National Identity Exchange Federation

Identity Assurance Framework

Version 1.1

July 24, 2015

Table of Contents

1 Introduction

The National Identity Exchange Federation (NIEF) provides a basic trust framework for agencies and their users to leverage and reuse local digital identities and associated attributes for various business purposes with partner agencies and communities of interest (COIs). The primary business purpose for these identities and attributes is to support information sharing subject to business-level access controls. NIEF is an outgrowth of the U.S. Dept. of Justice's Global Federated Identity and Privilege Management (GFIPM) program, and therefore uses and is heavily influenced by GFIPM concepts and terminology.

Within the NIEF framework, an agency can play one or more roles, including Identity Provider Organization (IDPO), Service Provider Organization (SPO), Attribute Provider Organization (APO), and Service Consumer Organization (SCO). The roles of IDPO and SPO are analogous to similar functions of "Identity Provider" or "Identity Provider Operator" and "Service Provider" or "Service Provider Operator" in other federated identity models. An IDPO is an organization that vets individuals, collects attributes about those individuals, and maintains those attributes in an accurate and timely manner; and an SPO is an agency that offers business-level services and acts as a relying party to IDPOs. For the purpose of this document, we do not further discuss the roles of APO or SCO, as they represent extensions to NIEF's basic identity assurance framework and are not necessary for a basic understanding of the framework.

The NIEF philosophy recognizes that IDPOs typically come to a federation or trust framework with a variety of local identity and attribute management policies and practices in place. One of NIEF's primary goals is to promote interoperability and efficiency by mapping each IDPO's local policies and practices into a common and consistent framework that SPOs can use for making risk-based decisions about trust. Accordingly, NIEF has adopted the standard NIST Level of Assurance (LOA) trust criteria, as per the NIST Special Publication 800-63-2 ("E-Authentication Guideline").[1] Specifically, NIEF supports LOA 2 and Non-PKI LOA 3 as defined by NIST in SP 800-63-2, and as used by the Federal Identity, Credentialing, and Access Management (FICAM) program in its policy documents and technical specifications.[2] NIEF has established a framework of policies, procedures, and technical specifications to ensure that relying parties (SPOs) can adequately trust asserted identities and their associated attributes at these well-defined NIST/FICAM LOAs.

1.1 Purpose and Intended Audience

The primary purpose of this document is to help the reader better understand the basic structure and nature of NIEF as an identity assurance framework for asserting digital identities and their associated attributes at NIST LOA 2 and NIST Non-PKI LOA 3. The intended audience includes representatives from current and prospective NIEF member agencies, as well as others who wish to understand NIEF's basic identity assurance structure.

[1] See http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf.
[2] See http://www.idmanagement.gov/identity-credential-access-management.

This document is non-normative, and does not constitute a formal component of the NIEF identity and trust framework. Where applicable, it includes pointers to other NIEF documents that are part of the formal NIEF framework.

1.2 List of References to Related Documents

This section contains references to other documents that are related to or cited by this document.

Document ID	Document Name and Description
NIST 800-63-2	*NIST Special Publication 800-63-2, E-Authentication Guideline* – Describes NIST guidance about requirements for asserting identities at various LOAs, as well as criteria for assessing risk at each LOA.
NIEF Gov	*NIEF Center Governance Documents* – Contains NIEF legal agreement templates and bylaws. Legal agreement templates are used to execute binding legal agreements between NIEF and its member agencies, with assignment of roles, responsibilities, liability, etc.
NIEF OPP	*NIEF Center Operational Policies and Procedures* – Describes basic operational policies and procedures that NIEF follows. Focuses primarily on the NIEF membership lifecycle and membership requirements.
NIEF CP	*NIEF Certificate Policy* – Describes NIEF policy relating to the use of sensitive private key material by NIEF and its members for the purpose of securing identity assertions and other sensitive communications.
NIEF Privacy	*NIEF Privacy Policy* – Describes NIEF policy relating to the release of identity and attribute data by both IDPOs and SPOs.
NIEF Audit	*NIEF Audit Policy* – Describes NIEF policy relating to the initial and ongoing audit of NIEF member agencies. Includes extensive description of NIEF audit requirements for IDPOs that wish to assert identities at LOA 2 and Non-PKI LOA 3.
NIEF Trust	*NIEF Cryptographic Trust Model* – Normative specification used by NIEF to ensure secure distribution of public key material and other trusted information to NIEF member agencies, in support of secure data exchange between NIEF member agencies. Based on the SAML Metadata Profile. The secure, cryptographically signed document is called the *NIEF Cryptographic Trust Fabric*.
NIEF CTFMP	*NIEF Cryptographic Trust Fabric Management Policy* – Describes NIEF policy relating to the operational lifecycle management of the *NIEF Cryptographic Trust Fabric.*
NIEF U2S Profile	*NIEF Web Browser User-to-System Profile* – Normative communication profile specification used by NIEF to ensure

	interoperable communication among NIEF member agencies based on the Security Assertion Markup Language (SAML) Single Sign-On (SSO) Profile. Conforms to, and further constrains, the FICAM SAML SSO Profile.[3]
NIEF S2S Profile	*NIEF Web Services System-to-System Profile* – Normative communication profile specification used by NIEF to ensure interoperable communication among NIEF member agencies based on the SOAP Web Services suite of protocols.
NIEF Attr	*NIEF Attribute Registry* – Normative specification used by NIEF to ensure consistency of user attribute assertion and interpretation among NIEF members.
NIEF AP	*NIEF Attribute Profile* – Normative specification used by NIEF to ensure consistent use of the attributes in the NIEF Attribute Registry among NIEF members.
NIEF Attr Enc	*NIEF Attribute Encoding Rules* – Normative specification used by NIEF to ensure consistent encoding of attributes from the NIEF Attribute Registry within specific structures, e.g., SAML assertions and NIEF Cryptographic Trust Fabric (i.e., SAML Metadata).

2 Levels of Assurance in NIEF

NIEF supports two Levels of Assurance (LOAs): NIST LOA 2 and NIST Non-PKI LOA 3. The requirements for each LOA are taken directly from [NIST 800-63-2] and the applicable FICAM guidance that was derived from [NIST 800-63-2]. Each LOA is orthogonal to, and may be used in conjunction with, any communication profile supported by NIEF.

When asserting an identity, an IDPO may also assert the LOA of the identity in the form of an attribute that can be consumed and used by an SPO. [NIEF Attr] defines an attribute called "FICAM Assurance Level Code", which an IDPO can use for this purpose.

When asserting the "FICAM Assurance Level Code" attribute, an IDPO must not assert any LOA for which it has not been explicitly certified by NIEF. NIEF publishes the list of LOAs for which each IDPO has been certified as part of its NIEF Cryptographic Trust Fabric document; see [NIEF Trust]. This provides each SPO with a trusted 3rd-party assertion of the LOA(s) at which each IDPO is permitted to assert identities.

For more information about the criteria and process used by NIEF to certify IDPOs at each LOA, please see Section 3 of this document.

3 Audit and Certification of Identity Provider Organizations

[3] See http://www.idmanagement.gov/sites/default/files/documents/SAML20_Web_SSO_Profile.pdf.

Before an IDPO may assert identities at NIST LOA2 or NIST Non-PKI LOA 3, NIEF must indicate via the NIEF Cryptographic Trust Fabric document that the IDPO has been certified to assert identities at one or both of those LOAs. To become certified at LOA 2, an IDPO must submit to an audit and meet all of the LOA 2 audit requirements, as per [NIEF Audit]. Similarly, to become certified at Non-PKI LOA 3, an IDPO must submit to an audit and meet all of the Non-PKI LOA 3 audit requirements, as per [NIEF Audit].

Note, as stated in Section 1, that NIEF's audit requirements at LOA 2 and Non-PKI LOA 3 are derived from, and consistent with, the requirements stipulated by [NIST 800-63-2] and applicable FICAM guidance. Note also that [NIEF Audit] imposes audit requirements on both an initial and ongoing (yearly) basis. All details about the audit format, including auditor qualifications, are described in [NIEF Audit].