



The Federation for Identity and
Cross-Credentialing Systems®

FIXS® ***IMPLEMENTATION GUIDELINES***

VERSION 3.1

JANUARY 31, 2008

www.fixs.org

Copyright 2007 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 BACKGROUND3**
- 2 FIXS ASSURANCE LEVELS6**
 - 2.1 OVERVIEW 6
 - 2.2 IDENTITY MANAGEMENT METHODOLOGIES..... 6
 - 2.3 IMPLEMENTING THE ASSURANCE LEVELS 7
 - 2.4 ASSURANCE LEVEL OVERVIEW..... 7
 - 2.4.1 High Trust Level (Level 4)..... 7
 - 2.4.2 Medium High Trust Level (Level 3)..... 8
 - 2.4.3 Medium Trust Level (Level 2)..... 8
 - 2.4.4 Low Trust Level (level 1)..... 9
 - 2.5 FIXS ASSURANCE LEVEL IMPLEMENTATIONS10
- 3 FIXS IMPLEMENTATION GUIDELINES..... 13**
 - 3.1 HIGH LEVEL (4) --- HSPD-12 COMPATIBLE CREDENTIALS13
 - 3.1.1 Users.....13
 - 3.2 HIGH LEVEL (4) --DOD LOGICAL ACCESS CREDENTIALS (LACS)/PHYSICAL ACCESS CREDENTIALS (PACS) CREDENTIAL15
 - 3.2.1 Users.....15
 - 3.3 MEDIUM HIGH LEVEL (3)--DOD AND COMMERCIAL USE PACS/LACS CREDENTIAL16
 - 3.3.1 Users.....16
 - 3.4 MEDIUM HIGH LEVEL (3)--NON-SECURITY CLEARANCE CONTRACTOR AND COMMERCIAL USE CREDENTIAL.....17
 - 3.4.1 Users.....18
 - 3.5 MEDIUM HIGH LEVEL (3)--FIRST RESPONDER EMPLOYEES20
 - 3.5.1 USERS20
 - 3.6 MEDIUM LEVEL (2)--FIRST RESPONDER EMPLOYEES22
 - 3.6.1 USERS22
- 4 ATTRIBUTE MANAGEMENT FOR MEDIUM HIGH LEVEL (3) ENHANCED FIRST RESPONDER CREDENTIALS.....25**
 - 4.1 ATTRIBUTE MANAGEMENT FOR MEDIUM HIGH LEVEL (3) CLINICAL FIRST RESPONDER CREDENTIALS25
 - 4.1.1 USERS25

EXHIBITS & APPENDICES

- TECHNICAL SPECIFICATION FOR CREATING A UNIQUE IDENTIFIER FOR A FIPS 201-ALIGNED FIXS™ CREDENTIAL28**
- APPENDIX A - SMART CARD TOPOLOGY REQUIREMENTS37**
- APPENDIX B - FIXS BARCODE REQUIREMENTS43**

1 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 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. 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.

At the present time the Federal Government has defined four recognized “security” 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, along with the standards and specifications for the credential/card itself. *FiXs has chosen to use FIPS 201 compliant smart card specifications for all Levels of Trust. Thus, the main*

differentiation between the levels is primarily the vetting process, documentation/verification, and biometric data collected, verified and maintained in the federated data model. FiXs- certified credentials also contain the appropriate data designating under which Level of Trust the credential was issued and classified accordingly.

The current Government sanctioned nomenclature for describing “Levels” is numerical (i.e. 4, 3, 2, 1) and described below. FiXs defines these levels with a non-numeric designation of Trust Level which provides a descriptive context associated by security level. Therefore, the remainder of this document and the accompanying Implementation Guidelines document will offer a corollary non-numeric description of levels to equate to the numerical levels used by the government:

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

The highest trust level, Level 4, or 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, or FiXs equivalent “Medium High” has not been defined at this time by a specific Federal Directive or Policy. FiXs members however have a requirement for this level of credential to meet their own use case situation(s), supporting constituencies such as: first responders, law enforcement, medical personnel, logistics personnel, maintenance and/or grounds personnel, etc. and others where the very highest level of background investigation is not warranted or practical. Accordingly, FiXs has promulgated Implementation Guidelines to accommodate these requirements and has presented these Implementation Guidelines to the Federal Government for consideration and adoption. FiXs-certified credential defined at the “medium high trust” level, or government Level 3, are aligned with PIV II, but differ from PIV I provisions in the enrollment process.

Level 2, or FiXs equivalent “Medium” is again aligned with PIV II, and differs somewhat from Level 3 in the enrollment process. The details for both the “medium high trust” and the “medium trust” levels are defined in detail in the FiXs Implementation Guidelines.

Level 1 or FiXs equivalent “Low”. is considered an un-acceptable level of trust for the Federal Government and for many use cases where a certain authoritative level of trust is needed or desired. FiXs “Certified Credentials” will at a future date assess the validity, requirements and resources required for this level. The level presently is not being used.

The FiXs Implementation Guidelines document provides the specific requirements for the vetting of sponsored individuals requesting credentials for “high”, medium high”, and “medium” trust levels”, and in specific market/functional venues. The accompanying CHUID section of the Implementation Guidelines deals with the specifics of the data and specifications of the card. Accordingly, these Operating Rules and the Implementation Guidelines must be read in tandem to implement FiXs cross-credentialing services.

Historically, FiXs has borrowed many of its operating 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 proven and established for the payments industry, NACHA – The Electronic Payments Association assisted with its knowledge and experience in development of the FiXs Operating Rules. This decades long experience and lessons learned allows FiXs to provide a proven and time-tested framework for inter-operable identity authentication similar to what has been achieved in the financial industry for financial transactions.

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, standards, and platforms. The objective is to establish the standards and operational framework for a secure and interoperable “Chain of Trust” for all members regardless of industry or professional designation(s).

The FiXs Implementation Guidelines document provides detail on the requirements for issuing FiXs-Certified Credentials at different levels of confidence or assurance. The FiXs Operating Rules contain minimum requirements for issuing FiXs-Certified Credentials. All FiXs-Certified Credentials, regardless of their level of assurance, must comply with the FiXs Operating Rules and these Implementation Guidelines. The FiXs Implementation Guidelines provide additional requirements that must be followed by Member Organizations and Subscribers, depending upon the level and type of Credential issued. These processes deal with, but are not limited to, identity verification, enrollment, security and audit. These Guidelines only address provisions that are more detailed than the requirements in the FiXs Operating Rules.

All FiXs Certified credentials will have the ability to be distinguished according to the Level of Trust assurance under which they were issued. The following guidelines are not inclusive of the life cycle management controls and will be addressed at a later date.

2 FIXS ASSURANCE LEVELS

2.1 Overview

An underlying objective, whether explicit or not, of most identity management programs is to manage risk. In order to do that, a Credential Issuer first defines an acceptable level of risk and then identifies standards, criteria and procedures that, to the extent possible, support this level. Sometimes, the risk level and standards are defined by an external organization, such as a government Agency or client. When this is the case, a Credential Issuer must adopt the prescribed processes and requirements. However, another aspect of identity management programs is striking an appropriate balance between risk management, cost and feasibility considerations. This can be achieved through a Federated approach. For instance, it is possible to enact standards or criteria that are too stringent and that unnecessarily eliminate otherwise qualified personnel from being issued a credential. In addition to defining an acceptable level of risk, Credential Issuers should also consider the demographic of the population to be credentialed and the resources (physical and/or logical) to which the credential holders will have access. Thus, by “federating” the approach, it is possible to accommodate these requirements

In order to streamline this process for Credential Issuers, FiXs has identified and endorsed several Assurance Levels, targeted at different user communities. When developing these Assurance Levels, FiXs first identified “target populations” that would require credentials and then analyzed what types of resource access the credential holder might need. For instance, contractors working on US Federal government contracts might need access to US Federal government facilities or logical resources (a government LAN). In this case, the User would require a FiXs HSPD-12 Compatible Credential, which is based on FiXs Assurance Level 4. This particular credential is intentionally aligned with the government’s “Personal Identity Verification” (PIV) standard. In another example, Emergency Responders requiring access to an emergency scene might qualify for one of the Assurance Level 3 credentials. The Assurance Levels are defined in Section 1.1, while implementation guidelines for the specific user groups are provided in Section 2.

2.2 Identity Management Methodologies

Two methodologies support the risk management feature of identity management programs: identity verification and identity vetting. **Identity verification** uses manual and electronic methods to prove, to some level of certainty, that an applicant is who he says he is. Manual methods of verification include visual review of identity documents, such as birth certificates or drivers licenses, by trained personnel. Electronic methods include electronic authentication of documents using a document authenticator, or a “knowledge-based challenge quiz” that involves asking the applicant questions to which only the applicant should know the answers.

Identity vetting assumes that, from a risk assessment standpoint, a likely predictor of a person’s future behavior is their past behavior. Identity vetting, then, uses various methods and tools to establish a profile of a person’s behavior. In most cases, Identity vetting begins with an Applicant providing a detailed

background history including past residences, employment history, educational background and any criminal record. Even though much of this information will be returned by the actual background check, asking a person to self report this information provides an additional measure of trustworthiness. Depending on the Assurance Level, a background check may include an FBI Name and Fingerprint check, a local records (criminal database) check, manual verification of the Applicant's educational attainment, and/or a credit history report which may validate the Applicant's reported residence history. Once this historical information is compiled, a trained Adjudicator must make a trustworthiness assessment of the Applicant prior to the Applicant being enrolled into a FiXs Domain Server.

A strong identity management program often utilizes both identity verification and identity vetting elements.

2.3 Implementing the Assurance Levels

Specific implementation standards, as proposed by user industry experts and approved by the FiXs Board, are provided in Section 2 of this document. Members wishing to issue FiXs Credentials must first identify which standards they intend to follow and then meet the requirements of the specified standard(s).

2.4 Assurance Level Overview

The FiXs Assurance Levels described below are aligned to the National Institute of Standards and Technology's (NIST) Information Security guidelines [NIST SP 800-63].

2.4.1 HIGH TRUST LEVEL (LEVEL 4)

The High Level of Trust, (Level 4), 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.

Examples of persons needing a High Trust Level (Level 4) credential include contractors on US government contracts, employees of FiXs Member Companies that require a High Level assurance credential, and individuals that currently have a clearance or that will be processed for a clearance. In this last case, the background check involved in the

clearance process may be substituted for the High Level assurance background check.

2.4.2 MEDIUM HIGH TRUST LEVEL (LEVEL 3)

The Medium High Trust level (Level 3), has not been defined, at this time, by a Federal Directive or Policy. FiXs members, however, have a requirement for using this level of credential in both the government and commercial sectors, and thus FiXs has developed a set of Guidelines to accommodate that Medium High (Level 3) requirement. These Guidelines have been offered to the Federal government for consideration and adoption. FiXs Credentials certified at the Medium High Trust Level are aligned and compliant with FIPS 201, but will differ from PIV I provisions relating to the enrollment and vetting processes.

The Medium High Trust Level is designed to provide a medium high level of assurance for employees and includes both identity verification and in some cases additional identity vetting/verification attributes (i.e. First Responder and Health Care personnel Credentials). This level will require a background check, using commercially available sources of data, and fingerprints will be collected digitally at time of enrollment and **will be** sent to the FBI for a National Criminal History Fingerprint check.

Possible uses of a Medium High Trust Level include; employees of FiXs Member Companies/Organizations who do not need daily or frequent access to federal resources to support a government contracts; and credentialing a First Responder community, or service personnel who need access to federal or commercial facilities or environs. The Medium High Trust credential can also be used for Commercial applications.

2.4.3 MEDIUM TRUST LEVEL (LEVEL 2)

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.

2.4.4 LOW TRUST LEVEL (LEVEL 1)

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.

2.5 FiXs Assurance Level Implementations

FiXs Credential Name	Assurance Level	Who
HSPD-12 Compatible Credentials	High (4)	<ul style="list-style-type: none"> • FiXs Member Company (or Subscriber) employees or contractors who perform work under a Federal government contract that includes the identity FAR clause. • Employees of a FiXs Member Company (or Subscriber) that requires an HSPD-12 Compatible Credential for some or all of their employees.
DoD Logical Access Credentials (LACS)/Physical Access Credentials (PACS) Credentials	High (4)	<ul style="list-style-type: none"> • FiXs Member Company (or Subscriber) employees or contractors on U.S. Department of Defense contracts who require long term (6 months or greater) access to DoD physical or logical resources. • FiXs Member Company (or Subscriber) employees who are required to authenticate to DoD resources at the highest level of assurance (Level 4).
DoD and Commercial use PACS/Short-term LACS Credentials	Medium High (3)	<ul style="list-style-type: none"> • FiXs Member Company (or Subscriber) employees or contractors who require physical access to a U.S. Department of Defense facility. • FiXs Member Company (or Subscriber) employees who are required to authenticate to DoD resources at a medium high level of assurance (3). • FiXs Member Company (or Subscriber) employees who do not have a requirement to authenticate to government facilities but do have a need for a medium high level of assurance for commercial use for physical/logical access.
Non-Security Clearance Contractor and Commercial use Credential	Medium High (3)	<ul style="list-style-type: none"> • Participants are those individuals needing physical access to Govt. facilities on a limited basis or for commercial uses not requiring access to government facilities. Examples of the would be: <ul style="list-style-type: none"> ○ Transportation Workers ○ Commercial Vendors <ul style="list-style-type: none"> ▪ Delivery Personnel ▪ Grounds personnel ▪ Repair Technicians ▪ Cleaning & Maintenance personnel ○ Facility Visitors for occasional official business ○ Leaders of tour groups, school personnel, on official tours ○ Health Care employees/patients ○ Financial/Insurance sector employees/customers

FiXs Credential Name	Assurance Level	Who
Enhanced First Responder	Medium High (3)	<ul style="list-style-type: none"> • Participants who may need a FiXs Medium High Level (3) Enhanced First Responder Credential may include first responders identified by the authority having jurisdiction as holding sensitive positions or requiring access to secure Federal, State, or local facilities. These individuals may include but are not limited to: <ul style="list-style-type: none"> ○ Police Officers ○ Sheriffs Officers ○ Corrections Officers ○ Municipal, County, State and Industrial Fire Fighters ○ Emergency Medical Technicians and Paramedics
Enhanced Clinical First Responder Credential	Medium High (3)	<ul style="list-style-type: none"> • Participants who may need a FiXs Medium High Level (3) Enhanced Clinical First Responder Credential may include first responders identified by the authority having jurisdiction as holding sensitive positions or requiring access to secure Federal, State, or local facilities. These individuals may include but are not limited to: <ul style="list-style-type: none"> ○ Physicians ○ Registered Nurses ○ Behavioral Health Professionals¹ ○ Advanced Practice Nurses² ○ Physicians Assistants ○ Dentists ○ Emergency Medical Technicians and Paramedics
Standard First Responder Credential	Medium (2)	<ul style="list-style-type: none"> • Participants who may need a FiXs Medium Level (2) Standard First Responder Credential may include but are not limited to: <ul style="list-style-type: none"> ○ Municipal, County, State and Industrial Fire Fighters ○ Emergency Medical Technicians ○ Public Works Employees ○ Red Cross, Salvation Army and other humanitarian volunteers ○ National Citizen Corps Volunteers

¹ Marriage and Family Therapists, Medical and Public Health Social Workers, Mental Health and Substance abuse Social Workers, Psychologists, and Mental Health Counselors. ESAR-VHP Interim Technical and Policy Guidelines, Standards, and Definitions – Version 2 June 2005

² Nurse Practitioners, Nurse Anesthetists, Certified Nurse Midwives, Clinical Nurses Specialists. ESAR-VHP Interim Technical and Policy Guidelines, Standards, and Definitions – Version 2 June 2005

FiXs Credential Name	Assurance Level	Who
Standard Clinical First Responder Credential	Medium (2)	<ul style="list-style-type: none"> • Participants who may need a FiXs Medium Level (2) Standard Clinical First Responder Credential may include but are not limited to: <ul style="list-style-type: none"> ○ Pharmacists ○ Licensed Practical Nurses ○ Respiratory Therapists and Technicians ○ Cardiovascular Technologist and Technicians ○ Radiological Technologists & Technicians ○ Surgical Technologists ○ Medical and Clinical Laboratory Technologists

3 FIXS IMPLEMENTATION GUIDELINES

3.1 High Level (4) --- HSPD-12 Compatible Credentials

A FiXs HSPD-12 Compatible Credential is based on a High Level assurance (4), set of processes, and the highest assurance level achievable. The credential aligns with the Federal government's "Personal Identity Verification" (PIV) standards. The FiXs HSPD-12 Compatible Credential requires two forms of government ID to verify the person's identity and uses a background check to evaluate a person's trustworthiness to have access to physical and logical resources.

3.1.1 USERS

Participants who may need a FiXs HSPD-12 Compatible Credential include:

- FiXs Member Company (or Subscriber) employees or contractors who perform work under a Federal government contract that includes the identity FAR clause.
- Employees of a FiXs Member Company (or Subscriber) that requires an HSPD-12 Compatible Credential for some or all of their employees.

High Level HSPD-12 Compatible Credentials

System Requirements

- Must adhere to the “FIPS PUB 201: Personal Identity Verification (PIV) of Federal Employees and Contractors” standards, including separation of system roles and revocation requirements.

Identity Verification Requirements:

- Applicant must appear in person
- Applicant must present 2 forms of government ID, per the I-9 form, one of which must be a photo ID

Identity Vetting Requirements:

- NAC:
 - Security/Suitability Investigations Index (SII)
 - Defense Clearance and Investigations Index (DCII)
 - FBI Name Check
 - FBI National Criminal History Fingerprint Check
- Written inquiries and searches of records:
 - Employment, going back 5 years
 - Education, going back 5 years and verifying highest degree
 - Residence, going back 3 years
 - References
 - Law enforcement checks, going back 5 years

Adjudication Standards:

The following criterion will be used to adjudicate the background investigations for persons requiring a FiXs HSPD-12 Compatible Credential. No person shall be granted such a credential if their background investigation reveals any of the following:

- Is, or is suspected of being, a terrorist;
- Is the subject of an outstanding warrant;
- Has deliberately omitted, concealed, or falsified relevant and material facts from any official form used to collect biographic information for the purpose of initiating a background check;
- Has presented false or forged identity source documents;
- Has been barred from Federal employment;
- Is currently awaiting a hearing or trial or has been convicted of a crime punishable by imprisonment of six (6) months or longer; or
- Is awaiting or servicing a form of pre-prosecution probation, suspended or deferred sentencing, probation or parole in conjunction with an arrest or criminal charges against the individual for a crime that is punishable by imprisonment of six (6) months or longer.

3.2 High Level (4) --DoD Logical Access Credentials (LACS)/Physical Access Credentials (PACS) Credential

The FiXs DoD LACS/PACS Credential is based on assurance Level 4 and is intended for individuals who will have long-term physical and/or logical access to DoD resources.

3.2.1 USERS

Participants who may need a DoD LACS/PACS Compatible Credential include:

- FiXs Member Company (or Subscriber) employees or contractors on U.S. Department of Defense contracts who require long term (6 months or greater) access to DoD physical or logical resources.
- FiXs Member Company (or Subscriber) employees who are required to authenticate to DoD resources at the highest level of assurance (Level 4).

High Level DoD LACS/PACS Credential
<p>System Requirements</p> <ul style="list-style-type: none">• Must adhere to the “FIPS PUB 201: Personal Identity Verification (PIV) of Federal Employees and Contractors” standards, including separation of system roles and revocation requirements.• In addition, the System must also capture the following:<ul style="list-style-type: none">○ Contract number under which the FiXs Member Company (or Subscriber) employee requires access to DoD resources, and○ Reference to any existing security clearance an Applicant might have.
<p>Identity Verification Requirements:</p> <ul style="list-style-type: none">• Applicant must appear in person• Applicant must present 2 forms of government ID, per the I-9 form, one of which must be a photo ID
<p>Identity Vetting Requirements:</p> <ul style="list-style-type: none">• NAC:<ul style="list-style-type: none">○ Security/Suitability Investigations Index (SII)○ Defense Clearance and Investigations Index (DCII)○ FBI Name Check○ FBI National Criminal History Fingerprint Check• Written inquiries and searches of records:<ul style="list-style-type: none">○ Employment, going back 5 years○ Education, going back 5 years and verifying highest degree○ Residence, going back 3 years○ References○ Law enforcement checks, going back 5 years

High Level DoD LACS/PACS Credential

Adjudication Standards:

The following criterion will be used to adjudicate the background investigations for persons requiring a FiXs DoD LACS/PACS Credential. No person shall be granted such a credential if their background investigation reveals any of the following:

- Is, or is suspected of being, a terrorist;
- Is the subject of an outstanding warrant;
- Has deliberately omitted, concealed, or falsified relevant and material facts from any official form used to collect biographic information for the purpose of initiating a background check;
- Has presented false or forged identity source documents;
- Has been barred from Federal employment;
- Is currently awaiting a hearing or trial or has been convicted of a crime punishable by imprisonment of six (6) months or longer; or
- Is awaiting or servicing a form of pre-prosecution probation, suspended or deferred sentencing, probation or parole in conjunction with an arrest or criminal charges against the individual for a crime that is punishable by imprisonment of six (6) months or longer.

3.3 Medium High Level (3)---DoD and Commercial Use PACS/LACS Credential

The FiXs DoD and Commercial Use PACS/Short-term LACS Credential, which is based on the Medium High assurance level, provides a medium high amount of assurance the credential holder is who they assert themselves to be and that they do not harbor any malicious or criminal intent.

3.3.1 USERS

Participants who may need a DoD and Commercial Use PACS/Medium High/ LACS Credential include:

- FiXs Member Company (or Subscriber) employees or contractors who, based on a contract with the DOD, require physical access to a DoD facility.
- An employee or contractor of a FiXs Member Company (or Subscriber) who, because of short term contractual terms, needs a credential for access.
- FiXs Member Company (or Subscriber) employees who are required to authenticate to DoD resources at a medium high level of assurance.
- FiXs Member Company (or Subscriber) employees who **do not** have a requirement to authenticate to DoD or other government entities but do have a commercial use requirement.

Medium High Level DoD and Commercial Use PACS/ LACS Credential
<p>System Requirements</p> <ul style="list-style-type: none"> • Must adhere to the “FIPS PUB 201: Personal Identity Verification (PIV) of Federal Employees and Contractors” standards, including separation of system roles and revocation requirements. • In addition, the System must also capture the following: <ul style="list-style-type: none"> ○ Contract number under which the FiXs Member Company (or Subscriber) employee requires access to DoD resources, and ○ Reference to any existing security clearance an Applicant might have.
<p>Identity Verification Requirements:</p> <ul style="list-style-type: none"> • Applicant must appear in person • Applicant must present 2 forms of government ID, per the I-9 form, one of which must be a photo ID
<p>Background Check Components:</p> <ul style="list-style-type: none"> • Terrorist watch list check • Law Enforcement checks, going back five (5) years • FBI Name Check • FBI National Criminal History Fingerprint Check
<p>Adjudication Standards:</p> <p>The following criterion will be used to adjudicate the background investigations for persons requiring a FiXs DoD PACS/Short-term LACS Credential. No person shall be granted such a credential if their background investigation reveals any of the following:</p> <ul style="list-style-type: none"> • Is, or is suspected of being, a terrorist; • Is the subject of an outstanding warrant; • Has deliberately omitted, concealed, or falsified relevant and material facts from any official form used to collect biographic information for the purpose of initiating a background check; • Has presented false or forged identity source documents; • Is currently awaiting a hearing or trial or has been convicted of a crime punishable by imprisonment of six (6) months or longer; or • Is awaiting or servicing a form of pre-prosecution probation, suspended or deferred sentencing, probation or parole in conjunction with an arrest or criminal charges against the individual for a crime that is punishable by imprisonment of six (6) months or longer.

3.4 Medium High Level (3)---Non-Security Clearance Contractor and Commercial Use Credential

The FiXs Non-Security Clearance and Commercial Use Credential, which is based on a Medium High Trust assurance level, provides a medium high amount of assurance that the credential holder is who he/she asserts themselves to be and that they do not harbor any malicious or criminal intent. Timely physical access is

imperative for the individual to be able to provide their service to the receiving Government office.

3.4.1 USERS

Participants who may need a Non-Security Clearance Contractor credentials include:

- Transportation Workers
- Commercial Vendors
- Maintenance Personnel
- Cleaning and Grounds Personnel
- Repair technicians
- Facility Visitors for occasional official business
- Leaders of tour groups, school personnel, etc who conduct tours
- Health Care Personnel
- Critical Infrastructure Supply Chain personnel

Medium High Level (3) – Non-Security Clearance and Commercial Use Credential for Commercial Vendors and Non-government employees and government contractors

System Requirements

Must adhere to the Fair Credit and Reporting Act (The FCRA) and other applicable laws. All identified job skills personnel/individuals must be informed, by the credential issuer, that by giving their approval under the “Identity Verification Requirement” and entering their personally identifiable data into the system, they consent and authorize FiXs and/or third party background screening provider(s) to perform background screenings checks for them that “requires physical or logical access to their job or agency-related activity but do not fall under the category of government employee or government contractor.

Identity Verification Requirements

- Applicants must have a sponsor (*authorizes the need for applicant to obtain physical and logical access to Federal facility*)
- Applicant must appear in person at Registration or Enrollment Station
- Applicant must present 2 forms of Government issued ID Per US Form I-9 or 6 CFR Part 37³, one of which must have a photo.
- Individual Information:
 - ✓ Date of birth;
 - ✓ Proof of SSN or ineligibility for an SSN;
 - ✓ The applicant’s address of principal residence; and
 - ✓ Lawful status in the United States.
 - ✓ Company-issued Employee Identification Number
 - ✓ Felony and Misdemeanor convictions
 - ✓ Outstanding warrant
 - ✓ Terrorist Watch List
- Applicants fingerprints will be collected electronically (ten flat or rolled)
- Applicants pin must be used to complete the transaction

³ A valid unexpired U.S. passport.9; A certified copy of a birth certificate; A consular report of birth abroad; An unexpired permanent resident card.; An unexpired employment authorization document (EAD); An unexpired foreign passport with valid U.S. visa affixed; A U.S. certificate of citizenship; A U.S. certificate of naturalization; or A REAL ID driver’s license or identification card issued subsequent to the standards established by this regulation.

Medium High Level (3) – Non-Security Clearance and Commercial Use Credential for Commercial Vendors and Non-government employees and government contractors

Identity Vetting Requirements

- **NAC I Commercial Equivalent Check (CEC).**
 - FBI Name and FBI National Criminal History Fingerprint Check
 - Terrorist Watch List
 - Local Law Enforcement agency check
 - Residency verification

- **Written Inquires and Search of Records**
 - Employment going back 5 years
 - Education going back 5 years
 - Residences going back 3 years (*Note: Separately, all overseas addresses*)
 - References (*3 personal, non- relatives*)

Adjudication Standards:

The following criteria will be used to adjudicate the background checks for persons requiring a FiXs Non-Security Clearance Contractor Credential at the Medium High Level (3). No person shall be granted such as credential if the background check reveals any of the following:

- Is or is suspected of being a terrorist;
- Has been charged or convicted under any provision of the Patriot Act
- Is the subject of an outstanding warrant;
- Has deliberately omitted, concealed, or falsified relevant or material facts from any official form used to collect biographic information for the purpose of initiating a background check;
- Has presented false or forged identity documents;
- Has a current Criminal (not civil) restraining order, or has had a criminal restraining order within the last five years, issued due to threat of violence or sexual assault
- Is on the Sex Offenders List (level 2 or 3) (in the last ten years level 2, life level 3)
- Is currently awaiting a hearing or trial or has been convicted of a crime punishable by imprisonment of six (6) months or longer; or
- Is awaiting or servicing a form of pre-prosecution probation; suspended or deferred sentencing, probation or parole in conjunction with an arrest or criminal charges against the individual for a crime that is punishable by imprisonment of six (6) months or longer.

3.5 MEDIUM HIGH LEVEL (3)--First Responder Employees

Enhanced First Responder Credential – Medium High Level (3) The FiXs Enhanced First Responder Credential, which is based on a Medium High Trust assurance level, provides a medium high amount of assurance that the credential holder is who he/she asserts themselves to be and that he does not harbor any malicious or criminal intent.

3.5.1 USERS

Participants who may need a FiXs Medium High Level Enhanced First Responder Credential may include first responders identified by the authority having jurisdiction as holding knowledge sensitive positions or requiring unlimited access to secure Federal, State, or local facilities.

Medium High Level (3) – Non-Security Clearance Credential for Enhanced First Responder Designees

Identity Verification Requirements

- Applicants must have a sponsor (*authorizes the need for applicant to obtain physical and logical access to Federal facility*)
- Applicant must appear in person at Registration or Enrollment Station
- Applicant must present 2 forms of Government issued ID Per US Form I-9 or 6 CFR Part 37⁴, one of which must have a photo.
- Applicants fingerprints will be collected electronically (ten flat or rolled)
- Applicant must appear in person
- Applicant must present 2 forms of Government issued ID Per US Form I-9 or 6 CFR Part 37, one of which must have a photo. Documents must include information supporting the claim of
 - Date of birth;
 - Proof of SSN or ineligibility for an SSN;
 - The applicant's address of principal residence; and
 - Lawful status in the United States.
- Applicants fingerprints will be collected electronically (ten flat or rolled)
- Applicants pin must be used to complete the transaction

⁴ A valid unexpired U.S. passport; A certified copy of a birth certificate; A consular report of birth abroad; An unexpired permanent resident card.; An unexpired employment authorization document (EAD); An unexpired foreign passport with valid U.S. visa affixed; A U.S. certificate of citizenship; A U.S. certificate of naturalization; or A REAL ID driver's license or identification card issued subsequent to the standards established by this regulation.

Medium High Level (3) – Non-Security Clearance Credential for Enhanced First Responder Designees

Identity Vetting Requirements

- Establish validity of the identity - Identity proofing using electronic methods providing identity proofing criteria from public record and publicly available sources to include verification of enrollment information and breeder documents required in Federal form I-9, to verify the identity exists, the identity is active (not deceased) and the components are related at a high level of assurance.
- Establish ownership of the identity - vetting fraudulently obtained breeder documents using a third party interactive knowledge based query process presenting a minimum of five questions with successful response to at least 3.
- Biometric Cross Reference – Submit and check biometric against existing records for identity duplication and or criminal record history – to include but not limited to the Automated Fingerprint Identification System (AFIS)
- Criminal History Record Information (CHRI) / Risk Analysis (include a data quality score?) - to include Local, County, State, Federal Criminal History Checks; Department of Corrections Checks, Sex Offender Registry (SOR within NCIC), Patriot Act, Terrorist Watch List, Interstate Identification Index (triple I), NICS Index (firearms disqualifying records), National Crime Information Center (NCIC), National Protection Order File (within NCIC)
- **Written Inquires and Search of Records**
 - Employment going back 5 years
 - Education going back 5 years
 - Residences going back 3 years (*Note: Separately, all overseas addresses*)
 - References (*3 personal, non-relatives*)

Medium High Level (3) – Non-Security Clearance Credential for Enhanced First Responder Designees

Adjudication Standards:

The following criteria will be used to adjudicate the background checks for persons requiring a FiXs Standard First Responder Credential. No person shall be granted such as credential if the background check reveals any of the following:

- Is or is suspected of being a terrorist;
- Has been charged or convicted under any provision of the Patriot Act
- Is the subject of an outstanding warrant;
- Has deliberately omitted, concealed, or falsified relevant or material facts from any official form used to collect biographic information for the purpose of initiating a background check;
- Has presented false or forged identity documents;
- Has a current Criminal (not civil) restraining order, or has had a criminal restraining order within the last five years, issued due to threat of violence or sexual assault
- Is on the Sex Offenders List (level 2 or 3) (in the last ten years level 2, life level 3)
- Is currently awaiting a hearing or trial or has been convicted of a violent crime punishable by imprisonment of six (6) months or longer; or
- Is awaiting or servicing a form of pre-prosecution probation; suspended or deferred sentencing, probation or parole in conjunction with an arrest or criminal charges against the individual for a crime that is punishable by imprisonment of six (6) months or longer.

3.6 MEDIUM LEVEL (2)--First Responder Employees

Enhanced First Responder Credential – Medium Level (2)

The FiXs Standard First Responder Credential, which is based on Medium Trust assurance level, provides a medium amount of assurance that the credential holder is who he/she asserts themselves to be and that they do not harbor any malicious or criminal intent.

3.6.1 USERS

Participants who may need a FiXs Medium Level (2) Standard First Responder Credential may include first responders identified by the authority having jurisdiction as holding sensitive positions or requiring access to secure Federal, State, or local facilities.

Medium Level (2) – Non-Security Clearance Credential for Standard First Responder Designees

System Requirements

Must adhere to the Fair Credit and Reporting Act (The FCRA) and other applicable laws, this is to inform all identified job skills/individuals that by giving their approval under the “Identity Verification Requirement” and entering their personally identifiable data, they consent and authorize FIX’s and/or third party background screening provider(s) to perform background screenings checks for them that “requires physical or logical access to their job or agency-related activity but do not fall under the category of government employee or government contractor. Must adhere to the “FIPS PUB 201 Personal Identity Verification (PIV) I of Federal Employees and Contractors” only as it relates to;

- Control Objectives
- Privacy Requirements

Identity Verification Requirements

- Applicants must have a sponsor (*authorizes the need for applicant to obtain physical and logical access to Federal facility*)
- Applicant must appear in person at Registration or Enrollment Station
- Applicant must present 2 forms of Government issued ID Per US Form I-9 or 6 CFR Part 37⁵, one of which must have a photo.
- Applicants fingerprints will be collected electronically index fingers for the sole purpose of tying the identity to the credential.
- Applicant must appear in person
- Applicant must present 2 forms of Government issued ID Per US Form I-9 or 6 CFR Part 37, one of which must have a photo. Documents must include information supporting the claim of
 - Date of birth;
 - Proof of SSN or ineligibility for an SSN;
 - The applicant’s address of principal residence; and
 - Lawful status in the United States.
- Applicants fingerprints will be collected electronically (ten flat or rolled) for identity and adjudication purposes
- Applicants pin must be used to complete the transaction

Identity Vetting Requirements

- Establish validity of the identity - Identity proofing using administrative/manual methods providing identity proofing criteria from breeder documents required in Federal form I-9, to verify the identity exists, the identity is active (not deceased) and the components are related at a moderate level of assurance.
- Criminal History Record Information (CHRI) / Risk Analysis (include a data quality score?) - to include Local, County, State as required by the laws governing the sponsoring authority

⁵ A valid unexpired U.S. passport; A certified copy of a birth certificate; A consular report of birth abroad; An unexpired permanent resident card.; An unexpired employment authorization document (EAD); An unexpired foreign passport with valid U.S. visa affixed; A U.S. certificate of citizenship; A U.S. certificate of naturalization; or A REAL ID driver’s license or identification card issued subsequent to the standards established by this regulation.

Medium Level (2) – Non-Security Clearance Credential for Standard First Responder Designees

Adjudication Standards:

The criteria to be used to adjudicate the background checks for persons requiring a FiXs Standard (level 2) First Responder Credential is determined by the State, County, and local, requirements and laws governing the sponsoring authority.

4 ATTRIBUTE MANAGEMENT FOR MEDIUM HIGH LEVEL (3) ENHANCED FIRST RESPONDER CREDENTIALS

The credentialing process for First Responders carry some unique characteristics due to program requirements of the Federal Emergency Management Agency recently clarified by verbiage in Public Law 110-53.

The terms “credentialed and credentialing”, for this community of users, carries the meaning of providing or having provided, respectively, documentation that identifies personnel and certifies the qualifications (**attributes**) of such personnel by ensuring that such personnel possess a minimum common level of training, experience, physical and medical fitness, and capability appropriate for a particular position in accordance with standards created under section 510;:⁶

The FiXs Enhanced First Responder Credential, which is based on the FiXs Medium High assurance level (3), provides a medium high level of assurance that the credential holder is who he/she asserts themselves to be and meets the minimum qualifications required by the federal government sited above

4.1 Attribute Management for Medium High Level (3) Clinical First Responder Credentials

The clinical first responder credential must meet the requirements of Emergency System for Advanced Registration of Health Professions Volunteers. Title 42, Chapter 6A, Sub-Chapter II, Part B, § 247d-7b⁷

4.1.1 USERS

Participants who may need a FiXs Medium High Level (3) Enhanced Clinical First Responder Credential may include but are not limited to:

- Physicians
- Registered Nurses
- Behavioral Health Professionals⁸
- Advanced Practice Nurses⁹
- Physicians Assistants
- Dentists
- Emergency Medical Technicians (EMT's) and Paramedics
- Pharmacists
- Licensed Practical Nurses
- Respiratory Therapists and Technicians

⁶ PUBLIC LAW 110–53- IMPLEMENTING RECOMMENDATIONS OF THE 9/11 COMMISSION ACT OF 2007, TITLE IV, SEC. 401- DEFINITIONS, § (a) (3)

⁷ Retrieved September 4th, 2007 from

www4.law.cornell.edu/uscode/html/uscode42/usc_sec_42_00000247---d007b

⁸ Marriage and Family Therapists, Medical and Public Health Social Workers, Mental Health and Substance abuse Social Workers, Psychologists, and Mental Health Counselors. ESAR-VHP Interim Technical and Policy Guidelines, Standards, and Definitions – Version 2 June 2005

⁹ Nurse Practitioners, Nurse Anesthetists, Certified Nurse Midwives, Clinical Nurses Specialists. ESAR-VHP Interim Technical and Policy Guidelines, Standards, and Definitions – Version 2 June 2005

- Cardiovascular Technologist and Technicians
- Radiological Technologists & Technicians
- Surgical Technologists
- Medical and Clinical Laboratory Technologists
- Medical and Clinical Laboratory Technicians including Phlebotomists
- Diagnostic Medical Sonographers
- Veterinarians

Clinical Licensure Verification Requirements

System Requirements

- Must adhere to the Fair Credit and Reporting Act (The FCRA) and other applicable laws, this is to inform all identified job skills/individuals that by giving their approval under the “Clinical Licensure Verification Requirement” and entering their personally identifiable data, they consent and authorize FIX’s and/or third party background screening provider(s) to perform qualifications screenings checks for them that “requires physical or logical access to their job or agency-related activity but do not fall under the category of government employee or government contractor. Must adhere to the Department of Health and Human Services Standard for Early System for Advanced Registration of Volunteer Health Professionals, Standards of the Joint Commission (JAHCO), and any applicable local, County or State Requirements

Licensure Verification Requirements

- Applicant must appear in person
- Applicant must present (dependent on profession);
 - Original copy of a state issued medical license with no restrictions, and or active and unrestricted state issued license to practice with the scope identified by the state
 - Original copy of MD. DO. PhD. MS. RN. Degree from an educational institution accredited by the authority having jurisdiction referenced under “evidence of credential – explanation of credential elements” from the emergency credentialing standard for that profession as defined in the HHS ESAR-VHP Standard.
 - Original copy of the DEA Registration Certificate for License Verification
 - Proof of Active Clinical practice through attestation or other documentation or peer reference from a credential holding peer (with ID reference), affirming that the individual is practicing medicine, or working within the scope of the profession being vetted, in a hospital or non hospital setting.
 - Proof of Active Clinical Hospital Privileges through attestation or other documentation or peer reference from a credential holding peer (with ID reference) , affirming that the individual is practicing medicine, or works within the scope of the profession being vetted and has privileges in a hospital setting.
 - Proof of State or National Certification to practice, under medical control, as a pre-hospital car provider
- Applicants pin must be used to complete the transaction

Clinical Licensure Verification Requirements

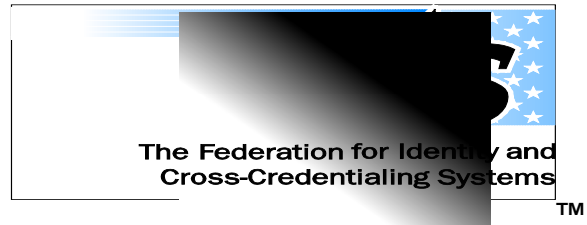
Licensure Vetting Requirements

- May include, dependent on professional, but not be limited to
- Primary Source Verification or delegation to a JCAHO accredited organization that has performed primary source verification of the individual's credentials.
- Degree, MD or DO through AAMC, AOA or ECFMG; for all others from an accredited institution
- Unencumbered Medical License from State of Issue
- Board Certification in recognized specialty or sub specialty from ABMS or AOA
- National Practitioner Databank Status
- Drug Enforcement Agency (DEA) License Verification with types
- Inspector General Status

Adjudication Standards:

The following criteria will be used to adjudicate the medical licensure and certifications for persons requiring a FiXs Clinical First Responder Credential. No person shall be granted such as credential if the licensure check reveals any of the following;

- Any failure to meet any of the credential elements for the profession as outlined in the Department of Health and Human Services Health resources Services Administrations "Standards and Guidelines for the Early System for the Advanced Registration of Volunteer Healthcare Professionals.
- Any Active Sanction on record with any State Inspector General
- Any Active disciplinary issue on file with the National Practitioner Databank



**TECHNICAL SPECIFICATION FOR CREATING A UNIQUE IDENTIFIER FOR
A FIPS 201-ALIGNED FIXS™ CREDENTIAL**

**Version 1.0, rev. 02
January 10, 2007**

Introduction

Homeland Security Presidential Directive -12 (HSPD-12) mandates the issuance of the Federal Information Processing Standard 201 (FIPS 201)-compliant Personal Identity Verification (PIV) card to all Federal employees and contractors starting October 27, 2006. The Department of Defense (DoD) Common Access Card (CAC) and the DoD Public Key Infrastructure (PKI) Programs are also being aligned to meet the additional set of requirements mandated by the Presidential Directive, HSPD-12. It is the objective of the Federation for Identity and Cross-Credentialing Systems™ (FiXs) organization to align any FiXs certified credential (also referred to as the FiXs credential) and the certified issuance process to meet, and “align” with, the requirements stated in FIPS 201.

The purpose of this Technical Specification is to define the FiXs certified credential's unique identification number, which is consistent with the guidance provided by key documents such as NIST's SP 800-73-1, *Interfaces for Personal Identity Verification*, published in March 2006 and the Technical Implementation Guidance for Smart Card Enabled Physical Access Control Systems (PACS), Version 2.3, dated December 20, 2005.

The topology of the FiXs certified card will follow the requirements of the FIPS 201 specification. These requirements are summarized in Appendix A Smart Card Topology Requirements and will not be discussed in detail in this specification. In addition, the FiXs smart card-based ID card topology will include a 3 of 9 barcode on the back of card that conforms to the FIPS 201 specification for an optional barcode. Details are included in Appendix B.

Background

Card Holder Unique Identifier (CHUID) Data Elements

NIST SP 800-73-1 specifies the PIV card application Card Holder Unique Identifier (CHUID) data object, which is further defined in PACS Version 2.3. Figure 1 “PACS V2.3 CHUID Data Model” shows the CHUID data model as it is defined in the PACS V2.3 specification. This data model is closely aligned with the PIV data model in SP 800-73-1. It includes both mandatory and optional data elements.

Data Element	Tag	Type	Max. Bytes	Mandatory/Optional
Buffer Length	EE	Fixed	2	M
FASC-N (SEIWG-012)	30	Fixed	25	M
Agency Code	31	Fixed	4	O
Organization Identifier	32	Fixed	4	O
DUNS	33	Fixed	9	O
GUID	34	Fixed	16	M
Expiration Date	35	Date (YYYYMMDD)	8	M
RFU	38- 3C			O
Authentication Key Map	3D	Variable	512	O
Asymmetric Signature	3E	Variable	2816	M
Error Detection Code	FE	LRC	1	M

Figure 1 PACS v2.3 CHUID Data Model

Federal Agency Smart Credential Number (FASC-N) Data Elements

The CHUID includes the Federal Agency Smart Credential Number (FASC-N), which uniquely identifies the card and cannot be modified post-issuance. Figure 2 “FASC-N” depicts the FASC-N data model as it is defined in NIST SP 800-73-1 and PACS V2.3 specifications.

Field name	Length (BCD digits)	Field description
AGENCY CODE	4	Identifies the government agency issuing the credential (9999 for FiXs)
SYSTEM CODE	4	Identifies the system the card is enrolled in and is unique for each site
CREDENTIAL NUMBER	6	Encoded by the issuing agency. For a given system no duplicate numbers are active
CS	1	CREDENTIAL SERIES (SERIES CODE) Field is available to reflect major system changes
ICI	1	INDIVIDUAL CREDENTIAL ISSUE (CREDENTIAL CODE) Recommend coding as a “1” always
PI	10	PERSON IDENTIFIER Numeric Code used by the identity source to uniquely identify the token carrier. (e.g. DoD EDI PN ID, TWIC credential number, NASA UUPIC)
OC	1	ORGANIZATION CATEGORY 1 - Federal Government Agency 2 - State Government Agency 3 - Commercial Enterprise 4 - Foreign Government (3 for FiXs)
OI	4	ORGANIZATION IDENTIFIER OC=1 – NIST SP800-87 Agency Code OC=2 – State Code OC=3 – Company Code OC=4 – Numeric Country Code (Used to Identify Companies for FiXs)

POA	1	PERSON/ORGANIZATION ASSOCIATION CATEGORY 1 – Employee 2 – Civil 3 – Executive Staff 4 – Uniformed Service 5 – Contractor 6 – Organizational Affiliate 7 – Organizational Beneficiary
SS	1	Start Sentinel. Leading character which is read first when card is swiped
FS	1	Field Separator
ES	1	End Sentinel
LRC	1	Longitudinal Redundancy Character

Figure 2 FASC-N Data Model

FiXs Implementation

Section 2.1 of the PACS Version 2.3 document explains how the CHUID could be used by non-federal issuers. The document states that Federal agencies shall only enroll CHUID credentials that are validated through the issuing agency or where the Agency Code is 9999 indicating the issuer is a non-federal entity.

Because FiXs is not a federal agency, FiXs plans to follow the specification and use the Code “9999” in the AGENCY CODE.

The FASC-N is not designed to insure uniqueness for non-federal issuers. When the FASC-N was originally developed, the entire FASC-N was set to binary coded decimal (all numeric) in order to be backward compatible with the SEIWG-012 number. The FASC-N encoding uses only BCD digits. Since alpha characters cannot be BCD encoded in the FASC-N, this limitation causes scalability issues. Another limitation in the FASC-N is that the OI field only accommodates 4-digits. This limits the number of organization identifiers to 9999 per Organization Category (OC). These limitations were recognized by the developers of the PACS Version 2.2 specification document and specification document that followed, i.e., PACS Version 2.3. This resulted in the addition of three optional fields to the CHUID. These fields have been included in the PIV CHUID described in FIPS 201 and NIST SP 800-73-1. The three optional fields are:

- **Agency Code** -Tag 31: For issuing agencies with alpha characters in their agency code
- **Organization Identifier** -Tag 32: An alphanumeric code that could be used as an extension to the numeric Organization ID (in the FASC-N) on the CHUID
- **Data Universal Numbering System (DUNS)** -Tag 33: For commercial organizations

For non-federal issuers, the optional data elements can extend the FASC-N to create a unique identifier when the Agency Code is encoded with 9999. If an Agency Code of

9999 is present in the FASC-N, then the Agency Code, DUNS, and/or Organization Code TLV records in the CHUID could indicate the identity of the credential issuer. It is anticipated that the FASC-N Tag 30 TLV record will always exist for industry compatibility for PACS that use the System Code and Credential Number as a credential identifier.

The PACS Version 2.3 document also states that for issuers not defined in SP 800-87, *Codes for the Identification of Federal and Federally Assisted Organizations*, the FASC-N can be constructed using an Agency Code of 9999; however this will not provide uniqueness of the FASC-N for federal agency applications. If a non-federal issuer has a requirement for federal interoperability, then a sponsoring agency could assign specific System Code(s) to the issuer. As mentioned above, when an Agency Code of 9999 is specified, a non-federal issuer must include an additional TLV record in the CHUID, such as the Organization Identifier number (Tag32) and/or DUNS number (Tag 33) to ensure uniqueness of the CHUID.

Conclusion

The FiXs system requires two data elements to operate properly. The first data element is the Organization Identifier. The Organization Identifier is used to route information between the FiXs/DCCIS Domain Servers in the FiXs and DCCIS systems. The Organization Identifier functions as a routing address and must be unique for each organization throughout the FiXs/DCCIS system. The second data element is the Person Identifier. The Person Identifier is used to identify a specific person's record within each of the organization's domains. The Person Identifier must be unique within each organization but does not have to be unique across the FiXs/DCCIS domain.

The NIST SP 800-73-1 and PACS Version 2.3 specifications both define a 10 digit Person Identifier in the FASC-N portion of the CHUID. This is more than sufficient to meet the needs of FiXs. FiXs plans to use the Person Identifier as defined in both specifications to uniquely identify persons within an organizational domain.

The FASC-N OI (4 BCD Digits) used to uniquely identify organizations has a size limitation, since it cannot accommodate more than 9999 FiXs credential issuing organizations. This limitation is not an immediate concern. It will become a problem as FiXs grows over the next few years. Therefore, a more robust numbering scheme will be needed once the number of FiXs member organizations exceeds 9999.

The FiXs infrastructure intends to use the FASC-N OI (4 BCD Digits-16 bits) combined with the CHUID OI (4 bytes alpha-numeric-32 bits). This will give FiXs a combined 48 bits from which to build a unique Organization Identification.

FiXs will implement these two data elements by combining them to create a unique 48 bit OI designator across FiXs for each FiXs member as follows:

1. The FASC-N OI will be used to represent the lower sixteen least significant bits (1-9999 BCD). *Note: The FASC-N OI (4 BCD Digits) will be restricted to the numeric digits only.*
2. The CHUID OI would be used to represent the upper thirty-two most significant bits (0000-ZZZZ). *Note: The CHUID OI could include both alpha and numeric characters, but for the initial 1-9999 FiXs members this would be all zeros.*

This method of implementation allows for short-term compatibility and implementation flexibility while providing the largest number of organizational identifier combinations long-term.

A subset of the CHUID information will also be used in the linear 1D barcode located on the rear of the smart card. The bar code specification is shown in Appendix B FiXs Barcode Requirements.

FiXs.org will generate the organizational identification number and ensure they are unique across FiXs on behalf of the DOD DMDC.

The unique FiXs credential identifier can be developed by assigning the following values to the following data elements within the FASC-N and CHUID:

1. Agency Code (within the FASC-N) will be assigned a value, 9999, to indicate that the card has been issued by a non-Federal issuer;
2. System Code (within the FASC-N) can be assigned a unique number ranging between 1 and 9999 to identify the FiXs enrollment and/or issuance system used by a FiXs member organization;
3. Credential Number (within the FASC-N) will be assigned a unique number ranging between 1 and 999,999 to identify the individual credential issued by a particular FiXs enrollment and/or issuance system used by a FiXs member organization;
4. Credential Series (Series Code) - within the FASC-N - can initially be assigned a value, 1, to indicate the first series and incremented up to 9 for additional series;
5. Individual Credential Issue (Credential Code) - within the FASC-N - should always be assigned a value, 1, as recommended by PACS Version 2.3;
6. Person Identifier (within the FASC-N) can be assigned a unique number ranging between 1 and 9,999,999,999 to uniquely identify the FiXs card holder within a specific FiXs member's Domain Server;
7. Organization Category (within the FASC-N) will be assigned a value, 3, to indicate that the card issuer is a commercial organization;
8. Organization Identifier (within the FASC-N) will be assigned a value between 1 and 9999 to identify the lower sixteen bits of the FiXs member's organization identifier;
Note: When the number exceeds 9999, the Organization Identifier (in the CHUID) will be combined to identify the FiXs member organization issuing the credential (as described in line item 10 below).
9. Person/Organization Association Category (within the FASC-N) can be assigned a value, 1, 3, 5, 6, or 7 to indicate that the cardholder's relationship with the FiXs member organization; and
10. The Organization Identifier (OI) in the CHUID, which is a 4-byte (32-bit) data element, will be assigned a value between 0000 and ZZZZ to identify the upper thirty-two bits of the FiXs member organization issuing the credential. Until the number of FiXs organizations exceeds 9999, the CHUID OI will be set to 0000 or omitted on systems that can not generate the optional field.

References

1. **Homeland Security Presidential Directive 12 (HSPD-12):** Policy for a Common Identification Standard for Federal Employees and Contractors (August 2004) Mandates the establishment of a standard for identification of Federal government employees and contractors and requires the use of a common identification credential for both logical and physical access to Federally controlled facilities and information systems.
<http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html>
2. **Federal Information Processing Standard (FIPS) 201-1:** Personal Identity Verification (PIV) of Federal Employees and Contractors (June 2006)
<http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>
3. Government Smart Card Interagency Advisory Board - Physical Access Interagency Interoperability Working Group, "*Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems (PACS), Version 2.3*", December 20, 2005.
4. National Institute of Standards and Technology (NIST), Special Publication (SP) 800-73-1, "*Interfaces for Personal Identity Verification*", March 2006.
5. DMDC, Card Technologies & Identity Solutions Division (CTIS), "*DoD Implementation Guide for Transitional PIV II SP 800-73 v1, Version 1.01*", March 2006.
6. Framework for Inter-Agency Authentication of Federal Personal Identity Verification (PIV) cards, Version 1.0

APPENDIX A

SMART CARD TOPOLOGY REQUIREMENTS

Introduction

The FiXs smart card-based ID card is based upon the minimum standards set forth in the National Institute of Technology & Standards' (NIST) FIPS Pub 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*. The most current version of FIPS 201 was published by the NIST in March, 2006. FIPS 201 lays the groundwork for a commonly-recognized and interoperable federal ID that:

- Is based on sound criteria for verifying an individual's true identity
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
- Can be rapidly authenticated electronically
- Is issued only by providers whose reliability has been established by an official accreditation process.

Visual Card Topology Requirements

FIPS Pub 201 (4.1.4 Visual Card Topology) lists the requirements for creating a visual layout that meets the requirements of HSPD-12. The smart card's visual topology consists of "zones" that specify where particular information resides, such as the card holder's name, department/agency, the card's expiration date, etc.. Some areas of the card are labeled as "reserved" and should not be used for printing. These areas are off-limits so that printing does not interfere with a card's Integrated Circuit Chip (ICC).

Where the printed text on the PIV card is required to be in Arial font, the point size and style (bold, normal) will alter depending on the zone.

Some flexibility is given during card design to allow organizations to customize certain aspects. These options are explained in FIPS Pub 201 (4.1.4.3, Optional Items on the Front of the Card and 4.1.4.4, Optional Items on the Back of the Card).

Requirements for the Front of the Card

Zone 1 – Photograph

A color photograph (minimum of 300 dots per inch (dpi) resolution), presenting the individual from the top of the head to the shoulders, is to be placed in the upper left corner of the front of the card, vertically. The background (backdrop) color to be used behind the photographed individual is not specified in FIPS 201, but per the recommendation of the Internal Committee for Information Technology Standards (INCITS) 385, the background color should be uniform throughout an organization's issuance locations. Complete and specific technical requirements for facial image capturing should conform to NIST Special Publication (SP) 800-76, *Biometric Data Specification for Personal Identity Verification*.

Zone 2 – Name of Individual

The full legal name of the card holder's identity is to be printed under the photograph in capital letters. The minimum font size acceptable is 10 point.

Zone 8 – Affiliation

The card holder's affiliation shall be printed in Zone 8. Examples include: "CONTRACTOR," "ACTIVE DUTY," and "CIVILIAN." The required font for the card holder's affiliation is 6 point Bold.

Zone 10 – Organization Affiliation

The card holder's organization name shall be printed here. Two lines are available for use, with 6 point Bold being the font requirement.

Zone 14 – Expiration Date

The card expiration date is to be printed in a YYYYMMDD format (example: 2007MAR30). A PIV card may be valid for up to 5 years, depending on your status. The expiration date is to be printed in 6 point Bold.

Requirements for the Back of the Card**Zone 1 – Agency Card Serial Number**

Each card created will be assigned a unique serial number from the agency/organization. This serial number will be required to be printed in 6 point Bold, left-justified.

Zone 2 – Issuer Identification

Printed in 6 point Bold and right-justified will be the issuing facility's information. This identifier will consist of six characters for the department code, four characters for the agency code, and a five-digit number that uniquely identifies the issuing facility within the department or agency.

Durability Requirements

FIPS 201 includes special provisions regarding durability requirements of the smart card. The printed information on the PIV card shall be printed so that the print cannot be rubbed off the actual card material through printing, laminating, and during normal wear and tear throughout the card's life cycle. In addition to this, the print is not to be obscured by any images (example: agency seal should not obscure the agency title).

No decals or stickers of any type are to be affixed to the PIV card. Electronic contact points should also be considered off-limits for printing. Printing on areas designated as "unusable" by FIPS 201 could result in difficulties reading and writing data to the card. No manual markings or embossing (unless done during manufacture of the card itself by the manufacturer) are allowed.

The following standards should be referenced to ensure FIPS 201 compatibility for contactless cards:

- [ISO7810]
- [ISO10373]
- [ISO7816]
- [ISO14443]

In addition to the aforementioned ISO standards, the PIV card must also conform to test methods used in [ANSI322]:

- Card flexure
- Static stress
- Plasticizer exposure
- Impact resistance
- Card structural integrity
- Surface abrasion
- Temperature and humidity-induced dye migration
- Ultraviolet light exposure
- Laundry tests

Requirements set forth from [ISO10373] require that the PIV card be able to withstand up to 2000 hours of southwestern United States sunlight exposure (actual, concentrated, or artificial). Furthermore, the PIV card shall also meet testing requirements in [G90-98] for concentrated sunlight exposure and [G155-00] for accelerated exposure.

Regular cleaning, using a mild soap and water mixture should not cause the PIV card to malfunction, nor should it cause the laminate to peel. No visible cracks or failures should be experienced following dynamic bending per [ISO10373].

Physical Requirements

PIV cards must be 27 to 33-mil thick (prior to lamination). Consideration should be taken to ensure that the lamination itself does not interfere with the operation of the smart card reader. See [ISO7810] for specific details.

Punching holes in PIV cards should be done carefully, and only after consulting with the manufacturer. Printed text and photo areas are off-limits for hole punching, and any zones that feature machine-readable technology are also off-limits. Hole punching may void a card's warranty.

Security Requirements

There are many requirements built into FIPS 201 to ensure the security of a PIV card, from the beginning authorization to issue a PIV card through the end of the card's life cycle (termination). The following list is a minimum of security standards to be followed when implementing PIV:

Security Features

Any security features used on a PIV card must be in accordance with durability requirements in ISO7810. Security features also must be free of defects, such as fading, discoloring, or tampering. Printed information is to be legible and not obscured by any images whatsoever. Electronic contact points are to be free from printing zones, so that data can be read and written without impediment. A PIV card is required to have at least one of the following security features:

- Optical Varying Structures – A security feature that lays a pattern down across a holographic image or diffracted image, creating a surface relief pattern that appears semi-transparent.
- Optical Varying Inks – Known as OVI, optical varying ink utilizes metal luster in which colors actually appear as pairs of colors instead of individualized. The pairs of ink changes as the viewing angle of the object changes. This color angular effect cannot be duplicated by copying machines and scanners. OVI is the most complex anti-forgery ink available today.
- Laser Etching and Engraving – Laser etching/engraving involves marking the PIV card with a low-power laser or reduced-power engraving technique so that the cards can be uniquely marked without damaging or destroying them.
- Holograms – Holograms are three dimensional images that are created by utilizing two laser beams; one for illuminating the object for visibility, and the other directed to the film or background plate.
- Holographic Images – A holographic image is the result of the reconstruction of a wavefront that is identical to the reflection of light from the original object.
- Watermarks – A shaded watermark can be used onto the card, incorporating tonal depth, creating a grayscale image.
- Personal Identification Number - Each PIV card will be assigned a numerical Personal Identification Number (PIN), which will be used to access the data on the smart card. The PIN is to be a minimum of 6 digits, and should only be known by the owner of the card. PIN transactions should always be encrypted, never transmitted in clear text. FIPS 140-2 (Level 3) Operator requirements lists specific details.
- Card Holder Unique Identifier - The Card Holder Unique Identifier (CHUID) is a unique number on every PIV card, which includes an element and the FASC-N. [SP800-73] defines the CHUID, and the format of the CHUID signature element is found in Section 4.2.2 of FIPS 201.
- Biometrics – Two fingerprint samples of the card holder will be stored on the PIV card. These fingerprints can be used during authentication processes. Biometrics are only permitted to be accessed via the contact interface, after valid presentation of the associated PIN.
- Encryption – One asymmetric key pair and corresponding certificate will be included on each PIV card. This will also include the status of the NACI for the individual. Cryptographic operations may be performed with the PIV card, using RSA or elliptical curve key pair generation. These cryptographic transactions are to be performed on the PIV card itself. The PIV

authentication private key is never to be exported off the card, and should only be accessed via the contact interface. Additionally, the utilization of X.509 certificates (including the FASC-N) to support physical access) is included. PIV cryptographic keys must meet Level 2 (or above) of FIPS 140-2 and physical security requirements (to protect keys in storage) must meet Level 3.

APPENDIX B

FIXS BARCODE REQUIREMENTS

Introduction

As described in Appendix A, the FiXs smart card-based ID card is based upon the minimum standards set forth in the National Institute of Technology & Standards' (NIST) FIPS Pub 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*. This FiXs smart card will include a 3 of 9 barcode on the back of card that conforms to the FIPS 201 specification for an optional barcode in Zone 8 as depicted in Figure 4-7 below.

All measurements are in millimeters and are from the top-left corner.
 All text is to be printed using the Arial font.
 Unless otherwise specified, the recommended font size is 5pt normal weight for tags and 6pt bold for data.

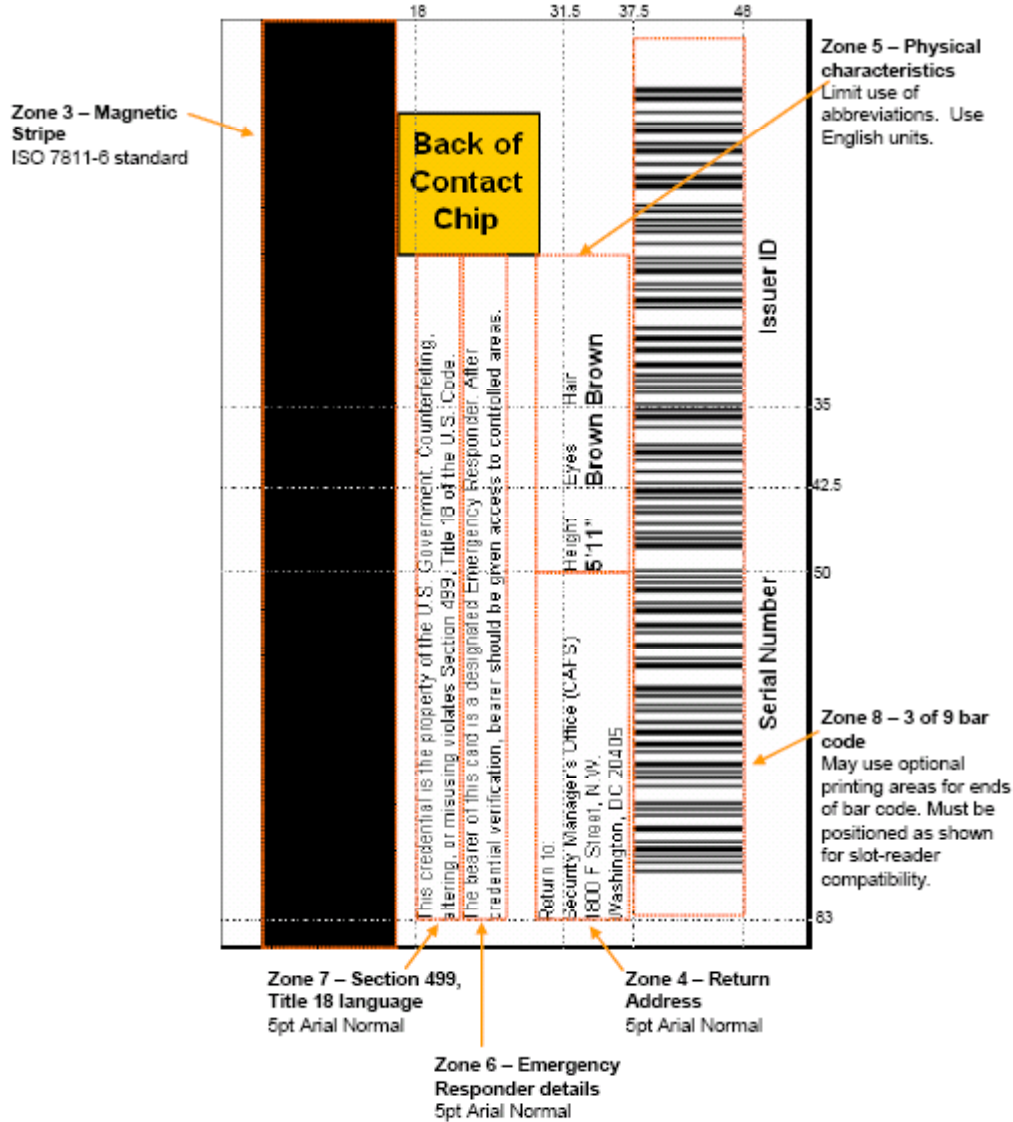


Figure 4-7. Card Back—Optional Data Placement—Example 1

FiXs Barcode Specification:

This FiXs barcode will consist of data elements selected from the CHUID. These data elements and the order in which they will be concatenated are described below:

1. Agency Code (within the FASC-N) will be assigned a value, 9999, to indicate that the card has been issued by a non-Federal issuer;
2. System Code (within the FASC-N) will be assigned a unique number ranging between 1 and 9999 to identify the FiXs enrollment and/or issuance system used by a FiXs member organization;
3. Credential Number (within the FASC-N) will be assigned a unique number ranging between 1 and 999,999 to identify the individual credential issued by a particular FiXs enrollment and/or issuance system used by a FiXs member organization;
4. Credential Series (Series Code) - within the FASC-N - will initially be assigned a value, 1, to indicate the first series and incremented up to 9 for additional series;
5. Individual Credential Issue (Credential Code) - within the FASC-N - should always be assigned a value, 1, as recommended by PACS Version 2.3;
6. Organization Category (within the FASC-N) will be assigned a value, 3, to indicate that the card issuer is a commercial organization;
7. Organization Identifier (within the FASC-N) will be assigned a value between 1 and 9999 to identify the lower sixteen bits of the FiXs member's organization identifier;

An example of a FiXs Barcode consisting of the following sample data is provided in Figure B-2 below:

- FASC-N Agency Code = 9999
- FASC-N System Code = 0001
- FASC-N CN = 123456
- FASC-N CS = 1
- FASC-N ICI = 1
- FASC-N OC = 3
- FASC-N OI = 0001



Figure B-2 Sample FiXs Barcode