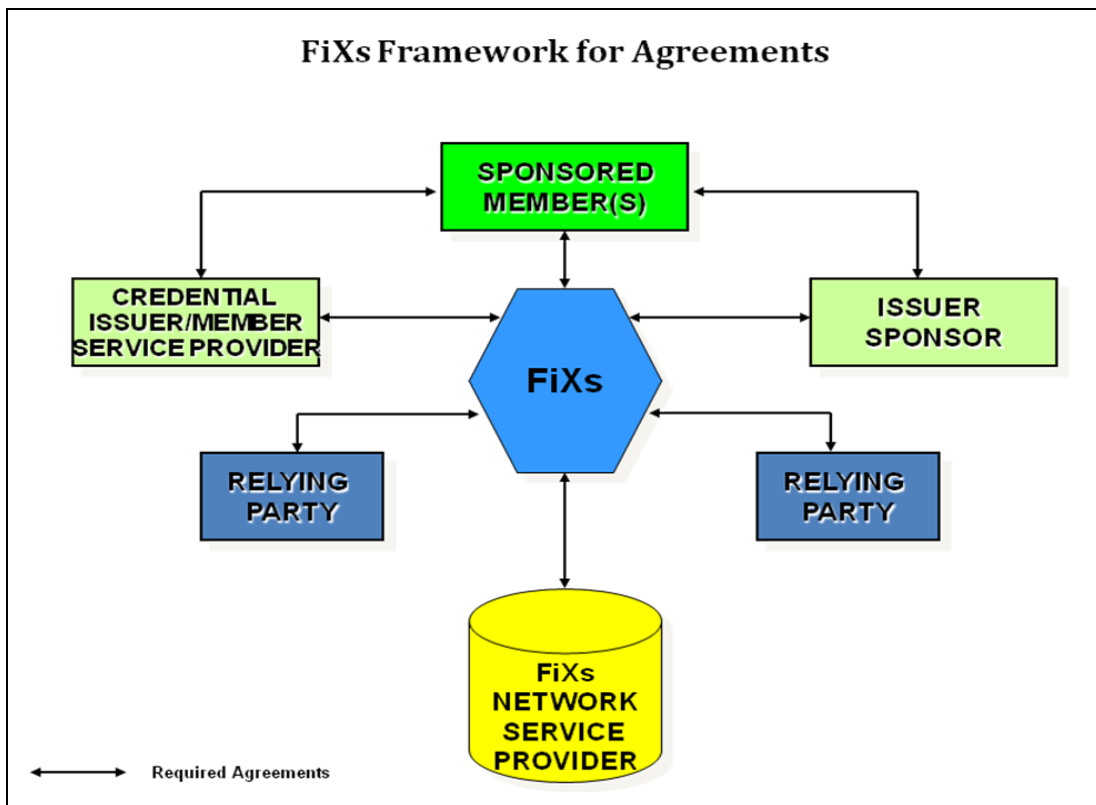


Figure 1.1 FiXs Agreement Process

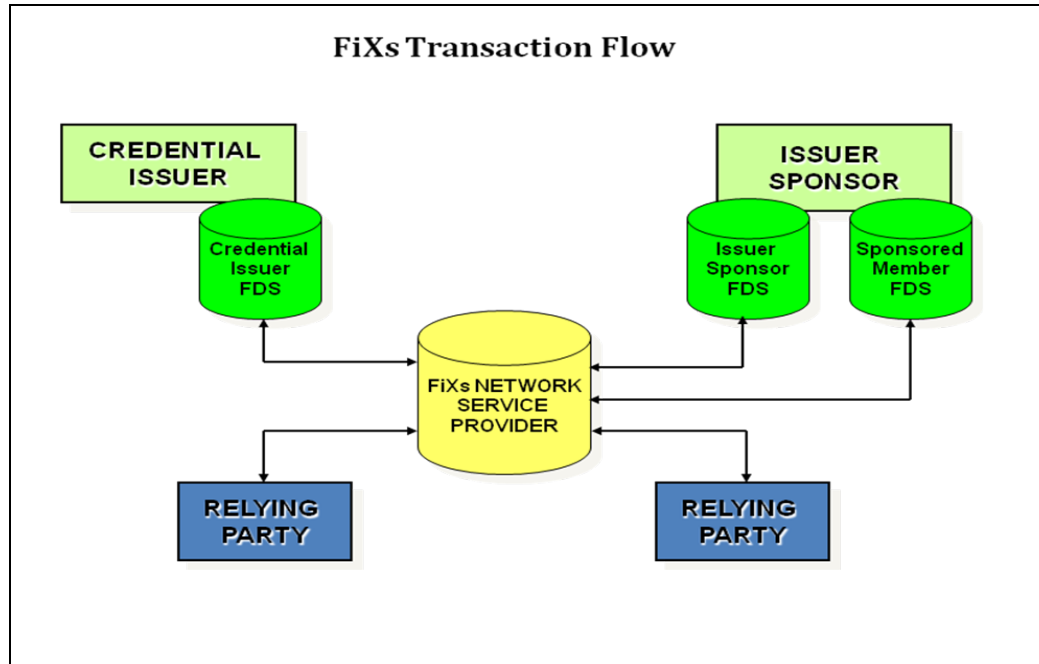


Figure 1.2 FiXs Transaction Flow

1.1 Personnel Definitions and Requirements

This section defines and describes the requirements associated with personnel that will perform FiXs functions for Credential Issuers and Relying Parties. Note that these are the functions that need to be discharged in the FiXs program. However, it is up to the Member Organization as to how these positions will be filled within the Organization (for example, a Member may opt to appoint an existing employee to take on a FiXs function as an additional role). These Rules must be posted so as to be easily accessible to all personnel whose responsibilities are addressed by these Rules. The only exceptions are that 1) the Domain Program Manager cannot serve as either a Facility Enroller or Facility Verifier, and 2) Facility Enrollers and Facility Verifiers must always be separate personnel. See Figure 1, Sample Organization Chart, for an illustration of how FiXs functions/positions can be organized.

1.1.1 PROGRAM MANAGER

The **Program Manager** (PM) manages and administers the FiXs program within a Member company or organizational domain. The PM has technical oversight of the program and is responsible for appointing the Domain Technical Administrator and Domain Functional Administrator for the Program.

1.1.1.1 Domain Technical Administrator

The PM must designate at least one **Technical Administrator** who has the authority to perform maintenance on the Enrollment System and/or the Authentication System for the Member Organization. The FiXs

Domain Administrator works with the Security Official of the Organization responsible for Physical Security to ensure a coordinated approach, particularly at the Authentication Station sites.

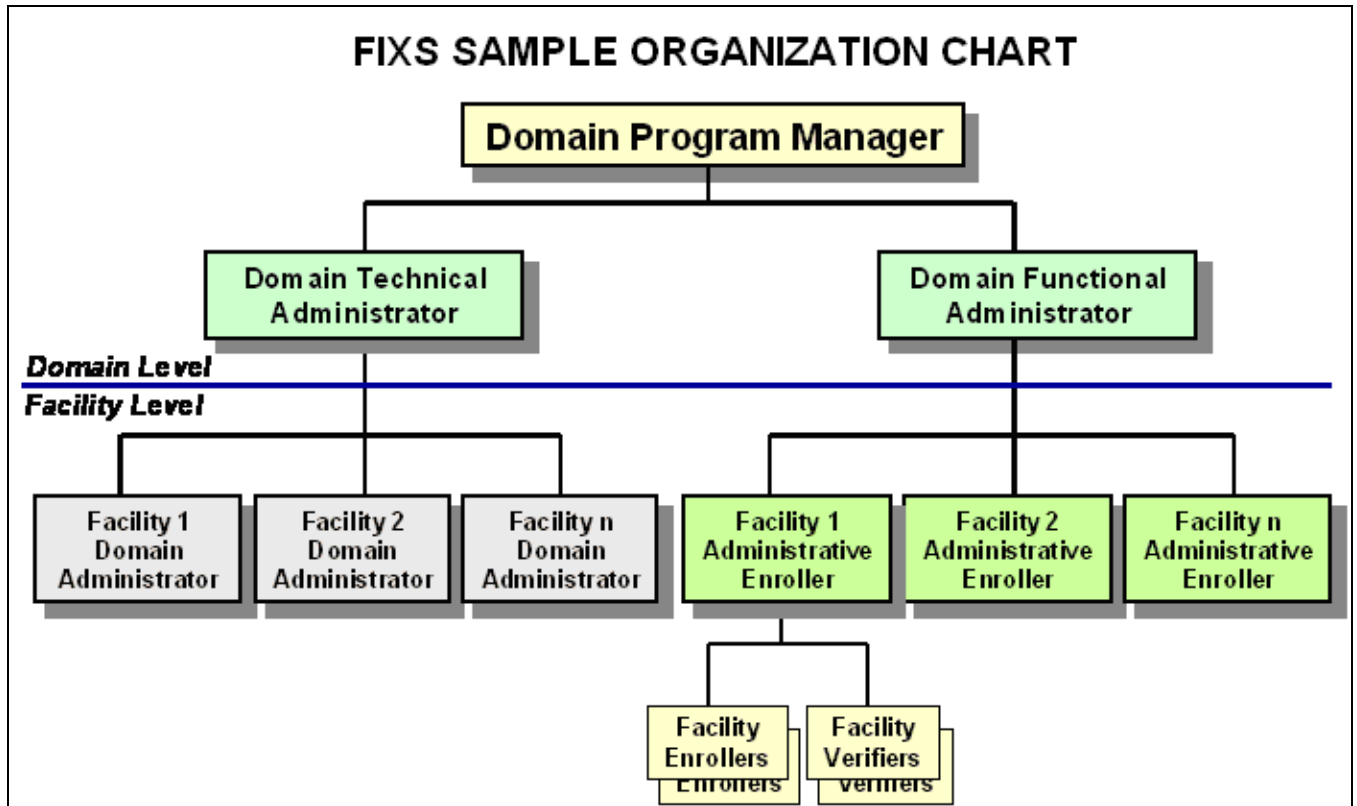


Figure 1.3: FiXs Sample Organization Chart

1.1.1.2 Domain Functional Administrator

The PM must designate a Domain Functional Administrator if the organization is participating in FiXs as a Credential Issuer. The **Domain Functional Administrator** is responsible for the enrollment functions and management of the enrollment personnel within the Member organization. The Domain Functional Administrator is authorized to enroll and train Facility Administrative Enrollers. In addition, the Functional Administrator must designate individuals within the organization who have the authority to attest to the applicant's need for a FiXs credential.

1.1.2 ENROLLMENT PERSONNEL REQUIREMENTS

The Credential Issuer is responsible for designating, training, and certifying Enrollment Personnel on the FiXs System. Enrollment Personnel must be vetted in accordance with 2.1.2, Verify Applicant Identification (Vetting/Identity Proofing). Enrollment Personnel are under the management and supervision of the Domain Functional Administrator.

FiXs Member Organizations are responsible for maintaining an up-to-date list of certified Enrollment Personnel, periodically reviewing their lists, ensuring current training is provided to all personnel and maintaining up-to-date certifications for all Enrollment Personnel. It is recommended that each FiXs Member Organization review its list of Enrollment Personnel at least on a yearly basis. These personnel categories are described below.

1.1.2.1 Facility Administrative Enrollers

A Credential Issuer must designate at least one Facility Administrator Enroller per Member facility. **Facility Administrative Enrollers** are responsible for enrolling and terminating new local Facility Enrollers using the Enrollment Operator Maintenance Web Application.

1.1.2.2 Facility Enrollers

Facility Enrollers are employees of a FiXs Credential Issuer who operate the Enrollment Client and are responsible for capturing the required FiXs ID data from FiXs Applicants. Facility Enrollers may be designated by the Facility Administrative Enroller, and once appointed must be trained and certified by Facility Administrative Enrollers to perform the functions described below on the Enrollment Client

1.1.2.2.1 Session Authentication

The Facility Enroller must authenticate himself/herself to the Enrollment Web Application at the beginning of each session using their FiXs credential/identification number and a biometric.

1.1.2.2.2 Capture Participant Enrollment Data

In a single session, the Facility Enroller must completely and successfully capture and store an applicant's digitized photograph, fingerprint biometrics, and name identification and demographic data. All data must be correctly entered during the single session.

1.1.2.3 Facility Verifiers

A Credential Issuer must designate at least one Facility Verifier per Member facility. A **Facility Verifier** is an employee within the organization who has the authority to perform the identity proofing tasks outlined in Section 2.1.2. In addition, the Facility Verifier is responsible for safeguarding background check documents and results in accordance with the policies and procedures outlined in the *National Industrial Security Program Operating Manual (NISPOM)*. *Facility Verifiers shall not dis-enroll participants.*

1.1.3 AUTHENTICATION PERSONNEL REQUIREMENTS

The Relying Party is responsible for designating, training, and certifying Authentication Personnel described in the sections that follow. The Relying Party is also responsible for maintaining an up-to-date list of certified Authentication Personnel, periodically reviewing their lists, ensuring current training is provided to all personnel and maintaining up-to-date certifications for all Authentication

Personnel. It is recommended that each Relying Party review its list of Authentication Personnel at least on a yearly basis.

1.1.3.1 Facility Domain Administrators

A FiXs Member organization must designate at least one Facility Domain Administrator per Member Facility. **Facility Domain Administrators** have the technical and operational responsibilities for individual FiXs facilities within a domain.

1.1.3.2 Authentication Station Operators

Authentication Station Operators operate the Authentication Client at Relying Party facilities. They must be trained and certified by the Facility Domain Administrator to perform Authentication Inquiries and routine administrative functions. These functions include:

1.1.3.2.1 Session Authentication/Log-On

Prior to processing FiXs Participants, the Authentication Station Operator must log in and authenticate to the system using their FiXs credential/identification number and biometric.

1.1.3.2.2 Authenticate Participant Credentials

The Authentication Station Operator must validate a FiXs Participant's credentials in accordance with the instructions provided on the Authentication Station after correctly entering the initial ID data.

1.1.3.2.3 Explicitly Accept or Reject the Credentials

Based on local operating procedures, the Authentication Station Operator decides whether to grant the Participant access. In accordance with Section 3.1.2.2, the Authentication Station Operator must explicitly record his or her decision about whether to grant the Participant access and the decision shall be recorded in the system Audit Log.

1.2 Systems Facility Definitions and Requirements

The Sections that follow describe the systems requirements at Credential Issuer facilities and Relying Party facilities that must be in place prior to starting FiXs operations. For a standard FiXs Member configuration and list of standard components as well as the standards and formats associated with data and messages, please refer to the *FiXs Technical Architecture and Specifications*.

1.2.1 FIXS TRUST BROKER INTERFACE REQUIREMENTS

Credential Issuers and Relying Parties (including the DoD) acting in each of these roles must maintain an interface to the FiXs Trust Broker system in compliance with the *FiXs Technical Architecture and Specifications*.

1.2.2 SYSTEM ASSESSMENT

The organization shall issue credentials only through systems and providers whose reliability has been established by the agency and so documented and approved in writing (i.e., certified) in accordance with the *FiXs Security Guidelines*.

1.2.3 CREDENTIAL ISSUER OPERATIONAL REQUIREMENTS

The Credential Issuer system supports enrollment of the FiXs Participant; maintenance of reliable connectivity for data access, storage of the participant data, log and audit trails; and, credential authentication. The hardware and software requirements association with these functions are described in the sections that follow. See Figure 2: Credential Issuing System.

1.2.3.1 Enrollment Site Certification Requirements

Enrollment Sites must be certified according to the procedures established by FiXs Guidelines. the DoD. The Domain Technical Administrator is responsible for ensuring that these procedures are followed and that all relevant documentation and checklists are signed.

1.2.3.2 Enrollment System Requirements

This section describes the system requirements for enrolling new FiXs members.

1.2.3.2.1 Enrollment Client (and Browser)

The **Enrollment Client** is a PC with a Web browser for network access to the FDS. It also contains a set of drivers for a web camera and a fingerprint reader.

1.2.3.2.2 Enrollment Web Server

The **Enrollment Web Server** is a standard web server (which resides on the FDS) that processes enrollments from the Authentication Client and stores the records in the Sponsor's FiXs Data Repository.

1.2.3.2.3 Enrollment Web Application Software

The **Enrollment Web Application Software** enables entry of new FiXs Participants into the Sponsor's FiXs Data Repository.

1.2.3.2.4 Operator Maintenance Web Application

The **Operator Maintenance Web Application Software** enables new local site Enrollment Operators to be created and terminated on the Sponsor's FiXs Data Repository. This operation can only be conducted by a designated Facility Domain Administrator at each local site and must be conducted in accordance with the *FiXs Security Guidelines*.

1.2.3.2.5 Smart Card Writer (Optional)

The Enrollment System may include a Smart Card Writer. The **Smart Card Writer** can be used to write ID data to the card and

record images for comparison to a scanned image on the Authentication Client. Captured data must conform to the specifications found in the *FiXs Technical Architecture and Specifications*.

1.2.3.2.6 Biometric Capturing Device

The Enrollment System must include a **Fingerprint Capturing Device** and software for capturing, reading, storing and comparing fingerprints or other devices as may be consistent with these operating rules for capturing biometrics. Captured data must conform to the specifications found in the *FiXs Technical Architecture and Specifications*. (Devices compliant with the software are listed in the *FiXs Technical Architecture and Specifications*.)

1.2.3.2.7 Digital Camera

The Enrollment System must include a **Digital Camera** capable of capturing digital photos and storing them in file formats as per the *FiXs Technical Architecture and Specifications*. (Devices compliant with the software are listed in the *FiXs Technical Architecture and Specifications*.)

1.2.3.2.8 Bar Code Reader/Printer

The Enrollment System must include a **Bar Code Reader/Printer** for storing and accepting current token barcodes or printing new barcodes for existing tokens as per the *FiXs Technical Architecture and Specifications*. (Devices compliant with the software are listed in the *FiXs Technical Architecture and Specifications*.)

1.2.3.2.9 Driver's License/Passport Reader

The Enrollment System must capture and validate information for enrollment in compliance with the *FiXs Technical Architecture and Specifications*.

1.2.3.2.10 Scanning Device

The Enrollment System must include a device that is capable of scanning physical documents into electronic form so that the documents may be electronically stored.

1.2.3.2.11 Enrollment System Performance Requirements

The Enrollment System must be available for use 24 hours a day 7 days a week.

1.2.3.2.12 Trusted Computing

In order to achieve higher levels of trust, assurance and security, interested FiXs members may (optionally) employ enrollment and/or authentication client machines with a hardware-based Trusted Platform Module (TPM) device. Such TPM devices are

implemented in accordance with open specifications, as defined by the Trusted Computing Group™.

For peripheral devices, such as trusted smart card readers/writers, fingerprint readers, keyboards, and secure PIN entry devices, there are even more secure, high assurance, trusted path devices that may be implemented, which offer an additional layer of trust, especially in sensitive or classified environments. Such devices are offered by a number of vendors and manufacturers, some of which are existing FiXs member companies.

1.2.4 FiXs Domain System Requirements

This section describes system requirements for FiXs Domain Server (FDS) and authentication system.

1.2.4.1 FiXs Domain Server

The *FiXs Domain Server (FDS)* platform contains the enrollment and authentication server software and it interfaces to the FiXs Data Repository, the FiXs Trust Broker, the Enrollment Client, and the Authentication Client.

1.2.4.2 FiXs Data Repository

The *FiXs Data Repository* stores the identification credentials and audit files associated with the FiXs Participants of the Member Organization and interfaces to the Member's FDS. Data and formats are described in the *FiXs Technical Architecture and Specifications*.

1.2.4.3 Hardware Security Modules

Provided by FiXs Program: A **Hardware Security Module (HSM)** must be attached to the FDS. The HSM device is used to encrypt messages that are being sent to the FiXs Trust Broker and to verify signatures of messages received from the FiXs Trust Broker. The HSM contains: a) the private key for the new FDS; and, b) the public key of the Trust Server. These HSMs are loaded by the FiXs Trust Broker and delivered securely to each FDS environment.

1.2.4.4 System Performance Requirements Authentication Processing

The Verification System must be operational 24 hours a day, 7 days a week, with an up-time availability of 99.99%. The FDS must process an Authentication Inquiry and return an Authentication Response in no more than 5 seconds.

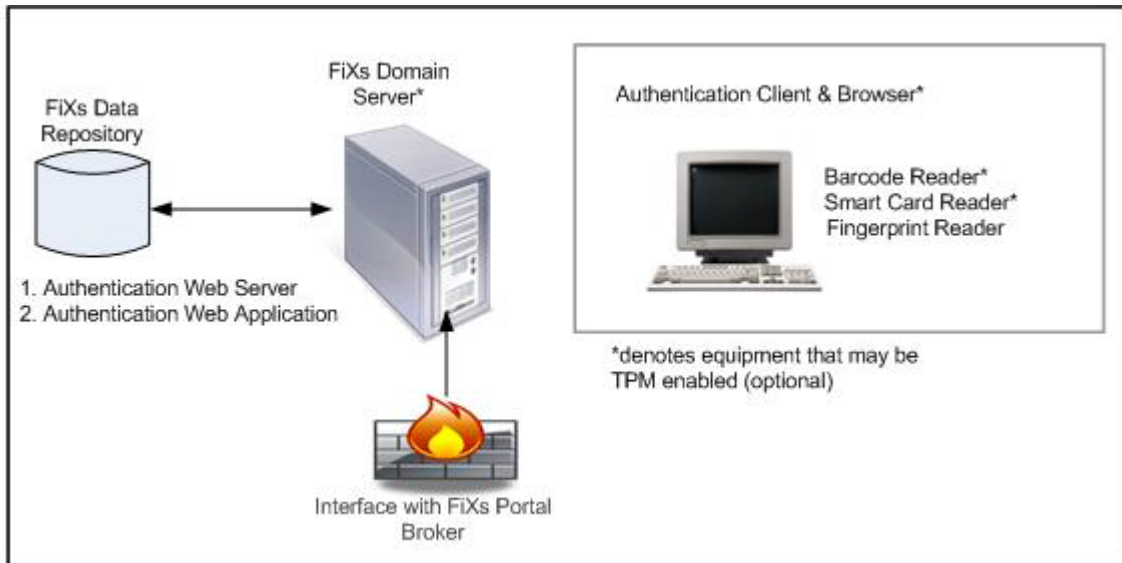


Figure 2: Credential Issuing System

1.2.5 RELYING PARTY OPERATIONAL REQUIREMENTS

The Relying Party system serves to originate Authentication Inquiries for FiXs Participants visiting the Relying Party's sites. The hardware and software requirements associated with this function are described in the sections that follow. See Figure 3: Relying Party System Requirements.

1.2.5.1 Relying Party Authentication Site Certification Requirements

Authentication Sites must be certified according to the procedures established by the FiXs Implementation Guidelines. The Facility Domain Administrator is responsible for ensuring that these procedures are followed and that all relevant documentation and checklists are signed, certified and remitted to DoD. (For the POC, certification is not required.)

1.2.5.2 Relying Party Authentication System Requirements

This section describes the system requirements for Relying Parties.

1.2.5.2.1 Authentication Client

The **Authentication Client** is a PC with a standard Web browser for access to the FDS. Each client will contain an embedded site ID file and a set of drivers for a bar code reader, a smart card reader, and a fingerprint reader.

1.2.5.2.2 Authentication Web Server

The **Authentication Web Server** is a standard web server (which resides on the FDS) that processes Authentication Inquiries and Responses between the Authentication Client and the FiXs Trust Broker and the Relying Party's FDS.

1.2.5.2.3 Authentication Web Server Application

The **Authentication Web Server Application** receives the ID credential information from the Client and returns identity information and fingerprint data for matching on the Client.

1.2.5.2.4 Fingerprint Reader for Authentication

The Authentication system must include a **Fingerprint Reader** in accordance with the *FiXs Technical Architecture and Specifications*. (Devices compliant with the software and drivers are listed in the *FiXs Technical Architecture and Specifications*.)

1.2.5.2.5 Smart Card Reader for Authentication

The Authentication system must include a **Smart Card Reader** in accordance with the *FiXs Technical Architecture and Specifications*. (Devices compliant with the software and drivers are listed in the *FiXs Technical Architecture and Specifications*.)

In order to support full interoperability with existing DoD CAC cards, FiXs Smart Card Readers and Writers should be compliant with current DoD CAC card standards; as of this writing, the current standard is Government Smart Card (GSC) Interoperability Specification (IS) version 2.0.

1.2.5.2.6 Bar Code Reader

The Authentication system may include a **Bar Code Reader** in accordance with the *FiXs Technical Architecture and Specifications*. (Devices compliant with the software and drivers are listed in the *FiXs Technical Architecture and Specifications*.)

1.2.5.2.7 Pin Pad

The Authentication System must include a device that enables a Participant to enter his or her Personal Identification Number (PIN) as part of the authentication process for a CAC or similar card.

1.2.5.2.8 Driver's License/Passport Reader

The Authentication System must include a device that is capable of validating the authenticity of a Participant's driver's license or passport.

1.2.5.2.9 Authentication System Performance Requirements

The Authentication System must be operational 24 hours a day, 7 days a week, with an up-time availability of 99%.

1.2.5.2.10 Trusted Computing

In order to achieve higher levels of trust, assurance and security, interested FiXs members may (optionally) employ enrollment and/or authentication client machines with a hardware-based Trusted Platform Module (TPM) device. Such TPM devices are

implemented in accordance with open specifications, as defined by the Trusted Computing Group™.

For peripheral devices, such as trusted smart card readers/writers, fingerprint readers, keyboards, and secure PIN entry devices, there are even more secure, high assurance, trusted path devices that may be implemented, which offer an additional layer of trust, especially in sensitive or classified environments. Such devices are offered by a number of vendors and manufacturers, some of which are existing FiXs member companies.

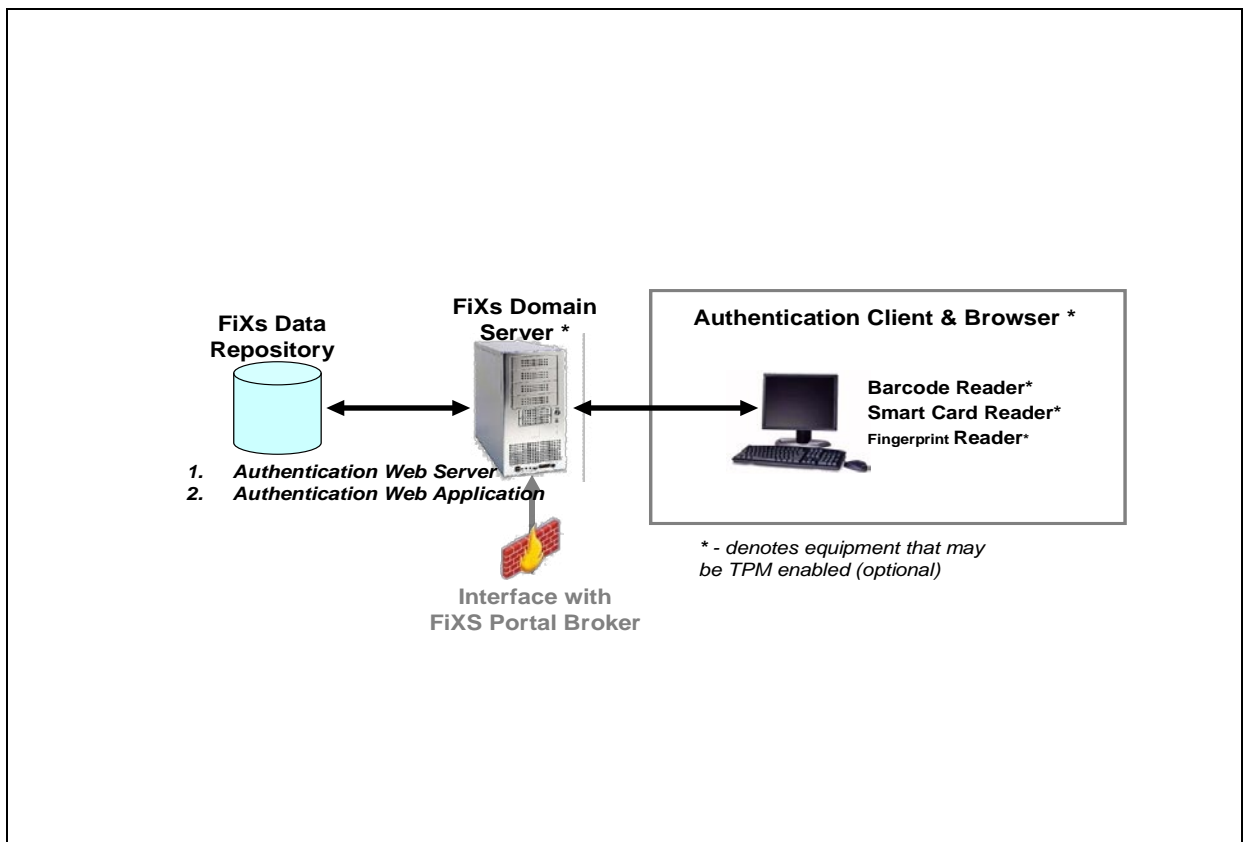


Figure 3: Relying Party System Requirements

1.2.6 MEMBER SERVICE PROVIDER REQUIREMENTS

A Member Service Provider (MSP) is a FiXs Founding Member that has agreed to provide equipment procurement and management services to FiXs Issuers and/or FiXs Relying Parties. In its role as MSP, designated Founding Members will

supply domain servers, enrollment equipment and authentication equipment (including required peripherals) to FiXs Issuers and Relying Parties that request these services. MSP services include equipment procurement, delivery and deployment; inventory management; equipment certification; equipment configuration; and documentation. Optionally, MSPs may also provide local application development and integration as well as consultative services to FiXs Issuers and Relying Parties.

1.2.7 RECORDS/FILES MAINTENANCE REQUIREMENTS

This section describes FiXs requirements for records and file maintenance.

1.2.7.1 FiXs File Updates

Credential Issuers are responsible for maintaining updated FiXs files including Enrollment Files, Control Files, Administrative Files, Revocation and Audit Files. These files must be updated and maintained by the FiXs Member Organization in a timely manner.

In some cases, such as the Control Files and certain Administrative Files, updates may be electronically communicated by the FiXs Trust Broker to the Credential Issuer's FDS server/s. It is the responsibility of the FiXs Issuer to ensure proper firewall connectivity, in order to receive, accept, process, and internally disseminate (if necessary) these updates.

1.2.7.2 Notification of Revocation of FiXs Status/Dis-Enrollment

A Credential Issuer must maintain a near-real-time list of participants that it has enrolled into the FiXs System. When an employee leaves a Sponsor or when a Sponsor's Program Manager revokes a Participant's authorization for FiXs participation, the Sponsor must notify the Credential Issuer in sufficient time to ensure that the participant is dis-enrolled and the FDS updated within three (3) hours.

For changes in employee status, such as change of name, termination, ineligibility, or other changes as noted in The Privacy Act of 1974, the FiXs Credential Issuer must complete the updates (including any revocation of credentials, if necessary) within three (3) hours.

Dis-enrolling a FiXs participant means that his or her identifier is no longer valid, and that all subsequent authentication attempts should result in a failure. The Relying Party shall be responsible for the actions of any participant who is granted access after the participant was successfully dis-enrolled in accordance with these Rules and the Relying Party received the appropriate message in response to an authentication request.

While the reason for any dis-enrollment may be provided to the FiXs Domain Administrator, such reason shall not be transmitted to the Authentication Station. All dis-enrollments shall be accomplished at the participant's FDS and shall be performed by the Facility Administrative

Enroller or a Facility Enroller. A Facility Verifier is not allowed to perform a dis-enrollment operation.

1.2.7.3 Audit Requirements

This section describes the auditing requirements for a FDS.

1.2.7.3.1 System Audits

Auditing of the FDS must be at a sufficient level to recreate any transaction successfully or unsuccessfully performed within the FiXs system. The software provided by the FiXs program will record the data to a level that is sufficient to satisfy these requirements.

2 CREDENTIAL ISSUER RESPONSIBILITIES

This Section describes the responsibilities for Credential Issuers in initiating and maintaining an **operational** FiXs system. FiXs Credential Issuers issue FiXs-Compliant Credentials to qualified users for themselves and/or other Sponsors, whether a Primary Trusted Organization or a Subscribing Party, and processes and responds to *Authentication Inquiries*. An Issuer Sponsor is a Credential Issuer that issues credentials to its own employees or sponsors other Credential Issuers and performs some or all of the Credential Issuer duties defined herein that the sponsored Credential Issuer chooses not to perform. In this case, the Issuer Sponsor assumes some or all of the following functions on behalf of the sponsored Issuer: enrollment and issuance; participant records management; FiXs domain server management; standards and specifications compliance; transaction processing; application integration; and coordination of human resources and security departments.

Credential Issuers shall have primary responsibility and liability for performance of the obligations of a Credential Issuer under these Rules, regardless of whether the obligations are performed by the Credential Issuer, Issuer Sponsor or a third party on behalf of the Credential Issuer. No delegation of duties by a Credential Issuer to an Issuer Sponsor or any other third party shall relieve such Credential Issuer of its liability for performance of such duties hereunder. The legal agreements process that binds FiXs member organizations are depicted in Figure 1.1.

There is a distinction to be made between credentials and a badge. **Credentials** refer to the representations of an individual's identity -- such as biometric images, photographs, and unique identifiers (social security numbers or employee IDs) – that are approved by an organization to authenticate an individual for access. A **badge** or **token** can either 1) “hold” these credentials (such as a photo on the face of a badge or a biometric on a bar code) or 2) hold the “keys” or “pointers” to the credentials that are accessible in a record on a remote system (such as a number stored on a bar code that identifies the system and the record); the credentials can be downloaded to a local client.

Note that as the issuer of the CAC card, DoD is exempt from Section 2.1, *Credential Issuance* because CAC holders are automatically enrolled to the DCCIS system without any alterations to the CAC credential and identifier.

2.1 Credential Issuance

The ***Credential Issuance*** process consists of four steps: 1) validate applicant's need for FiXs credentials; 2) verify applicant identification; 3) enroll applicant into FiXs system; and 4) issue or record Participant's valid FiXs identifier. These steps are described in the section that follows.

2.1.1 VALIDATE APPLICANT'S NEED FOR FiXs CREDENTIALS

As a requisite for starting the FiXs credential issuance process, the Facility Verifier must receive a request in writing from the sponsoring FiXs Program Manager, or his/her designated agent on behalf of the applicant.

2.1.2 VERIFY APPLICANT IDENTIFICATION (VETTING/IDENTITY PROOFING)

Verifying the applicant's identification is the process by which the Credential Issuer validates the identity information provided by the Applicant. This process must be completed for all FiXs Applicants regardless of whether the same or similar documentation has been verified as part of the organizations' regular employment process. This process can also be referred to as "Vetting" or "Identity Proofing."

2.1.3 VERIFICATION PROCESS REQUIREMENTS

The identity proofing, registration and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a credential without the cooperation of another authorized person.

2.1.3.1 Verify Employee's Identification

The Facility Verifier must verify the applicant's identification per the procedures prescribed below.

2.1.3.1.1 FiXs Member Participant Applicants

Upon validation of an Applicant's need for FiXs credentials, the Credential Issuer is required to fulfill application requirements specified in FiXs Guidelines:

2.1.3.1.1.1 AUTHENTICATE DOCUMENTS

The Facility Verifier must validate a Social Security Number or an Alien Registration number in addition to other presented documents and electronically verify the authenticity of the ID documents. If the Social Security Number or the Alien Registration number and one other form of identification cannot be electronically validated, the participant cannot be enrolled in the FiXs System. Electronic verification shall be accomplished via a commercially available means that uses an encoding reading device authorized by FiXs. The device shall validate that the documents are not counterfeit and have not been altered and shall display the appropriate machine

readable data.

**2.1.3.1.1.2 AUTHENTICATE APPLICANT USING A
KNOWLEDGE-BASED AUTHENTICATION SERVICE**

The Credential Issuer must access a Knowledge-Based Authentication Service authorized by FiXs that provides on-line look-up from multiple databases to generate a series of random questions that only the true person who owns the identity can answer. The Applicant answers the questions and the Document Verification Service returns an answer to the Facility Verifier indicating whether the applicant has successfully answered the questions. (This procedure must be performed with the Applicant present.)

To comply with this rule, the Member Organization must have Encoder Reader Devices and must subscribe to a Document Verification Service. See *FiXs Technical Architecture and Specifications*.

**2.1.3.1.1.3 COLLECT AND STORE APPLICANT
BIOMETRIC(S)**

The Facility Verifier will capture the Applicant's digitized photo, collect, and store fingerprints to bind the identification documents to the Applicant's biometrics for the first time. The Facility Verifier must collect the applicant's fingerprints using the 10-fingerprint system at a Fingerprint Capture Station that complies with *FiXs Technical Architecture and Specifications* for fingerprint capture and storage and store the record.

**2.1.3.1.1.4 ELECTRONICALLY STORE APPLICANT'S
SOURCE DOCUMENTS**

Documents that are verified to complete the I-9 Form must be electronically stored either by: 1) scanning the documents or 2) retaining an electronic version of the document that is otherwise available.

2.1.3.1.1.5 CERTIFY AUTHENTICATION PROCESS

Either on the I-9 Form or as an attachment, the Facility Verifier will include and electronically sign the following statement: "Addendum to Certification, Section 2: I also attest, under the penalty of perjury, that I have examined the photo identification document presented by the employee and that to the best of my ability I conclude that the photographic image and the employee are one in the same individual."

2.1.3.1.1.6 COMPLETE NATIONAL AGENCY CHECK

The Facility Verifier must have a background check conducted on the Applicant, which, at a minimum, must include a National

Agency Check (NAC) in accordance with DoD Directive 5200.2-R Personnel Security Program. A NAC that has been conducted within four years will satisfy the requirements contained in this subparagraph, and a new NAC does not have to be conducted.

The process shall ensure completion and successful adjudication of a National Agency Check (NAC) and National Agency Check with Written Inquiries (NACI). A completed NAC is sufficient for interim credential issuance; however, the NACI must still be completed within six (6) months of the application date. The credential shall be revoked if the results of the investigation so justify. If the NACI is not completed within six (6) months, the NAC will be deemed revoked. A new NAC must be completed if the NAC will expire within six (6) months of the application date.

Note that this requirement may also be satisfied by locating and referencing a completed and successfully adjudicated NACI.

2.1.4 ENROLL APPLICANT INTO FiXs SYSTEM

Once the Applicant's identity has been verified, he or she can be enrolled into the Credential Issuer's FDS. This process makes the Applicant's (now a FiXs Participant) record of credentials available for retrieval by a Relying Party for authentication. The Enrollment process is described in the sections that follow.

2.1.4.1 Verify Applicant's Reference Biometric

The Facility Enroller instructs the Applicant to scan his biometric and initiates a biometric verification check. If there is a positive match, the Facility Enroller proceeds to the next step. (If the Identity Proofing – Section 2.1.2 – and Enrollment – Section 2.1.4 – are performed at the same time, this step can be omitted.)

2.1.4.2 Enroll Applicant into FiXs FDS System

Enrolling an applicant refers to the creation of a valid FiXs Participant record in the FiXs Data Repository. All FiXs Participants must be enrolled (have a valid record) in the Issuer's FiXs Data Repository. To enroll a new employee as a FiXs Participant, the Facility Enroller must collect the required enrollment ID data as prescribed in Section 2.1.3.

2.1.4.2.1 Create a New Participant Record

The Facility Enroller creates a new record for the Applicant in the FiXs Data Repository and performs the following steps:

2.1.4.2.1.1 ENTER REQUIRED APPLICANT DATA

The Enrollment Operator enters the Applicant's first and last

names, ORGANIZATION name; and, Employee ID number into the record. (See *FiXs Technical Architecture and Specifications* for details.)

2.1.4.2.1.2 UPLOAD FiXs ENROLLMENT ID DATA INTO APPLICANT'S RECORD

The Facility Enroller uploads the Applicant's Photograph File and Biometric File of the Applicant's fingerprints taken during the vetting/identity proofing process to the Applicant's record.

2.1.5 ISSUE PARTICIPANT VALID FiXs IDENTIFIER

The final step in the Credential Issuance process is to issue the Participant a valid FiXs Identifier that can be used to access the Participant's credentials. Valid identifiers include:

2.1.5.1 DoD EDI PIN for CAC Cardholders

The DoD EDI PIN (as the DoD's Employee ID) associated with the CAC card with the selected organization (e.g., Army, Navy, etc.) is a valid FiXs identifier.

2.1.5.2 Organization Name and Employee ID for non-CAC Cardholders

The combination of the Participant's Member/Organization Code and ID and organization-assigned Employee ID number is a valid FiXs identifier.

2.1.5.3 Identifier Access Method

The Authentication Station Operator must be able to access the valid FiXs identifier to initiate the authentication process. The Participant can provide the Authentication Station Operator access to the identifier in one of four ways:

2.1.5.3.1 No Token/Verbal Communication of Organization and Employee ID

The Participant can verbally provide the Authentication Station Operator with the Member Organization name (from which the ID is obtained) and Employee ID number.

2.1.5.3.2 Presentation of Company/Organization Badge

The Participant can present the Authentication Station Operator with a Company or Organization Badge from which the valid FiXs identifier can be read visually or by machine (e.g., all valid Barcode 39 codes can be scanned and sent in their entirety to a FiXs member organization as a credential string). (See *FiXs Technical Architecture and Specifications*.)

2.1.5.3.3 Presentation of FiXs Badge

The Participant can present the Authentication Station Operator with a FiXs Badge (organizations can opt to issue separate FiXs badges rather than use the existing employee badge) from which

the valid FiXs identifier can be read visually read or by machine.

2.1.5.3.4 DoD EDI PIN for CAC Cardholders

The DoD EDI PIN (as the DoD's Employee ID) associated with the CAC card with the selected organization (e.g., Army, Navy, etc.) is a valid FiXs identifier.

2.1.5.4 Expiration Date

All credentials must have an expiration date. A revocation process must exist such that an expired or invalidated credential is swiftly revoked.

2.1.6 APPEALS PROCESS

Credential Issuers shall maintain an appeals process for employees who are denied a credential or whose credentials are revoked.

2.2 Transaction Request Processing

The Credential Issuer is required to process Authentication Inquiries from its Authentication Clients and from Relying Parties. An **Authentication Inquiry** is an electronic transaction originating either from 1) the Issuer's Authentication Client or 2) a Relying Party (through the FiXs Trust Broker), which requests the authentication of a credential and credential holder. The Credential Issuer must return an Authentication Response to the originator of the Authentication Inquiry. An **Authentication Response** is a reply from the Credential Issuer to an Authentication Inquiry that sends a denial or transmits credential information (photo and fingerprints) to the Relying Party.

2.2.1 PROCESSING AUTHENTICATION INQUIRIES

When a Credential Issuer receives an Authentication Inquiry from an Authentication Client (either its own or from that of a Relying Party), the Credential Issuer's FDS checks that the credential information matches a valid record in its FiXs Data Repository. If it does, an Authentication Response is prepared and sent back as described below.

2.2.2 INITIATING AUTHENTICATION RESPONSES

The Credential Issuer's FDS retrieves the applicable files, as specified in the appropriate FiXs Guidelines, creates a valid XML Authentication Response message and transmits it back to the Authentication Client.

3 SPONSORING ORGANIZATIONS INTO THE FIXS NETWORK

Primary Trusted Organizations (PTO) and/or Subscribers are known as "Sponsors". They sponsor individual users who are employees or contractual agents of the Sponsor to receive a FiXs-certified credentials and into the FiXs Network by assuming responsibility for the acts and omissions of the Participants they sponsor.

3.1 Vetting

Any organization applying to be a PTO or Sponsor must be vetted by a FiXs-Approved Vetting Organization.

3.2 Sponsorship of Employees

To sponsor an employee and/or contractual agent to receive a FiXs-certified credential and into the FiXs Network, the Sponsor must assert in writing to the Credential Issuer that its employees, contractual agents, or other users have a bonafide need a FiXs-Certified Credential. The Sponsor must indemnify FiXs and FiXs Member Organizations that provide services in support of FiXs, for the acts and omissions of the applicants it sponsors through the execution of a Terms of Use Agreement.

3.3 Adhere to FiXs Foundational Documents

Sponsors must abide by the Terms of Use Agreement, adhere to the governance framework as provided for in the FiXs Foundational Documents, and adhere to the seven-step credential management process outlined in the Trust Model.

3.4 PROCESS FOR ENABLING SPONSOR ORGANIZATIONS

In accordance with FiXs' agreements for populating the metadata tables to inter-operate with the DCCIS Gateway Broker and the FiXs Trust Broker, updated versions of the FiXs Assigned Commercial Organization Codes table will be provided to the Department of Defense (DoD) on a regular basis. The criteria for providing these updated are as follows:

1. All firms who apply for FiXs membership will be subject to the standard FiXs organizational vetting process.
2. Upon successful adjudication of the vetting process FiXs and acceptance into membership in FiXs, a unique organizational code will be assigned and maintained in a local FiXs database.
3. FiXs will then query the newly vetted company and ascertain if they have a need/requirement to have FiXs-certified credentials issued to their employees and/or contractual agents.
4. If the company respond affirmatively and intends to have FiXs-certified credentials issued to their employees and/or contractual agents, they will be asked to sign the FiXs standard "Terms of Use Agreement". This agreement is a legal document which compels the company to abide by all the FiXs operating rules; policies; standards; security requirements; and audit procedures.
5. Upon the proper execution of this document, FiXs will then notify DoD via formal letter entitled, "FiXs Assigned Commercial Organizational Codes," and request DoD coordination on adding the company's organization code to the metadata table.
6. DoD will turn around the request within 72 hours.
7. FiXs will load the Organization Codes in the FiXs Trust Broker and DoD will load the Organization Codes in the DCCIS Trust Broker and then the next time the Brokers synch, the updates will be reflected in both tables.
8. FiXs will maintain a repository of all executed Terms of Use Agreements and DoD will have access to that repository.

9. The Terms of Use Agreements will be subject to audit and process review by both the FiXs audit team and the DoD audit team.
10. This process is to be set forth in the MOU between DoD/DMDC and FiXs.
11. All companies are subject to the described process before FiXs will notify and coordinate with DMDC on updates to the metadata tables.
12. FiXs also maintains a process of assigning a unique system that is comparable to a FASC-N code for all FiXs-certified credential issuers. These codes will be assigned sequentially.

4 RELYING PARTY RESPONSIBILITIES

FiXs Relying Parties are responsible for electronically authenticating FiXs Participants who visit their facilities. This chapter describes the responsibilities of Relying Parties in the FiXs system.

4.1 Visitor Transaction Processing

In the FiXs System, the Relying Party will be responsible for initiating and processing the transactions that will authenticate the FiXs Participant.

4.1.1 CREDENTIAL VALIDATION AND TRANSACTION ROUTING

The processing or re-routing of a transaction to the FiXs Trust Broker is determined at the Relying Party's FDS. When compiling an Authentication Inquiry, the software determines whether it is a home or remote transaction and transmits the Inquiry either to its FDS or to the FiXs Trust Broker for routing to the appropriate Member's FDS. A **Home Transaction** refers to an Authentication Inquiry that is processed at the same FDS as the originating Relying Party. In this case, the employee is being authenticated at an employee facility. A **Remote Transaction** refers to an Authentication Inquiry that is routed through the FiXs Trust Broker to be processed at a FDS other than of the originating Relying Party. In this case, the employee is a visitor to the location of the Authentication Station. The credential validation is processed as described in the sections that follow:

4.1.1.1 Initiating Authentication Inquiry

When a visitor arrives, the Authentication Station Operator asks whether the individual is a FiXs member. If yes:

4.1.1.1.1 Enter Data to FiXs Application

The Authentication Station Operator selects the visitor's home organization on the first FiXs screen. The system displays instructions as to what data to enter or which credentials to use for authentication. Depending on the level of the credential being read, the Authentication Station Operator will be instructed to perform one of the following procedures:

4.1.1.1.1 READ BAR CODE DATA

The Authentication Station Operator inserts the token/badge into the bar code reader, which reads the ID number and transmits it as a string of data to the FDS.

4.1.1.1.2 READ CAC CHIP DATA

The Authentication Station Operator inserts the CAC card into the smart card reader. The FiXs Participant enters his/her PIN using either a PIN pad or keyboard and a string of data is extracted from the card chip and sent to the FDS.

4.1.1.1.3 REQUEST EMPLOYEE ID NUMBER

The Authentication Station Operator will be required to request and enter the employee's ID number into the Authentication Web Application Software.

4.1.1.2 Transaction Routing

Using the organization data selected, the Authentication Inquiry with the credential information can be routed to the record-holding FDS. A transaction is a "home" or "remote" transaction as described below.

4.1.1.2.1 Home Transactions

If the Authentication Client determines that a request can be processed internally, this is a Home transaction. In this case, the Relying Party's FDS processes the transaction in the same manner as described below in Section 3.1.2; however, the transaction is locally processed and no data is transmitted to the FiXs Trust Broker.

4.1.1.2.2 Remote Transactions

If the Authentication Client determines that a request cannot be processed internally based on the selected organization code, it then creates an Authentication Inquiry and forwards it to the FiXs Trust Broker for processing as per Section 3.1.2 below.

4.1.2 PROCESSING AUTHENTICATION RESPONSES

Based on the information the Authentication Station Operator submits during the visitor intake process, the system will return instructions to perform one or more of the following transactions to authenticate the individual.

4.1.2.1 Complete Credential Holder Authentication

To complete an authentication transaction, the Authentication Station Operator must perform one or more of the following operations.

4.1.2.1.1 Visual Comparison of Downloaded Photo to Badge Holder

The Authentication Station Operator visually compares the photo transmitted from the server or downloaded from the card to the Badge Holder/Visitor. The Operator enters the results of the visual match onto the Authentication Client application.

4.1.2.1.2 Biometric Scan and Comparison

The Authentication Station Operator instructs the visitor to initiate a biometric scan using the fingerprint reader. The system performs a comparison against the downloaded biometric and indicates the results of the comparison on the Authentication Client.

4.1.2.2 Determine Access Authorization

Based on the results of the authentication process, the Authentication Stations Operator decides whether the FiXs Participant will be offered access based on local operating procedures. The Authentication Station Operator shall enter his or her decision into the Authentication Station and the decision shall be recorded in the system Audit Log. Note that the FiXs authentication process does not automatically authorize access; it is only an authentication procedure. Access decisions will always be left to the discretion and procedures established at the Relying Party's organization.

4.2 Exception Processing

Exception Processing refers to the procedures that will be followed when the FiXs System as per the normal procedures described in these Operating Rules cannot authenticate a credential or participant. The requirements for addressing these conditions are described in the section that follows.

4.2.1 BADGE/TOKEN-NOT-PRESENT

In the event that an individual claiming to be a FiXs Participant requests entry to a FiXs Member facility but does not have a badge or token, the Authentication Station Operator will ask for the individual's company name and Employee ID number and continue with the normal authentication procedures as described in Section 3.1.1.1.

4.2.2 OTHER EXCEPTIONS

In the event that an individual claiming to be a FiXs Participant cannot be authenticated by means of a FiXs Authentication Inquiry/Response, then the individual cannot be admitted as a FiXs Member and the entry admittance process can no longer be considered a FiXs Transaction. In such cases, the Relying Party Organization may choose local security processes and procedures to allow or deny admittance. Such exception conditions can include, but are not necessarily limited to: unrecognized participant, unreadable badge/token and inability to reach an employer's FDS (issuer system down, FiXs Trust Broker down, relying party system down, etc.).

5 FiXs TRUST BROKER RESPONSIBILITIES

This Section describes the responsibilities of FiXs Trust Broker in the FiXs System. Serving as the operation intermediary between the Credential Issuers and Relying Parties, the FiXs Trust Broker is responsible for management and administration of the FiXs broker function as well as the day-to-day operations of the FiXs Trust Broker including system administration. These requirements are described in the sections that follow.

5.1 System Administration Requirements

This section describes the system administration requirements associated with the FiXs Trust Broker.

5.1.1 DESIGNATE FiXs TRUST BROKER SYSTEM ADMINISTRATOR

Any organization that has a Trust Broker that Connects to the FiXs Trust Broker must designate an Administrator for the FiXs Trust Broker. The System Administrator shall be responsible for the tasks described in Sections 5.1.2 and 5.1.3.

5.1.2 MEMBER INTERFACE MANAGEMENT

The FiXs Trust Broker Administrator is responsible for configuration management of the FiXs System communications and interfaces.

5.1.3 MAINTENANCE OF CONTROL DATA

The FiXs Trust Broker Administrator is responsible for maintaining a set of control tables that is used to share and update FiXs Member organization names, characteristics, and list of acceptable tokens. In this role, the FiXs Trust Broker must update the control tables upon activation of new FiXs Member Organizations; de-activation of existing FiXs Member Organizations and Participants; and changes submitted by existing FiXs Member Organizations and Participants. Control table changes are transmitted to all FDSs on a regular and frequent basis. Upon receiving changes to the control tables from FiXs Members, the FiXs Trust Broker must update them as soon as possible, but no later than 24 hours after receiving the changes.

5.1.4 ACTIVATION AND DE-ACTIVATION OF FiXs DOMAINS

Upon authorization of the Administrator of connecting Trust Brokers, the FiXs Trust Broker Administrator will activate and de-activate FDSs from the Trust Broker.

5.1.4.1 Initiation of Domain Enrollment Process

For security purposes, Domain Enrollment Process Initiation begins with the Member's official representative signing the trading partner agreement using a "chain-of-trust" process linked to the Member's first system enroller. Membership in the FiXs System is initiated when a senior management representative of the applying Member Company or organization signs a trading partner agreement with the Operating Entity. (For the POC and pilot, the Operating Entity is the DMDC.) A letter is sent to the Operating Entity (DMDC) by the authorized representative

appointing two individuals from the company or organization to serve as the Domain Technical Administrator and the first Facility Enroller.

The Operating Entity sends an Authorized Agent to the company location to officially open the FDS and to witness the initial enrollees being entered into the FiXs System. (This Authorized Agent's credentials were included on the application prior to delivery to the company or organization.) At the same time, the credentials of the Authorized Agent are removed from the FDS. This process is certified on paper by the Authorized Agent and the company/organization representative and is placed in the audit files of the new Member and of the Operating Entity.

Refer to the *FiXs Technical Architecture and Specifications* regarding key management associated with this Initiation of Domain Enrollment Process.

5.1.4.2 Activation of FiXs Domains

For new FiXs Members, a FDS ID will be assigned to the new FDS and entered into the system along with contact and control information. The control information will then be transmitted to other FDSs. Upon receiving notification of activation of a new Participant, the FiXs Trust Broker Administrator must update the Control Tables as soon as possible, but no later than three (3) hours after receiving the notification.

5.1.4.3 De-Activation of FiXs Domains

For dis-enrollment of FiXs Member Organizations, the FDS ID will be de-activated in the FiXs system and contact and control information removed. Notification of de-activation will then be transmitted to the remaining FDSs.

5.1.4.4 Dis-Enrollment, Reinstatement and Re-Enrollment of Participants

Upon receiving notification that a Participant is no longer eligible to be included in FiXs, the FiXs Trust Broker Administrator must dis-enroll them as soon as possible, but no later than three (3) hours after receiving the notification.

Upon receiving notification that an employee who was formerly enrolled in the system is again eligible for enrollment, the Facility Enroller can reinstate the employee into the FiXs Data Repository without conducting the identity vetting process specified under 2.1.2, Verify Applicant Identification (Vetting/Identity Proofing), provided the reinstatement occurs within twelve (12) months of dis-enrollment.

If an employee becomes eligible for enrollment twelve (12) months after dis-enrollment, the employee must be re-enrolled in accordance with Section 2.1.3.

5.1.5 SYSTEM PERFORMANCE REQUIREMENTS

The FiXs Trust Broker must be operational 24 hours a day, 7 days a week, with an up-time availability of 99.99%. Authentication Inquiry Transactions must be transmitted to the Credential Issuing FDS in no more than 2.5 seconds. Authentication Responses must be processed and transmitted to the Relying Party in no more than 2.5 seconds.

5.2 Transaction Processing and Routing

The FiXs Trust Broker must route and process transactions between FiXs Credential Issuers and Relying Parties. The FiXs Trust Broker receives Authentication Inquiries from Relying Parties and transmits them to Credential Issuers for processing. It then receives the Authentication Responses and relays them back to the appropriate Relying Parties. In addition, the FiXs Trust Broker Administrator performs control data transactions. Refer to the *FiXs Technical Architecture and Specifications* for transaction/message format and encryption requirements.

5.2.1 AUTHENTICATION INQUIRIES

When a transfer is sent from a Relying Party to the FiXs Trust Broker requesting authentication of a FiXs Participant of a Remote Credential Issuer, the FiXs Trust Broker: 1) decrypts the header to determine the FDS destination; 2) validates the digital signature of the originating FDS; 3) adds FDS control data to the transfer and re-encrypts it; and 4) transmits it to destination FDS.

5.2.2 AUTHENTICATION RESPONSES

When a Remote Credential Issuer returns an Authentication Response, the FiXs Trust Broker: 1) decrypts the transfer; 2) adds FDS control data to the response and re-encrypts it; and 3) transmits the response to the Relying Party.

5.2.3 AUDIT CONTROL DATA TRANSACTIONS

The FiXs Trust Broker must notify FDS domains of control table updates by: 1) updating the internal Control Date and Time that accompanies all transfers, and 2) responding to FiXs Control Data Requests with a FiXs Control Data Response that updates control data and resets the Control Date and time in the FiXs domain.

6 SECURITY REQUIREMENTS

6.1 General Security Requirements

Each Participating FiXs organization, shall comply with the *FiXs Security Guidelines*, which specify procedures to prevent unauthorized access or misuse of any FiXs related component including hardware, software, peripherals, data, system components, network, security keys, credentials and documentation. The *FiXs Security Guidelines* are hereby incorporated by reference.

6.2 Infrastructure Requirements

The FDS must be capable of supporting HTTPS (SSL) protocol. The Member Organization's network and firewall must be configured to allow HTTPS incoming and outgoing transmissions, with outgoing transmissions being limited to the FiXs Trust Broker. In addition, the FDS must be placed within the Organization's firewall. For additional details, please refer to the *FiXs Technical Architecture and Specifications* and the *FiXs Security Guidelines*.

6.3 Audit Requirements

Each participating organization is responsible for maintaining complete and up-to-date records of events related to the FiXs Network. FiXs transactions must be re-creatable from start to finish including identification of the individual(s) performing the transaction. Event logs and transaction audit data will be held indefinitely by each participating organization or until directed otherwise via direction from the FiXs Program Manager. FiXs event logs will be maintained in a secure manner and made available for reference from an authorized Government official.

Note that installing the FiXs application software ensures compliance with the minimum level of FiXs auditing requirements.

6.4 Security Authorizations

6.4.1 GENERAL

Authority to access any FiXs system component is based upon the required functions associated with the employee's position. Below are functions attributed to specific functions/positions within the FiXs domain that require authorized access.

Note that there can be no duplication in the following roles: 1) the Domain Program Manager cannot serve as either a Facility Enroller or Facility Verifier, and 2) Facility Enrollers and Facility Verifiers must always be separate personnel.

6.4.2 DOMAIN TECHNICAL ADMINISTRATOR

The Facility Domain administrator is authorized to:

- initialize a FiXs domain for enrollment according to the procedures described in Section 4.1.4.1 and authorize the participating organizations initial participants;
- perform all software maintenance and trouble shooting functions. This includes system configuration, network connectivity, database initialization, and installation of Server and client components and peripherals;
- install operating system patches, FiXs software and COTS patches; and
- operational and troubleshooting procedures of the local system components, FiXs Domain Server FiXs Clients and FiXs Data Repository.

6.4.3 DOMAIN FUNCTIONAL ADMINISTRATOR

The Domain Administrative Enroller is authorized to:

- enroll and train Facility Administrative Enrollers.

- authorize applicants to receive FiXs credentials or to designate other individuals within the facility authorize applicants.

6.4.4 FACILITY DOMAIN ADMINISTRATORS

The Facility Domain Administrator is authorized to enroll, train and certify Authentication Station Operators.

6.4.5 FACILITY ADMINISTRATIVE ENROLLER

The Facility Administrative Enroller authorized to enroll, train and certify Facility Enrollers.

7 LIABILITIES AND INDEMNIFICATION

This Section describes the liabilities associated with participation in the FiXs System.

7.1 Liability under these Rules

These Rules are made solely and specifically among and for the benefit of Members and Participants. No Person who is not a Member or a Participant shall have any rights, interest or claims under these Rules or be entitled to any benefits under or on account of these Rules, whether as a third party beneficiary or otherwise. A Member or Participant shall have no liability for violation of these Rules to any person who is not a Member or a Participant and the liability of a Member or Participant to any other Member or Participant for any violation of these Rules shall be strictly limited to any remedy or liability provided in Subsection 6.2.

7.2 Liability to Members and Participants

A Member or Participant shall be liable to another Member or Participant for a violation of these Rules to the extent that such liability is provided for under a contract or agreement between individual Members or Participants, all as modified under Subsection 8.1.2 of these Rules, or is provided for under other law, including the SAFETY Act (Pub. Law 107-296) or other applicable federal law.

8 PRIVACY

8.1 Privacy

Member Organizations must comply with the Privacy provisions of the *FiXs Policy*, which is hereby incorporated by reference.

9 FIXS GOVERNANCE

The Federation for Identity and Cross-Credentialing Systems (FiXs) is the legal and business entity that manages Member Partnership Agreements and maintains the FiXs Foundational Documents. FiXs shall develop membership criteria, voting procedures, and an Operating Rules Committee for the updating of these Operating Rules. The FiXs Bylaws shall

also set forth the protocol for establishing a Board of Directors, Committees and official meetings.

This Section describes the business requirements and responsibilities of the operating entity

9.1 FiXs Business Requirements

9.1.1 ESTABLISH FiXs MEMBER PARTNERSHIP AGREEMENT(S)

An organization seeking membership in FiXs is required to enter into an agreement with FiXs. By this agreement, the Member Organization agrees to comply with the FiXs Operating Rules and other documents incorporated herein by reference.

9.1.2 EFFECT OF RULES

To the extent that individual Member Organizations have agreed to be bound by these Rules and have entered into, or enter into, a contract or agreement between such Members where the performance of the contract or agreement will involve these Rules or credentials issued under these Rules, these Rules will serve as a supplement to the contract or agreement as if these Rules were fully set forth in the contract or agreement. To the extent that there is a conflict between the terms of the contract or agreement and these Rules, between the parties to the contract or agreement, the terms of the contract or agreement shall control. With respect to all other parties these Rules shall control.

9.2 Public Statements

Unless the consent of the Operating Entity is first obtained, Participants shall not in any manner advertise or publish or release for publication any statement regarding the FiXs project.

10 MEMBERSHIP APPROVAL, AUTHORIZATION TO OPERATE AND COMPLIANCE MONITORING

10.1 Summary

This chapter explains the process for vetting and accepting members and for certifying members to perform roles defined in these Rules. The process for Founding Members is depicted in Figure 9.1. The process for new members is depicted in Figure 9.2.

10.1.1 Membership Process

Founding members in good standing, as defined by the Membership Committee, shall be Member Organizations without going through the membership vetting process. Any other organization that wants to become a FiXs Member Organization must submit an application to the Membership Committee for review. The applicant must then be vetted by a FiXs-approved financial institution. The Membership Committee will then make a recommendation to the FiXs Executive Board with regard to approval or denial of the application.

10.1.2 Certification of Member Organizations

Organizations approved for membership will be eligible to apply for certification for an Authorization to Operate (ATO), and thereby perform roles defined in these rules. Founding Members may receive an ATO certification as a Credential Issuer, Issuer Sponsor, Relying Party, or as a Member Service Provider. Full Members and Network User Associate Members, as defined in the FiXs Bylaws, may receive ATO certification as a Credential Issuer, Issuer Sponsor or Relying Party. In order to be an ATO certified Member Service Provider, Relying Party, Credential Issuer, or Issuer Sponsor, an applicant must submit an application to the Performance Monitoring and Compliance Subcommittee of the Membership Committee to be assessed by a Third Party Assessor certified by the International Information System Security Certification Consortium and the National Security Agency's InfoSec Assessment Methodology, as recognized by the Department of Defense. The Subcommittee will make a recommendation to the Executive Board about whether to certify an applicant.

10.1.3 Issuing Identifiers to Individuals

A Credential Issuer or Issuer Sponsor is authorized to issue identifiers to individuals as provided for in these Rules.

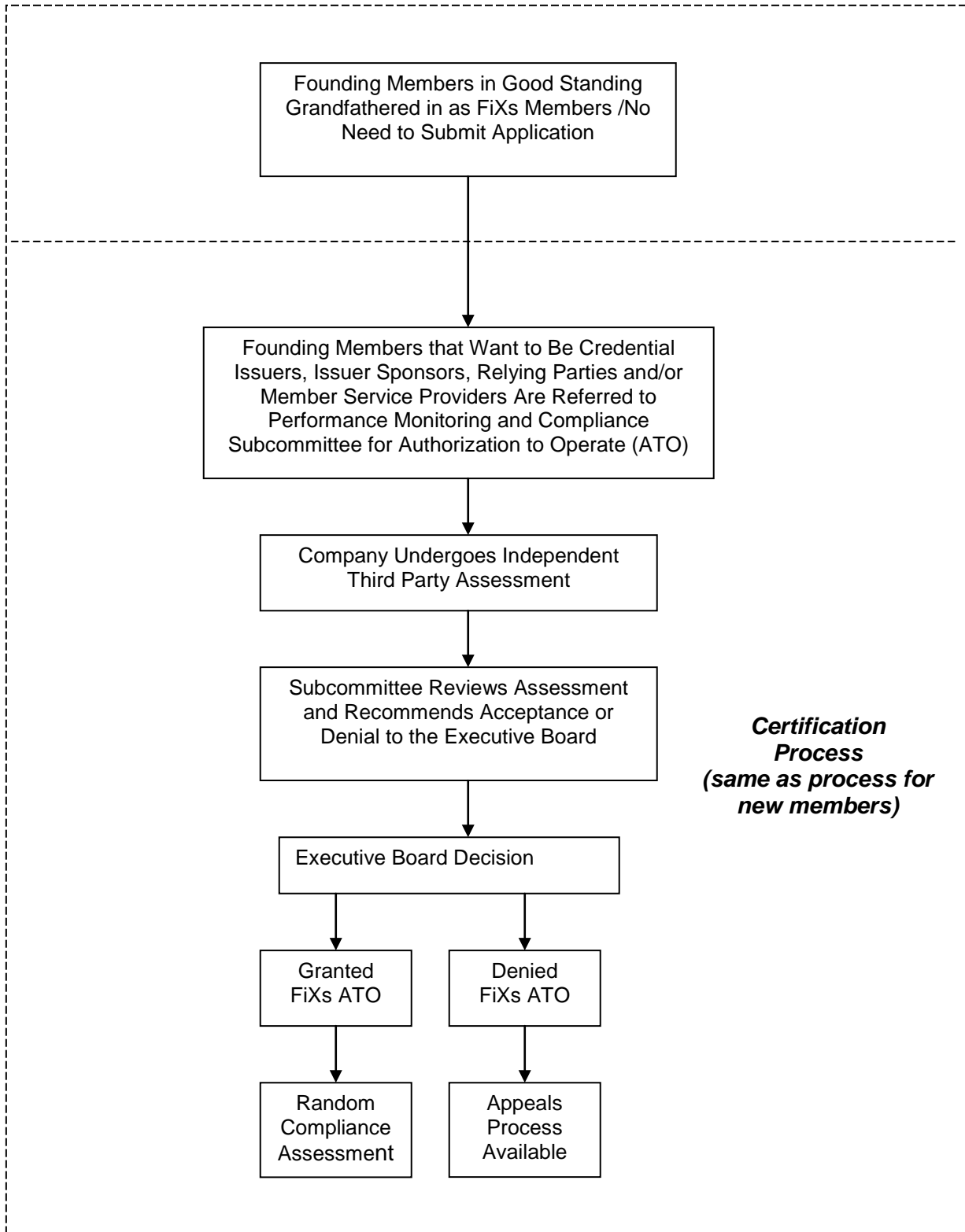


Figure 10.1. Process for Founding Members

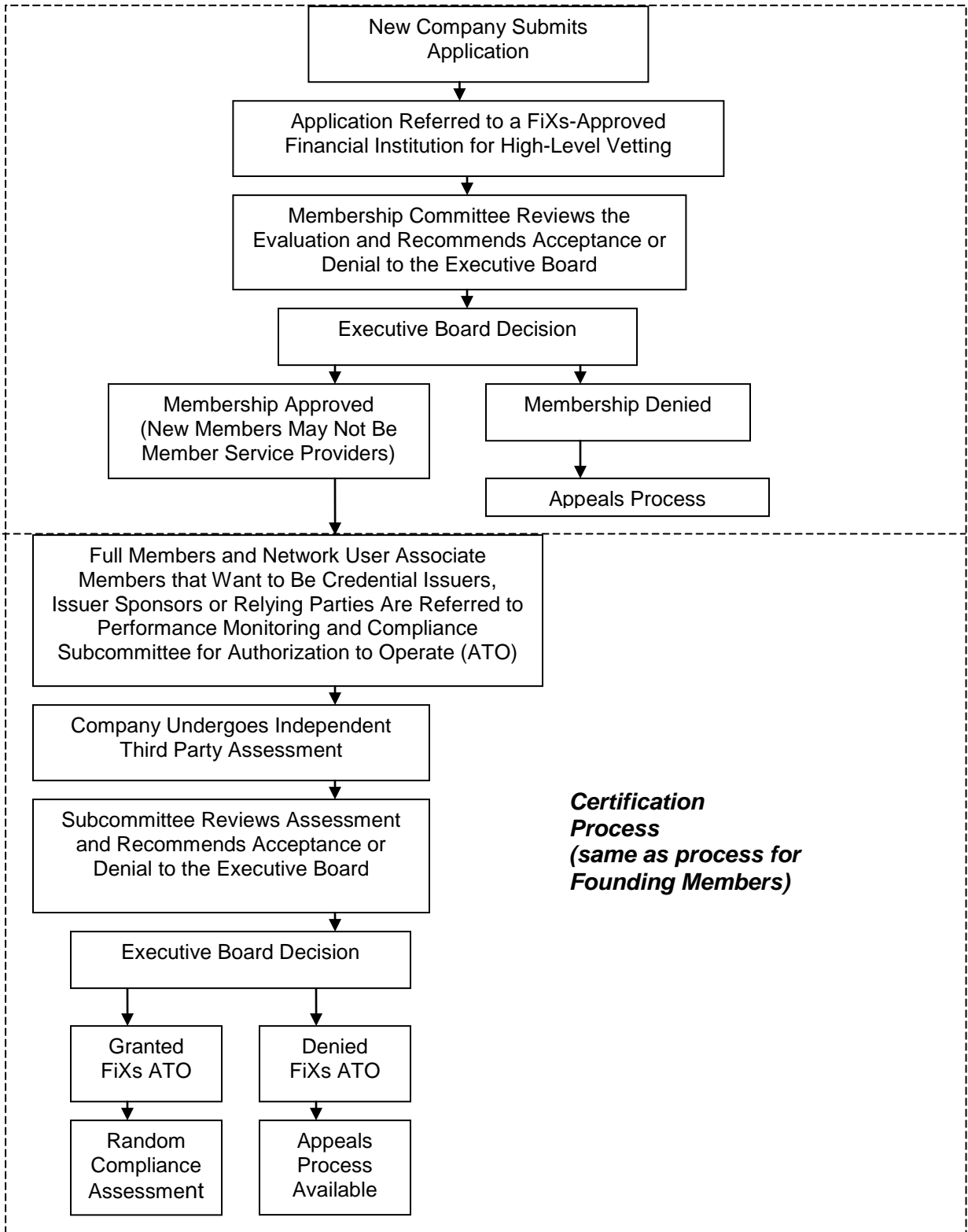


Figure 10.2 – Membership Process For New Members

10.2 Vetting Requirements for Member Organizations

This section specifies how organizations may be approved as FiXs Member Organizations.

10.2.1 APPLICATION FOR MEMBERSHIP

10.2.1.1 Founding Members

Founding Members as defined in the FiXs Bylaws shall be Member Organizations as long as they remain in good standing, as defined by the Membership Committee.

10.2.1.2 Other Members

Any organization that seeks to become a FiXs Member Organization, with the exception of Founding Members, must submit an application to the Membership Committee.

10.2.2 MEMBERSHIP REVIEW AND APPROVAL PROCESS

10.2.2.1 Review by a FiXs-Approved Vetting Organization

When the Membership Committee has received an application for membership, it shall request that the applicant obtain a review by a financial institution approved by FiXs as a vetting organization. The Approved Vetting Organization shall provide a written report to the Membership Committee warranting that the applicant meets the criteria specified by the Membership Committee for FiXs Member Organizations. The Committee may opt to waive review of an Association or non-profit organization, an organization that meets federal government bonding requirements, or of any member that joined FiXs prior to June 1, 2005.

10.2.2.2 Membership Committee Recommendation to the Executive Board

The Membership Committee shall consider the review by the FiXs-approved vetting organization in recommending approval or denial of a membership application to the FiXs Executive Board.

10.2.2.3 Decision by the Executive Board

The FiXs Executive Board shall approve or deny membership applications.

10.2.2.4 Appeals Process

Any applicant whose membership application is denied by the FiXs Executive Board may appeal the decision to a Review Panel comprised of the FiXs Officers. The decision of the Review Panel will be final and binding.

10.2.3 CERTIFICATION OF AUTHORIZATION TO OPERATE

10.2.3.1 Authorization To Operate

In order to serve as a Credential Issuer, Issuer Sponsor, Relying Party or a Member Service Provider, a Member Organization must be certified as having Authorization to Operate (ATO) under these Rules.

10.2.3.2 Eligible Organizations

The following organizations may apply for ATO certification:

10.2.3.2.1 Full Members

Full Members may apply to serve as a Credential Issuer, Issuer Sponsor, Relying Party or a Member Service Provider.

10.2.3.3 Application for ATO Certification

Member Organizations that want to be ATO certified, shall submit an application to the Performance Monitoring and Compliance Subcommittee of the Membership Committee.

10.2.3.4 Independent Assessment of Applicants for an ATO

Applicants for ATO certification must be assessed by an Independent Third Party Assessor certified in accordance with the Information System Security Certification Consortium and the National Security Agency's InfoSec Assessment Methodology, which are recognized by the Department of Defense. Independent Third Party Assessors shall use the Compliance Matrix and Check list referenced in Section 9.2.3.5 in assessing the applicant.

10.2.3.5 Performance Metrics and Compliance Assessment Checklist

FiXs shall develop a matrix of compliance factors from each of the FiXs policy documents listed below. From this compliance matrix, a series of independent checklists will be developed, each of which may be applied independently or jointly. The FiXs Executive Committee will approve the checklists. Once approved, a Board-appointed FiXs Member will negotiate the matrix and checklist(s) with the government. After consensus approval, the independent Third Party Assessors will begin assessments of FiXs elements using the approved checklists that are designed to assess the applicant's compliance with the following FiXs documents:

- FiXs Trust Model;
- FiXs Policy;
- FiXs Operating Rules;
- FiXs Technical Architecture and Specifications; and
- FiXs Security Guidelines.

The assessing organization shall report to the Performance Monitoring and Compliance Committee, which shall make a recommendation with regard to certification to the FiXs Executive Committee.

- 10.2.3.6 FiXs Executive Committee Action**
The FiXs Executive Board shall either approve or deny ATO certification to the applicant.
- 10.2.3.7 Appeals Process**
Any applicant whose ATO is denied by the FiXs Executive Committee may appeal the decision to a Review Panel comprised of the FiXs Officers. The decision of the Review Panel will be final and binding.
- 10.2.3.8 Random Compliance Assessments**
Credential Issuers, Issuer Sponsors and Member Service Providers will be assessed on a random, periodic basis for compliance with FiXs/DCCIS policies and procedures. Such random compliance assessments will be performed by Independent Third Party Assessors, which shall be conducted using the matrix of compliance factors provided for in 9.2.3.5.
- 10.2.3.9 Government Compliance Assessment**
Federal agencies may assess the entire FiXs system or any of its components to ensure compliance with its regulations and conformance with the intent of FiXs/DCCIS policy. These assessments are random, with or without notice, prompted by indicators from the network or other forms of inspection. The government assessments will conform to the assessment format used by Independent Third Party Assessors, using the same FiXs/government negotiated checklist(s) as provided for in 9.2.3.5.

11 MISCELLANEOUS

11.1 Voluntary Termination of Members

Each Credential Issuer, Issuer Sponsor or Relying Party that voluntarily terminates its processing of transactions shall provide written notice to FiXs and shall continue to be bound by these Rules with respect to transactions occurring before such termination.

11.2 Amendment to These Rules

These Rules may be amended from time to time in accordance with the procedures set forth in the FiXs Bylaws; as such Bylaws may be amended from time to time in accordance with its terms.

12 DEFINITIONS

Applicant. An employee or user designated by a Subscriber or Subscribing Party who applies to become a Participant in the FiXs Network and completes the requirements of the identity proofing process.

Approved Vetting Organization. An organization that has a written agreement with FiXs to review applications to become a Member Organization.

Audit Control Data Transaction. A transaction to update to the FDS control tables. These updates include new data and modifications regarding new Members and Participants and dis-enrolled Members and Participants.

Authentication Client. A personal computer with a standard Web browser for access to the *Authentication Web Server* that contains software and drivers for a bar code reader, a smart card reader, and a fingerprint reader with software. The *Authentication Station Operator* uses the *Authentication Client* to conduct *Authentication Inquiries*.

Authentication Inquiry. A transaction originating from an Authentication Client, which requests the authentication of a credential holder from, the credential holder's home FDS.

Authentication Response. A reply from the Credential Issuer to an Authentication Inquiry that sends a denial or transmits credential information (photo and fingerprints) to the Relying Party.

Authentication Station. The physical area which houses the Authentication Client, Fingerprint Reader, Smart Card Reader and Bar Code Reader and where the Authentication Station Operator performs Authentication Transactions (usually a Visitor Security Station).

Authentication Station Operator. An employee or contractor of the Relying Party who operates the *Authentication Client* and conducts *Authentication Inquiries*.

Authentication Web Server. A standard web server that processes Authentication Inquiries and Responses between the Relying Party's Authentication Client and the FiXs Trust Broker.

Authentication Web Server Application. The application, which receives and processes the ID credential information from the Client and returns identity information and fingerprint data for matching on the Client.

Badge/Token. A card or other device that holds these bearer's credentials (such as a photo on the face of a badge or a biometric on a bar code) or that holds the "keys" or "pointers" to the credentials that are accessible in a record on a remote system.

Bar Code Reader/Printer. A device that stores and accepts current token barcodes or that prints new barcodes for existing tokens.

Biometric. For the purposes of the FiXs Operating Rules, a biometric refers to the file of the Participant's scanned fingerprints that are stored at his/her home FDS and retrieved for comparison at the time of an Authentication Inquiry.

Chain of Trust. The trust that is established by a series of agreements that bind Member Organizations, Subscribing Parties, the FiXs Trust Model, the FiXs Policy, the FiXs Operating Rules, the FiXs Technical Architecture and Specifications, the FiXs Security Guidelines and other FiXs Foundational Documents as may be specified from time to time by the FiXs Board of Directors.

Contractual Agent. An individual, other than an employee, who is sponsored as a user on the FiXs Network

Credential Issuance: The process by which a FiXs Participant is provided with a FiXs Identifier which consists of four steps: 1) validate applicant's need for FiXs credentials; 2) verify applicant identification; 3) enroll applicant into FiXs system; and 4) issue or record the Participant's valid FiXs identifier.

Credential Issuer. A FiXs Member that issues FiXs-Compliant Credentials to qualified users for themselves and/or other Sponsors or Subscribing Parties and processes and responds to *Authentication Inquiries*.

Cross Credential Request Handler Software. Installed on the Authentication Client, this software interfaces with the Authentication Web Server to transmit Authentication Inquiries to the FiXs Trust Broker.

Common Access Card (CAC). The official identification card issued to DoD personnel that includes applications for physical and logical access. CAC cards are de facto FiXs Identifiers.

Defense Cross-Credentialing Identification System (DCCIS).

Digital Camera. A camera capable of capturing digital photos and storing them in file formats as per the *FiXs Technical Architecture and Specifications*.

Document Verification Service. A service that provides responses to authentication queries from multiple databases to verify identification documents.

Domain Functional Administrator. A Member Organization employee responsible for the enrollment functions and management of the enrollment personnel within the Member Organization.

Domain Technical Administrator. A Member Organization employee who has the authority to perform infrastructure maintenance applications on the Enrollment System and/or the Authentication System for the FiXs Program.

Encoding Reader Device. Device that reads and displays the data on the bar code and/or magnetic stripe.

Enrollment. Refers to the creation of a valid FiXs Participant record in the FiXs Data Repository.

Enrollment Client. A PC with a standard Web browser for access to the *Enrollment Web Server* that includes software, a bar code reader and a fingerprint reader. The *Facility Enroller* uses the Enrollment Client to capture FiXs ID data and issue the FiXs Certified Credential.

Enrollment Web Server. A standard web server that processes enrollments from the Authentication Client and stores the records in the Sponsor's FiXs Data Repository.

Enrollment Web Application Software. Software that enables entry of new FiXs Participants into the Sponsor's FiXs Data Repository.

Exception Processing. Procedures to be followed when a credential or participant cannot be authenticated by the FiXs System as per the normal procedures described in these Operating Rules.

Facility Administrative Enrollers. Member employees who are responsible for enrolling and terminating new local Facility Enrollers using the Enrollment Operator Maintenance Web Application.

Facility Enrollers. Employees of a FiXs Credential Issuer or Issuer Sponsor who perform enrollment services for Credential Issuers.

Facility Domain Administrators. Member employees who have the technical and operational responsibilities for individual FiXs facilities within a domain.

Facility Verifier. Employee of a FiXs Credential Issuer who has the authority to perform the identity proofing tasks.

Federated Model of Trust. An approach to establishing trust that relies on agreements, standards and technologies to make identity portable across disparate organizations.

Federation for Identity and Cross-Credentialing Systems (FiXs). A non-profit, non-stock corporation incorporated under the laws of the Commonwealth of Virginia. FiXs is the legal and business entity that manages the FiXs Network and maintains oversight and compliance with established operating principles.

Fingerprint Capturing Device. A device with software for capturing, reading, storing and comparing fingerprints that is used at enrollment.

Fingerprint Reader. A device used at the Authentication Station to scan the Participant's fingerprint for comparison against the downloaded image.

FiXs Applicant. See **Applicant**.

FiXs Certified Credential or FiXs Credential. An identity credential issued by an approved FiXs Credential Issuer who has contracted to follow the FiXs Trust Model and all corollary policies, rules, guidelines and implementation standards for vetting, enrolling, maintaining and revoking identity credentials. The organization has also agreed to allow an independent FiXs contractor to certify and periodically audit the above conditions for issuance and use of the credential(s).

FiXs Credential Issuer. See **Credential Issuer**.

FiXs Data Repository. Database that stores the identification credentials and audit files associated with the FiXs Participants of the Member Organization and interfaces to the Member's FDS.

FiXs Domain Server (FDS). The platform that contains the enrollment and authentication server software and that interfaces to the FiXs Data Repository, the FiXs Trust Broker, the Enrollment Client, and the Authentication Client.

FiXs Foundational Documents. Documents approved by the FiXs Board of Directors that form the logical and functional foundation for the FiXs Network: These documents include, but are not limited to: the Trust Model; the FiXs Policy; the FiXs Operating Rules; the FiXs Implementation Guidelines; the FiXs Security Guidelines and the FiXs Technical Architecture and Specifications .

FiXs Identifier. The unique identifier used to access a Participant's or user's authentication files. For CAC holders, this identifier is the DoD EDI PIN. For non-CAC holders, it is the combination of the FiXs designated Participant's Member/Organization Code and ID and the Organization-assigned Employee ID number.

FiXs Member or FiXs Member Organization. See **Member** or **Member Organization**.

FiXs Network. The end-to-end system comprising the physical infrastructure, operating principles and processes to authenticate FiXs Certified Credentials.

FiXs Operating Entity. See **Operating Entity**.

FiXs Participant. See **Participant**.

FiXs Relying Party. See **Relying Party**.

FiXs System. See **Federation for Identity and Cross-Credentialing Systems (FiXs)/Defense Cross-Credentialing Identification System (DCCIS)**.

FiXs Trust Broker. The intermediary between Credential Issuers and Relying Parties that serves as the *operational intermediary* by processing Authentication Inquiries from Relying Parties to Credential Issuers and Authentication Responses from Credential Issuers to Relying Parties via the FiXs Trust Broker..

FiXs Program Manager. See **Program Manager**.

Hardware Security Module. A device is used to encrypt messages that are being sent to the FiXs Trust Broker and to verify the digital signatures of messages received from the FiXs Trust Broker.

Home Transaction/Home FDS. Refers to an Authentication Inquiry that is processed at the same DCCIS FDS as the originating Relying Party. In this case, the employee is being authenticated at an employee facility.

Independent Third Party Assessor. An independent organization certified in accordance with the Information System Security Certification Consortium and the National Security Agency's InfoSec Assessment Methodology that performs assessments for compliance with the Compliance Matrix and Checklist approved by the FiXs Executive Board.

Identity Proofing. The process by which the Member Organization validates the identity information provided by the applicant at the time of employment.

Issuer Sponsor. A Credential Issuer that also sponsors other Credential Issuers and performs some or all of the Credential Issuer duties defined herein that the sponsored Credential Issuer chooses not to perform. In this case, the Issuer Sponsor assumes some or all of the following functions on behalf of the sponsored Issuer: enrollment and issuance; participant records management; FiXs domain server management; standards and specifications compliance; transaction processing; application integration; and, human resources and security departments coordination.

Member. See **Member Organization.**

Member Organization. A company, agency, or organization that formally applies, and is accepted, for membership in FiXs on other than a Subscriber basis. This organization may then participate in either a voting or non-voting capacity in the FiXs governance process to help set the vision and evolution of the FiXs Network

Member Partnership Agreement. Legal document signed by Member Organization representatives with the FiXs Operating Entity, which binds the Member to the FiXs Operating Rules.

Member Service Provider. A Member Service Provider (MSP) is a FiXs Founding Member that has agreed to provide equipment procurement and management services to FiXs Issuers and/or FiXs Relying Parties. In its role as MSP, designated Founding Members will supply domain servers, enrollment equipment and authentication equipment (including required peripherals) to FiXs Issuers and Relying Parties that request these services. MSP services include equipment procurement, delivery and deployment; inventory management; equipment certification; equipment configuration; and documentation. Optionally, MSPs may also provide local application development and integration as well as consultative services to FiXs Issuers and Relying Parties.

Operator Maintenance Web Application Software. Software that enables new local site Enrollment Operators to be created and terminated on the Sponsor's FiXs Data Repository.

Organizational Code. The unique identifying number that is assigned to a Credential Issuer or Issuer Sponsor.

Participant. Refers to the individual employee or subcontractor of a Member Organization that qualifies to participate in the FiXs System.

Primary Trusted Organization or PTO. The entity that sponsors individual users who are to be issued a FiXs-Certified Credential in accordance with all FiXs processes, and policies and that agrees to be responsible for the acts and omissions of its employees or Contractual Agents. A PTO may also be a Credential Issuer, Issuer Sponsor or Subscriber.

Program Manager. A Program Manager (PM) is an employee who manages and administers the FiXs program within a Member company or organizational domain. The PM has technical oversight of the program and is responsible for appointing the Domain Technical Administrator and Domain Functional Administrator for the Program.

POC and pilot. Refers to the “Proof-of-Concept” and pilot Phase of the FiXs System.

Relying Party. A FiXs Member that either relies on the FiXs credential to authenticate the identity of a Participant and/or initiates authentication inquiries to the Credential Issuer and processes the responses in accordance with FiXs Operating Rules.

Remote Transaction. Refers to an Authentication Inquiry that is routed through the FiXs Trust Broker to be processed at a FDS other than of the originating Relying Party.

Smart Card Reader. A device used to read and process data that resides on a smart card.

Smart Card Writer. A device used to write ID data to a smart card and record images for comparison to a scanned image on the Authentication Client.

Sponsor. An organization that uses the services of an Issuer Sponsor to host its FiXs operations and that sponsors Participants into the FiXs Network. A Sponsor is responsible for the acts and omission of the Participants that it sponsors. There are two kinds of Sponsors a member and a non-member . In this case, the Issuer Sponsor hosts the Sponsors FDS and processes its FiXs authentication transactions.

Subscriber or Subscribing Party. A non-member organization that is a Primary Trusted Organization sponsoring individual users to be issued FiXs Certified Credentials. Subscribers agree to Terms of Use policies. .

Terms of Use. The legal agreement between FiXs, FiXs Member Organizations, and Subscribing Parties regarding each parties agreement to adhere to FiXs rules, policies, and procedures for utilizing a FiXs Certified Credential.

Transaction. Refers to an **Authentication Inquiry**, an **Authentication Response** or an **Audit Control Data Transaction**.

Trust Broker. See FiXs Trust Broker.

Trusted Adjudicator. An administrator who assigns privileges at the customer level for granting privileges, to include physical or logical access.

13 REFERENCES

14 REVISION HISTORY

| Version | Date | Comments |
|---------|-----------------|--|
| 1.0 | September 2005 | Initial Issue |
| 1.1 | | |
| 1.2 | January 2007 | Pages 23-25: Added "FiXs Assurance Levels" as Section 2 |
| 2.0 | March 2007 | Added Section 2.1.3.1.1.6 Complete National Agency Check |
| 3.0 | September 2007 | Changes to Levels-Sections 1-4 |
| 3.1 | October 1, 2008 | Added as an appendix, Logical Operating Rules Version 1.0 as approved by Board vote on October 1, 2008 |
| 3.2 | November 2008 | Updated to comply with requirements of DMDC. |
| | | |



FIXS® LOGICAL OPERATING RULES
Appendix to FiXs Operating Rules

Version 1.0
October 1, 2008

www.fixs.org

Copyright 2008 by the Federation for Identity and Cross-Credentialing Systems, Inc.

All Rights Reserved

Printed in the United States of America

10400 Eaton Place, Suite 500A

Fairfax, VA 22030

(703) 591-9255

Table of Contents

| | | |
|----------|---|-----------|
| 1 | GENERAL REQUIREMENTS AND DEFINITIONS..... | 60 |
| 1.1 | Level 1 (FiXs equivalent “Low”)..... | 60 |
| 1.2 | Level 2 (FiXs equivalent “Medium”) | 60 |
| 1.3 | Levels 3 (FiXs equivalent “Medium High”) | 60 |
| 1.4 | Level 4, (FiXs equivalent_“High”)..... | 61 |
| 1.5 | Framework..... | 61 |
| 1.6 | Certificate Validation | 61 |
| 1.7 | FiXs Logical Trust Model | 61 |
| 1.7.1 | DoD PKI..... | 62 |
| 1.7.2 | Federal PKI common Policy Framework (FPCPF)..... | 63 |
| 1.7.3 | Federal Bridge Certification Authority (FBCA) | 63 |
| 1.8 | Certificate Profile | 64 |
| 1.8.1 | Fixs Person Designator Identifier (PDI)..... | 64 |
| 1.8.2 | FiXs Assurance Level..... | 64 |
| 1.9 | Credential Issuer Responsibilities..... | 65 |
| 1.10 | Certificate Practice Statement..... | 66 |
| 1.11 | Registration Practice Statement | 66 |
| 1.12 | Life Cycle Technical Controls | 67 |
| 1.12.1 | Physical Safeguards..... | 67 |
| 1.12.2 | Access Controls..... | 68 |
| 1.12.3 | Equipment | 68 |
| 1.12.4 | Upgrades | 68 |
| 1.12.5 | Development Environment Security | 68 |
| 1.12.6 | Configuration Management Security | 68 |
| 1.12.7 | NETWORK SECURITY CONTROLS..... | 68 |
| 1.13 | Uniqueness Across the FiXs Network..... | 68 |
| 2 | SPONSORS..... | 70 |
| 3 | RELYING PARTY RESPONSIBILITIES..... | 71 |
| 3.1 | Application Provisioning | 71 |
| 3.1.1 | TRUST DETERMINATION TECHNIQUES AND PARAMETERS | 72 |
| 3.1.2 | ENABLE APPLICATION AUTHENTICATION..... | 72 |

| | | |
|------------|--|------------|
| 3.1.3 | User Repository/ Privilege Management..... | 73 |
| 3.1.4 | DIGITAL SIGNATURES AND STORAGE CONSIDERATIONS..... | 75 |
| 3.2 | Documenting Compliance | 76 |
| 3.2.1 | Identity/Qualifications of Compliance Auditor..... | 76 |
| 3.2.2 | Compliance Auditor’s Relationship to Audited Party..... | 76 |
| 3.2.3 | LIFE CYCLE MANAGEMENT STRATEGY | 76 |
| 3.3 | Exception Processing | 76 |
| 4 | FiXs VALIDATION SERVICE PROVIDER RESPONSIBILITIES | 77 |
| 4.1 | TRUST DETERMINATION..... | 78 |
| 4.1.1 | Path-Based Trust..... | 78 |
| 4.1.2 | Validation Protocols..... | 78 |
| 4.1.3 | Other Trust Determination Techniques | 79 |
| 4.1.4 | Checking Certificate Revocation List | 79 |
| 4.1.5 | Online Certificate Status Check | 79 |
| 4.1.6 | Standard Certificate Validation Protocol (SCVP) | 80 |
| 4.1.7 | Fully PD-Val Capable Web Servers | 80 |
| 4.1.8 | Other Techniques and Protocols..... | 80 |
| 4.2 | OCSP Responder Self-Signed Certificate | 80 |
| 4.3 | OCSP Responder Certificate | 81 |
| 4.4 | OCSP Request Format | 81 |
| 4.5 | OCSP Response Format | 82 |
| 5 | SECURITY REQUIREMENTS | 83 |
| 6 | LIABILITIES AND INDEMNIFICATION | 84 |
| 7 | PRIVACY | 85 |
| 7.1 | Privacy..... | 85 |
| 8 | DEFINITIONS..... | 86 |
| 9 | REFERENCES..... | 96 |
| 10 | REVISION HISTORY | 107 |

FIXS LOGICAL OPERATING RULES

Background

The Federation for Identity and Cross-Credentialing Systems® (FiXs®) is a not-for-profit 501 c (6) trade association comprised of a coalition of industry and public sector organizations whose objective is to support efforts to develop standards supporting the creation and deployment of a secure interoperable identity cross-credentialing network. These Logical Operating Rules supplement the FiXs Operating Rules which define the operational requirements and obligations of FiXs Member Organizations utilizing the FiXs Network and are a part of a larger set of governance documents that lay the foundation for establishing trust in and the operations of the FiXs Network. The other documents, known as the FiXs Foundational Documents, include:

- The Trust Model;
- FiXs Policy;
- Implementation Guidelines;
- The Technical Architecture and Specifications; and
- Security Guidelines.

The FiXs Network provides a highly-scalable, secure, auditable solution set, whereby participating organizations can authenticate FiXs-Certified Credentials (also known as FiXs Credentials) issued to users from other participating organizations or “Subscribers” as well as authenticate the credentials issued by other related organizations (i.e. cross-credential). FiXs relies on a Federated Model of Trust, which is discussed more fully in the FiXs Trust Model. The federated identity model establishes trust between member organizations through the use of agreements, standards and technologies that make an “identity credential” portable across the organizations.

Initially, FiXs established a trusted relationship between certain FiXs Member Organizations and the DoD’s Defense Cross-Credentialing Identification System (DCCIS). The federation enabled participating Department of Defense (DoD) and industry facilities to achieve strong, and interoperable identity verification and authentication of participating contractor/private sector personnel who presented a company-issued trusted credential (i.e. FiXs-certified credential). Similarly, participating industry locations also recognized the DoD-issued Common Access Card (CAC) and the Defense Biometric Identity System (DBIDS) credential, which required no modifications in order to operate with FiXs and DCCIS. This initial proof-of-concept established the baseline for further expansion.

FiXs, which is the only organization authorized to inter-operate a cross-credentialing system with the U.S. Department of Defense, is deployed in a federated manner to enable other government agencies, first responders, and industry partners to authenticate the identity of individuals who seek access to their physical or logical assets in either the government or commercial environment.

In a federated system each sponsoring organization maintains its own database of enrolled members. Privacy and security are maintained because no identity information is held centrally or maintained in the infrastructure except in the employee's host organization domain server.

While the initial FiXs Operating Rules focused on the assured authentication of individuals that supported the physical access functionality and individual vetting requirements to obtain a FiXs credential, the FiXs Logical Operating Rules extend that paradigm into Logical Access functionality.

These FiXs Logical Operating Rules match logical access credentials with the FiXs credential that support the levels of assurance defined in the FiXs Operating Rules and FiXs Implementation Guidelines, as specified by the Federal Government. For the highest levels of assurance, the FiXs credential shall hold and protect digital certificates that have been established and are certified to inter-operate with the Federal Government. Thereby, combining its federated system to enable other government agencies, first responders, and industry partners to reliably authenticate the identity of individuals who seek access to both physical and logical assets in either the government or commercial environment. In all cases however, the privileges or authorities actually granted is a decision of the cognizant system owner/manager.

At the present time the Federal Government has defined four recognized levels of credentials and/or trust. It is generally accepted that each level is defined by three distinct processes; one that defines the vetting process that is accomplished prior to a credential being issued; the second defines the standards for the data, and its placement on the credential, and the standards and specifications for the credential/card itself; and the third defines the chain of trust and accountability of these process (the subject of this document).

FiXs standards entail the use the FIPS 201 compliant smart card specifications for all Levels of Trust. Thus, the differentiation between the levels is primarily with the vetting process, documentation/ verification, and biometric data collected, verified and maintained in the federated data model; as well as the life cycle management of the digital certificate and private keys issued to and protected by the credential. FiXs-certified credentials also contain the appropriate data designating under which Level of Trust the credential was issued and classified.

The current Government sanctioned nomenclature for "Levels" is numerical (i.e. 1, 2, 3, & 4) and described below. FiXs correlates these levels with a textual designation of Trust Level that provides a descriptive context associated by each level. Therefore, the remainder of this document and the accompanying Guideline documents will provide a corollary textual description of levels to equate to the standard government numerical designation:

"High Trust" = 4; "Medium High Trust" = 3; "Medium Trust" = 2"; and "Low Trust" = 1"

Level 1 (FiXs equivalent "Low"). This level (if required) is currently considered an unacceptable level of trust for official Federal Government use purposes. FiXs assigns the Low Level Trust (Level 1) the working definition of: a level of assurance that requires minimal proof of identity but no background check, and no document verification, therefore, it provides little or no level of trust assurance.

FiXs Credential Issuers are not permitted to enroll Users at a Low Trust Level (1); load any data into a FiXs Domain Server; nor attempt to authenticate such credentials across the FiXs Network.

Examples of a Low Level (1) credentials are shopper discount cards and public email accounts. Because these “credentials” may be granted by non-FiXs Members or Subscribers without any kind of identity verification, FiXs Members or Subscribers are cautioned against granting rights to a bearer.

At a future date FiXs may assess the validity, requirements, and resources required for this level of credential. The Level I – “Low” is not used currently.

The FiXs Medium Trust Level (Level 2) applies to a level of assurance required by a specific implementation. This will require a background check, using commercially available sources of data, and fingerprints will be collected digitally at time of enrollment, solely for the purpose of linking to the issued credential. At this level the fingerprints **will not** be sent to the FBI for a National Criminal History Fingerprint Check.

The Medium Level may suit those commercial vendors who may require frequent access to facilities in order to provide deliveries; or stock shelves/vending machines; or provides maintenance services. This Medium Level may provide adequate acceptable risk for granting local privileges at lower threat levels, but may not be acceptable as threat levels rise. This level may also be used to accommodate persons who may temporarily work in positions of public trust, such as certain categories of first responders, health care workers or volunteers who help out at a disaster scene (i.e., Red Cross and other volunteers; public works employees; emergency technicians, etc.). The Medium Level credential can also be used for Commercial applications.

This level is intended for applications handling sensitive medium value information based on the relying party’s assessment, with the exception of transactions involving issuance or acceptance of contracts and contract modifications. Examples of medium assurance applications include:

- Non-repudiation for small and medium value financial transactions other than transactions involving issuance or acceptance of contracts and contract modifications
- Authorization of payment for small and medium value financial transactions
- Authorization of payment for small and medium value travel claims
- Authorization of payment for small and medium value payroll
- Acceptance of payment for small and medium value financial transactions

Level 3, (FiXs equivalent “Medium High”) has not been defined by a Federal Directive or Policy at this point in time. FiXs members and industry at-large, however, have a requirement for this level of credential and accordingly, FiXs has developed standards to comply with this requirement and proposes these Guidelines to the Federal Government for consideration and adoption. FiXs Credentials certified at Level 3 are aligned with PIV II (as defined in the FiXs Operating Rules), but differ from PIV I provisions relating to the enrollment process. The vetting

and issuance process mirror the process performed by the Federal Government for a Level 4 credential with the exception of the use of commercial sources instead of having the involvement of the Office of Personnel Management (OPM). Accordingly, this assurance level of credential is considered as the “commercial equivalent” of the Level 4 credential. For logical access control purposes, the digital credential created and protected in this environment shall carry a medium hardware assertion. The DoD has defined this as “Medium Hardware Assurance” and General Services Administration (GSA) has designated this as “Common Hardware”.

Level 4, (FiXs equivalent “High”) is aligned with Homeland Security Presidential Directive 12 (HSPD 12). HSPD 12, dated August 27, 2004, entitled “Policy for a Common Identification Standard for Federal Employees and Contractors” which directed promulgation of a federal standard for secure and reliable forms of identification for federal employees and contractors. In March 2006, the National Institutes of Standards and Technology (NIST) issued Federal Information Processing Standards 201 (FIPS 201) for Personal Identity Verification (PIV) of federal employees and contractors. The PIV standard consists of two parts – PIV-I and PIV-II. PIV-I satisfies control objectives, including enrollment requirements, of HSPD 12. PIV-II specifies implementation standards, including physical card characteristics, and use of identity credentials on integrated circuit cards for a federal personal identity verification systems. For logical access authentication purposes, a digital credential created and protected in this environment shall carry a hardware assertion. The DoD has defined this as “Medium Hardware Assurance” and GSA as “Common Hardware”.

Since Level 3 and 4, of “high” and “medium high assurance” credentials carry a hardware assertion, these logical credentials are available for all applications operating in environments appropriate for medium assurance but which require a higher degree of assurance and technical non-repudiation based on the relying party’s assessment. Examples include:

- All applications appropriate for medium assurance certificates
- Mobile code signing
- Applications performing contracting and contract modifications

The FiXs Implementation Guidelines provides the specific requirements for the vetting of sponsored individuals requesting credentials in specific market/ functional venues. The accompanying Card Holder Unique Identifier (CHUID) section of the Guidelines deals with the specifics of the data and specifications of the card. Accordingly, these FiXs Logical Operating Rules, the FiXs Operating Rules and the FiXs Implementation Guidelines are all complementary must be incorporated concurrently to implement FiXs cross-credentialing physical and logical authentication services.

Historically, FiXs has emulated many of its concepts and standards from the electronic payments industry. In the electronic payments industry, specific operating rules provide a uniform business and legal framework, as well as standard formats, for the exchange of financial payments among and between a diverse group of institutions and individuals. To rely on the principles already established for the payments industry, NACHA – The Electronic Payments Association, or formally known as the National Automated Clearing House Association, assisted with its knowledge and experience in development of the FiXs Operating Rules. FiXs also adopts standards-based certificate validation protocols that provide a flexible,

cost effective, and robust validation solution ideally suited to a wide range of client applications in diverse operating environments. At the core of this validation solution is a sophisticated digital certificate status responder capable of servicing Online Certificate Status Protocol (OCSP), Server-based Certificate Validation Protocol (SCVP), or CRL requests for full or delta CRL downloads; providing mechanisms to obtain and manage CA Certificates, Certificate Revocation Lists (CRL), and CA issued listings of non-sequential certificate serial numbers to service requests.

It is recognized that processing, or authenticating, an individual's identity credential is largely analogous to processing a payment. FiXs encourages maximum participation among industry at-large to adopt this common set of standards to create a consistent, seamless, and secure operational framework and avoid the disruption and risks of implementing differing internal practices and platforms. The overall objective is to establish a secure and interoperable "Chain of Trust" for all members (including contractors, delivery and repair personnel, transport workers, law enforcement, first responders and others, needing access to facilities).

16 GENERAL REQUIREMENTS AND DEFINITIONS

This Section defines the requirements for starting FiXs logical authentication operations. The general requirements associated with FiXs Member Organizations as well as administrative and system requirements in their roles as Credential Issuers, Primary Trusted Organizations (PTOs) and Relying Parties are detailed in the FiXs Operating Rules; and, are included herein by reference.

In the case of the requirements necessary to effect the proper life cycle management of the digital certificate protected on the FiXs-certified credential, Certificate Policies (CPs), referenced herein, and the associated Certification Practice Statements (CPSs) shall be relied upon to describe the establishment and operation of the Public Key Infrastructure (PKI) and the policies and procedures relating to holding or using certificates issued onto a FiXs credential. Each CP is applicable to all individuals that will be interacting with the Federation; DoD activities; other government agencies; and associated individuals and contractors. The purpose of each CPS is to inform individuals relying (Relying Parties) on certificates issued and credential holders (holders of certificates) of their duties and obligations. It is also to advise those parties of the policies, practices and procedures that are used for issuing, validating and revoking these certificates.

FiXs recognizes the need to interoperate within various domains and has a requirement to establish trust relationships with Certification Authorities (CAs) that achieve a satisfactory assurance level. The CPs referenced herein shall be enforced in full, in accordance with the policies asserted by each:

- Department of Defense PKI Certificate Policy (DoD PKI CP)
- United States (US) Government Certificate Policy (CP) for External Certification Authorities (ECA) [ECA CP]
- Federal PKI Common Policy Framework [FPCPF]
- Federal Bridge Certificate Authority [FBCA]

16.1 Level 1 (FiXs equivalent “Low”)

The digital certificates at this level shall assert basic assurance as stipulated by the FBCA, at a minimum.

16.2 Level 2 (FiXs equivalent “Medium”)

The digital certificates at this level shall assert medium assurance as stipulated by the DoD PKI CP, the ECA CP and the FBCA; as well as, certificates that assert the common policy under the FPCPF.

16.3 Levels 3 (FiXs equivalent “Medium High”)

The digital certificates at this level shall assert:

- Medium hardware assurance as stipulated by the DoD PKI CP, the ECA CP
- Federal Common Hardware as stipulated by the FPCPF; or,
- High or medium hardware assurance as stipulated in the FBCA CP that are also approved for DoD use, refer to Section 1.7.3.

16.4 Level 4, (FiXs equivalent_“High”)

The digital certificates at this level shall assert:

- Medium hardware assurance as stipulated by the DoD PKI CP and the ECA CP;
- Federal Common Hardware as stipulated by the FPCPF; or,
- High or medium hardware assurance as stipulated in the FBCA CP that are also approved for DoD use, refer to Section 1.7.3.

16.5 Framework

At all levels, FiXs members shall adhere to the policy framework governing the public key infrastructure component defined by the policy referenced for each level or higher. These policies require the use of FIPS 140 validated cryptographic modules for all cryptographic operations and the protection of trusted public keys. The policy for users with hardware cryptographic modules mandates a Level 2/medium assurance validation, which is achieved by FiXs via the PIV card.

The CPs that comprise this framework are consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 2527, Certificate Policy and Certification Practice Statement Framework. These policies define a PKI consisting of products and services that provide and manage X.509 certificates for public key cryptography that FiXs shall trust. The certificates issued under these policies identify the individual named in the certificate and bind that person to a particular public/ private key pair and the FiXs credential. FiXs will trust these PKIs for the following security management services:

- Key generation/ storage
- Certificate generation, update, renewal, rekey, and distribution
- Certificate revocation list (CRL) generation and distribution
- Directory management of certificate related items
- Certificate token initialization/programming/management
- System management functions (e.g., security audit, configuration management, archive.)

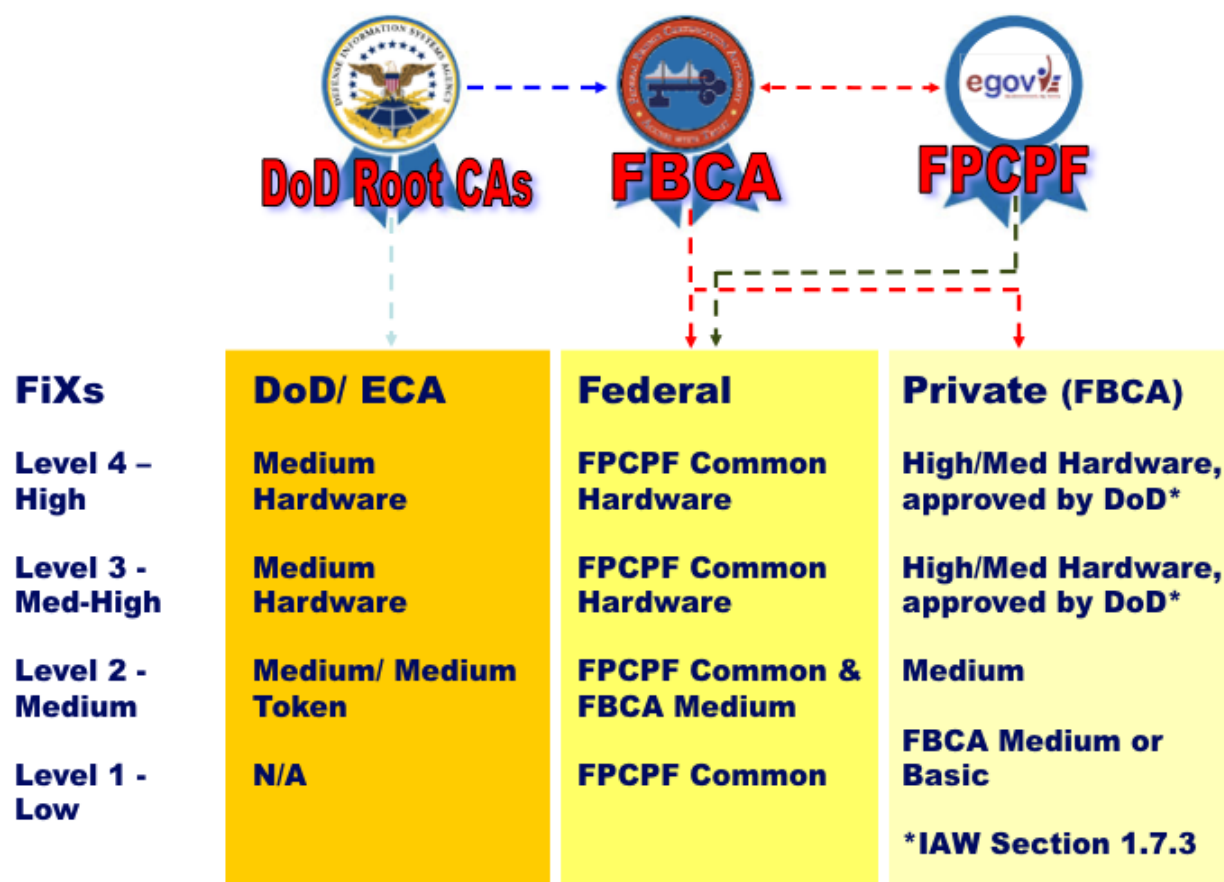
16.6 Certificate Validation

The FiXs Network includes a cost effective, quick deployment offering that provides full relying party integration and compliance with the smart card credential deployed under DoD PKI, FBCA, and HSPD-12. The FiXs validation service provides monitoring and validation for all FBCA-approved, DoD internal and external ECA, ACES and others as they come online.

16.7 FiXs Logical Trust Model

The FiXs logical trust model supports hierarchical PKI, mesh PKI, and single certification authority implementations. As such, FiXs adheres to the constraints established for the secure distribution of self-signed certificates for use as trust anchors, defined in each CP. Additionally, no FiXs credential holder shall hold more than one active FiXs-certified credential. The current FiXs logical trust model is depicted in the following figure.

Practice note: The combination of the Certificate Policy (applied) with the FiXs foundational documents and the FiXs Logical Operating Rules provide individual vetting and the credential uniqueness necessary to provide the appropriate levels of assurance, as defined above, for both physical and logical authentication.



16.7.1 DOD PKI

Two Certificate Policies exist under the DoD PKI Policy Management Authority (PMA): the DoD PKI CP and the ECA CP.

These policies define various levels of assurance including Medium Hardware and Medium. DoD and ECA compliant certificates asserting the following Medium Hardware Assurance object identifiers (OIDs) shall be recognized by the FiXs network as asserting FiXs level 3 or 4:

id-US-dod-mediumhardware::= {2.16.840.1.101.2.1.11.9}

id-eca-medium-hardware::= {2.16.840.1.101.3.2.1.12.2}

DoD and ECA compliant certificates asserting the following Medium assurance OIDs shall be recognized by the FiXs network as asserting FiXs level 2:

id-US-dod-medium::= {2.16.840.1.101.2.1.11.5}

id-eca-medium ::= {2.16.840.1.101.3.2.1.12.1}
id-eca-mediumtoken ::= {2.16.840.1.101.3.2.1.12.3}¹

16.7.2 FEDERAL PKI COMMON POLICY FRAMEWORK (FPCPF)

The FPCPF defines two levels of assurance Common Hardware and Common. FPCPF compliant certificates asserting the following Common Hardware assurance OIDs shall be recognized by the FiXs network as asserting FiXs level 3 or 4:

id-fpki-common-hardware ::= {2 16 840 1 101 3 2 1 3 7}
id-fpki-common-authentication ::= {2 16 840 1 101 3 2 1 3 13}
id-fpki-common-High ::= {2 16 840 1 101 3 2 1 3 16}

FPCPF compliant certificates asserting the following Common assurance level OIDs shall be recognized by the FiXs network as asserting FiXs level 2:

id-fpki-common-policy ::= {2 16 840 1 101 3 2 1 3 6}
id-fpki-common-devices ::= {2 16 840 1 101 3 2 1 3 8}
id-fpki-common-cardAuth ::= {2 16 840 1 101 3 2 1 3 17}

16.7.3 FEDERAL BRIDGE CERTIFICATION AUTHORITY (FBCA)

FBCA-compliant CAs do not assert a FBCA OID the trust of these certificates must be based on the issuing CAs cross certificate with the Federal Bridge.

In accordance with the DoD CIO Memorandum, dated July 22, 2008, "Approval of External Public Key Infrastructures" and DoD Instruction 8520.2, upon successful completion of interoperability testing [defined in Attachment 1 of that memorandum], those policy oids and root CAs approved for use within DoD information systems, shall be incorporated into this document, by reference. NOTE: the DoD document to be referenced is TBD.

FBCA-compliant certificates cross-certified with the federal bridge at High or Medium Hardware assurance and approved for DoD use, shall be recognized by the FiXs network as asserting FiXs level 4 or 3. FBCA compliant certificates cross-certified with the federal bridge at Medium assurance shall be recognized by the FiXs network as asserting FiXs level 2. FBCA compliant certificates cross-certified with the federal bridge at Basic assurance shall be recognized by the FiXs network as asserting FiXs level 1.

16.7.3.1 Access Certificate for Electronic Services (ACES)

The ACES Program makes available the services that federal agencies need to implement PKI and digital signature services required by the Paperwork Reduction Action of 1995, the Government Paperwork Elimination Act of 1998 (GPEA), the E-SIGN Act, and the E-Government Act of 2002. Cross-certified with the Federal Bridge at the medium assurance level, the ACES CP provides an outward looking PKI from the Government and is intended to be trusted across Federal agencies

¹ Medium Token Assurance is intended for applications handling sensitive medium value information. These certificates are vetted in accordance with the requirements of Medium Assurance.

that provide electronic services to the Public. ACES compliant certificates asserting the following Medium assurance level OIDs shall be recognized by the FiXs Network as asserting FiXs medium assurance or “level 2”:

- ACES Authorized CA Certificates: {2 16 840 1 101 3 2 1 1 1}
- Business Representative Digital Signature Certificates: {2 16 840 1 101 3 2 1 1 3}
- Business Representative Encryption Certificates: {2 16 840 1 101 3 2 1 1 3}
- Federal Employee Digital Signature Certificates: {2 16 840 1 101 3 2 1 1 6}
- Federal Employee Encryption Certificates: {2 16 840 1 101 3 2 1 1 6}
- State and Local Employee Digital Signature Certificates: {2 16 840 1 101 3 2 1 1 6}
- State and Local Employee Encryption Certificates: {2 16 840 1 101 3 2 1 1 6}

ACES-compliant certificates asserting the following medium hardware assurance level OIDs shall be recognized by the FiXs Network as asserting FiXs “medium high” (level 3) or “high” (level 4):

- Digital Signature Certificates on hardware: {2 16 840 1 101 3 2 1 1 7}
- Encryption Certificates on hardware: {2 16 840 1 101 3 2 1 1 7}

16.8 Certificate Profile

All certificates issued to a FiXs-certified credential must be constructed in accordance with the Certificate Policy that is asserted in the certificate. Certificates may also include the following FiXs attributes in the CN or as a dnQualifier:

16.8.1 FIXS PERSON DESIGNATOR IDENTIFIER (PDI)

Certificates issued on a FiXs-certified credential, that are used to identify the credential as such, will include the FiXs PDI that will consist of a *unique identification string* [unique to the credential holder]. The unique identifier shall be same for all certificates issued to a single credential holder and is unique to all credentials across the FiXs Network.

16.8.2 FIXS ASSURANCE LEVEL

Certificates issued on a FiXs-certified credential that are used to identify the credential as such will include an identifier preceding the *unique identification string* that will designate the FiXs assurance level [or the level of identity vetting that was employed] 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”

The following sample DNs are provided:

```
cn=Smith.John.J.FiXs41234567890, ou=<subscribing organization>,  
ou=<CAprovider>, o=U.S. Government, c=US
```

```
dnQualifier=FiXs41234567890, cn=John J. Smith, ou=<structural container>,  
ou=<subscribing organization>, o=U.S. Government, c=US
```

16.9 Credential Issuer Responsibilities

In addition to the “Credential Issuers Responsibilities” defined in Section 2 of the FiXs Operating Rules, it is the responsibility of the Credential Issuer to ensure that the certificates issued to the FiXs credential are in compliance with the CPS associated with the CA or Certificate Manufacturing Authority (CMA) being employed, that applies to the X.509 version 3 certificates with assurance levels as defined in the appropriate CP. The processes and procedures in each CPS are applicable to individuals who manage the certificates, who directly use these certificates, and individuals who are responsible for applications or servers that rely on these certificates.

The chosen PKI shall be co-operated and managed by the FiXs Issuer and the CA, where the FiXs Issuer is responsible for management of the FiXs Card Management System (CMS) including communications, facility, etc. and the roles described in the CP regarding entities responsible for enrollment and registering of individuals; and, adjudication/ issuance of the FiXs credential and associated certificates. The FiXs Issuer’s responsibility for performing all associated roles and functions controlling CMS including the registration, identification and authentication, issuance, and customer service processes; includes the auditing of these roles and functions.

The following services are necessary to meet the requirements of the associated CP, but may be provided external to the CA or CMA:

- Registration: A FiXs credential applicant must appear in person before a Registrar to witness and certify the validity of documents and to take affidavits and depositions), as stipulated by the Policy Authority, present valid identification and accept the FiXs credential holder obligations.
- Enrollment: A Federal Information Processing Standards (FIPS) 140-2 Level 3 Secure Socket Layer (SSL) connection from the FiXs CMS to the CA/ CMA.
- Enrollment Validation: The FiXs CMS registration process validates the applicant’s enrollment information.
- Adjudication/ Issuance: Face-to-face custody exchange of the FiXs credential by the Issuer to the credential holder.

Based on the FiXs (FIPS-201 compliant) enrollment and registration provided by the FiXs Issuer, the CA/ CMA provides the following:

- Certificate Manufacturing: When notified by the FiXs CMS of a valid enrollment request, the CA/ CMA manufactures the requested certificate(s) for delivery to a FIPS 201 compliant card.

- Certificate Publishing: The CA/ CMA publishes it to a directory. The directory may be accessed via Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) gateway or via the LDAP protocol.
- Encryption Key Storage: Optional storage of escrowed encryption keys.
- Key Recovery: If encryption key escrow is selected, a Key Recovery Practice Statement (KRPS) shall detail the escrow and recovery processes.
- Certificate Status information: In the form of Certificate Revocation Lists (CRLs) distribution and Online Certificate Status Protocol (OCSP) responses.

It is the responsibility of the FiXs Issuer and the CA/ CMA to ensure that all of the requirements of the appropriate CP are met and are periodically audited by its independent auditor against the CPS and operates primary and secondary secure data centers in conformance with the Department of Defense (DoD), National Security Agency (NSA), U.S. General Services Administration (GSA) and best commercial practices.

16.10 Certificate Practice Statement

While the referenced CP defines the assurance can be placed in a certificate issued by a CA, the Certificate Practice Statement (CPS) states how the CA establishes that assurance. Each CA that issues certificates to FiXs credentials shall have an approved CPS corresponding to one or more of the referenced CPs, for the appropriate level of assurance. A FiXs issuer shall only issue credentials with certificates that hold and assert the appropriate level of assurance as defined by this document.

16.11 Registration Practice Statement

The FiXs Issuer and the CA will define the separation of roles and special procedures used to manage FiXs credentials in accordance with the requirements of the appropriate CP or as may be more stringent than that set forth in the policy and the FiXs Operating Rules. Prior to issuance of certificates to a FiXs credential, the Issuer will coordinate with the CA/ CMA to ensure that the procedures for authentication of personnel are documented in a Registration Practice Statement (RPS) and comply with the appropriate CP, and submitted to FiXs for approval. The RPS shall require that registration, issuing and activation functions ensure that the applicant's identity information is verified. The RPS shall require that minimal procedures for authentication of employees and affiliated personnel are detailed, and shall clearly define those functions that are internal or outsourced. At a minimum, the RPS shall require authentication procedures include the following steps:

- The identity of the person performing the identification
- A signed declaration by that person that he or she verified the identity of the Applicant as required by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury)
- Unique identifying number(s) from the ID(s) of the applicant
- The biometric of the applicant
- The date and time of the verification

- A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury).

In all cases a biometric of the applicant (e.g., a photograph and fingerprint in accordance with FIPS 201) shall be recorded and maintained by the Issuer (as defined in the RPS) to establish an audit trail for dispute resolution. (Handwritten signatures and other behavioral characteristics are not acceptable as biometrics for the purposes of this environment.)

Certificates issued on a FiXs-certified credential shall be delivered via a GSA FIPS-201 approved CMS, refer to FIPS 201 Evaluation Program Approved Product List (<http://fips201ep.cio.gov/apl.php>).

The RPS will also define the process for the periodic FiXs File Updates, in accordance with Section 1.2.7.1 of the FiXs Operating Rules. In particular, a mechanism will be defined that will require the Subscribing Party to verify the Credential Holders authority to hold a FiXs-certified credential. It is the responsibility of the FiXs Issuer to ensure proper firewall connectivity in order to receive, accept, process, and internally disseminate (if necessary) these updates. As a requisite for continued use of the FiXs credential, the Credential Issuer must receive periodic updates from the FiXs Sponsor's Program Manager, or his/her designated agent on behalf of the applicant. This verification shall be in writing and signed, or digitally signed, with an active FiXs or CAC credential using a Medium Hardware Assurance certificate.

16.12 Life Cycle Technical Controls

Individuals with FiXs "trusted" roles shall use security management tools and procedures to ensure that the operational systems and networks adhere to the security requirements that check the integrity of the system data, software, discretionary access controls, audit profiles, firmware, and hardware to ensure secure operation.

Security management controls shall include the execution of tools and procedures to ensure that the operational system and network adhere to configured security. These tools and procedures include checking the integrity of the security software, firmware, and hardware to ensure their correct operation.

Components used for the issuance of FiXs credential shall be protected at the border and protection rules monitored. A network traffic recording, intrusion detection, and forensic analysis system shall be used to monitor intrusion attempts and policy verification (rated at EAL 2 in accordance with Intrusion Detection System Protection Profile (IDSPP)). Firewall, IDS, and network system configurations shall be documented and updates controlled and documented. Weekly review of the firewall and network system configurations against installation plans and procedures shall be made to ensure that no unauthorized changes are made to these systems. Detailed procedures for maintaining and inspecting the Firewall/ IDS and network devices and any anomaly detected shall be documented.

16.12.1 PHYSICAL SAFEGUARDS

Physical security safeguards and access controls shall continuously provide for protection against access or modifications to hardware/ software by unauthorized

individuals. Hardware tokens will be stored in a security container. The CPUs, Redundant Array of Inexpensive Disks (RAID)/ external drives, monitors, keyboards, and mice will be sealed with Tamper Resistant Seals in accordance with paragraph 8-308, ISM and Tab B, Code A, Quantum Information and Computation (QUIC); in order to detect surreptitious entry into the equipment and associated peripherals. The seal will be inspected (and results logged) every month to ensure that it serves its intended use.

16.12.2 ACCESS CONTROLS

Unescorted entry to the facility hosting the CMS or access to any server components (hardware/ software) shall be limited to personnel who are cleared for access and whose need to access the components has confirmed.

16.12.3 EQUIPMENT

A FiXs CMS server is to be dedicated to administrating the system and shall only have software installed necessary to perform CMS functions. All upgrades will be from the original equipment manufacturers and software vendors.

16.12.4 UPGRADES

The configuration of related systems, as well as any modifications or upgrades, shall be documented. These systems shall have the capability installed and operating to detect unauthorized modifications to these systems software and configurations.

16.12.5 DEVELOPMENT ENVIRONMENT SECURITY

Assembly and maintenance of related systems will be accomplished in the controlled environment. Only designated personnel will perform maintenance on the related system.

16.12.6 CONFIGURATION MANAGEMENT SECURITY

Issuing related system(s) Configuration Management (CM) records shall be maintained and controlled (stored in a locked container).

16.12.7 NETWORK SECURITY CONTROLS

Access to any enrollment/ issuance data shall be protected. The issuer organization will certify compliance with these requirements, in writing to within the constraints of the RPS, annually.

16.13 Uniqueness Across the FiXs Network

Each FiXs Credential Issuers shall enforce credential uniqueness and ensure the following:

- The applicant does not hold an active FiXs credential
- The name contains the applicant's identity and organization affiliation that is meaningful to humans
- The naming convention is as described in the corresponding CP and CPS

Practice note: *This does not prevent devices from sharing a Fully Qualified Domain Name (FQDN) as CN.*

Each FiXs Credential Issuer will support special procedures that ensure that each individual holds only one active FiXs credential.

In all cases a biometric of the applicant (e.g., a photograph or fingerprint) shall be recorded and maintained by the Credential Issuer to verify uniqueness across the FiXs network and establish an audit trail for dispute resolution (handwritten signatures and other behavioral characteristics are not accepted as biometrics for the purposes of this requirement). Prior to credential issuance the Credential Issuer will verify that the credential holder's biometric does not exist in any FiXs Domain Server.

Practice note: All certificates issued on a FiXs credential shall be issued via a GSA FIPS-201 approved CMS, refer to FIPS 201 Evaluation Program Approved Product List (<http://fips201ep.cio.gov/apl.php>).

Additionally, the Credential Issuer shall record the process (es) followed for issuance of each certificate. The process documentation and authentication requirements shall include the following:

- The identity of the person performing the identification
- A signed declaration by that person that he or she verified the identity of the Applicant as required by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) and that he or she verified, via the FiXs network that the applicant does not hold another FiXs credential
- Unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s)
- The biometric of the applicant
- The date and time of the verification

A declaration of identity signed by the applicant using a handwritten signature that includes that assertion that the applicant does not hold another FiXs-certified credential, performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury).

17 SPONSORS

No Additional Stipulations.

18 RELYING PARTY RESPONSIBILITIES

Relying parties are those persons and entities that accept and rely upon FiXs credentials for purposes of verifying digital signatures. A Relying Party is an individual or organization that, by using another's certificate can:

- Verify the integrity of a digitally signed message.
- Identify the creator of a message, or establish confidential communications with the holder of the certificate.
- Rely on the validity of the binding of the credential holder's name to a public key.

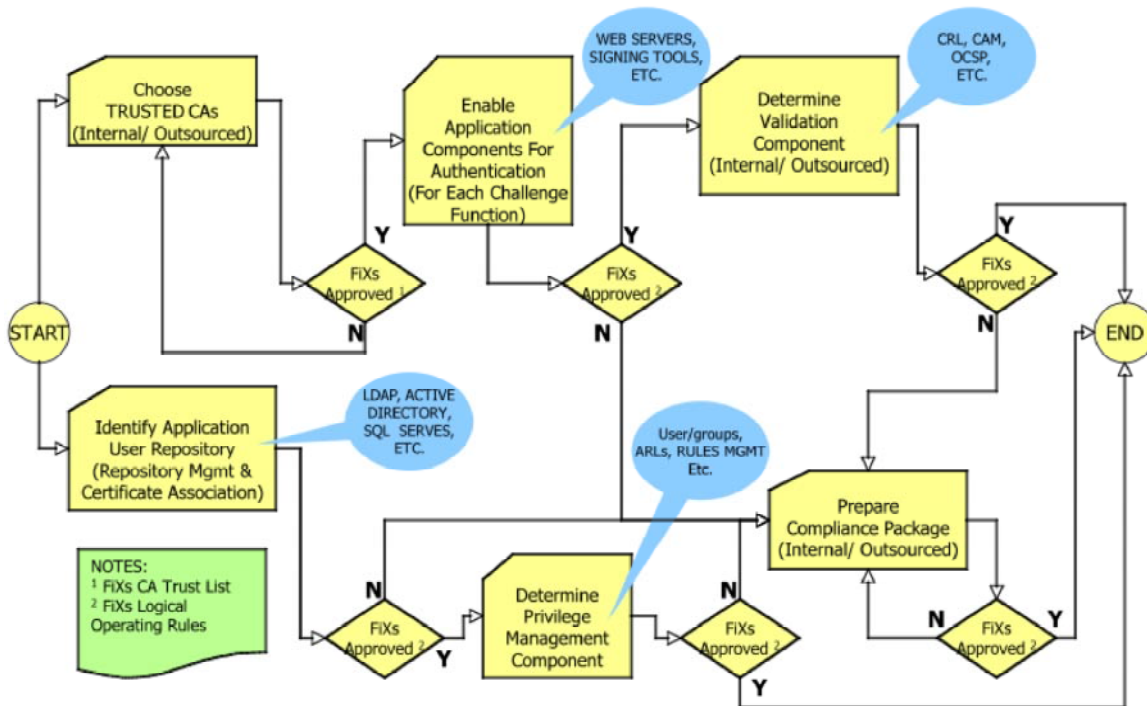
A Relying Party, at their own risk, may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

To assist Relying Parties to meet their responsibilities for logical authentication a FiXs credential provides the following:

- Clear verification of medium hardware assurance via Federal OIDs, as stipulated in Section 1.6
- Unique identity across all FiXs credentials
- Identification of FiXs assurance level
- Highly available revocation information
- The assurance of a FiXs vetted credential, as stipulated in the FiXs Operating Rules, that includes a background investigation of all Level 3 and 4 FiXs credential holders

18.1 Application Provisioning

In the FiXs-based system, the Relying Party will be responsible for initiating and processing the transactions that will validate the FiXs participant's digital certificate. A relying party must determine the level of assurance (or trust) that will be acceptable for authenticating to a particular application or network.



18.1.1 TRUST DETERMINATION TECHNIQUES AND PARAMETERS

A FiXs Relying Party can establish cross-domain PKI trust using a variety of techniques. Manually, a relying party can review and add the appropriate trust anchors for each applicable PKI into their application or network trust store(s). A FiXs Validation Service Provider (refer to Section 5) can be used to automate this by providing trust based on (a) path discovery and path validation, and/or (b) specific trust lists either derived from the Federal Bridge Certificate Authority.

18.1.2 ENABLE APPLICATION AUTHENTICATION

Possibly the single most important function the digital certificates on the FiXs credential can perform for Relying Parties is Identification and Authentication for applications and implementing such that it builds a Reduce Sign On (RSO) enterprise.

FiXs Relying Parties need to be cognizant of X.509 Digital Certificate technology in order to plug directly into the FiXs recognized PKIs. In order to use certificates for user authentication, an application today needs to recognize and correctly use Trusted Third Party (TTP) certificates. The application needs to correctly parse the CA chain hierarchy containing a Root CA, Intermediate CA and End Entity certificates.

18.1.2.1 APPLICATION (COMPONENT) CERTIFICATES

Relying Party computing and communications components (web servers, routers, firewalls, authentication stations, etc.) may be named as certificate subjects. In such cases, the component must have a human PKI Sponsor as described in the

ECA CP. The PKI Sponsor is responsible for providing the approved Registration Authorities, through an application form, correct information regarding:

- Equipment identification
- Equipment public keys
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the ORC ECA to communicate with the PKI sponsor when required in accordance with the appropriate CPS.

18.1.2.2 APPLICATION (COMPONENT) PRIVATE KEY PROTECTION

At a minimum FiXs Relying Party computing and communications components (web servers, routers, firewalls, authentication stations, etc.) shall protect the certificate private key(s) in a hardware device such as a Trusted Platform Module, as stipulated in the DoD CIO Memorandum, *Encryption of Sensitive Unclassified Data at rest on Mobile Computing Devices and Removable Storage Media*, dated July 03, 2007.

18.1.3 USER REPOSITORY/ PRIVILEGE MANAGEMENT

Possibly the single most important function the digital certificates on the FiXs credential can perform for Relying Parties is Identification and Authentication for applications and doing it in a way that builds a Reduce Sign On (RSO) enterprise. Arguably, the most important part of any application is the design of the user database. Many times the user database becomes a stovepipe database joining hundreds of others for which each user must have a name and password. Additionally, the application program office must take on the responsibility of verifying the identity of individuals before they are given an account. The Federal PKIs provide an efficient and elegant method to solve this most important aspect of application development.

Managing access control efficiently remains a challenge. In a broad sense, there are two prevalent types of applications. One type has many users across regions and would benefit from the integration of role-based access. The other type has fewer users and requires a higher degree of assurance in explicitly granting and denying access. Although the integration of the digital certificates on FiXs credentials into access control can help with the problem of expired accounts and globally revoked access, it does not address the general access management problem. The use of directories can provide support, but only if both types of access requirements are addressed.

18.1.3.1 Basic Access Control

Individual certificates include a Distinguished Name (DN), which contain as a minimum, a common name, organization and country; and, may contain organizational units. This information constitutes a branch in the Directory Information Tree (DIT). For some applications, digital certificates containing a branch within the DIT (e.g., Service, specific contractor affiliation, foreign national, etc.) may be satisfactory for access. For this case, access may be granted to all holders of approved certificates within the tree branches accepted by the server.

For example, by configuring an open systems secure web server to trust ECA certificates, a particular web enabled database could allow access to only ECA certificate holders with a ou=FiXs. The application would then only allow user or external application interactions through that authenticated route. For all other potential activity, its resources and that of its server would be unavailable or strictly controlled.

18.1.3.2 More Defined Access Control

Some Relying Party applications may require stricter access control based on the identity of the certificate holder. This is a local issue managed by the server administrator. In this case, the application not only needs to authenticate the user, but provide a mechanism that determines roles and privileges based on user identity. For example, affiliated users may be able to view data posted by a specific application; however, to make changes or updates to that data, it may be necessary for the user to be a member of a small sub-group that is not identified by the certificate.

The Relying Party's application must have a repository of access control information that facilitates the desired privilege control based on the user identified in the certificate. The repository would contain entries for all registered users of any application within the network (Note: It does not need contain user entries for all certificate holders within the FiXs community) and contain groups representing roles and access privileges. In many cases, this information would parallel user name and password repository information currently employed by the application.

Application owners can also determine if existing roles meet access requirements or provide a group manager who can maintain explicit access permissions. Given this capability, the Relying Party can then apply its own local access rules to ensure only those with a need to know can access particular data files. By using an open systems LDAP directory (to manage users and groups/roles), access control management can be accomplished across the Internet securely. The application may also maintain the access control lists that reside in another repository at the discretion of the application manager. This approach is particularly efficient when user roles, privileges and allowed accesses change frequently, and when an enterprise contains diverse applications.

18.1.3.3 Access Control Mechanisms

The mechanism by which an enterprise repository should be populated with user information must be addressed. By using a secure repository gateway, first time users can establish accounts by presenting their certificates to a directory validated by the gateway. A registration request web form can be used to create a user account, based on the user certificate presented, and to record access privilege request information. Upon reviewing the requests of the user, each application owner can assign privileges to individual accounts, confident of the identity of the requester. Alternatively, the application owner can make provisions for bulk registration by downloading certificate information, in whole or part, from each trusted CA repository.

Many applications use a DBMS to hold the user database. Web applications may use the authorization features of the DBMS or the authorization features of the web server. Many web applications have web servers with mechanisms that interoperate with LDAP directories.

A common scenario is for local application and process owners to independently manage user access and privileges via access control lists (ACLs) or similar mechanisms on the application server. This is done on a recurrent, dynamic, ongoing basis across the enterprise for each and every different application environment --- quite a significant amount of overhead when viewed as an aggregate effort, enterprise-wide.

A directory can be the repository for user information, user public key certificates, and lookup information (email, phone, address, etc.). Numerous commercial organizations have reduced administrative costs and increased administrative accuracy and efficiency by leveraging an enterprise directory as a unifier and control mechanism; for example, by integrating human resources and network access controls with the enterprise PKI and its directory. Application access and privilege management can also be automated using the existing repository of a PKI, reducing administrative overhead and strengthening ownership controls, with minimal impact to existing application systems. This approach retains full control for the data owners within strict accordance to enterprise security policies. The repository can accommodate access control and other user information (attributes) down to the individual entry, so that it can be used to implement security policies as well as application owner-directed access control. Servers can build and store ACLs using the users and groups/roles according to the application owners controlled processes.

18.1.4 DIGITAL SIGNATURES AND STORAGE CONSIDERATIONS

If you are receiving or collecting something that is signed digitally, whether once or several times by several signatories, you must have (1) a means to capture the form and the data on that form; (2) a means to capture the signature (hash) and the public key to decipher the hash and (3) a validation of the signature at that time and place (proven time-stamp).

This means the recipient will need three signatures to establish non-repudiation of the signed document/ form. First is the signature of the person or persons who signed the form; second is the signature of the validation mechanism; and third is the signature of the time stamping entity.

To complete the transaction and provide a complete record for the recipient and the provider, a receipt (also signed and date-stamped) could be provided and filed with the document/form.

As a related matter having nothing to do with non-repudiation, the recipient must be able to use the information received, so his file must be such that the data on the form can be parsed and reassembled, sorted and/or collected with other information received from other providers.

At the time the information is first received, recall and use of the information is straightforward, but many users do not consider the fact that they must be able to determine non-repudiation of electronic data and electronic signatures years later, just as is required for signed (paper) legal documents. In order to do this, one must be able to recreate the ability to decipher the information using a public key no longer in use, and prove the signatures were valid at the time they were affixed.

This means the recipient will need three signatures to establish non-repudiation of the signed document/form. First is the signature of the person or persons who signed the form; second is the signature of the Validation Authority; and third is the signature of the time stamping entity.

18.2 Documenting Compliance

FiXs certified Relying Parties operating under the standards of the Federation, shall conduct a compliance audit no less than once every three (3) years. Additionally, the FiXs has the right to require periodic or ad hoc inspections.

18.2.1 IDENTITY/QUALIFICATIONS OF COMPLIANCE AUDITOR

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the CPS' and CP's trusted by the Relying Party.

18.2.2 COMPLIANCE AUDITOR'S RELATIONSHIP TO AUDITED PARTY

The compliance auditor either shall be a private firm, which is independent from the entities being audited, or it shall be sufficiently separated organizationally from those entities to provide an unbiased, independent evaluation. An example of the latter situation may be the approach of an Agency Inspector General. The FiXs shall determine whether a compliance auditor meets these requirements.

The Relying Party is responsible for identifying and engaging a qualified auditor of operations.

18.2.3 LIFE CYCLE MANAGEMENT STRATEGY

The most important features of sound life cycle management are:

- Keeping the system fully functional throughout installation of any change;
- Ensuring security is not breached and the auditability of system security is maintained throughout;
- Ensuring system archives are unaffected and the ability to retrieve signed documents is maintained;
- Developing a rigorous and comprehensive test and evaluation process as part of the planning for each step of the modernization;
- Ensuring training is conducted for operators and managers beforehand such that personnel are fully prepared to deal with display and procedural changes.

18.3 Exception Processing

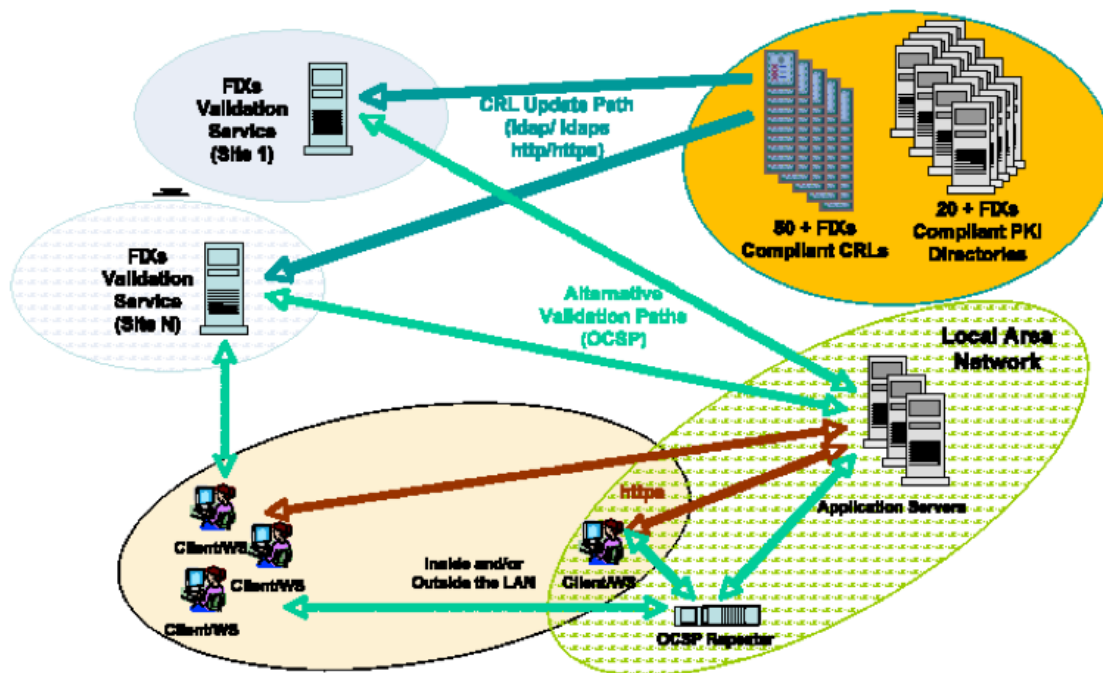
No stipulation.

19 FiXs VALIDATION SERVICE PROVIDER RESPONSIBILITIES

A FiXs Validation Service Provider is a FiXs Network component, similar to a trust broker that provides revocation status. A FiXs Validation Service Provider shall conform to the stipulations of the CPs for which it serves validation information. All FiXs Validation Service Provider practice updates, as well as any subsequent changes will be updated in their compliance documentation and submitted to the FiXs Board for conformance assessment. The Validation Service Provider practices include:

- Conformance to the stipulations of the US Government CPs
- Ensuring that certificate and revocation information is accepted only from valid CAs
- Include only valid and appropriate responses
- Maintain evidence that due diligence is exercised in validating certificate status

A FiXs Validation Service Provider resides on the FiXs Network as depicted in the figure below.



A FiXs Validation Service Provider provides OCSP responses to credential holders and is responsible for:

- Providing certificate revocation status to the Relying Parties upon request
- Ensuring that the status and validation responses contain authentication and integrity services commensurate with the assurance level of the certificate being checked
- Two party administration of the Validation Service Components

A FiXs Validation Service Provider shall ensure that:

- An accurate and up-to-date CRL, from the authorized CA, is used to provide the revocation status
- Revocation status responses provide authentication and integrity services commensurate with the assurance level of the certificate being checked

19.1 TRUST DETERMINATION

A FiXs Validation Service Provider shall support different validation parameters (i.e., a list of trust anchors, or a list of CAs on a trust list), and shall support applications selection of these parameters by applications for validation based on rules provided by the application and specific instructions provided in the validation request.

In some cases, the type of trust determination possible is dictated by the validation request protocol. For example, in OCSP, only hashed data from the certificate is provided, rather than the certificate itself. In general, this precludes path discovery and validation, which require the entire certificate to seed the process. For OCSP, the Federal Government recommends a trust list based trust based validation process.

In cases where the specifics of the request protocol do not preclude particular trust determination techniques, a validation service can provide a variety of techniques. At a minimum, a FiXs Validation Service Provider shall be capable of providing trust based on both (a) path discovery and path validation, and (b) trust lists.

The FiXs Validation Service Provider shall support the application's capability to specify validation parameters either as required settings for all validation requests from the application, or by providing a default with the option of per-request overrides of the path settings when transmission of per-request settings is supported by the validation protocol.

19.1.1 PATH-BASED TRUST

For path-based trust, the FiXs Validation Service Provider shall support the application's capability to specify (at a minimum) allowable trust anchors and has the option of setting path processing starting point policy requirements. For trust lists, a FiXs Validation Service Provider shall support the application's capability to be able to list either the direct issuing CA or the hierarchical root of the issuing chain.

19.1.2 VALIDATION PROTOCOLS

For validation protocols that do not provide a mechanism for the application to identify themselves (and thus select their validation parameters), a FiXs Validation Service Provider shall provide a method outside the protocol for identification of the requestor, such as identifying the network address from which an address comes, or by providing different service network addresses to each application.

This validation parameter selection mechanism shall also be extensible such that an application may have multiple validation parameter sets that they may utilize. For example, this could be implemented by an application using multiple "virtual" identities, each of which select a particular set of validation parameters.

19.1.3 OTHER TRUST DETERMINATION TECHNIQUES

There are other possibilities for trust determination. For example, an application manager may decide that it must determine trust locally and wish to utilize the FiXs Validation Service Provider for a near real-time status check only, or it may designate an external service for trust determination.

FiXs shall take these trust determination options, and the possibility of future options, into account when enhancing their technical architecture.

19.1.4 CHECKING CERTIFICATE REVOCATION LIST

FiXs standards support checking of CRLs to determine certificate validation status, online, near real-time, including all subtypes of CRLs (delta, indirect, partitioned, etc). The requirements for path validation of CRLs is provided by the PD-VAL documentation will specify the exact types of CRLs that the FiXs recognized PKIs process.

As part of the application defined validation parameters, the FiXs validation system supports controls over the caching of CRLs. Some applications require constraints on the amount of time a CRL is cached for (or disable caching completely) regardless of the CRL's expiration date. Other applications may require caching of CRLs until their internal expiration.

The FiXs validation system supports a number of techniques to obtain CRLs, at a minimum: processing CRL Distribution Point (CDP) extensions when present and querying one or more directory systems (such as the FBCA LDAP servers), based on the assumption that CRLs will be stored under the distinguished name of the issuer of the certificate. Optionally, the FiXs validation system could provide support for a local "hint database" of rules to obtain commonly needed CRLs that are not located by either of the above methods.

The FiXs validation system could also provide support pre-fetching of large CRL's that particular applications use frequently. This feature would be further enhanced if the FiXs validation system could automatically determine the list of CRLs that would be useful to pre-fetch, and if the system automatically scheduled downloading replacements when pre-fetched CRLs expire.

19.1.5 ONLINE CERTIFICATE STATUS CHECK

A FiXs Validation Service Provider shall support multiple techniques to determine whether OCSP is supported for a particular certificate, and if so, determining the correct OCSP responder to contact. At a minimum, a FiXs Validation Service Provider shall support processing the Authority Information Access (AIA) extension to search for OCSP server addresses, and shall support a database of OCSP responders for known CA's that utilize OCSP but do not populate the AIA extension.

A FiXs Validation Service Provider shall support the OCSP protocol as specified in IETF RFC 2560 or latest specification. This provides a Managed OCSP responder for applications unable to use AIA fields to directly contact issuer's responders

and/or the application-specific trust determination in addition to an online status check.

19.1.6 STANDARD CERTIFICATE VALIDATION PROTOCOL (SCVP)

A FiXs Validation Service Provider shall support SCVP, as SCVP is the protocol identified as “proper” by the IETF for use in requesting delegated path validation (DPV). There are a number of features within the SCVP protocol definition that are “optional.” That is, it either indicates that a server “SHOULD” or “MAY” support the option or combination of options. For such functionality, FiXs shall implement the “optional” component if any authorized application requires it. Otherwise the functionality need not be implemented; although the FiXs validation system should return a correct “not implemented” code should a request for an unimplemented feature be received.

19.1.7 FULLY PD-VAL CAPABLE WEB SERVERS

A FiXs Validation Service Provider shall toolkits that can be plugged into web servers that provide full, pd-val (path discovery and validation). Because this model is necessitated by COTS web server design, but has an unfortunate side effect: if the native mechanism rejects a certificate, the toolkit will never have a chance to validate the certificate. To ensure that the native mechanism does not cause false negatives, the native mechanism requires a high degree of trust. A FiXs Validation Service Provider shall maintain a “hints list” approved by the FiXs Logical Operating Rules subcommittee.

19.1.8 OTHER TECHNIQUES AND PROTOCOLS

As part of support for application defined validation it is likely that other near real-time, online status checking protocols will come into common use in the future, and/ or that applications may come up with other special exception rules (for example, they may wish to override certificate AIA fields in certain circumstances, or have test certificates return fixed status results without actually processing an on-line check). A FiXs Validation Service Provider will update capability as the FiXs Logical Operating Rules evolve.

19.2 OCSP Responder Self-Signed Certificate

Any self-signed OCSP responder used for verifying certificates asserting a policy OID reference herein are required to meet the certificate profile stipulated below and the stipulations above.

FiXs disclaims any liability for loss due to use of any validation information relied on by any party that does not comply with this stipulation.

Note: The following profile is for a FiXs entity that chooses to deploy a Self-Signed OCSP responder.

| Field | Value |
|--------------------------------|--|
| Version | V3 (2) |
| Serial Number | Must be unique |
| Issuer Signature Algorithm | sha-1WithRSAEncryption {1 2 840 113549 1 1 5} |
| Issuer Distinguished Name | cn=<OCSP Responder Name>, ou=<Company Name>, ou=<CA Name>, o=U.S. Government, c=US |
| Validity Period | 3 years from date of issue in Generalized Time format |
| Subject Distinguished Name | cn=<OCSP Responder Name>, ou=<Company Name>, ou=<CA Name>, o=U.S. Government, c=US |
| Subject Public Key Information | 1024 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} |
| Issuer Unique Identifier | Not Present |
| Subject Unique Identifier | Not Present |
| Issuer's Signature | sha-1WithRSAEncryption {1 2 840 113549 1 1 5} |
| Extensions | Not Present |

19.3 OCSP Responder Certificate

Note: This profile is used only for Validation Service Provider

| Field | Value |
|--------------------------------|--|
| Version | V3 (2) |
| Serial Number | Must be unique |
| Issuer Signature Algorithm | Refer to Certificate Policies referenced |
| Issuer Distinguished Name | Refer to Certificate Policies referenced |
| Validity Period | 1 month from date of issue in UTCT format |
| Subject Distinguished Name | Refer to Certificate Policies referenced |
| Subject Public Key Information | Refer to Certificate Policies referenced |
| Issuer Unique Identifier | Not Present |
| Subject Unique Identifier | Not Present |
| Issuer's Signature | Refer to Certificate Policies referenced |
| Extensions | |
| Authority key identifier | Octet String, Refer to Certificate Policies referenced |
| Subject key identifier | Octet String, Refer to Certificate Policies referenced |
| Key usage | c=yes; nonRepudiation, digitalSignature |
| Extended key usage | c=yes; id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9} |
| Certificate policies | c=no; Refer to Certificate Policies referenced |
| Subject Alternative Name | http URL for the OCSP Responder |
| Authority Information Access | c=no; calssuers= <http URL for the issuers root> |
| No Check | id-pkix-ocsp-nocheck; {1 3 6 1 5 5 7 48 1 5} |

19.4 OCSP Request Format

FiXs OCSP requests are not required to be signed. A FiXs Validation Service Provider's OCSP responder will not check the signature on the request. See RFC2560 for detailed syntax. The following table lists which fields that are required by a FiXs Validation Service Provider's OCSP responder.

| Field | Expected Value |
|----------------|--|
| Version | V1 (0) |
| Requester Name | Not Required |
| Request List | List of certificates – generally this should be the list of two certificates: ECA certificate and end entity certificate |
| Signature | Not Required |
| Extensions | Not Required |

19.5 OCSP Response Format

The following table lists fields to be populated by a FiXs compliant OCSP Responder. Refer to RFC 2560 for detailed syntax.

| Field | Expected Value |
|---------------------|--|
| Response Status | Successful Malformed Request Internal Error Try Later |
| Response Type | id-pkix-ocsp-basic {1 3 6 1 5 5 7 48 1 1} |
| Version | V1 (0) |
| Responder ID | Hash of Responder public key |
| Produced At | Generalized Time |
| List of Responses | Each response will contain certificate id; certificate status ² , thisUpdate, nextUpdate ³ , |
| Extension | |
| Nonce | Will be present if nonce extension is present in the request |
| Signature Algorithm | sha-1WithRSAEncryption {1 2 840 113549 1 1 5} |
| Signature | Present |
| Certificates | Applicable certificates issued to the OCSP Responder |

² If the certificate is revoked, the OCSP Responder will provide revocation time and revocation reason from CRL entry and CRL entry extension.

³ The OCSP Responder will use thisUpdate and nextUpdate from CA CRL.

20 SECURITY REQUIREMENTS

In addition to the security requirements set forth in Section 6 of the FiXs Operating Rules the security requirements set forth in the appropriate CP shall be adhered to.

21 LIABILITIES AND INDEMNIFICATION

The liabilities and indemnifications of the appropriate CP apply.

22 PRIVACY

22.1 Privacy

Member Organizations must comply with the privacy provisions of the *applicable CP*, which are hereby incorporated by reference.

23 DEFINITIONS

Applicant. An employee or user designated by a Subscriber or Subscribing Party who applies to become a Participant in the FiXs Network and completes the requirements of the identity proofing process.

Approved Vetting Organization. An organization that has a written agreement with FiXs to review applications to become a Member Organization.

Audit Control Data Transaction. A transaction to update to the FDS control tables. These updates include new data and modifications regarding new Members and Participants and dis-enrolled Members and Participants.

Authenticate. Relates to a situation where one party has presented an identity and claims to be that identity. Authentication enables another party to gain confidence that the claim is legitimate.

Authentication Client. A personal computer with a standard Web browser for access to the *Authentication Web Server* that contains software and drivers for a bar code reader, a smart card reader, and a fingerprint reader with software. The *Authentication Station Operator* uses the *Authentication Client* to conduct *Authentication Inquiries*.

Authentication Inquiry. A transaction originating from an Authentication Client, which requests the authentication of a credential holder from the credential holder's home FDS.

Authentication Response. A reply from the Credential Issuer to an authentication Inquiry that sends a denial or transmits credential information (photo and fingerprints) to the Relying Party.

Authentication Station. The physical area which houses the Authentication Client, Fingerprint Reader, Smart Card Reader and Bar Code Reader and where the Authentication Station Operator performs Authentication Transactions (usually a Visitor Security Station).

Authentication Station Operator. An employee or contractor of the Relying Party who operates the *Authentication Client* and conducts *Authentication Inquiries*.

Authentication Web Server. A standard web server that processes Authentication Inquiries and Responses between the Relying Party's Authentication Client and the FiXs Trust Broker.

Authentication Web Server Application. The application, which receives and processes the ID credential information from the Client and returns identity information and fingerprint data for matching on the Client.

Badge/Token. A card or other device that holds these bearer's credentials (such as a photo on the face of a badge or a biometric on a bar code) or that holds the "keys" or "pointers" to the credentials that are accessible in a record on a remote system.

Bar Code Reader/Printer. A device that stores and accepts current token barcodes or that prints new barcodes for existing tokens.

Biometric. For the purposes of the FiXs Operating Rules, a biometric refers to the file of the Participant's scanned fingerprints that are stored at his/her home FDS and retrieved for comparison at the time of an Authentication Inquiry.

Card Management System. FIPS-201 compliant application to manage PIV-compliant card life-cycle management.

Certificate Authority Administrator. A Certificate Authority Administrator (CAA) is an individual who is the responsible party for a CMA. The CAA possesses the private key of the CMA's certificate. The CAA may be collocated with the CMA, but may also perform administration tasks remotely.

Certificate Policy. A Certificate Policy is a document that defines the policy requirements that must be met by any CMA implemented under the policy.

Certificate Practice Statement. A Certificate Practice Statement (CPS) is a document that details the requirements and procedures that are followed by a CA in issuing and maintaining certificates, and the purposes and allowed uses of those certificates.

Certificate. A data record that, at a minimum: (a) identifies the CMA issuing it; (b) names or otherwise identifies its credential holder; (c) contains a public key that corresponds to a private key under the control of the credential holder; (d) identifies its operational period; and (e) contains a certificate unique serial number and is digitally signed by the CMA issuing it. As used in this CPS, the term of "Certificate" refers to certificates that expressly reference the OID of this CMA in the "Certificate Policies" field of an X.509 v.3 certificate.

Certificate Management System. A Certificate Management System (Netscape and RSA Keon) provides a highly scalable, easily deployable certificate infrastructure for supporting encryption, authentication, tamper detection, and digital signatures in networked communications. It is based on open standards and protocols such as Public-Key Cryptography Standard (PKCS) #7, 10, 11, and 12, Secure Sockets Layer (SSL), Lightweight Directory Access Protocol (LDAP), and the X.509 certificate formats recommended by the International Telecommunications Union (ITU). Certificate Management System is highly customizable and configurable, permitting rapid integration with existing client and server software, customer databases, security systems, and authentication procedures.

Certificate Manufacturing Authority (CMA). An entity that is responsible for the manufacturing and delivery of certificates, but is not responsible for identification and authentication of certificate subjects (i.e., a CMA is an entity that is delegated or outsourced the task of actually manufacturing the certificate).

Certificate Practice Statement (CPS). A Certification Practice Statement is a statement of the practices that a certification authority employs in issuing, suspending, revoking, and renewing certificates and providing access to same, in accordance with specific

requirements (i.e., requirements specified in this CPS, requirements specified in a contract for services).

Certificate Repository. A certificate repository is a system that holds certificates and information about all active certificates including revocation information.

Certificate Revocation List. A Certificate Revocation List (CRL) is a list of certificates that have been revoked but have not yet expired. A CRL should be digitally signed by the CMA to ensure its validity to relying parties.

Certification Authority. A certification authority is an entity that is responsible for authorizing and causing the issuance of a Certificate. The actual certificate is from the CMA.

Chain of Trust. The trust that is established by a series of agreements that bind Member Organizations, Subscribing Parties, the FiXs Trust Model, the FiXs Policy, the FiXs Operating Rules, the FiXs Technical Architecture and Specifications, the FiXs Security Guidelines and other FiXs Foundational Documents as may be specified from time to time by the FiXs Board of Directors.

Contractual Agent. An individual, other than an employee, who is sponsored as a user on the FiXs Network

Credential Holder: A person who (1) is the subject named or identified in a FiXs credential and associated certificate issued to such person and (2) holds a private key that corresponds to a public key listed in that certificate, and (3) the person to whom digitally signed messages verified by reference to such certificate are to be attributed.

Credential Issuance: The process by which a FiXs participant (applicant) is provided with a FiXs Identifier which consists of four steps: 1) validate applicant's need for FiXs credentials; 2) verify applicant identification; 3) enroll applicant into FiXs system; and 4) issue or record the Participant's valid FiXs identifier.

Credential Issuer. A FiXs Member that issues FiXs-Certified Credentials to qualified users for themselves and/or other Sponsors or Subscribing Parties and processes and responds to *Authentication Inquiries*.

Cross Credential Request Handler Software. Installed on the Authentication Client, this software interfaces with the Authentication Web Server to transmit Authentication Inquiries to the FiXs Trust Broker.

Common Access Card (CAC). The official identification card issued to DoD personnel that includes applications for physical and logical access. CAC cards are de facto FiXs Identifiers.

Defense Cross-Credentialing Identification System (DCCIS).

Digital Camera. A camera capable of capturing digital photos and storing them in file formats as per the *FiXs Technical Architecture and Specifications*.

Digital Certificate. A digital certificate is electronic information that indicates the identity of the credential holder, the identity of the CMA, the operational period of the certificate, and the public key of the credential holder. The certificate is digitally signed by the issuing CMA to show validity.

Digital Signature. A digital signature is a string of bits associated with a collection of data (e.g., a file, document, message, transaction); this string of bits can only be generated by the holder of a private key, but can be verified by anyone with access to the corresponding public key.

Some algorithms include additional steps (e.g., one-way hashes, timestamps) in this basic process.

Document Verification Service. A service that provides responses to authentication queries from multiple databases to verify identification documents.

Domain Functional Administrator. A Member Organization employee responsible for the enrollment functions and management of the enrollment personnel within the Member Organization.

Domain Technical Administrator. A Member Organization employee who has the authority to perform infrastructure maintenance applications on the Enrollment System and/or the Authentication System for the FiXs Program.

Encoding Reader Device. Device that reads and displays the data on the bar code and/or magnetic stripe.

End Entity. An end entity is any individual or server who holds a digital certificate. See also credential holder.

Enrollment. Refers to the creation of a valid FiXs Participant record in the FiXs Data Repository.

Enrollment Client. A PC with a standard Web browser for access to the *Enrollment Web Server* that includes software, a bar code reader and a fingerprint reader. The *Facility Enroller* uses the Enrollment Client to capture FiXs ID data and issue the FiXs Certified Credential.

Enrollment Web Server. A standard web server that processes enrollments from the Authentication Client and stores the records in the Sponsor's FiXs Data Repository.

Enrollment Web Application Software. Software that enables entry of new FiXs Participants into the Sponsor's FiXs Data Repository.

Exception Processing. Procedures to be followed when a credential or participant cannot be authenticated by the FiXs System as per the normal procedures described in these Operating Rules.

Facility Administrative Enrollers. Member employees who are responsible for enrolling and terminating new local Facility Enrollers using the Enrollment Operator Maintenance Web Application.

Facility Enrollers. Employees of a FiXs Credential Issuer or Issuer Sponsor who perform enrollment services for Credential Issuers.

Facility Domain Administrators. Member employees who have the technical and operational responsibilities for individual FiXs facilities within a domain.

Facility Verifier. Employee of a FiXs Credential Issuer who has the authority to perform the identity proofing tasks.

Federal Information Processing Standards (FIPS). The federal standards that prescribe specific performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc. Federal agencies are expected to apply these standards as specified unless a waiver has been granted in accordance to agency waiver procedures.

Federated Model of Trust. An approach to establishing trust that relies on agreements, standards and technologies to make identity portable across disparate organizations.

Federation for Identity and Cross-Credentialing Systems (FiXs). A non-profit, non-stock 501c(6) trade association incorporated under the laws of the Commonwealth of Virginia. FiXs is the legal entity that manages and maintains standards oversight and compliance with established operating principles of the FiXs Network.

Fingerprint Capturing Device. A device with software for capturing, reading, storing and comparing fingerprints that is used at enrollment.

Fingerprint Reader. A device used at the Authentication Station to scan the Participant's fingerprint for comparison against the downloaded image.

FiXs Applicant. See **Applicant**.

FiXs Certified Credential or FiXs Credential. An identity credential issued by an approved FiXs Credential Issuer who has contracted to follow the FiXs Trust Model and all corollary policies, rules, guidelines and implementation standards for vetting, enrolling, maintaining and revoking identity credentials. The organization has also agreed to allow an independent FiXs contractor to certify and periodically audit the above conditions for issuance and use of the credential(s).

FiXs Credential Issuer. See **Credential Issuer**.

FiXs Data Repository. Database that stores the identification credentials and audit files associated with the FiXs Participants of the Member Organization and interfaces to the Member's FDS.

FiXs Domain Server (FDS). The platform that contains the enrollment and authentication server software and that interfaces to the FiXs Data Repository, the FiXs Trust Broker, the Enrollment Client, and the Authentication Client.

FiXs Foundational Documents. Documents approved by the FiXs Board of Directors that form the logical and functional foundation for the FiXs Network: These documents include, but are not limited to: the Trust Model; the FiXs Policy; the FiXs Operating Rules; the FiXs Implementation Guidelines; the FiXs Security Guidelines and the FiXs Technical Architecture and Specifications .

FiXs Identifier. The unique identifier used to access a Participant's or user's authentication files. For CAC holders, this identifier is the DoD EDI PIN. For non-CAC holders, it is the combination of the FiXs designated Participant's Member/Organization Code and ID and the Organization-assigned Employee ID number.

FiXs Member or FiXs Member Organization. See **Member** or **Member Organization**.

FiXs Network. The end-to-end system comprising the physical infrastructure, operating principles and processes to authenticate FiXs Certified Credentials.

FiXs Operating Entity. See **Operating Entity**.

FiXs Participant. See **Participant**.

FiXs Relying Party. See **Relying Party**.

FiXs System. See **Federation for Identity and Cross-Credentialing Systems (FiXs)/Defense Cross-Credentialing Identification System (DCCIS)**.

FiXs Trust Broker. The intermediary between Credential Issuers and Relying Parties that serves as the *operational intermediary* by processing Authentication Inquiries from Relying Parties to Credential Issuers and Authentication Responses from Credential Issuers to Relying Parties via the FiXs Trust Broker..

FiXs Program Manager. See **Program Manager**.

Government. Federal Government and authorized agencies and entities.

Hardware Security Module. A device is used to encrypt messages that are being sent to the FiXs Trust Broker and to verify the digital signatures of messages received from the FiXs Trust Broker.

Home Transaction/Home FDS. Refers to an Authentication Inquiry that is processed at the same DCCIS FDS as the originating Relying Party. In this case, the employee is being authenticated at an employee facility.

Hypertext Transfer Protocol over SSL (HTTPS). HTTPS is the use of Secure Socket Layer (SSL) for data transfer via the World Wide Web. HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP. SSL uses a 128-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

Independent Third Party Assessor. An independent organization certified in accordance with the Information System Security Certification Consortium and the National Security Agency's InfoSec Assessment Methodology that performs assessments for compliance with the Compliance Matrix and Checklist approved by the FiXs Executive Board.

Identity Proofing. The process by which the Member Organization validates the identity information provided by the applicant at the time of employment.

Internet Engineering Task Force (IETF). The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

Issuer. An Issuer is an individual who is responsible for authorizing certificate requests.

Issuer Sponsor. A Credential Issuer that also sponsors other Credential Issuers and performs some or all of the Credential Issuer duties defined herein that the sponsored Credential Issuer chooses not to perform. In this case, the Issuer Sponsor assumes some or all of the following functions on behalf of the sponsored Issuer: enrollment and issuance; participant records management; FiXs domain server management; standards and specifications compliance; transaction processing; application integration; and, human resources and security departments coordination.

Key Changeover. The procedure used by an Authority to replace its own private key (e.g., due to compromise) and replace current valid certificates issued with old key.

Key Pair. Means two mathematically related keys, having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (2) even knowing one key, it is computationally infeasible to discover the other key.

Member. See **Member Organization.**

Member Organization. A company, agency, or organization that formally applies, and is accepted, for membership in FiXs on other than a Subscriber basis. This organization may then participate in either a voting or non-voting capacity in the FiXs governance process to help set the vision and evolution of the FiXs Network

Member Partnership Agreement. Legal document signed by Member Organization representatives with the FiXs Operating Entity, which binds the Member to the FiXs Operating Rules.

Member Service Provider. A Member Service Provider (MSP) is a FiXs Founding Member that has agreed to provide equipment procurement and management services to FiXs Issuers and/or FiXs Relying Parties. In its role as MSP, designated Founding Members will supply domain servers, enrollment equipment and authentication equipment (including required peripherals) to FiXs Issuers and Relying Parties that request these services. MSP services include equipment procurement, delivery and deployment; inventory management; equipment certification; equipment configuration; and documentation. Optionally, MSPs may also provide local application development and integration as well as consultative services to FiXs Issuers and Relying Parties.

Mutual Authentication. Parties at both ends of a communication activity authenticate each other (see authentication).

Object Identifier (OID). An object identifier is a specially formatted number that is registered with an internationally recognized standards organization.

Operational Period of a Certificate. The operational period of a certificate is the period of its validity. It would typically begin on the date the certificate is issued (or such later date as specified in the certificate), and ends on the date and time it expires as noted in the certificate.

Operator Maintenance Web Application Software. Software that enables new local site Enrollment Operators to be created and terminated on the Sponsor's FiXs Data Repository.

Organizational Code. The unique identifying number that is assigned to a Credential Issuer or Issuer Sponsor.

Out-of-band. Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party using U.S. Postal mail to communicate with another party where current communication is online communication).

Participant. Refers to the individual employee or subcontractor of a Member Organization that qualifies to participate in the FiXs System.

Primary Trusted Organization or PTO. The entity that sponsors individual users who are to be issued a FiXs-Certified Credential in accordance with all FiXs processes, and policies and that agrees to be responsible for the acts and omissions of its employees or Contractual Agents. A PTO may also be a Credential Issuer, Issuer Sponsor or Subscriber.

Private Key. The key of a key pair used to create a digital signature. This key must be kept a secret.

Program Participants. Collectively, the CMAs, Registrars, Certificate Manufacturing Authorities, Repositories, credential holders, Relying Parties, and Policy Authority authorized to participate in the public key infrastructure defined by this CPS.

Program Manager. A Program Manager (PM) is an employee who manages and administers the FiXs program within a Member company or organizational domain. The PM has technical oversight of the program and is responsible for appointing the Domain Technical Administrator and Domain Functional Administrator for the Program.

POC and pilot. Refers to the “Proof-of-Concept” and pilot Phase of the FiXs System.

Public Key. The key of a key pair used to verify a digital signature. The public key is made freely available to anyone who will receive digitally signed messages from the holder of the key pair. The public key is usually provided via a certificate issued by an CMA and is often obtained by accessing a repository. A public key is used to verify the digital signature of a message purportedly sent by the holder of the corresponding private key.

Public Key Infrastructure. A Public Key Infrastructure (PKI) is a system of policies, CAs, certificates, information repositories, and trusted individuals, that is used to verify and authenticate individuals and servers, and to encrypt and decrypt information exchanged by these individuals and servers.

Registrar. An entity that is responsible for identification and authentication of certificate subjects, and issues certificates.

Relying Party. A FiXs Member that either relies on the FiXs credential to authenticate the identity of a Participant and/or initiates authentication inquiries to the Credential Issuer and processes the responses in accordance with FiXs Operating Rules.

Remote Transaction. Refers to an Authentication Inquiry that is routed through the FiXs Trust Broker to be processed at a FDS other than of the originating Relying Party.

Repository. A database containing information and data relating to certificates, and a CA, as specified in this CPS.

Responsible Individual. A trustworthy person designated by a Sponsoring Organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.

Revoke a Certificate. Means to prematurely end the operational period of a Certificate from a specified time forward.

Secure Sockets Layer. A protocol for providing data security layered between application protocols (such as HTTP, Telnet, NNTP, or FTP) and TCP/IP. This security protocol supports data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.

Smart Card Reader. A device used to read and process data that resides on a smart card.

Smart Card Writer. A device used to write ID data to a smart card and record images for comparison to a scanned image on the Authentication Client.

Sponsor. An organization that uses the services of an Issuer Sponsor to host its FiXs operations and that sponsors Participants into the FiXs Network. A Sponsor is responsible for the acts and omission of the Participants that it sponsors. There are two kinds of Sponsors a member and a non-member . In this case, the Issuer Sponsor hosts the Sponsors FDS and processes its FiXs authentication transactions.

Subscriber or Subscribing Party. A non-member organization that is a Primary Trusted Organization sponsoring individual users to be issued FiXs Certified Credentials. Subscribers agree to Terms of Use policies.

Suspend a Certificate. Means to temporarily suspend the operational period of a Certificate for a specified time period or from a specified time forward.

Terms of Use. The legal agreement between FiXs, FiXs Member Organizations, and Subscribing Parties regarding each parties agreement to adhere to FiXs rules, policies, and procedures for utilizing a FiXs Certified Credential.

Transaction. Refers to an **Authentication Inquiry**, an **Authentication Response** or an **Audit Control Data Transaction**.

Trust Broker. See FiXs Trust Broker.

Trusted Adjudicator. An administrator who assigns privileges at the customer level for granting privileges, to include physical or logical access.

Trustworthy System. Means computer hardware, software, and procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions, and (d) adhere to generally accepted security procedures.

Valid Certificate. Means a certificate that (1) an Authorized CA has issued, (2) the credential holder listed in it has accepted, (3) has not expired, and (4) has not been revoked. Thus, a certificate is not "valid" until it is both issued by a CA and has been accepted by the credential holder.

24 REFERENCES

The following documents contain information that provides background, examples, or details about the contents of this policy.

| Number | Title | Revision | Date |
|------------------------|---|-------------|-----------------------|
| DoD Instruction 8520.2 | Public Key Infrastructure (PKI) and Public Key (PK) Enabling http://www.dtic.mil/whs/directives/corres/html/852002.htm | | 01 April 2004 |
| DoD CIO Memo | Approval of External Public Key Infrastructures http://www.afei.org/documents/20080722DoDExternalPKI Memo.pdf | | 22 July 2008 |
| HSPD-12 | Policy for a Common Identification Standard for Federal Employees and Contractors, http://csrc.nist.gov/policies/Presidential-Directive-Hspd-12.html | | 27 Aug 2004 |
| OMB Circular No. A-123 | Management Accountability and Control, http://www.whitehouse.gov/omb/circulars/a123/a123.html | | Revised June 21, 1995 |
| ABADSG | Digital Signature Guidelines, http://www.abanet.org/scitech/ec/isc/dsgfree.html | | 1 Aug 1996 |
| FIPS112 | Password Usage, http://csrc.nist.gov/publications/index.html | | 5 May 1985 |
| FIPS140 | Security Requirements for Cryptographic Modules, http://csrc.nist.gov/publications/index.html | | 21 May 2001 |
| FIPS186 | Digital Signature Standard, http://csrc.nist.gov/fips/fips186-2.pdf | | 20 Jan 2000 |
| FIPS201 | Personal Identity Verification of Federal Employees and Contractors, http://csrc.nist.gov/publications/index.html | | 25 Feb 2005 |
| FOIAACT | 5 U.S.C. 552, Freedom of Information Act, http://www4.law.cornell.edu/uscode/5/552.html | | |
| FWPP | U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, http://www.iatf.net | Version 1.4 | 1 May 2000 |
| IDSPP | Intrusion Detection System Protection, http://www.iatf.net | Version 1.4 | 4 Feb 2002 |
| ISO9594-8 | Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, ftp://ftp.bull.com/pub/OSIdirectoty/ITU/97x509final.doc | | 1997 |
| ITMRA | 40 U.S.C. 1452, Information Technology Management Reform Act, | | |

| Number | Title | Revision | Date |
|-----------|--|------------------|----------------|
| | http://www4.law.cornell.edu/uscode/40/1452.html | | |
| NAG69C | Information System Security Policy and Certification Practice Statement for Certification Authorities, | Revision C | Nov 1999 |
| NS4009 | NSTISSI 4009, National Information Systems Security Glossary | | Jan 1999 |
| NSD42 | National Policy for the Security of National Security Telecom and Information Systems, http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version) | | 5 Jul 1990 |
| PKCS-1 | PKCS #1 v2.0: RSA Cryptography Standard, http://www.rsa.com | | 1 Oct 1998 |
| PKCS-12 | Personal Information Exchange Syntax Standard, http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html | | Apr 1997 |
| ECA CP | <i>US Government Certificate Policy for External Certification Authorities</i> | Version 3.1 | 30 August 2006 |
| ECAKRP | <i>Key Recovery Policy for External Certification Authorities</i> | Version 1.0 | 4 Jun 2002 |
| FBCA CP | X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA), http://www.cio.gov/fkipa/documents/FBCA_CP_RFC3647.pdf | Version 2.6 | 16 Aug 2007 |
| ACES CP | <i>Revised Certificate Policy For Access Certificates for Electronic Services</i> | | 6 May 2004 |
| FPCPF CP | X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, http://www.cio.gov/fkipa/documents/CommonPolicy.pdf | Version 3647-1.1 | 16 Aug 2007 |
| FPKI-PROF | Federal PKI Certificate and CRL Extensions Profile, http://csrc.nist.gov/pki/ | | 31 May 2002 |
| CCP-PROF | X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program | Draft | 5 Jan 2006 |
| RFC3647 | Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, http://www.ietf.org/rfc/rfc3647.txt | | Nov 2003 |
| RFC2510 | Certificate Management Protocol, Adams and Farrell, http://www.ietf.org/rfc/rfc2510.txt | | Mar 1999 |
| SDN702 | SDN.702, Abstract Syntax for Utilization with Common Security Profile (CSP), Version 3 X.509 Certificates and Version 2 CRLs, http://www.armadillo.Huntsville.al.us/Forteza_docs/sdn702 | Revision 3 | 31 Jul 1997 |

| Number | Title | Revision | Date |
|--------|----------|----------|------|
| | rev3.pdf | | |

The following Federal laws, mandates, and instructions provide the security policy framework for the EI development, operations, and security:

- Privacy Act of 1974 (Public Law 93-579), December 1974
- Federal Managers Financial Integrity Act (FMFIA), September 1982
- Computer Security Act of 1987, January 1988
- Paperwork Reduction Act (Public Law 104-13), May 1995
- Information Technology Management Reform Act of 1996 (Clinger-Cohen Act) (Public Law 104-106), February 1996
- USA PATRIOT Act (Public Law 107-56), October 2001
- E-Government Act of 2002 (Public Law 107-347), December 2002
- Federal Information Security Management Act of 2002 [FISMA] (Public Law 107-347, Title III), December 2002
- Code of Federal Regulations, Title 5, Administrative Personnel, Part 731, Suitability, Subpart A, Scope, Section 106, *Designation of Public Trust Positions and Investigative Requirements*, (5 C.F.R. 731.106)
- Code of Federal Regulations, Title 5, Administrative Personnel, Part 930, Programs for Specific Positions and Examinations, Subpart C, Sections 930.301 through 930.305, *Employees Responsible for the Management or Use of Federal Computer Systems*, (5 C.F.R. 930.301-305)
- Presidential Decision Directive 63 (PDD-63), *Critical Information Protection*, May 1998
- Homeland Security Presidential Directive (HSPD) 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004
- Homeland Security Presidential Directive (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*
- Department of Defense Instruction 8500.2, *Information Assurance Implementation*, February 2003
- Department of Defense, Chief Information Officer Memorandum, *Encryption of Sensitive Unclassified Data at rest on Mobile Computing Devices and Removable Storage Media*, July 03, 2007
- Director of Central Intelligence Directive 6/3 Manual, *Protecting Sensitive Compartmented Information within Information Systems*, June 1999
- Director of Central Intelligence Directive 6/3 Manual, *Protecting Sensitive Compartmented Information within Information Systems*, May 2000
- Office of Management and Budget (OMB) Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000
- Office of Management and Budget, Circular A-130, Management of Federal Information Resources, Appendix III, *Security of Federal Automated Information Systems*, as revised November 2000

- Office of Management and Budget Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 2001
- Office of Management and Budget Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*, August 2003
- Office of Management and Budget, Federal Enterprise Architecture Program Management Office, *Business Reference Model (v2.0)*, June 2003
- Office of Management and Budget Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003
- Office of Management and Budget Memorandum M-04-04, *E-Authentication for Federal Agencies*, December 2003
- Office of Management and Budget Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD)12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2005
- Office of Management and Budget Memorandum M-06-16, *Protection of Sensitive Information*, June 2006
- Office of Management and Budget Memorandum M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, July 2006
- National Institute of Standards and Technology Federal Information Processing Standards (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001
- National Institute of Standards and Technology Federal Information Processing Standards (FIPS) Publication 180-2, *Secure Hash Standard (SHS)*, August 2002
- National Institute of Standards and Technology Federal Information Processing Standards (FIPS) Publication 186-2, *Digital Signature Standard (DSS)*, January 2000
- National Institute of Standards and Technology Federal Information Processing Standards (FIPS) Publication 188, *Standard Security Labels for Information Transfer*, September 1994
- National Institute of Standards and Technology Federal Information Processing Standards (FIPS) Publication 190, *Guidelines for the Use of Advanced Authentication Technology Alternatives*, September 1994
- National Institute of Standards and Technology Federal Information Processing Standards (FIPS) Publication 197, *Advanced Encryption Standards (AES)*, November 2001
- National Institute of Standards and Technology Federal Information Processing Standards (FIPS) Publication 198, *The Keyed-Hash Message Authentication Code (HMAC)*, March 2002
- National Institute of Standards and Technology Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
- National Institute of Standards and Technology Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006

- National Institute of Standards and Technology Federal Information Processing Standards (FIPS) Publication 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006
- International Organization for Standardization/International Electrotechnical Commission 17799, *Code of Practice for Information Security Management*, June 2005
- International Organization for Standardization/International Electrotechnical Commission 27001, *Information Security Management System Requirements*, October 2005
- National Security Telecommunications and Information Systems Security (NSTISSI) 7003, *Protective Distribution Systems (PDS)*, December 13, 1996
- NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995
- NIST Special Publication 800-13, *Telecommunications Security Guidelines for Telecommunications Management Network*, October 1995
- NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996
- National Institute of Standards and Technology Special Publication 800-15, *Minimum Interoperability Specifications for PKI Components (MISPC)*, Version 1, September 1997
- National Institute of Standards and Technology Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998
- National Institute of Standards and Technology Special Publication 800-17, *Modes of Operation Validation System (MOVS): Requirements and Procedures*, February 1998
- National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006
- National Institute of Standards and Technology Special Publication 800-19, *Mobile Agent Security*, October 1999
- National Institute of Standards and Technology Special Publication 800-20, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures*, April 2000
- National Institute of Standards and Technology Special Publication 800-21-1, *Second Edition, Guideline for Implementing Cryptography in the Federal Government*, December 2005
- National Institute of Standards and Technology Special Publication 800-22, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, May 2001
- National Institute of Standards and Technology Special Publication 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use Tested/Evaluated Products*, August 2000
- National Institute of Standards and Technology Special Publication 800-24, *PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does*, August 2000
- National Institute of Standards and Technology Special Publication 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, October 2000

- National Institute of Standards and Technology Special Publication 800-27, Revision A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, June 2004
- National Institute of Standards and Technology Special Publication 800-28, *Guidelines on Active Content and Mobile Code*, October 2001
- National Institute of Standards and Technology Special Publication 800-29, A *Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2*, June 2001
- National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002
- National Institute of Standards and Technology Special Publication 800-31, *Intrusion Detection Systems (IDS)*, November 2001
- National Institute of Standards and Technology Special Publication 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001
- National Institute of Standards and Technology Special Publication 800-33, *Underlying Technical Models for Information Technology Security*, December 2001
- National Institute of Standards and Technology Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002
- National Institute of Standards and Technology Special Publication 800-35, *Guide to Information Technology Security Services*, October 2003
- National Institute of Standards and Technology Special Publication 800-36, *Guide to Selecting Information Security Products*, October 2003
- National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004
- National Institute of Standards and Technology Special Publication 800-38A, *Recommendation for Block Cipher Modes of Operation – Methods and Techniques*, December 2001
- National Institute of Standards and Technology Special Publication 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, May 2005
- National Institute of Standards and Technology Special Publication 800-38C, *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*, May 2004
- National Institute of Standards and Technology Special Publication 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication (Draft)*, April 2006
- National Institute of Standards and Technology Special Publication 800-40, Version 2, *Creating a Patch and Vulnerability Management Program*, November 2005
- National Institute of Standards and Technology Special Publication 800-41, *Guidelines on Firewalls and Firewall Policy*, January 2002
- National Institute of Standards and Technology Special Publication 800-42, *Guide on Network Security Testing*, October 2003
- National Institute of Standards and Technology Special Publication 800-43, *Systems Administration Guidance for Windows 2000 Professional*, November 2002

- National Institute of Standards and Technology Special Publication 800-44, *Guidelines on Security Public Web Servers*, September 2002
- National Institute of Standards and Technology Special Publication 800-45A (Draft), *Guidelines on Electronic Mail Security*, August 2006
- National Institute of Standards and Technology Special Publication 800-46, *Security for Telecommuting and Broadband Communications*, August 2002
- National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002
- National Institute of Standards and Technology Special Publication 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*, November 2002
- National Institute of Standards and Technology Special Publication 800-49, *Federal S/MIME V3 Client Profile*, November 2002
- National Institute of Standards and Technology Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003
- National Institute of Standards and Technology Special Publication 800-51, *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*, September 2002
- National Institute of Standards and Technology Special Publication 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementation*, June 2005
- National Institute of Standards and Technology Special Publication 800-53 Revision 1, *Recommended Security Controls for Federal Information Systems*, December 2006
- National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems (Second Public Draft)*, April 2006
- National Institute of Standards and Technology Special Publication 800-54, *Border Gateway Protocol Security (Draft)*, September 2006
- National Institute of Standards and Technology Special Publication 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003
- National Institute of Standards and Technology Special Publication 800-56A, *Recommendations for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2006
- National Institute of Standards and Technology Special Publication 800-57, *Recommendation on Key Management*, August 2005
- National Institute of Standards and Technology Special Publication 800-58, *Security Considerations for Voice Over IP Systems*, January 2005
- National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003
- National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004
- National Institute of Standards and Technology Special Publication 800-61, *Computer Security Incident Handling Guide*, January 2004
- National Institute of Standards and Technology Special Publication 800-63, Version 1.0.2, *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Guidelines*, April 2006

- National Institute of Standards and Technology Special Publication 800-64, Revision 1, *Security Considerations in the Information System Development Life Cycle*, June 2004
- National Institute of Standards and Technology Special Publication 800-65, *Integrating Security into the Capital Planning and Investment Control Process*, January 2005
- National Institute of Standards and Technology Special Publication 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005
- National Institute of Standards and Technology Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, May 2004
- National Institute of Standards and Technology Special Publication 800-68, *Guidance for Security Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, October 2005
- National Institute of Standards and Technology Special Publication 800-69, *Guidance for Security Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist*, September 2006
- National Institute of Standards and Technology Special Publication 800-70, *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*, May 2005
- National Institute of Standards and Technology Special Publication 800-72, *Guidelines on PDA Forensics*, November 2004
- National Institute of Standards and Technology Special Publication 800-73, Revision 1, *Interfaces for Personal Identity Verification*, April 2006
- National Institute of Standards and Technology Special Publication 800-76-1, *Biometric Data Specification for Personal Identity Verification (Draft)*, September 2006
- National Institute of Standards and Technology Special Publication 800-77, *Guide to IPsec VPNs*, December 2005
- National Institute of Standards and Technology Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, April 2005
- National Institute of Standards and Technology Special Publication 800-79, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*, July 2005
- National Institute of Standards and Technology Special Publication 800-81, *Secure Domain Name System (DNS) Deployment Guide*, May 2006
- National Institute of Standards and Technology Special Publication 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security (Draft)*, September 2006
- National Institute of Standards and Technology Special Publication 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005
- National Institute of Standards and Technology Special Publication 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006
- National Institute of Standards and Technology Special Publication 800-85A, *PIV Card Application and Middleware Interface Test Guidelines*, April 2006
- National Institute of Standards and Technology Special Publication 800-85B, *PIV Data Model Test Guidelines*, July 2006

- National Institute of Standards and Technology Special Publication 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, August 2006
- National Institute of Standards and Technology Special Publication 800-87, *Codes for the Identification of Federal and Federally-Assisted Organizations*, January 2006
- National Institute of Standards and Technology Special Publication 800-88, *Guidelines for Media Sanitization*, September 2006
- National Institute of Standards and Technology Special Publication 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications*, November 2006
- National Institute of Standards and Technology Special Publication 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, June 2006
- National Institute of Standards and Technology Special Publication 800-92, *Guide to Computer Security Log Management*, September 2006
- National Institute of Standards and Technology Special Publication 800-94, *Guide to Intrusion Detection and Prevention (IDP) Systems* (Draft), August 2006
- National Institute of Standards and Technology Special Publication 800-95, *Guide to Secure Web Services* (Draft), August 2006
- National Institute of Standards and Technology Special Publication 800-96, *PIV Card/Reader Interoperability Guidelines*, September 2006
- National Institute of Standards and Technology Special Publication 800-97, *Guide to IEEE 802.11: Establishing Robust Security Networks* (Draft), June 2006
- National Institute of Standards and Technology Special Publication 800-98, *Guidance for Security Radio Frequency Identification (RFID) Systems* (Draft), September 2006
- National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, October 2006
- National Institute of Standards and Technology Special Publication 800-101, *Guidelines on Cell Phone Forensics* (Draft), August 2006
- Government Accountability Office, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6, January 1999
- DISA Security Technical Implementation Guides (STIGs) and Checklists at <http://csrc.nist.gov/pcig/cig.html>
- GSA Order CIO 2140.2, *System Development Life Cycle (SDLC) Policy Handbook*, April 20, 2004
- GSA Order CIO 2160.2, *GSA Electronic Messaging Policy*
- GSA Order CIO 2100.2, *GSA Wireless Local Area Network (LAN) Security*, October 30, 2005
- GSA Order CIO P 2100.1D, *GSA Information Technology (IT) Security Policy*, June 21, 2007
- GSA Order CPO 1878.2, *Conducting Privacy Impact Assessment*, May 28, 2004
- GSA Order CPO 1878.1, *GSA Privacy Act Program*, October 27, 2003
- GSA Order CIO 2104.1, *GSA Information Technology (IT) General Rules of Behavior*, July 3, 2003
- GSA Handbook ADM P 9732.1C, *Suitability and Personnel Security*, February 17, 2006

- CIO Instructional Letter 05-03 Mandatory IT Security Training for Agency and Contractor Employees with Significant Security Responsibilities, April 21, 2005
- IT Security Procedural Guide: Bluetooth Security Hardening, CIO-IT Security-07-36, March 7, 2007
- IT Security Procedural Guide: Web Application Security Guide, CIO-IT Security-07-35, Revision 1, February 12, 2007
- IT Security Procedural Guide: CISCO CALL Manager and Unity Hardening, CIO-IT Security-07-34, February 12, 2007
- IT Security Procedural Guide: McAfee VirusScan 8.0i, CIO-IT Security-06-33, Revision 1, February 21, 2007
- IT Security Procedural Guide: Media Sanitization Guide, CIO-IT Security-06-32, December 21, 2006
- IT Security Procedural Guide: Firewall Change Request, CIO-IT Security-06-31, November 8, 2006
- IT Security Procedural Guide: Handling IT Security Incidents, CIO-IT Security-01-02, Revision 3, July 23, 2006
- Standard Operating Procedure For GSA HSPD-12 Personnel Security Process, October 26, 2005
- IT Security Procedural Guide: Home Users Guide, CIO-IT Security-04-24, Revision 1, September 29, 2005
- IT Security Procedural Guide: Developing a Configuration Management (CM) Plan, CIO-IT Security-01-05, Revision 1, September 9, 2005
- IT Security Procedural Guide: Termination and Transfer, CIO-IT Security-03-23, Revision 1, August 29, 2005
- IT Security Procedural Guide: Auditing and Monitoring, CIO-IT Security-01-08, Revision 1, June 29, 2005
- IT Security Procedural Guide: Password Generation and Protection, CIO-IT Security-01-01, Revision 1, June 23, 2005
- IT Security Procedural Guide: Access Control, CIO-IT Security-01-07, Revision 1, June 23, 2005
- IT Security Procedural Guide: FISMA/POA&M Implementation, CIO-IT Security-04-26, Revision 4, May 26, 2005
- IT Security Procedural Guide: IT Security Training and Awareness Program, CIO-IT Security-05-29, Revision 1 April 27, 2006
- IT Security Procedural Guide: Contingency Plan Testing, CIO-IT Security-06-29, Revision 1, February 22, 2007
- IT Security Procedural Guide: Managing Enterprise Risk, CIO-IT Security-06-30, Revision 3, March 20, 2007
- IT Security Procedural Guide: Windows XP Professional Hardening, CIO-IT Security-03-22, Revision 6a, March 3, 2006
- IT Security Procedural Guide: Oracle Database Hardening, CIO-IT Security-05-28, March 29, 2005
- IT Security Procedural Guide: CISCO Router Hardening, CIO-IT Security-05-27, March 8, 2005

- IT Security Procedural Guide: Windows 2000 Professional Hardening, CIO-IT Security-02-15, Revision 3, November 16, 2004
- IT Security Procedural Guide: Windows 2003 Server Hardening, CIO-IT Security-04-25, Revision 2, June 21, 2006
- IT Security Procedural Guide: Sun Solaris Hardening, CIO-IT Security-02-20, August 30, 2002
- IT Security Procedural Guide: IIS 5.0 Server Hardening Implementation Guide, CIO-IT Security-02-19, July 24, 2002
- IT Security Procedural Guide: IIS 5.0 Server Hardening, CIO-IT Security-02-18, July 24, 2002
- IT Security Procedural Guide: Windows 2000 Server Hardening Implementation Guide, CIO-IT Security-02-17, July 24, 2002
- IT Security Procedural Guide: Windows 2000 Server Hardening, CIO-IT Security-02-16, July 24, 2002
- IT Security Procedural Guide: Microsoft IIS 4.0 Hardening, CIO-IT Security-01-14, May 14, 2001
- IT Security Procedural Guide: Windows NT 4.0 Hardening, CIO-IT Security-01-13, May 14, 2001
- GSA Internet Explorer 6.0 Configuration Guide
- FTS CIO Policy Memo 03-08 Account Closeout Procedures
- FTS CIO Policy Memo 03-04 Local Workstation Access Rights
- Computer Fraud & Abuse of 1986, as amended, Public Law 99-474
- OMB Memorandum M-01-08

25 REVISION HISTORY

| Version | Date | Comments |
|---------|--------------------|--|
| 0.1 | November 2007 | First Draft of LOR created |
| 0.2 | November 2007 | Minor edits |
| 0.3 | November 2007 | Modified to add Practice note under Section 1.6 FiXs Logical Trust Model; Section 1.7, Credential Uniqueness and Section 1.8, FiXs Assurance Level; Section 2.4 Uniqueness Across the FiXs Network; under Section 4 Relying Party Responsibility added language regarding FiXs Credentials assistance to Relying Parties in meeting their responsibilities for logical authentication; also to add Section 4.1.2.1 Application (Component) Certificates and Section 4.1.2.2 Application (Component) Private Key Protection; under Definitions, added the definition for Credential Holder; under References, added reference to DoD CIO memorandum dated July 3, 2007. |
| 0.4 | March 26, 2008 | Modified to add Registration Practice Statement (RPS) to section 2.2. |
| 0.5 | June 9, 2008 | Modified to update Sections 1.7 (to accommodate Federal PKI Common Policy DN restrictions) and 1.8. |
| 1.0 | September 25, 2008 | Final baseline edits. |
| 1.0 | October 1, 2008 | Board voted approval of Version 1.0 and approves making the Version 1.0 an appendix to the FiXs Operating Rules. |
| | | |