



FiXs Trusted Broker (FTB) Gateway: Operating and Interface Specification and Statement of Objectives

August 22, 2008

Final 1.0

Copyright 2008® by the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

All Rights Reserved

10400 Eaton Place, Suite 500A

Fairfax, VA 22030

(703) 591-9255

Preface

The charter of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs) is to promulgate the necessary technical and operational standards; implement the governance and trust models; provide an open communications forum; and maintain non-attributable, objective oversight of the operations of a network “switch” whereby the commercial sector and public sector organizations can securely authenticate identity credentials among and between themselves (cross-credential).

FiXs provides a trusted mechanism for federated identity infrastructure within and between public and private sector organizations with accuracy and trust through the application of a Federated Trust Model. The network capabilities can be accessed worldwide, in remote or fixed environments, wired or wirelessly, and in real-time. A key component to the network integrity is its strong credential authentication and revocation processes, as governed by the FiXs operating rules

The FiXs Trusted Broker (FTB) has an interface to the Department of Defense’s Defense Cross-Credentialing Identification System (DCCIS) and its’ related Trusted Gateway Broker (TGB) as well as potential interface connections to other Trust Broker’s that may be established in conjunction with the FiXs Network. The FiXs Trust Broker also has interfaces with the FiXs Domain Server(s) (FDS) and authentication systems.

The purpose of the network is to route and process authentication inquiries from networked authentication devices across the FiXs Network, and where applicable to the DCCIS, to the authoritative data store, or domain server, and return an authentication response.

Modeled after the financial industry’s highly-secure and widely-accepted ATM (Automated Teller Machine) approach, the FiXs network is a secure, scalable system that provides trusted, interoperable identity verification and credential authentication for network users accessing a range of government and commercial facilities. The FiXs network meets federally-mandated requirements, supports physical and logical access applications and integrates with an organization’s existing personnel system, while leveraging the network’s economies of scale

Revision History

This guide will be upgraded periodically as needed. Please make sure you have the latest version of this guide and that the guide is compatible with the version of software being used. Updated versions of this guide are available from FiXs.

Version	Release Date	Description
0.3	2-22-08	Initial Draft Release (compatible with the DoD TGB release 0.3)
0.4	3-17-08	CCB Revision 1
1.0	3-20-08	Board of Directors Version CCB Revision 2 - Draft for Comment
2.0	5-15-08	Board of Directors Approved Version CCB Revision 3 - Posted for Comment
3.0	8-22-08	FiXs Officers Approved Version Final 1.0

Contents

1.0	About This Specification	1
2.0	Statement of Objectives	1
3.0	FiXs Overview – Key Components and Architecture.....	2
3.1	FiXs SECURITY	2
3.2	COMPLIANCE WITH FiXs POLICIES, STANDARDS, AND GOVERNANCE.....	2
3.3	ARCHITECTURAL OVERVIEW.....	2
4.0	Requirements	4
4.1	TRUST GATEWAY BROKER (TGB) REQUIREMENTS.....	4
4.2	SECURITY REQUIREMENTS	5
4.3	IMPLEMENTATION REQUIREMENTS	5
4.4	DATA REQUIREMENTS.....	5
4.5	REFERENCE STANDARDS	6
5.0	FTB Service Level Requirements	7
6.0	Schemas.....	9
6.1	CONTROL DATA SCHEMA DEFINITION	9
6.2	ENVELOPE SCHEMA DEFINITION	14
6.3	PAYLOAD SCHEMA DEFINITION	16
7.0	Glossary	19

1.0 About This Specification

The FiXs Trusted Broker (FTB) and Interface Specification is designed as an aid for FiXs users, developers and service providers by providing specifications that will allow operation of the FTB and integration of FiXs Domain Servers with the FTB. This guide also supports the on-going configuration baseline and requirements/specifications for operating the FTB. This guide is updated by the FiXs CCB under the auspices of the FiXs Executive Committee and the FiXs Board of Directors as specified in the FiXs By-Laws.

The information in this guide is effective at the time it was written and may change under the direction of the CCB with minimum notice. By providing the requirements and interface specifications for the FTB along with the Service Level Agreements required by FiXs, this document will serve as a Statement of Work for any organization seeking to contract for operation of the FTB and the associated network.

2.0 Statement of Objectives

This guide will also be used to serve as a statement of objectives for the solicitation for a service provider to operate and maintain the FTB. As a statement of objectives this document has two functions – to provide those specifications required for the operation of the FTB within the FiXs operating environment as well as those minimum requirements that must be met to ensure that FiXs members receive a high level of service and one that can be relied upon commensurate with the importance of function the FiXs Federation was set up to perform – real time Federated credential authentication. However, as a statement of objectives these specifications and requirements are meant to be at a higher level as may be necessary to totally instantiate the network. This is done for two reasons – first to encourage innovation and efficiency by our service provider and second to allow the service provider to specify the operating system and operating environment most efficient for their bid. Since this specification is a statement of objectives, the winning service provider is expected to provide to the FiXs Board of Directors very specific information on how the service provider intends to meet the requirements stated in Section 4 of this document and the service levels they will provide in each of the areas called out in Section 5 of this document.

In addition, service providers responding to the solicitation to operate the FTB will have to follow the acquisition process specified by the FiXs Board of Directors. The details of the acquisition process to be followed, the make up of the evaluation team and the evaluation criteria are detailed in the FiXs® Trust Broker (FTB) Acquisition Plan which is posted on the FiXs® website and meant to be used in conjunction with this statement of objectives.

3.0 FiXs Overview – Key Components and Architecture

The FiXs Trusted Broker (FTB) and the FiXs Domain Server (FDS) are the key components in the implementation of the FiXs network. The FDS provides access to different FiXs member organization databases, making it possible for them to authenticate visitors carrying authorized FiXs Certified credentials issued by fellow FiXs member organizations or the exchange of such information with FiXs authorized partner organizations such as the Department of Defense (DoD) through the FTB.

FiXs members communicate with other members or other FTBs using XML. The XML message is passed from the source FiXs partner through a FTB to other connected applications. The receiving applications are responsible for deciphering and acting on the information contained in the XML message. This XML message and its schema represent the interface between each member in the FiXs network. It is the responsibility of these applications to encrypt and decrypt the information before passing the data to other partners.

3.1 FiXs Security

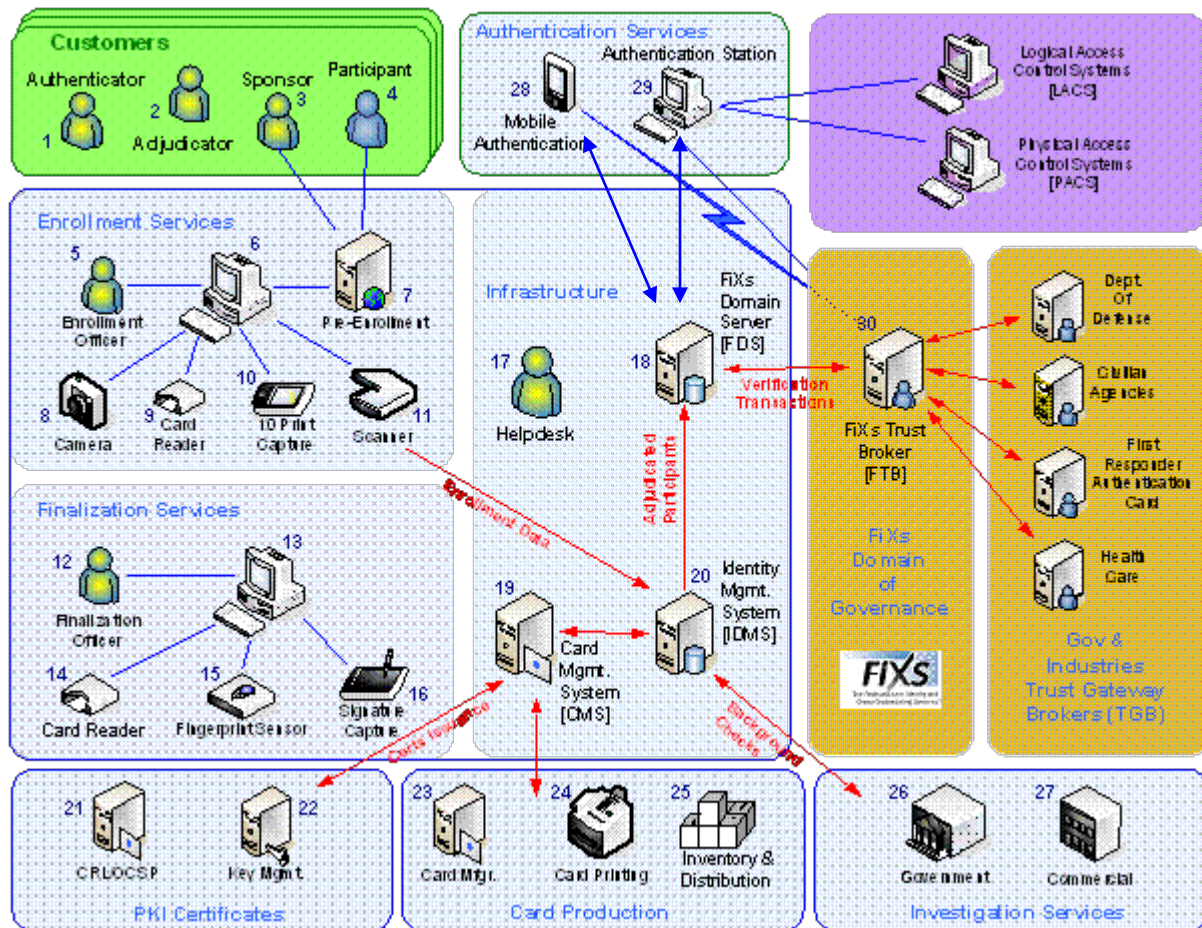
FiXs adheres to its own security principles published in the “FiXs Security Guidelines v2.0 3.29.07” for the transmission of private information over open networks. This includes the need to maintain confidentiality, the need to ensure data integrity, the need to guarantee that information to be sent cannot be repudiated, and that all entities involved in communications, either human agent or machine, are authenticated.

3.2 Compliance with FiXs Policies, Standards, and Governance

All services provided hereunder shall at all times comply with all FiXs Policies, Standards, specifications, governance requirements, and management directives. Should there be any real or apparent conflicts between any of those requirements and the requirements under this SOW, the former shall take precedence.

3.3 Architectural Overview

This section provides a high-level overview of the FiXs Network and its related components and interfaces. The diagram below facilitates the understanding of the workflows in the FiXs network and the technical architecture that drives the requirements in this document for the FTB.



The basic key components of the architecture are:

Enrollment and Issuance Workstation(s): An Enrollment and Issuance Workstation consists of a PC with a standard web browser which is used to access the web-based enrollment application. An enrollment and issuance workstation also includes peripheral devices such as a fingerprint reader, camera, barcode reader, card production equipment.

Authentication Station: The desktop authentication station allows credential holders to be authenticated across the FiXs Network and to the DOD DEERS database for government employees.

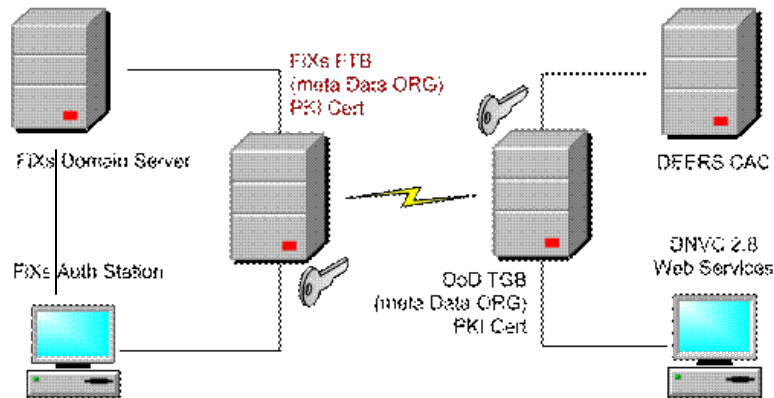
Handheld Authentication Device/Authentication Workstation: Enrolled contractors credentials may also be authenticated via a FiXs-certified handheld device or FiXs-certified mobile authentication device.

Wireless Hubs: At locations where handheld devices are used, a wireless hub will be installed so that the handheld authentication devices can communicate to the backend devices.

FiXs Domain Server (FDS): A FiXs Domain Server is maintained for each unique organization whose employees are enrolled. A single FDS may be properly partitioned to maintain enrollment

data on multiple organizations in a secure logical manner. The FDS maintains a repository of contractors' enrollees' information associated with each organization.

Trusted Gateway Broker (TGB): The Trusted Gateway Broker, or FiXs Trust Broker (FTB) facilitates communication between FDS servers and authentication stations and routes validation and authentication requests to the appropriate FiXs Domain Server or DCCIS domain server and FiXs and DoD National Visitors Center (DNVC) authentication stations as well as interfaces with the DoD's Trusted Gateway Broker.



4.0 Requirements

4.1 FiXs Trust Broker (FTB) Requirements

- 1) The FTB sends out system control data to domain servers that submit a control data request.
- 2) The FTB pushes out system control data to domain servers when the FTB re-starts.
- 3) The system control data contains information in two sections: the FiXs organization, and the Government partners. It includes the public keys of each organization on the list.
- 4) Every time the FiXs FTB re-starts, it generates an updated control data file by updating the FiXs section of the system control data, and merges it with the existing Government partners' control data. It does not modify the Government partners' information.
- 5) The FTB periodically checks the heart beat of domain servers. The FTB will give up on contacting a domain server after three failed attempts.
- 6) The FTB acts like a router, by passing but not deciphering data.
- 7) The FiXs FTB has the ability to communicate with multiple TGBs and domain servers within the government community or commercial networks.
- 8) The FiXs FTB is the central point of contact in communications with the DoD TGB.
- 9) The FiXs FTB runs on an RDBMS server such as Oracle.
- 10) The FTB will support both https and http (internal only) connections.
- 11) The FTB maintains and uses a metadata table for organization codes for commercial and government organizations.

-
- 12) The application shall be based on a single code base upon which advancements, modifications, and additions may more easily be executed.
 - 13) The FTB documentation will be provided as part of the baseline configuration. Any changes shall conform the policies of the FiXs Configuration Control Board and be fully documented as a modification to the baseline configuration documentation.
 - 14) The FTB shall be supplied with “Web Logs” to monitor system performance
 - 15) The FTB shall be supplied with “sniffer” capability to isolate transaction protocols.
 - 16) The FTB shall be equipped with appropriate load-generating capability for usage planning purposes.
 - 17) The FTB shall be equipped with an automated error (alarm) and email generation system and email alerts must be generated to system administrators for any event that impairs the full functionality of the FiXs network.
 - 18) The FTB shall be programmable using a standard web interface with appropriate tools designed to make the application flexible and user friendly.

4.2 Security Requirements

- 1) FTB in the system uses secure communication channels to ensure confidentiality.
- 2) The source domain servers encrypt the message payload in such a way that it can only be read by the destination domain servers.
- 3) The destination domain servers validate the integrity of the message payload received from the source domain servers.
- 4) The destination domain servers ensure non-repudiation of the message payload received from the source domain servers. The domain servers validate the integrity of the overall message sent by the FTB, and the FTB validates the overall messages sent by the domain servers.
- 5) The domain servers ensure non-repudiation of the overall message sent by the FTB, and the FTB ensures non-repudiation of the overall messages sent by the domain servers.
- 6) The domain server and FTB each have their own digital certificates (public keys) and private keys used for SSL, digital signatures, and encryption.
- 7) All digital certificates used for SSL, digital signatures, and encryption must be issued by a single authorized Certificate Authority (CA).
- 8) The FiXs FTB has two digital certificates, one for SSL, and the other for digital signatures and encryption.
- 9) Each domain server that connects to the FiXs FTB has a signature certificate for digital signatures. It will not require the SSL certificate if it is in the CA trust chain.

4.3 Implementation Requirements

- 1) The main system interface is a web based application accessible through a web browser.

4.4 Data Requirements

- 1) The FTB stores a copy of every domain server’s public key certificate, its own private key, and its own X.509 certificate.

-
- 2) Each domain server stores a copy of the FTBs public key certificate, its own private key, and its own X.509 certificate.

4.5 Reference Standards

Consistent with FiXs Security Guidelines, Version 2.0, dated 29 March 2007, the FTB must be flexible enough to incorporate the standards and policies of:

- 3.5.1 The General Services Administration eAuthentication
- 3.5.2 The Liberty Alliance
- 3.5.3 The Standards, Regulations and Policies of State and Local Governments who utilize the FiXs Network
- 3.5.4 The Standards, Regulations and Policies of Commercial Interests who utilize the FiXs Network
- 3.5.5 The Standards, Regulations and Policies of Foreign Entities, Government and Commercial, who utilize the FiXs Network

5.0 FTB Service Level Requirements

The general level of service, Standard, and Acceptable Level of Quality shall be established for each FTB service level requirement. When a Requirement is listed as mandatory, there is no specific Acceptable Level of Quality other than compliance.

FTB Service Metrics

Requirement	Standard	Metric
FTB Service Availability	99.99%	$Availability = \frac{Uptime}{Uptime + Unplanned Downtime}$
Time to Restore	Less than 2 hours	Time to restore shall be calculated based on the initial log discovery of the outage plus the actual time evolved until system restoration. An exact representation of measures taken and critical obstacles (incorrect information from an adjoined FiXs Domain) shall be maintained as a matter of record.
FTB Routing Accuracy	99.99%	$Accuracy = \frac{Total Transactions}{Total Transactions + Erroneous Routing Attempts}$ <p>An automated feature shall record as an error any attempt to misroute control data. Problem Identification and remediation must be recorded as a matter of record.</p>
FTB Throughput and Response	2 Sec for Authentication 5 Sec for Biometric	The FTB must be capable of timely response even with a high level of network activity. The FTB configuration must be capable of transparently adding routing capability. A minimum capability of 50 transactions per second must be present at IOC. The standard applies to the time from authentication station entry to full response at the authentication station.
FTB Network Monitoring	99.9%	$Monitoring = \frac{Restarts}{Restarts + Failed Control Data Exchange}$ <p>On restart, the FTB shall generate control data to connected Domain Servers and the Brokers of other Connected Federations. Failures of this exchange must generate an alarm and email notification to the Network Manager.</p>
FTB Domain Connections	99.99%	After three failed attempts to contact any FiXs Domain Server, the FTB must alarm and generate an email

		notification to the network manager.
FTB COOP capability	99.9%	FTB Coop capability will be supplied by FiXs for disaster recovery. Contractor responsible for meeting availability requirement and throughput and response requirement
Planned Downtime	Mandatory	Planned downtime for system maintenance may not exceed 2 hours in any week.

6.0 Schemas

6.1 Control Data Schema Definition

Element	Attribute	Type	Description
ControlDataDateTime		dateTime	The timestamp of the current Control Data Table
Category			The grouping of DDSs into Federal, State, Commercial, or Foreign Government categories. There are a maximum of four categories.
	CategoryName	String	Valid Values: <ul style="list-style-type: none">• Federal Government Agency• State Government Agency• Commercial Enterprise• Foreign Government
	CategoryCode	String	Valid Values: <ul style="list-style-type: none">• 01 (Federal Government Agency)• 02 (State Government Agency)• 03 (Commercial Enterprise)• 04 (Foreign Government)
TGB			The list of TGBs under a category.
	TGBName	String	The Trust Gateway Broker name.
	TGBCode	String	The Trust Gateway Broker code.
Attributes (TGB)			
	EnableEncryption	Boolean	True if this TGB can process encrypted data.

Element	Attribute	Type	Description
	PrimeInCategory	Boolean	True if this TGB is the prime repository for the meta data in its category (this TGB is responsible for maintaining all data for the Commercial Enterprise).
	EnableAdvancedCompression	Boolean	True if this TGB can use advanced compression techniques.
PublicKey (TGB)			The public key of the Digital Certificate that was issued to this TGB.
	Algorithm	String	The standard algorithm name for this (Public) key. (RSA, DSA, etc.)
	Format	String	The name of the primary encoding format of this key. (e.g. RAW, SunX509)
DDS			The list of DDSs that belong to a TGB.
	DDSName	String	The DCCIS Domain Server name.
	DDSCode	String	The Unique DCCIS Domain Server code.
Attributes (DDS)			
	EnableEncryption	Boolean	True if this DDS can process encrypted data.
	UseMinutiae	Boolean	True if this DDS can accept fingerprint templates in the industry standard format.
	EnableAdvancedCompression	Boolean	True if this DDS can use advanced compression techniques.
PublicKey (DDS)			The public key of the Digital Certificate that was issued to this DDS.

Element	Attribute	Type	Description
	Algorithm	String	The standard algorithm name for this (Public) key. (RSA, DSA, etc.)
	Format	String	The name of the primary encoding format of this key. (e.g. RAW, SunX509)
Organizations			A list of organizations that belong to this DDS.
	OrganizationName	String	The Organization Name. Must be unique across the entire DCCIS Domain.
	OrganizationCode	String	The Organization Code. Must be unique within the DDS Domain.
Associations			

Element	Attribute	Type	Description
	AssociationName	String	<p>The person's association to the organization.</p> <p>Valid Values:</p> <ul style="list-style-type: none"> • Employee (e.g., hourly or salaried employee) • Government Civil (state or federal government workers, appropriated and non-appropriated fund) • Government Executive Staff or Appointee (includes (SES)) • Uniformed Service (includes active duty, guard and reserve) • Contractor (i.e., contracting to identifying organization) • Organizational Affiliate (those affiliated based on work environment or location, for DoD includes Foreign National, Foreign Military and members of other government agencies working at DoD sites) • Organizational Beneficiary (those whose association only involves receiving benefits from the organization, for DoD this would be family members, retirees, DAV, etc.)

Element	Attribute	Type	Description
Associations (Continued)			Valid Values <ul style="list-style-type: none"> • Employee • Civil • Political Appointee/SES • Uniform Service • Contractor • Affiliate • Beneficiary
	AssociationCode	String	The person's association (code) to the organization. Valid Values: <ul style="list-style-type: none"> • 00 - Employee • 01 - Civil • 02 - Political Appointee/SES • 03 - Uniform Service • 04 - Contractor • 05 - Affiliate • 06 - Beneficiary
Tokens			
	TokenName	String	The name of the token accepted by an Organization. Valid values: <ul style="list-style-type: none"> • Employee Identifier • Bar Code • CAC Card
	TokenCode	String	The token code accepted by an Organization. Valid values: <ul style="list-style-type: none"> • 00 (Employee Identifier) • 01 (Bar Code) • 02 (CAC Card)

6.2 Envelope Schema Definition

Element	Attribute	Type	Description
SourceDDSCode		String	The originator of this Message.
DestinationDDSCode		String	The destination of this Message.
DCCISMsgTypeCode		String	The message type. Valid Values: <ul style="list-style-type: none"> • 01 – Authentication Request • 02 – Authentication Response • 03 – Control Table Request • 04 – Control Table • 05 – Remote Domain Server is not available • 06 – XML Schema Version is out of date • 07 – Control Data Table is out of date • 08 – Heart Beat • 09 – Remote Trust Gateway is not available • 10 – Remote Authentication Request Not Processed • 98 – Trust Gateway shutdown message • 99 – Fatal Service Exception
DCCISXMLSchemaVersion		String	The XML schema version for both the payload and control data table.
DCCISTransactionIdentifier		String	A unique identifier assigned to this DCCIS transaction. The message originator is responsible for assigning a unique identifier to each message.
ControlDataDateTime		dateTime	The timestamp of the current Control Data Table
Payload		hexBinary	The encrypted message payload. This can be either the Control Data XML or the Payload XML. The message type is used to determine which xml schema to expect.

Element	Attribute	Type	Description
PayloadKey		hexBinary	This is the symmetric key that was used to encrypt the payload. The PayloadKey has been encrypted using asymmetric encryption and can only be decrypted using the Destination DDS's private key.
EnvelopeSignature		hexBinary	The digital signature of this envelope. It includes all fields with the exception of the Payload and PayloadKey.

6.3 Payload Schema Definition

Element	Attribute	Type	Description
TokenString		String	The unique code that was obtained from the DCCIS Member. It may have been obtained from a CAC, Bar Code, or entered by the member.
OrganizationCode		String	The DCCIS Member's organization.
TokenCode		String	The token code that was presented by the member at the authentication station.
FingerImage		hexBinary	The fingerprint image.
FingerImageType		String	The fingerprint image type <ul style="list-style-type: none"> • 01 – Bit Map • 02 – JPEG • 03 – TIFF • 04 – GIF • 05 – Raw image • 06 – Pattern Template • 07 – Minutiae Template
FingerCaptureCode		String	The finger capture code. Indicates the fingerprint the Image represents.
FingerImageHeight		int	The image height. Only needed for raw '05' finger print images.
FingerImageWidth		int	The image width. Only needed for raw '05' finger print images.
FingerImageResolution		int	The image resolution in Dots Per Inch (DPI)

Element	Attribute	Type	Description
ReturnCode		String	The result of the request. Valid Values: <ul style="list-style-type: none"> • 00 - Success • 01 – Member Not Found • 02 – Member not in specified organization • 03 – Poor fingerprint quality • 04 – Fingerprint match successful • 05 – Fingerprint match failed
SecurityClassificationIdentifier		String	Reserved for future use.
LastName		String	A member's last name.
FirstName		String	A member's first name.
MiddleName		String	A member's middle name.
Cadency		String	The cadency name (Sr, Jr, III) of a member.
Nationality		String	The citizenship of the DCCIS member.
Association		String	Used to describe the association that the member has with the organization. For commercial DCCIS, this will generally be employee. For DoD, the associations: <ul style="list-style-type: none"> • 00 - Employee • 01 - Civil • 02 - Political Appointee/SES • 03 - Uniform Service • 04 - Contractor • 05 – Affiliate • 06 - Beneficiary
PhotoImage		hexBinary	The Member's photograph.
ImageType		String	The image type (JPEG, GIF, TIFF)
CaptureCode		String	Finger Sequence Number that is available for the DCCIS Member.

Element	Attribute	Type	Description
VetType		String	The vetting type or level for the DCCIS Member. (Reserved for future use.)
VetDate		dateTime	The vetting date. (Reserved for future use.)

7.0 Glossary

DCCIS – Defense Cross Credentialing Identification System

The DCCIS application provides web access to different DCCIS member organization databases, making it possible for them to authenticate visitors carrying authorized ID cards issued by fellow DCCIS member organizations. To compensate for differences in identification systems and credentials used, DCCIS can read a range of media and accept a range of credentials.

DMDC – Defense Manpower Data Center

A Defense Support Activity which is the most comprehensive repository of personnel, manpower, training, and financial data in the DoD. DMDC owns and manages DEERS, including AWS.

DoD (DOD) – Department of Defense

The collection of federal agencies responsible for safeguarding national security.

FiXs: The Federation for Identity and Cross-Credentialing Systems

FTB: FiXs Trusted Broker

HTTP – HyperText Transport Protocol

The underlying protocol used by the Internet which defines how messages are formatted and transmitted, as well as what actions web servers and browsers should take in response to various commands.

PKI – Public Key Infrastructure

Public-key infrastructure (PKI) is the combination of software, encryption technologies, and services that enables DoD to protect the security of their communications and business transactions. PKI integrates the Common Access Card (CAC), digital certificates, public-key cryptography, and certificate authorities into total, enterprise-wide network security architecture.

PO – Project Officer: An individual representing DMDC and assigned to a customer for the purposes of implementing AWS.

XML – eXtensible Markup Language: A simple, very flexible text format derived from SGML (ISO 8879). Originally designed to meet the challenges of large-scale electronic publishing, XML is also playing an increasingly important role in the exchange of a wide variety of data on the Web. For more information about XML, refer to <http://www.w3.org/XML/>