National Identity Exchange Federation

Terminology Reference

Version 1.2

July 31, 2018

Table of Contents

1. Introduction and Purpose

By its nature, the National Identity Exchange Federation (NIEF) involves collaboration among many disparate groups and individuals, and each collaborator brings a unique set of experiences in terms of problems encountered and terminology used to describe those problems and the solutions to those problems. In particular, NIEF makes use of federated identity management standards and other related technical standards, many of which contain terminology that may cause confusion when used in the context of other standards and technologies.

The NIEF Terminology Reference has been developed to maximize the level of precision in other NIEF documents and minimize the level of confusion that readers may face as they work through and try to interpret these documents within the context of their experiences and prior knowledge. This document attempts to define and reconcile common terms from the following technologies, technical standards, and related initiatives, as those terms relate to NIEF.

1. Security Assertion Markup Language (SAML)
2. Web Services (WS-*)
3. Web Services Interoperability (WS-I)
4. Global Reference Architecture (GRA)
5. OpenID Connect (OIDC)
6. OAuth

2. NIEF Identity Trust Framework

This document is one component of the NIEF Identity Trust Framework. See [NIEF OPP] for more information about the full NIEF Identity Trust Framework.

3. References

This section contains references that are relevant to NIEF, as well as SAML, GRA, Web Services, OAuth, and OpenID Connect industry standards and profiles, and other topics that are closely related to NIEF.

Document ID	Document Name and URL
NIEF OPP	NIEF Center Operational Policies and Procedures
NIEF Attrs	NIEF Attribute Registry
NIEF U2S	NIEF Web Browser User-to-System Profile
NIEF S2S	NIEF Web Services System-to-System Profile
GRA WS-SIP	Global Reference Architecture Web Services Service Interaction Profile

GRA RS WS-SIP	Global Reference Architecture Reliable Secure Web Services Service Interaction Profile
SAML2	Security Assertion Markup Language (SAML) 2.0 is an XML-based standard for exchanging authentication and authorization data between identity providers and service providers. SAML is a product of the OASIS Security Services Technical Committee (SSTC). http://wiki.oasis-open.org/security
SOAP	SOAP is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks. SOAP was originally an acronym for "Simple Object Access Protocol," but the name was subsequently changed to SOAP. SOAP is currently maintained by the XML Protocol Working Group of the World Wide Web Consortium (W3C). http://www.w3.org/2000/xp/Group/
WS-Sec	Web Services Security (WS-Security) is a communications protocol for applying security to Web Services. It describes how to attach signatures, encryption headers, and other security tokens to SOAP messages. WS-Security is under the control of OASIS. http://docs.oasis-open.org/wss/
WS-Sec SAML	Web Services Security (WS-Security) SAML Token Profile is an OASIS standard that specifies how to use SAML 1.1 and SAML 2.0 assertions with the WS-Security standard. http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLTokenProfile.pdf
WS-I BP	WS-I Basic Profile (WS-I BP) is a standard that promotes interoperability between Web Services in general. It is a product of the Web Services Interoperability Organization. http://www.ws-i.org/deliverables/workinggroup.aspx?wg=basicprofile
WS-I BSP	Web Services Interoperability Basic Security Profile (WS-I BSP) is a standard that promotes interoperability for secure Web Services. It is based on SOAP and WS-Security and provides guidance on the use of various WS-Security token formats. It is based on the WS-I Basic Profile (WS-I BP) and is a product of the Web Services Interoperability Organization. http://www.ws-i.org/deliverables/workinggroup.aspx?wg=basicsecurity
WS-Addr	Web Services Addressing (WS-Addressing) is a transport-agnostic standard used to communicate message-addressing information in Web Services. It is under the control of the World Wide Web Consortium (W3C) WS-Addressing Working Group. http://www.w3.org/2002/ws/addr/
WS-Trust	Web Services Trust Language (WS-Trust) is a Web Services specification and OASIS standard that provides extensions to the WS-Security standard for the issuance, renewal, and validation of security tokens, as well as establishing and brokering trust relationships between participants in a secure Web Services message exchange. http://docs.oasis-open.org/ws-sx/ws-trust/
WS-Policy	Web Services Policy Framework (WS-Policy) is a specification that enables Web Services providers and consumers to exchange policy information and requirements related to security, quality of services, and various other aspects of Web Services. It is under the control of the World Wide Web Consortium (W3C) WS-Policy Working Group. http://www.w3.org/2002/ws/policy/
WS-SC	Web Services Secure Conversation Language (WS-SecureConversation) is a specification that enables sharing of security contexts for Web Services. It works in conjunction with WS-Security, WS-Trust, and WS-Policy. http://docs.oasis-open.org/ws-sx/ws-secureconversation/

WS-RM	Web Services Reliable Messaging (WS-ReliableMessaging) is a specification that allows SOAP messages to be delivered reliably between distributed applications in the presence of software component, system, or network failures. It is an OASIS standard, under the control of the OASIS Web Services Reliable Exchange (WS-RX) Technical Committee. http://docs.oasis-open.org/ws-rx/wsrm/
WS-Fed	WS-Federation is an identity federation specification that defines mechanisms for allowing disparate security realms to broker information on identities, identity attributes, and authentication. It was ratified as an OASIS standard in May 2009. http://docs.oasis-open.org/wsfed/
WS-I RSP	Web Services Interoperability Reliable Secure Profile (WS-I RSP) is a standard that promotes interoperability for secure, reliable messaging capabilities for Web Services. It is designed to be composed with the Web Services Interoperability Basic Profile (WS-I BP) and the Web Services Interoperability Basic Security Profile (WS-I BSP), and it profiles WS-Addressing, WS-SecureConversation, and WS-ReliableMessaging. It is a product of the Web Services Interoperability Organization. http://www.ws-i.org/deliverables/workinggroup.aspx?wg=reliablesecure
FIPS 140-2	Federal Information Processing Standard (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules*, is a U.S. government computer security standard used to accredit cryptographic modules. It was initially published on May 25, 2001, and most recently updated on December 3, 2002. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
XML-Encryption	*XML Encryption Syntax and Processing*, W3C Recommendation December 10, 2002, specifies a process for encrypting data and representing the result in XML. The data may be arbitrary data (including an XML document), an XML element, or XML element content. http://www.w3.org/TR/xmlenc-core/
XML-Signature	*XML Signature Syntax and Processing (Second Edition)*, W3C Recommendation June 10, 2008, specifies XML digital signature processing rules and syntax. XML Signatures provide integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML that includes the signature or elsewhere. http://www.w3.org/TR/xmldsig-core/
JSON	Internet Engineering Task Force (IETF) Request For Comments (RFC) 7159, "The JavaScript Object Notation (JSON) Data Interchange Format". JSON is a lightweight, text-based, language-independent data interchange format. It was derived from the ECMAScript Programming Language Standard. JSON defines a small set of formatting rules for the portable representation of structured data. https://tools.ietf.org/html/rfc7159
JWS	Internet Engineering Task Force (IETF) RFC 7515, "JSON Web Signature (JWS)", May 2015. JWS represents content secured with digital signatures or Message Authentication Codes (MACs) using JavaScript Object Notation (JSON) based data structures. Cryptographic algorithms and identifiers for use with this specification are described in the separate JSON Web Algorithms (JWA) specification and an IANA registry defined by that specification. Related encryption capabilities are described in the separate JSON Web Encryption (JWE) specification. https://tools.ietf.org/html/rfc7515

JWE	Internet Engineering Task Force (IETF) RFC 7516, "JSON Web Encryption (JWE)", May 2015. JWE represents encrypted content using JavaScript Object Notation (JSON) based data structures. Cryptographic algorithms and identifiers for use with this specification are described in the separate JSON Web Algorithms (JWA) specification and IANA registries defined by that specification. Related digital signature and MAC capabilities are described in the separate JSON Web Signature (JWS) specification. https://tools.ietf.org/html/rfc7516
JWK	Internet Engineering Task Force (IETF) RFC 7517, "JSON Web Key (JWK)", May 2015. A JWK is a JavaScript Object Notation (JSON) data structure that represents a cryptographic key. This specification also defines a JSON Web Key Set (JWK Set) JSON data structure that represents a set of JWKs. Cryptographic algorithms and identifiers for use with this specification are described in the separate JSON Web Algorithms (JWA) specification and IANA registries defined by that specification. https://tools.ietf.org/html/rfc7517
JWA	Internet Engineering Task Force (IETF) RFC 7518, "JSON Web Algorithms (JWA)", May 2015. The JWA specification registers cryptographic algorithms and identifiers to be used with the JSON Web Signature (JWS), JSON Web Encryption (JWE), and JSON Web Key (JWK) specifications. It defines several IANA registries for these identifiers. https://tools.ietf.org/html/rfc7518
JWT	Internet Engineering Task Force (IETF)RFC 7519, "JSON Web Token (JWT)", May 2015. JWT is a compact, URL-safe means of representing claims to be transferred between two parties. The claims in a JWT are encoded as a JavaScript Object Notation (JSON) object that is used as the payload of a JSON Web Signature (JWS) structure or as the plaintext of a JSON Web Encryption (JWE) structure, enabling the claims to be digitally signed or MACed and/or encrypted. https://tools.ietf.org/html/rfc7519
OAuth Core	Internet Engineering Task Force (IETF) Request For Comments (RFC) 6749, "The OAuth 2.0 Authorization Framework" specifies a framework that enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf. https://tools.ietf.org/html/rfc6749
OAuth Bearer	Internet Engineering Task Force (IETF) Request For Comments (RFC) 6750, "The OAuth 2.0 Authorization Framework: Bearer Token Usage" specifies how to use bearer tokens in HTTP requests to access OAuth 2.0 protected resources. Any party in possession of a bearer token (a "bearer") can use it to get access to the associated resources (without demonstrating possession of a cryptographic key). To prevent misuse, bearer tokens need to be protected from disclosure in storage and in transport. https://tools.ietf.org/html/rfc6750
OAuth Assertions	Internet Engineering Task Force (IETF) RFC 7251, "Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants",May 2015. This specification provides a framework for the use of assertions with OAuth 2.0 in the form of a new client authentication mechanism and a new authorization grant type. Mechanisms are specified for transporting assertions during interactions with a token endpoint, as well as general processing rules. https://tools.ietf.org/html/rfc7521

OAuth JWT	Internet Engineering Task Force (IETF) RFC 7523, "JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants", May 2015. This specification defines the use of a JSON Web Token (JWT) Bearer Token as a means for requesting an OAuth 2.0 access token as well as for use as a means of client authentication. https://tools.ietf.org/html/rfc7523
OAuth SAML2	Internet Engineering Task Force (IETF) RFC 7522, "SAML 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants", May 2015. This specification defines the use of a Security Assertion Markup Language (SAML) 2.0 Bearer Assertion as a means for requesting an OAuth 2.0 access token as well as for use as a means of client authentication. https://tools.ietf.org/html/rfc7522
OAuth DCR	Internet Engineering Task Force (IETF) RFC 7591, "OAuth 2.0 Dynamic Client Registration Protocol", July 2015. This specification defines mechanisms for dynamically registering OAuth 2.0 clients with authorization servers. Registration requests send a set of desired client metadata values to the authorization server. The resulting registration responses return a client identifier to use at the authorization server and the client metadata values registered for the client. The client can then use this registration information to communicate with the authorization server using the OAuth 2.0 protocol. This specification also defines a set of common client metadata fields and values for clients to use during registration. https://tools.ietf.org/html/rfc7591
OIDC Core	"OpenID Connect Core 1.0", November 8, 2014. OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It enables Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner. This specification defines the core OpenID Connect functionality: authentication built on top of OAuth 2.0 and the use of Claims to communicate information about the End-User. It also describes the security and privacy considerations for using OpenID Connect. http://openid.net/specs/openid-connect-core-1_0.html
OIDC Disc	"OpenID Connect Discovery 1.0", November 8, 2014. This specification defines a mechanism for an OpenID Connect Relying Party to discover the End-User's OpenID Provider and obtain information needed to interact with it, including its OAuth 2.0 endpoint locations. http://openid.net/specs/openid-connect-discovery-1_0.html
OIDC DCR	"OpenID Connect Dynamic Client Registration 1.0", November 8, 2014. This specification defines how an OpenID Connect Relying Party can dynamically register with the End-User's OpenID Provider, providing information about itself to the OpenID Provider, and obtaining information needed to use it, including the OAuth 2.0 Client ID for this Relying Party. http://openid.net/specs/openid-connect-registration-1_0.html
RFC 2119	Internet Engineering Task Force (IETF) Request For Comments (RFC) 2119, "Key Words for Use in RFCs to Indicate Requirement Levels," is a document that specifies best current practices regarding the use of key words that relate to requirements in technical and policy standards. It is mainly intended for use as an interpretive guide for understanding language in other IETF RFCs and standards; however, its language is generally applicable to all normative technical standards. https://tools.ietf.org/html/rfc2119

4. Basic NIEF Terms and Definitions

This section introduces and defines several fundamental NIEF terms.

Trust and Interoperability Framework: Any formal structure that enables a group of organizations or communities to establish and manage trust relationships among themselves for the purpose of accomplishing or enabling the accomplishment of a specific set of IT-related business goals. A Trust and Interoperability Framework may include a variety of components that serve to facilitate trust and interoperability, including the following.

- *Onboarding and Participation/Membership Policies* for ensuring that each framework participant follows a set of well-defined and formally agreed upon steps to remain in good standing and trustworthy among the other participants

- *Certificate Policies* for ensuring that each framework participant follows well-defined and formally agreed upon practices in the management of its sensitive cryptographic key material, thereby helping to ensure the integrity of transactions between its participants

- *Security Policies* for ensuring that each framework participant follows well-defined and formally agreed upon practices in the management of physical and logical security within its organization, thereby helping to ensure the integrity of transactions between its participants

- *Privacy Policies* for ensuring that each framework participant follows well-defined and formally agreed upon practices regarding the collection, use, and release of all Personally Identifiable Information (PII) that is exchanged between participants

- *Dispute Resolution Policies* for ensuring that framework participants follow well-defined and formally agreed upon practices regarding the adjudication of disputes that may arise between them within the context of the framework

- *Cryptographic Specifications and Profiles* for enabling cryptographic capabilities, such as data encryption and digital signatures, among framework participants

- *Communication Protocol Specifications and Profiles* for enabling interoperable communications and the exchange of mutually understood data among framework participants

- *Data Specifications and Profiles* for enabling the exchange of data structures and payloads that are formally agreed upon and mutually understood at both the syntactic and semantic levels, in support of the framework's business goals

- *Risk and Assurance Frameworks and Profiles* for enabling participants in the Trust and Interoperability Framework to make sensible decisions about the level of risk engendered by specific business decisions

- *Agreements and Contracts* for ensuring that each framework participant operates in accordance with the framework's policies, and also for ensuring that each framework participant understands the roles, responsibilities, and liabilities associated with its participation in the framework

Federated Identity Trust Framework: A Trust and Interoperability Framework that exists for the purpose establishing trust among multiple distinct security domains towards a goal of trusted identity and attribute sharing, authentication, and access control within a Community of Interest (COI) or among a set of partner agencies.

Identity Federation: A type of Federated Identity Trust Framework that is characterized by a trust architecture in which each participant executes a formal agreement or contract with an Identity Federation Management Organization (IFMO). Participating organizations in an Identity Federation are typically called "members", and the agreement between a member and the IFMO is typically called a "membership agreement". An Identity Federation is typically organized under a well defined, written set of bylaws or other governance processes, and operates according to a well defined, written set of operational policies and procedures.

Identity Federation Management Organization (IFMO): A management organization (usually comprised of Identity Federation members) that is responsible for the governance, policies, procedures and implementation of an Identity Federation. *The NIEF Center is best characterized as an IFMO.*

Identity Provider Organization (IDPO): An organization that vets individuals, collects attributes about these individuals, and maintains those attributes in an accurate manner. The IDPO may operate one or more Identity Provider (IDP), Assertion Delegate Service (ADS), Attribute Provider (AP), and/or Attribute Consumer (AC) endpoints, in a federated identity trust framework.

Credential Service Provider (CSP): An equivalent term for an IDPO, as defined under the Federal Identity, Credentialing, and Access Management (FICAM) program.

Service Provider Organization (SPO): An organization that operates one or more SAML Service Provider (SP), Web Service Provider (WSP), OpenID Connect (OIDC) Relying Party (RP), REST Service Provider (RSP), Authorization Service (AS), REST AS, and/or Attribute Consumer (AC) endpoints in a federated identity trust framework.

Relying Party (RP): An equivalent term for an SPO, as defined under the Federal Identity, Credentialing, and Access Management (FICAM) program. Note that the term "OIDC RP" refers to a service endpoint is not related to the unqualified "RP" term.

Service Consumer Organization (SCO): An organization that operates one or more Web Service Consumer (WSC) and/or REST Service Consumer (RSC) endpoints in a federated identity trust framework.

Attribute Provider Organization (APO): An organization that vets and collects specific attributes about individuals, maintains those attributes in an accurate manner, and provides those attributes to other organizations in a federated identity trust framework as needed, subject to applicable attribute release and privacy policies, for access control and auditing purposes. An APO operates one or more Attribute Provider (AP) endpoints in a federated identity trust framework.

Identity Provider (IDP): A software entity that performs user authentication each time an individual presents themselves to a federated identity trust framework or issues user assertions about the individual for a given information technology session. These user assertions are presented to endpoints deployed by Service Provider Organizations (SPOs) in a federated identity trust framework for the purposes of access control and audit.

SAML Identity Provider (IDP): An IDP that issues SAML assertions to SAML Service Providers in accordance with the NIEF Web Browser User-to-System Profile [NIEF U2S], which conforms to and further constrains the SAML Single Sign-On Profile.

OpenID Connect (OIDC) Identity Provider (IDP): An IDP that issues OpenID Connect ID tokens to OpenID Connect Relying Parties in accordance with the NIEF OpenID Connect Single Sign-On Service Interaction Profile, which is normatively specified in the NIEF REST Services Profile [NIEF REST] and which conforms to and further constrains the OpenID Connect Single Sign-On specification [OIDC Core].

SAML Service Provider (SP): A software entity that provides one or more electronic information services to users within a federated identity trust framework via the NIEF Web Browser User-to-System Profile [NIEF U2S], which conforms to and further constrains the SAML Single Sign-On Profile. A SAML Service Provider makes access control decisions about users based on attributes about those users that are asserted by Identity Providers and Attribute Providers, as well as entity attributes asserted about the user's home organization and its systems by the Identity Federation Management Organization or other trusted 3rd parties. Asserted attributes may conform to [NIEF Attr] or other attribute dictionaries.

OpenID Connect (OIDC) Relying Party (RP): A software entity that provides one or more electronic information services to users within a federated identity trust framework via the NIEF OpenID Connect Single Sign-On Service Interaction Profile, which is normatively specified in the NIEF REST Services Profile [NIEF REST]. An OIDC RP makes access control decisions about users based on attributes about those users that are asserted by Identity Providers and Attribute Providers, as well as entity attributes asserted about the user's home organization and its systems that are asserted by the Identity Federation Management Organization or other trusted 3rd parties. Asserted attributes may conform to [NIEF Attr] or other attribute dictionaries.

Web Service Provider (WSP): A software entity that provides one or more electronic information services to a federated identity trust framework via the NIEF Web Services System-to-System Profile [NIEF S2S], which conforms to and further constrains the Global Reference Architecture Reliable Secure Web Services Service Interaction profile [GRA RS WS-SIP]. A Web Service Provider may make access control decisions about users based on attributes about those users that are asserted by Identity Providers and Attribute Providers, as well as entity attributes asserted about the user's home organization and its systems, and about the applicable Web Service Consumer Organization and its systems, by the Identity Federation Management Organization or other trust 3rd parties. Asserted attributes may conform to [NIEF Attr] or other attribute dictionaries.

REST Service Provider (RSP): A software entity that provides one or more electronic information services to a federated identity trust framework via the NIEF REST Services Profile [NIEF REST]. [NIEF REST] contains several service interaction profiles that specify requirements for RSPs that conform to and further constrain HTTP, OAuth [OAuth Core], and OpenID Connect [OIDC Core]. An RSP may make access control decisions about users based on attributes about those users that are asserted by Identity Providers and Attribute Providers, as well as entity attributes asserted about the user's home organization and its systems, and about the applicable REST Service Consumer Organization and its systems, by the Identity Federation Management Organization or other trusted 3rd parties. Asserted attributes may conform to [NIEF Attr] or other attribute dictionaries.

Web Service Consumer (WSC): A software entity that connects to and consumes data from one or more Web Service Providers (WSPs) operated by Service Provider Organizations. A WSC can act either on behalf of a specific user, or on behalf of the Service Consumer Organization (SCO) that manages it. WSCs connect to WSPs using the NIEF Web Services System-to-System Profile [NIEF S2S].

REST Service Consumer (RSC): A software entity that connects to and consumes data from one or more REST Service Providers (RSPs) operated by Service Provider Organizations. An RSC can act either on behalf of a specific user, or on behalf of the Service Consumer Organization (SCO) that manages it. RSCs connect to RSPs using the NIEF REST Services Profile [NIEF REST].

Authorization Service (AS): A software entity that makes authorization decisions on behalf of NIEF Web Service Providers (WSPs) and issues authorization tokens that can be used at those WSPs. An AS must conform to the NIEF Web Services Authorization Service Service Interaction Profile, which is normatively specified in [NIEF S2S].

REST Authorization Service (AS): A software entity that makes authorization decisions on behalf of NIEF REST Service Providers (RSPs) and issues authorization tokens that can be used at those RSPs. A REST AS must conform to the NIEF REST Consumer-Authorizer Service Interaction Profile, the NIEF REST Single Sign-On Consumer-Authorizer Service Interaction Profile, or the NIEF REST Delegated-

Consumer-Authorizer Service Interaction Profile, which are normatively specified in [NIEF REST].

Assertion Delegate Service (ADS): A software entity that issues delegated user assertions, to allow for the proper implementation of assertion delegation chains within service interactions in a federated identity trust framework.

SAML Assertion Delegate Service (ADS): An Assertion Delegate Service that reissues SAML assertions to requestors as needed, to allow for the proper implementation of SAML assertion delegation chains within Web Services interactions between WSCs and WSPs in a federated identity trust framework. A SAML ADS must conform to the NIEF Web Services SAML Assertion Delegate Service Service Interation Profile, which is normatively specified in [NIEF S2S].

REST Assertion Delegate Service (ADS): An Assertion Delegate Service that issues SAML assertions or OpenID Connect (OIDC) ID tokens to requestors as needed, to allow for the proper implementation of delegation chains within Web or REST services interactions between WSCs and WSPs, or between RSCs and RSPs, in a federated identity trust framework. A REST ADS must conform to the NIEF REST Assertion Delegate Service Service Interaction Profile, which is normatively specified in [NIEF REST].

Attribute Provider (AP): A software entity that provides secure, programmatic access to attributes about users in a federated identity trust framework.

SAML Attribute Provider (AP): An Attribute Provider that conforms to the NIEF Web Services Attribute Provider Service Interaction Profile, which is normatively specified in [NIEF S2S].

REST Attribute Provider (AP): An Attribute Provider that conforms to the NIEF REST Attribute Provider Service Interaction Profile, which is normatively specified in [NIEF REST].

Attribute Consumer (AC): A software entity that submits requests to retrieve attributes about users from an AP in a federated identity trust framework.

SAML Attribute Consumer (AC): An Attribute Provider that conforms to the NIEF Web Services Attribute Provider Service Interaction Profile, which is normatively specified in [NIEF S2S].

REST Attribute Consumer (AC): An Attribute Provider that conforms to the NIEF REST Attribute Provider Service Interaction Profile, which is normatively specified in [NIEF REST].

User Assertion: A digital artifact about a user that expresses metadata about the user's identity, the user's attributes, and/or an authentication event. Assertions used within NIEF may be SAML assertions or OpenID Connect ID tokens.

Transaction: An event between two software entities in a federated identity trust framework in which an attempt is made to exchange sensitive information, subject to applicable access controls.

Session: An arrangement between two software entities in a federated identity trust framework, and also possibly including a user, for the purpose of establishing and maintaining a security context in which multiple transactions can be performed over a period of time.

Cryptographic Trust Fabric: A digital artifact or set of digital artifacts containing entity descriptors of trusted system endpoints. An Identity Federation may maintain a cryptographic trust fabric that contains entity descriptors for endpoints that are trusted within the federation.

Entity Descriptor: A digital artifact that contains endpoint configuration data, cryptographic key data, and various informational attributes about a system endpoint.

NIEF Cryptographic Trust Fabric: A cryptographic trust fabric that is signed by the NIEF Identity Federation Manager Organization and serves as a run-time trust anchor for all transactions in NIEF.

5. NIEF Roles and Responsibilities

This section contains a series of three tables that provide descriptions of the basic roles and responsibilities that exist within NIEF. Table 1 addresses roles and responsibilities from an organizational standpoint, and Table 2 approaches them from a technical standpoint. Table 3 illustrates how the set of NIEF organizational roles maps onto the set of NIEF technical roles.

NIEF Organizational Roles and Responsibilities	
Role	***Responsibilities***
Identity Federation Management Organization (IFMO)	1. Vet prospective federation member organizations for membership. 2. Provide authentication credentials to member organizations. 3. Provide mechanism for authenticating member organizations.
Identity Provider Organization (IDPO)	1. Vet end users for access to the federation. 2. Provide authentication credentials to end users. 3. Authenticate end users. 4. Generate user assertions containing attributes from [NIEF Attr] or other attribute dictionaries.
Attribute Provider Organization (APO)	1. Vet and maintain end-user attributes from [NIEF Attr] or other attribute dictionaries. 2. Provide these attributes to authorized federation member organizations.
Service Provider Organization (SPO)	1. Provide application-level services to federation end users. 2. Perform access control based on attributes from [NIEF Attr] or other attribute dictionaries.
Service Consumer Organization (SCO)	1. Consume application-level data on behalf of users, or on behalf of a federation member organization.

Table 1: NIEF Organizational Roles and Responsibilities

NIEF Technical Roles and Responsibilities	
Role	***Responsibilities***
Certificate Authority (CA)	1. Sign cryptographic certificates for member systems. 2. Sign the NIEF Cryptographic Trust Fabric document. 3. Distribute the NIEF Cryptographic Trust Fabric document to all NIEF participant organizations.
Identity Provider (IDP)	1. Perform authentication for end users. 2. Generate user assertions containing user attributes from [NIEF Attr] or other attribute dictionaries. 3. Conform to the NIEF Web Browser User-to-System Profile or the NIEF OpenID Connect Single Sign-On Service Interaction Profile.
SAML Identity Provider (IDP)	1. Perform authentication for end users. 2. Generate SAML assertions containing user attributes from [NIEF Attr] or other attribute dictionaries. 3. Conform to the NIEF Web Browswer user-to-System Profile
OpenID Connect Identity Provider (IDP)	1. Perform authentication for end users. 2. Generate OpenID Connect ID tokens containing user attributes from [NIEF Attr], [OIDC Core], or other attribute dictionaries. 3. Conform to the NIEF OpenID Connect Single Sign-On Service Interaction Profile.
SAML Service Provider (SP)[1]	1. Provide Web-based access to application-level services for end users. 2. Enforce resource access control policies based on user attributes from [NIEF Attr] or other attribute dictionaries. 3. Conform to the NIEF Web Browser User-to-System Profile.
OpenID Connect Relying Party (RP)	1. Provide Web-based access to application-level services for end users. 2. Enforce resource access control policies based on user attributes from [NIEF Attr] or other attribute dictionaries. 3. Conform to the NIEF OpenID Connect Single Sign-On Service Interaction Profile.

[1] In some NIEF documents, a SAML Service Provider is also called a Service Provider.

Web Service Consumer (WSC)	1. Provide a connecting point through which a NIEF participant organization can connect to NIEF Web Service Providers (WSPs).[2] 2. Conform to the NIEF Web Services System-to-System Profile.
REST Service Consumer (RSC)	1. Provide a connecting point through which a NIEF participant organization can connect to NIEF REST Service Providers (RSPs).[3] 2. Conform to the NIEF REST Services Profile.
Web Service Provider (WSP)	1. Provide Web Services-based access to application-level services for NIEF participant organizations and their end users. 2. Conform to the NIEF Web Services System-to-System Profile.
REST Service Provider (RSP)	1. Provide REST Services-based access to application-level services for NIEF participant organizations and their end users. 2. Conform to the NIEF REST Services Profile.
Authorization Service (AS)	1. Make authorization decisions on behalf of other NIEF Web Service Providers (WSPs) and issue authorization tokens that can be used at those WSPs. 2. Conform to the NIEF Web Services System-to-System Profile.
REST Authorization Service (AS)	1. Make authorization decisions on behalf of other NIEF REST Service Providers (RSPs) and issue authorization tokens that can be used at those RSPs. 2. Conform to the NIEF REST Services Profile.
SAML Assertion Delegate Service (ADS)	1. Translate SAML assertions into delegated SAML assertions that can be used by NIEF Web Service Consumers (WSCs) when communicating with NIEF Web Service Providers (WSPs) on behalf of users. 2. Conform to the NIEF Web Services SAML Assertion Delegate Service Service Interation Profile.

[2] It is possible to configure a Web Service Consumer (WSC) such that it acts as a proxy into various Web Service Providers (WSPs) in the federation on behalf of entities on the WSC's local network that are not in a NIEF Cryptographic Trust Fabric. There is a potential security risk associated with this configuration, particularly in the case where a Web Services request is not associated with a user. It may be necessary for [NIEF OPP] to be modified in the future to prohibit this type of "open proxy" configuration for a WSC.

REST Assertion Delegate Service (ADS)	1. Translate SAML assertions or OpenID Connect ID tokens into delegated SAML assertions or delegated OpenID Connect ID tokens that can be used by NIEF Web Service Consumers (WSCs) or REST Service Consumers (RSCs) when communicating with those service providers on behalf of users. 2. Conform to the NIEF REST Assertion Delegate Service Service Interaction Profile.
SAML Attribute Provider (AP)	1. Provide authorized access to user attributes for federation member organizations. 2. Conform to the NIEF Web Services Attribute Provider Service Interaction Profile.
SAML Attribute Consumer (AC)	1. Request and obtain user attributes from APs on behalf of federation member organizations. 2. Conform to the NIEF Web Services Attribute Provider Service Interaction Profile.
REST Attribute Provider (AP)	1. Provide authorized access to user attributes for federation member organizations. 2. Conform to the NIEF REST Attribute Provider Service Interaction Profile.
REST Attribute Consumer (AC)	1. Request and obtain user attributes from APs on behalf of federation member organizations. 2. Conform to the NIEF REST Attribute Provider Service Interaction Profile.

Table 2: NIEF Technical Roles and Responsibilities[4]

[3] It is possible to configure a REST Service Consumer (RSC) such that it acts as a proxy into various REST Service Providers (RSPs) in the federation on behalf of entities on the RSC's local network that are not in a NIEF Cryptographic Trust Fabric. There is a potential security risk associated with this configuration, particularly in the case where a REST Services request is not associated with a user.

[4] Entities that act in these technical roles are required to appear in NIEF Cryptographic Trust Fabric.

NIEF Organizational Role Mapping to NIEF Technical Roles	
Organizational Role	***Technical Roles***
Identity Federation Management Organization (IFMO)	• Certificate Authority (CA)
Identity Provider Organization (IDPO)	• SAML Identity Provider (IDP) • OpenID Connect Identity Provider (IDP) • SAML Assertion Delegate Service (ADS) • REST Assertion Delegate Service (ADS) • SAML Attribute Provider (AP) • SAML Attribute Consumer (AC) • REST Attribute Provider (AP) • REST Attribute Consumer (AC)
Attribute Provider Organization (APO)	• SAML Attribute Provider (AP) • REST Attribute Provider (AP)
Service Provider Organization (SPO)	• SAML Service Provider (SP) • OpenID Connect (OIDC) Relying Party (RP) • Web Service Provider (WSP) • REST Service Provider (RSP) • Authorization Service (AS) • REST Authorization Service (AS) • SAML Attribute Consumer (AC) • REST Attribute Consumer (AC)
Service Consumer Organization (SCO)	• Web Service Consumer (WSC) • REST Service Consumer (RSC)

Table 3: NIEF Organizational Role Mapping to NIEF Technical Roles

6. NIEF Service-Oriented Architecture Terminology Map

Table 4 below contains a "Terminology Map" that provides a concise comparison between NIEF and several other prominent identity management paradigms in terms of what terminology is used to express various aspects of each paradigm.

NIEF Service-Oriented Architecture Terminology Map					
	NIEF	*SAML*	*WS-*/WS-I*	*GRA[5]*	*OIDC / OAuth[6]*
Organizational Roles					
	Identity Federation Management Organization (IFMO)	N/A	N/A	N/A	N/A
	IDP Organization (IDPO)	N/A	N/A	N/A	N/A
	AP Organization (APO)	N/A	N/A	N/A	N/A
	SP Organization (SPO)	N/A	N/A	N/A	N/A
	SC Organization (SCO)	N/A	N/A	N/A	N/A
Technical Roles					
	Certificate Authority (CA)	N/A	N/A	N/A	N/A
	Identity Provider (IDP)	Same as NIEF	WS-Federation: Identity Provider, or Security Token Service in the role of Identity Provider, or Security Token Service in the role of Attribute Service[7], Abbreviated as IP/STS	N/A	OpenID Connect: OpenID Provider.
	SAML Service Provider (SP)	Service Provider	WS-Federation: Resource or Relying Party	Service Provider	N/A
	OpenID Connect (OIDC) Relying Party (RP)	N/A	N/A	N/A	OpenID Connect: Relying Party

[5] The Global Reference Architecture (GRA) is based on principles of Service-Oriented Architecture (SOA), in which many types of entities can play the role of a Service Provider. The SOA concept of a Service Provider is more general than the NIEF concept of a Service Provider, which is a service that provides an interface to application data for the benefit of end users.

[6] OpenID Connect 1.0 is an extension of OAuth 2.0.

[7] WS-Federation defines an attribute service to enable privacy protection for certain attributes.

					OAuth: Client
	Web Service Consumer (WSC)	N/A	WS-Federation: Requestor	Service Consumer	N/A
	REST Service Consumer (RSC)	N/A	N/A	N/A	OpenID Connect: Relying Party OAuth: Client
	Web Service Provider (WSP)	N/A	WS-Federation: Resource or Relying Party	Service Provider	N/A
	REST Service Provider (RSP)	N/A	N/A	N/A	OAuth: Resource Server
	Authorization Service (AS)	N/A	WS-Federation: Security Token Service in the role of Authorization Service[8]	Service Provider	N/A
	REST Authorization Service (AS)	N/A	N/A	N/A	OAuth: Authorization Server
	SAML Assertion Delegate Service (ADS)	N/A	N/A	N/A	N/A
	REST Assertion Delegate Service (ADS)	N/A	N/A	N/A	N/A
	SAML Attribute Provider (AP)	SAML Core: SAML Authority[9], SAML Metadata: Attribute Authority[10]	WS-Federation: Security Token Service in the role of Attribute Service, Abbreviated as IP/STS	N/A	N/A
	SAML Attribute Consumer (AC)	SAML Metadata: Attribute Requester[11]	WS-Federation: Requestor	N/A	N/A

[8] WS-Federation supports the concept of authorization via an STS but does not specifically define an Authorization Service.

[9] See Section 3.3.4 of [SAML2], "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0", available at http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.

[10] See Section 2.4.7 of [SAML2], "Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0", available at http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf.

[11] See [SAML2], "SAML Metadata Extension for a Standalone Attribute Requester, Committee Draft 01, 11 April 2005", available at the following URL.

https://www.oasis-open.org/committees/download.php/13845/sstc-saml-metadata-ext-cd-01.pdf.

	REST Attribute Provider (AP)	N/A	N/A	N/A	OpenID Connect: OpenID Provider
	REST Attribute Consumer (AC)	N/A	N/A	N/A	OpenID Connect: Relying Party
Other					
	Assertion	Assertion	Security Token	N/A	OpenID Connect: ID Token
	Assertion Attribute	Assertion Attribute	Claim	N/A	OpenID Connect: Claim

Table 4: NIEF Terminology Mapping to Service-Oriented Architecture Paradigms