



The Federation for Identity and
Cross-Credentialing Systems®

FiXS[®] Trust Model
Version 3.0

September 1, 2010

www.fixs.org

Copyright 2010 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

1.0 GENERAL REQUIREMENTS AND DEFINITIONS3

2.0 FIXS' OBJECTIVES4

3.0 THE FIXS CHAIN OF TRUST.....6

4.0 FIXS' SEVEN DISTINCT PROCESSES8

5.0 BACKGROUND ON FEDERATED TRUST.....10

REFERENCES12

1.0 General Requirements and Definitions

Trust in the security of personal identity information exchanged over the Internet and other networks are vital for the effective operation of all organizations, both commercial and public sector. Trust is particularly important when the intent of a transaction is to grant physical or logical access privileges to appropriately authorized personnel. This trust can only be accomplished through the establishment and operations of a strong security profile, and Trust Model, from both a governance and operational perspective.

Organizations must address the issues of user identity, authentication, confidentiality, privacy, and integrity of data accessed and/or transferred, and the ability to hold transacting parties accountable for their actions in order to establish this security profile. A Trust Model is the foundation for establishing this profile because it establishes the framework, operating rules, and a transaction model that allows for identity credentials to be trusted across organizations.

The purpose of this document is to describe the manner in which “trust”, or the “Trust Model”, is established across the Federation for Identity and Cross-Credentialing Systems, Inc. ®(FiXs) Network. It also addresses the roles and responsibilities that FiXs Member Organizations and Subscribing Parties will assume when participating in the operations of the FiXs Network.

The FiXs Network provides a highly-scalable, secure, auditable solution set, whereby FiXs Member Organizations can authenticate **FiXs-Certified Credentials** (also known as “FiXs Credentials”) issued to users from participating organizations or Subscribers. The FiXs Network provides data from identity credentials that are compatible, or “aligned”, with the precepts of HSPD-12 and PIV-I and utilize FIPS 201 standards., as well as lower-level credentials, to various authentication nodes that can then be used to authenticate the identity of employees, contract personnel, and various other authorized credential holders or “users”. Additional data authentication can also be transmitted across the Network so that local decision makers can grant physical or logical access privileges. The FiXs Network is interoperable between member organizations and with other credentialing networks (i.e. the Department of Defense Cross-Credentialing Identification System Network or “DCCIS”). Trust in the FiXs Network is built on a common set of rules, responsibilities, and contractual obligations for all participating organizations, which are set forth in the FiXs Foundational Documents (see Definitions for precise meaning of capitalized terms).

FiXs does not issue credentials directly. FiXs establishes the rules, specifications, policies, and procedures that authorized or “approved” issuing Member Organizations must use in issuing FiXs-Certified Credentials. These prescribed foundational agreements and operating rules provide a consistent and reliable level of “trust” that may be presumed across participating entities. FiXs does not participate in determining what privileges should be granted to any user or set of users. Privileges are the province of the facility or system “owner”. However, FiXs does provide a solution for organizations with role-based work environments where employees and authorized agents are afforded privileges consistent with the organization’s own unique requirements. These FiXs Certified Credentials can then be authenticated and managed over a trusted network by other Member Organizations based on this Trust Model. FiXs-

Certified Credentials shall carry the FiXs logo/mark for “branding” and/or recognition purposes consistent with FiXs Policy to support ready identity authentication operations. .

An organization decides what role it wishes to participate in FiXs either in an active membership capacity or as a Subscriber. An organization may desire to just “subscribe” to the FiXs Network, and thus be a “Subscriber Member”. In this capacity they are assigned a unique organization code and then sponsor their employees or individual users to be issued credentials for identity authentication across the Network. Other firms/organizations may desire to join as a full or associate member engaging in the governance and policy promulgation of the Federation. Some members may opt to participate as a “Credential Issuer” whereby they issue and manage credentials of their own employees as well as issue to users from other firms as part of a service that they may choose to offer.

Prior to joining the FiXs Network in any capacity, the organization must be vetted before it is accepted into the FiXs membership or allowed to Subscribe to use FiXs-Certified Credentials. This vetting process provides an assessment of the organization’s validity and corporate standing to be a “trusted organization,” which includes the vetting of the organizations official. If the organization desires to sponsor individuals to be issued FiXs Certified Credentials, after signing the appropriate agreements they will be designated, , as the “**Primary Trusted Organization**” standing behind those individuals (credentials). These Primary Trusted Organizations are then assigned an Organizational Code which is tied to the FiXs-Certified Credentials issued to the individual(s) they have sponsored.

Once the Primary Trusted Organization is established, the individuals sponsored by that organization, undergoes the applicable level of identity verification, enrollment, and credential issuance for the trust level of credential requested.

All participating organizations are required to, sign and abide by the “Terms of Use” for credentials, adhere to the operating principles and policies of the Federation, and maintain their membership in the Federation in “Good Standing” as may be applicable.

2.0 FiXs Trust Model Objectives

The specific objectives of FiXs are to:

1. Establish the appropriate and reliable level of trust and confidence in the identification, vetting, proofing, and enrollment of every organization that participates in the FiXs Network, as well as the sponsored individuals being, issued FiXs-Certified Credentials;
2. Manage the FiXs-Certified Credentials life-cycle process in accordance with all applicable issuance, security, privacy and other applicable rules and/or legislation (i.e., state, federal or local legislation; Department of Defense Policies or Directives; or customer installation or facility policies);
3. Facilitate the secure electronic authentication of FiXs-Certified Credentials, and authentication of selected identity information, across disparate domains, in an interoperable manner that maintains the highest levels of security and privacy of data; and,

4. Provide data to a Trusted Adjudicator/Agent (i.e. gate guard or building monitor, web site or application owner/monitor) who can reliably authenticate the identity of an individual with such confidence that they can render a decision regarding the exercise of privileges, whether physical access, logical access or other type of appropriate access in accordance with the policies, rules and/or legislation that might govern that adjudicator's domain of responsibility.

Overall, FiXs does not set privileges to grant or deny any type of physical or logical access privileges. FiXs does provide the trusted infrastructure (logical, physical, and operational) which all participating members use in providing a high confidence level in the true identity of an individual who is presented for authentication. The results from that determination can then be used for the provisioning of privileges consistent with established policies or the participating organization.

FiXs has successfully worked with the U. S. Department of Defense (DoD) in establishing a mutually-trusted, interoperable community wherein DoD contractors, vendors, and trading partners are able to use approved and accepted identity credentials to authenticate data to authenticate an individual's identity. Currently, FiXs is the only organization established to inter-operate a cross-credentialing infrastructure and systems with the DoD.

FiXs and the Defense Manpower Data Center (DMDC) have signed a formal Memorandum of Understanding attesting to maintaining this trusted relationship with the DoD. FiXs is committed to including other partners throughout the Federal Government, within the first responder community, with other public and private sector organization and commercial entities that seek a scalable, rules-based, interoperable identity verification and authentication capabilities.

The FiXs operating model along with the foundational principles is depicted in Figure 1, below. In all cases, the personal identifying information of an individual credential holder is securely maintained in, and at, the single FiXs-certified location designated by the sponsoring party of the credential holder. The data may not be captured and reused for any purpose other than the authentication instance in question.

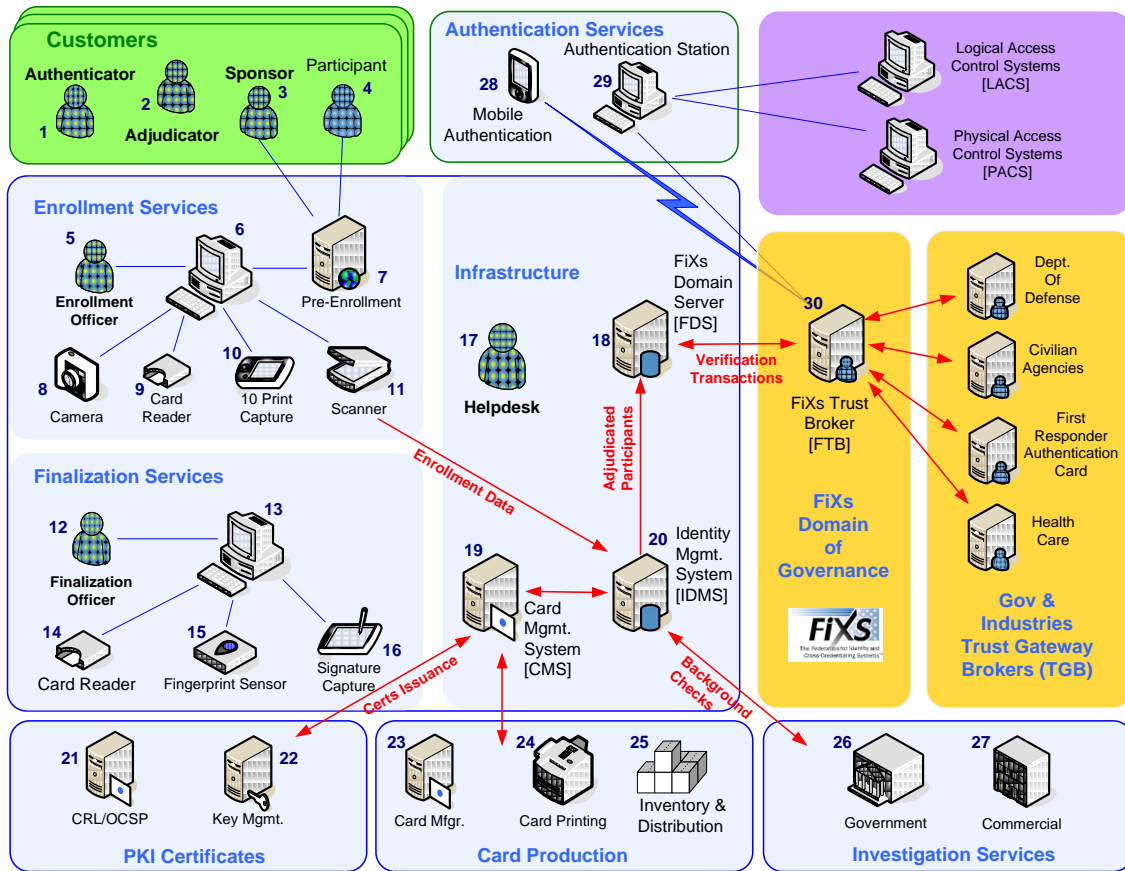


Figure 1 – FiXs Trust Model, Showing Multi-Party Trust with DoD and Various Other Member Organizations

3.0 The FiXs Chain of Trust

The “Chain of Trust” in the FiXs-Certified Credential life cycle and Network begins with two inter-related components. The first is a trusted organization and the second is a trusted individual identity. When the two components are linked, an individual’s identity can be authenticated and managed over the FiXs Network by other participating Member Organizations. Once issued, a FiXs-Certified Credential can then be used across the FiXs Network in various role-based work place environments to provision privileges consistent with the objectives and unique requirements of that member organization.

A Primary Trust Organization (“PTO”), or Sponsoring Party, initiates this Chain of Trust by agreeing to attest to the need for such a credential; the validity of their employees’ identity; and accepting responsibility for the acts and omissions of its employees or other individuals they may sponsor for obtaining FiXs-Certified Credentials to be used over the FiXs Network. In order to become a PTO and prior to the issuance of FiXs Certified Credentials to its employees, the PTO must provide sufficient information on the organization and legal representative to be vetted by a FiXs Member Organization approved to do the vetting. This vetting shall be conducted in accordance with the FiXs Operating Rules and Implementation Guidelines in order to establish a consistent and reliable measure of authenticity and trust worthiness to interact with other FiXs Member Organizations or Subscribing Member Parties.

It is possible that an individual employee of one organization may also belong to another organization(s) (i.e. volunteer groups, social organizations, second employers, etc.) who may also be a member or Subscriber to the FiXs Network. In such cases, the individual and each organization must mutually agree on which organization shall be designated as the PTO for the applicable user on the FiXs Network. After that primary designation, secondary or tertiary credentials can be tied, or linked back, to the primary credential designation, provided that the issuing organizations adhere to FiXs issuing and revocation rules.

The PTO is also responsible for initiating the process to revoke a FiXs Credential based upon the applicable credential revocation requirements. If the employee or sponsored user leaves the organization, or no longer requires a FiXs Credential, the FiXs Credential shall immediately be revoked and the Chain of Trust with the individual shall be broken. The individual may move to another organization to establish a new Chain of Trust or they may later re-establish it within the same organization, if required. At that time a new FiXs-Certified Credential will be issued.

As shown in Figure 2 below, the foundation for the Chain of Trust is built on key building blocks. Some of these building blocks are written documents that outline the FiXs Trust Model, the organization's policies, rules or technical specifications. Others are physical assets, such as the physical infrastructure of the network and endpoints, and still others are processes, like the implementation procedures and standards involved in making the system operational.

In summary, PTOs, through their adherence to this Trust Model and other Foundational Documents form the critical link upon which individual FiXs-Certified Credentials may be issued, authenticated, and, ultimately, trusted.

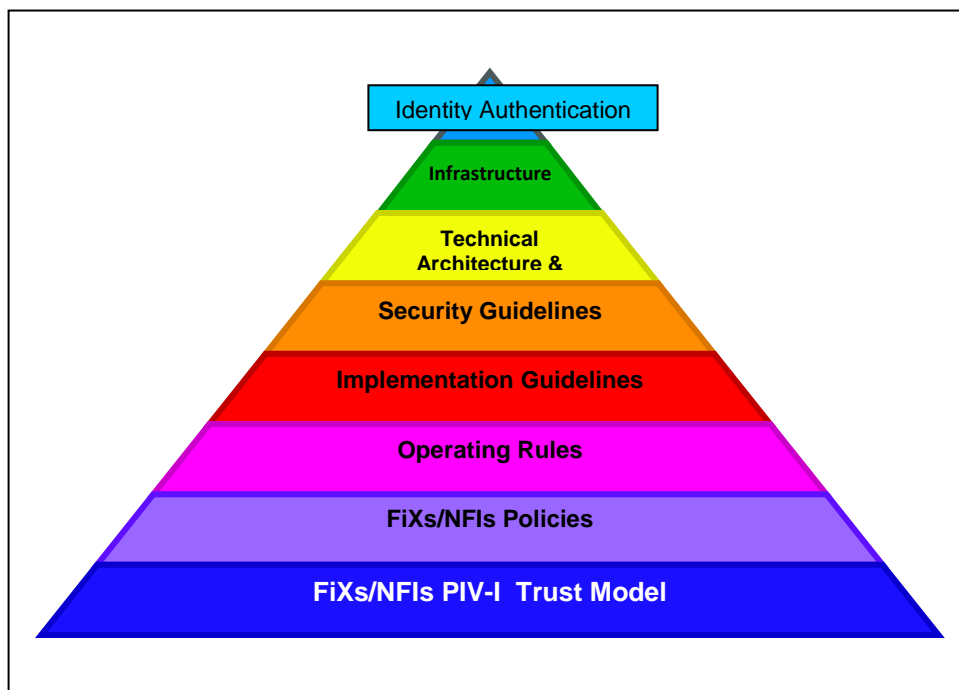


Figure 2: Trust Model, Rules, Policies, Guidelines and the Physical Infrastructure Forming the Foundation for the FiXs Chain of Trust

Summary of Roles and Responsibilities of Primary Trusted Organizations:

- Must be vetted by a FiXs-Approved Organization in accordance with the FiXs Operating Rules.
- Assert the need that its employees, contractual agents, or other users be issued trusted credentials that allow for authentication of Credentials across the FiXs Network.
- Sponsor and attest its employees and/or other users to be issued Credentials
- Abide by the Terms of Use as provided for in the FiXs Policy and Foundational Documents and Trust Model.
- Adhere to the 8-step credential management life-cycle process outlined in Figure 3 of this document.
- Indemnify FiXs and other FiXs Member Organizations, including Member Organizations that may provide services in support of the FiXs, for the acts or omissions of its employees or sponsored users.

4.0 FiXs’ Eight Distinct Processes

There are seven distinct processes that support the issuance and use of FiXs Certified Credentials. These key processes are: **Validating Need; Verifying and Vetting Identity; Adjudicating; Enrolling; Issuing; Authenticating; and Revoking.** These processes are integral to the effective operation of the Trust Model.

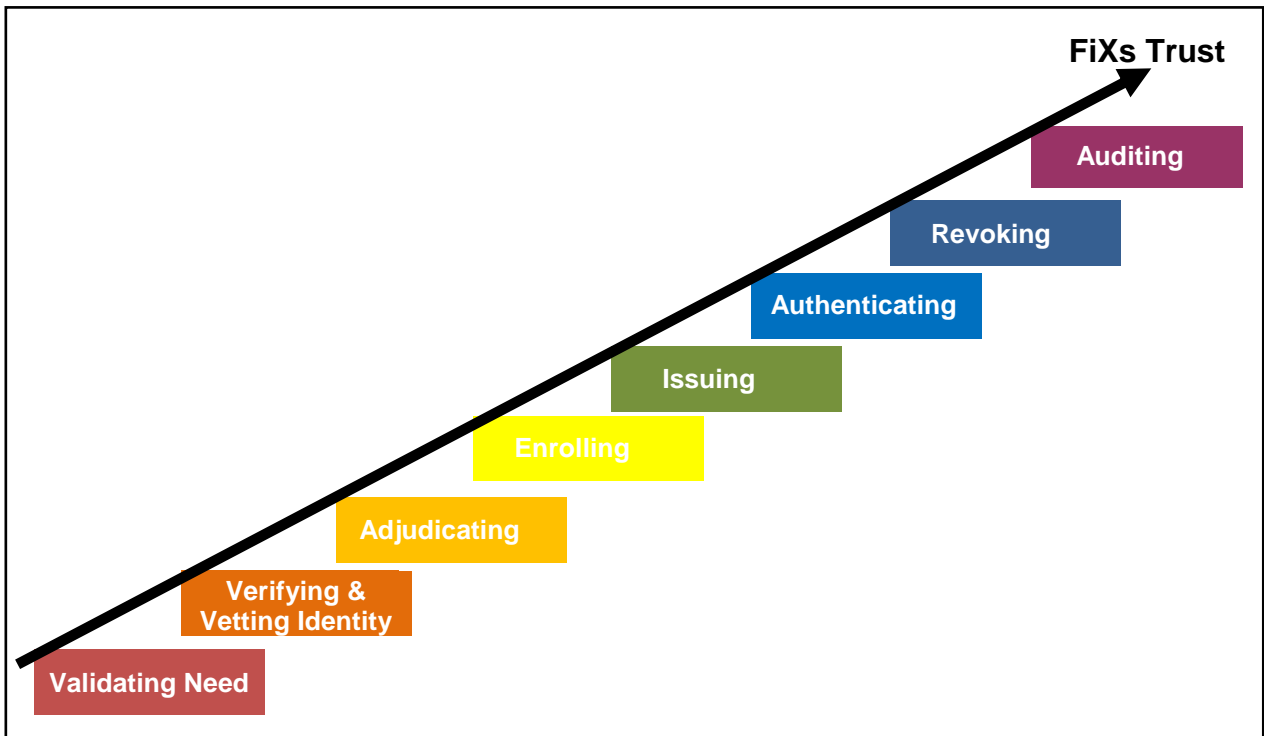


Figure 3– Eight distinct processes of Credential Management

This table provides a high-level description of the individual steps in the management of FiXs Certified Credentials. More detail on each of these steps can be found in FiXs Operating Rules and the FiXs Technical Architecture and Specifications and Implementation Guidelines.

1. Validate Need

A pre-requisite for starting the Credential issuance process is to validate the Organization's need to sponsor their employees for a FiXs Credential. The TPO must submit an application requesting the appropriate vetting as an entity doing, or having a need to do business, with the DoD. Once the organization is accepted then they must attest to their employee's need for a FiXs credential. This written request will be to the FiXs Credential Issuer verifying the Applicant's need for a credential.

2. Verify and Vetting

The FiXs Credential Issuer verifies or "proves" the Applicant's identity and then vets that identity using the process outlined in the FiXs Operating Rules of the FiXs approved organization.

3. Adjudicate

The designated Trusted Adjudicator/Agent determines whether the Applicant may be a participant/user of the Interoperable Network(s) that use data for transacting identity authentications requiring FiXs credentials by being enrolled into a trusted identity Domain Server/database.

4. Enroll

The FiXs Credential Issuer enrolls the Applicant (now a Participant) in the trusted database using the approved documentation and biometric data. This process makes the Participant's record of credentials available for retrieval by any Relying Party for Authentication whenever a credential is presented for authentication.

5. Issue

The FiXs Credential Issuer issues the Participant a Valid FiXs Identifier(s) (following the FiXs technical specifications) that can be used to access the Participant's credentials.

6. Authenticate

A Relying Party transmits an Authentication Inquiry to a trusted FiXs Domain Server/database to validate identity data presented.

7. Revoke

FiXs provides for the timely revocation of identity credentials of a Participant once the validated need lapses or is terminated. Timely revocation is critical to system security and relying party trust.

8. Audit

FiXs provides a compliance audit mechanism to ensure that the FiXs requirements are being implemented and enforced at the issuer [PKI and CMS], network gateways, and relying party environments.

All Authorized FiXs providers shall undergo a Security Certification and Accreditation (C&A), or commercial equivalent managed under a legal governance structure, in accordance with the Federal Information Security Management Act (FISMA) of the E-Government Act of 2002, and associated NIST standards, regulations, and guidelines, and DoD IT Security policies, procedures, and guidelines, as a condition of obtaining and retaining approval to operate as an Authorized FiXs provider. The purpose of the C&A process shall be to verify that the Authorized FiXs provider has in place and follows a system that assures that the quality of its services conforms to the FiXs requirements. Re-accreditation should occur after any significant change in the system, but at least every three years. It should be done more often where there is a high risk and potential magnitude of harm. This requirement does not replace any additional annual auditing requirements stipulated by the PKI(s) approved under the FiXs architecture.

5.0 Background on Federated Trust

It is important to understand what is meant by “trust”, especially in the context of FiXs as it relates to interoperability with other organizations, such as the Department of Defense (DoD), other governmental organizations, and commercial enterprises. FiXs has chosen to adopt the **Federated Model of Trust** as the basis for identity management. This model of trust was chosen for several reasons, namely:

1. The nature of its affiliations with members and advisors. Members commit to a contractual obligation whereby they agree to comply with the FiXs Foundational Documents and operating principles.
2. The DoD, acting on its own authority and guidance, has also independently chosen to collaborate with FiXs and is participating in FiXs in the role of an “advisor”.
3. Each member retains control over the location and security of its own personnel data as well as that of any subscribing parties that it may contract with for credential issuance purposes.
4. Employees and sponsored agents are vetted and only enrolled into a single FiXs domain as designated by the sponsor/subscribing party
5. There is no central database of identity credential information.
6. FiXs Members and Subscribers are bound by a multi-party contract through formal agreement or acceptance of Terms of Use.

Additionally, a variety of methods can be employed to establish trust at different levels of assurance among Subscribing parties. The appropriate level of assurance is determined by the underlying technology as well as the Operating Rules, Implementation Guidelines, and the overriding business service requirement.

The X.509 specification, a widely used standard for defining digital certificates provides a suitable clarification on trust, stating that *“Entity ‘A’ trusts entity ‘B’ when ‘A’ assumes that ‘B’ will behave exactly as ‘A’ expects it to behave.”* According to this description, trust deals with assumptions, expectations and behavior. This implies that trust cannot be measured quantitatively and there is a certain amount of risk associated with resulting trust. The FiXs Trust Model addresses this risk by establishing how trust is established and enforced throughout the lifecycle of a trusted FiXs Credential.

In order to clarify the application of a Federated Trust Model, it seems appropriate to consider other instantiations of a Trust Model. The Liberty Alliance Project¹ offers a well-recognized approach, which can be used as an objective basis for comparison.

Historically, the Liberty Alliance defined “**Community Trust**” as follows:

“Community Trust applies when the business trust between a pair of entities is derived from their enrollment in a common authentication infrastructure and acceptance of its practices, without reliance on other business agreement paths.

¹ The Liberty Alliance (Project) is comprised of over 100 member companies representing a wide variety of industries and over a billion customers, with operations all over the globe. Each of the member companies either owns or operates large communities of interest or is the developer of core technology that can enable a federation of online communities. The role of the Liberty Alliance Project is to support the development, deployment and evolution of an open, interoperable standard for federated network identity. For more information on the Liberty Alliance, please visit their web site at <http://www.projectliberty.org>

As such, the entities' mutual trust in a business sense is based on their membership in a community constructed and linked for authentication purposes.²

In the Community Trust model, an *organization* (e.g., an industry consortium or a community) sponsors, endorses, or adopts one or more trust establishment services to provide and manage the credentials needed by entities to create and maintain authentication trust among them. (In the FiXs Trust Model, the FiXs Federation could be seen as the "organization.") The service(s) could be operated by the sponsoring organization, or could be provided by an independent service delivery organization. In Community Trust, some level of business trust, although not provided by either direct or brokered business agreements, can be derived from participation in a shared authentication infrastructure (for example PKI, Kerberos, or PGP "webs of trust"). The assumption is that the authentication infrastructure will, in addition to allowing entities to be identified, further identify them as belonging to some community. Different options imply different degrees of organizational involvement and, potentially, of organizational liability. Liberty's Community Trust model presumes neither direct nor indirect business agreement paths between communicating entities.

In the FiXs Trust Model, members join FiXs for their unique business reasons, not necessarily because they share a common cryptographic trust establishment infrastructure. The concept of "membership in a community constructed and linked for authentication purposes" applies only to the extent that members are interested in trustfully authenticating identity credentials for the purpose of authoritatively proving identities.

The Liberty Alliance Project also defined "**Brokered Trust**" as follows:

"Brokered Trust describes the case where two entities do not have direct business agreements with each other, but do have agreements with one or more intermediaries so as to enable a business trust path to be constructed between the entities. The intermediary brokers operate as active entities, and are invoked dynamically via protocol facilities when new paths are to be established."

In Liberty's Brokered Trust model, active intermediaries are invoked and involved when federation and/or authentication transactions span multiple administrative domains. These approaches constrain the set of components that must be involved in inter-domain trust management, but require the use of additional protocol facilities. Further, Brokered Trust models depend on availability of appropriate intermediaries in order to construct a path to federate a user's relationship and/or to authenticate a particular session.

As an example situation where Brokered Trust may be applicable, Member A receives a request to be processed from Member B, with which it shares no prior formal business relationship. The underlying Trust Model must decide whether to trust Member A's original request and Member B's subsequent response. In this situation, overall trust is composed of the combination of business trust, based on direct/indirect business agreements, and authentication trust, which is based on the underlying direct/indirect authentication infrastructure. To put it simply, there is no direct business trust in a Liberty Alliance Brokered Trust model. Conversely, in the FiXs Trust Model all participating members have a formal relationship through acknowledgement and agreement to the "Terms of Use" for such credentials.

² Liberty Trust Model Guidelines: <http://www.oasis-open.org/committees/download.php/6158/sstc-saml-trustmodels-2.0-draft-01.pdf>

Note: For FiXs Definitions/Terminology, see [Master Glossary of Terms/Definitions](#)

References

Industry and Academia

- ITU-T Recommendation X.509, Public-Key and Attribute Certificate Frameworks, International Telecommunications Union -Telecommunications Standardization Sector, March 2000.
- Housley, R., eds. (April 2002). "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 3280, The Internet Engineering Task Force <http://www.rfceditor.org/rfc/rfc3280.txt>
- [X.509] "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks," ITU-T (2000). ITU-T Recommendation X.509 (2000) | ISO/IEC 9594-8:2000,
- FEGC Report by the DoD/Industry working Group for Strong Authentication and Secure Communications, ***"An On-Going Assessment of Government Information Assurance, e-Business Policy, and Implementation in a Changing 'Trust' Environment"***, 3 May 2002.
- FEGC Report prepared for DMDC and DoD, ***"Developing an Interoperability Demonstration Pilot for the Defense Cross-credentialing Identification System (DCIS)"***, version 4.1, dated 6 March 2003.
- Liberty Alliance Project, ***"Liberty Alliance Trust Models"***, draft version 1.0-14, 13 April 2003.

DoD Common Access Card (CAC) Program

- U.S. Department of Defense, Memorandum from Deputy Secretary of Defense – John J. Hamre, ***"Smart Card Adoption and Implementation"***, 10 November 1999.
- U.S. Department of Defense, Memorandum from DoD CIO and USD (P&R), ***"Common Access Card (CAC)"***, 16 January 2001
- U.S. Department of Defense, Department of Defense DIRECTIVE – ASD (C3I)/DoD CIO, ***"Smart Card Technology"***.
- U.S. Department of Defense, Memorandum from Connie K. DeWitte – Deputy Assistant Secretary of the Navy (Safety), ***DODPUB Change- 5200.8R DOD Physical Security Program"***, 2 June 2003.
- Memorandum of Understanding between The Federation for Identity and Cross Credentialing Systems and Defense Manpower Data Center signed January 10, 2006
- Letter from U.S. Department of Defense, Defense Manpower Data Center, acceptance of Card Holder Unique Identifier (CHUID) solution for assigning unique organizational codes to non-Federal government entities dated 6 December, 2007
- Defense Cross Credentialing Identification System (DCCIS) Initial Operating Capability (IOC) letter dated 16 July, 2007
- Memorandum of Understanding between The Federation for Identity and Cross Credentialing Systems and Defense Manpower Data Center signed February 12, 2009
- 2010 FiXs Notification on Credential Usage with US NORTHCOM (May, 2010)

- DTM 09-12

DoD PKI Program

- U.S. Department of Defense, "**Target Public Key Infrastructure User Requirements**", 29 February 2000.
- U.S. Department of Defense, "**Class 3 PKI Public Key-Enabled Application Requirements**", version 1.0, 13 July 2000.
- U.S. Department of Defense, "**Class 3 PKI Interface Specifications**", version 1.2, 10 August 2000.
- U.S. Department of Defense, "**PKI Implementation Plan**", version 3.1, 18 December 2000.
- U.S. Department of Defense, "**Public Key Infrastructure (PKI) Policy Update**", 21 May 2002.
- U.S. Department of Defense, "**Certificate Policy for External Certificate Authorities**", version 1.10, 14 November 2002.
- U.S. Department of Defense, "**Public Key Infrastructure Roadmap**", 13 June 2003.
- U.S. Department of Defense, "**X.509 Certificate Policy**", version 10, 2 Mar 2009

Federal Identity Management

- FIPS 201-1: Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006
- HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors, 27 August 2004
- NIST SP 800-63: Electronic Authentication Guideline, April 2006
- NIST SP 800-76-1: Biometric Data Specification for Personal Identity Verification, January 2007
- NIST SP 800-79-1: Guidelines for the Accreditation of Personal Identity (PIV) Verification Card Issuers, June 2008
- NIST SP 800-116: A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS), November 2008
- NIST SP 800-73: Interfaces for Personal Identity Verification (4 Parts), February 2010