Glossary

Assertion: A SAML message from an IdP to an SP, issued upon successful authentication of a user, which conveys information about the authentication event and any attribute information released to the SP.

Attribute: A piece of information, typically a name-value pair or a name-multiple values set, typically containing information about a federated user. Typical items include name, email address and user identifier.

Authentication: The act of using a set of credentials (a username plus something you know, typically a password. See Multi-Factor Authentication for more info on other types.) To prove who you are to an electronic system you are trying to access.

Authorization: The use of information about you, your roles in business processes, your status as an employee or student, etc. to allow you a certain level of access and privilege within a system.

Delegated Administrator: A person who has been authorized by a Site Administrator to maintain one or more SAML entity descriptors in the Federation Manager.

Duo Security: A cloud-based multi-factor authentication service used by the Federation Manager via the MFA IdP Proxy to add an additional layer of authentication security for certain access to the Federation Manager (specifically, Registration Authority Administrator access)

Duo Verify API: A Duo Security API similar to Twilio, which can be used to place automated phone calls to people. In the Federation Manager, it is used for password reset phone verification of Site Administrators.

Encryption Key/Certificate: A SAML encryption key contained inside an X.509 certificate wrapper, published in federation metadata, used by an IdP to encrypt assertions to an SP (the SP's public key and IdP's private key are used for this purpose). Also used by an SP to encrypt authentication requests and Single Logout (SLO) user identifiers in messages to IdPs (the SP's private key and the IdP's public key are used for this purpose).

Endpoint: A web service URL used by a SAML deployment to communicate with other SAML deployments.

Entity: A SAML deployment.

Entity Descriptor: A SAML XML metadata construct which describes a SAML deployment (unique identifier, endpoints, key material, user interface material, in the case of IdPs, scope).

entityID: The globally unique identifier for a SAML entity descriptor in metadata. Always a URI in Research and Education Federation metadata - usually a URL, sometimes a URN. This is just a unique identifier, it does not have to be resolvable via HTTP/etc.

Identity Federation (aka Trust Federation): A security and trust infrastructure for the exchange of user identity information, authentication, and related event-driven information via a secure system of signed SAML metadata. Other technologies such as RADIUS (eduroam), ABFAB Kitten, "Moonshot" /federated GSSAPI, or OpenID Connect may be used, but SAML is the pervasive technology in use in Research and Education today.

Federation Operator: The organization which operates an identity federation securely, including participant organizational and administrator onboarding practices and metadata registration, signing and publication processes.

FM: Federation Manager application, InCommon's customer relationship management and SAML metadata management user interface.

FMDB: Federation Manager Database.

IdP: (SAML) Identity Provider. A SAML deployment, typically at a user's university, company, or research project/agency, which provides for secure authentication using the user's home organization credentials. Identity information (attributes) may be encoded in an assertion by an Identity Provider to a Service Provider once a user has authenticated.

iMIS: A legacy/deprecated business system that Internet2 used for contact management before switching to SalesForce.

InCommon: A legal entity of Internet2 which operates Internet2's trust and identity service offerings, including the InCommon Federation, Certificate Service, eduroam and Duo Security offerings.

Metadata: In this context, one or more SAML XML documents which contain SAML EntityDescriptor(s) - if more than one, the EntityDescriptors are wrapped in a root EntitiesDescriptor.

Metadata Aggregate: A SAML metadata document containing more than one EntityDescriptor elements wrapped in a root EntitiesDescriptor.

Metdata Aggregation: A process of building a SAML metadata aggregate from source information, normally stored in a database such as the FMDB.

Metadata Signing: The process of using a secure private key to apply an XML Digital Signature to a SAML XML metadata document.

Metadata Signing Key: The private key used to sign SAML metadata, kept offline and highly secured. The corresponding public key is what federation members use/trust, in order to verify the XML Digital signature on InCommon SAML XML metadata aggregates and/or per-entity metadata documents.

MFA IdP Proxy: A modified SimpleSAMLphp gateway operated by Cirrus Identity on behalf of InCommon Operations. This gateway adds a call to Duo Security's multi-factor authentication service into each federated SSO session with certain (elevated security) parts of the Federation Manager.

Multi-Factor Authentication (MFA): The use of two or more of the following factors to authenticate a person to a service: 1) something you know (password); 2) something you have (one-time password, mobile device 'push', etc.); 3) something you are (fingerprint, etc.). The use of more than one authentication factor adds assurance that the person is who they claim to be.

Ops (aka InCommon Operations): Internet2 staff responsible for operating InCommon services.

Organization: A legal entity which is eligible to become an InCommon Participant.

Organizational Onboarding: The process of contracting with, verifying various identities and domains associated with an organization which is in the process of becoming an InCommon participant.

Participant: An organization which has completed Organizational Onboarding - has signed an InCommon Participation Agreement, paid the necessary fee, and successfully verified an Executive Contact.

Participation Agreement (PA): The legal document which is the basis for Organizations to become InCommon Participants.

Per-Entity Metadata: The delivery of SAML entity descriptors via a mechanism which allows metadata clients to request individual entity descriptors, normally signed with an XML Digital Signature, one at a time rather than through the use of an aggregate of multiple entity descriptors wrapped in a root EntitiesDescriptor. For more information, see: https://tools.ietf.org/html/draft-young-md-query-saml-06

PKI: Public Key Infrastructure - a type of X.509 certificate-based trust infrastructure rooted in public key certificate authorities. The web browser TLS certificate authority ecosystem is one example of a PKI. InCommon's SAML metadata is a nontraditional PKI in that trust is manually configured based on a trusted XML signing key used to sign federation SAML metadata. The public keys of all entities in the trust are published in this signed metadata, and are thus trusted due to the signature on the metadata.

Private Key: A cryptographic key used to perform encryption/decryption operations which must be kept secret. One half of a cryptographic keypair, the other half is the public key, which is shared.

Public Key: A cryptographic key used to perform encryption/decryption operations which is publicly shared. One half of a cryptographic keypair, the other half is the private key, which must never be shared.

RA: Registration Authority - an organizational role responsible for the trustworthy onboarding of Organizations and their named roles/staff, as well as registration of their metadata according to written RA procedures.

RA Administrator: An RA administrator vets and approves submitted metadata. They are members of the Internet2 staff. See also the public wiki page on various FM users.

SalesForce: A cloud-based customer relationship management system used as the primary CRM for Internet2.

Scope: A SAML metadata extension and attribute governance/security mechanism used by SPs to enforce realm name uniqueness on 'scoped' values asserted by IdPs, for example: the user identifier (eduPersonPrincipalName) nroy@internet2.edu, where the half of the identifier to the right of the '@' sign (internet2.edu) is a Scope which may only be used by an IdP (or Attribute Authority) entity in metadata so decorated with an appropriate shibmd:Scope value by the Federation Operator.

Security Assertion Markup Language (SAML): A set of standards for the trustworthy exchange of authentication, authorization, entity and other relevant identity/security information, implemented in XML, governed by the OASIS Security Services Technical Committee (SSTC).

Single Sign On (SSO): A technology used to securely authenticate users and then provide relevant user information to applications which need it throughout the lifetime of the user's single sign on session. Examples of web-based SSO include SAML, CAS, PubCookie, OpenID Connect and CoSign. Examples of non-web SSO include Kerberos (which may be used in web contexts using mechanisms such as SPNEGO/GSSAPI), RADIUS as implemented in eduroam, SAML ECP, IETF AbFab "Kitten" (aka SASL+SAML, as implemented in services such as FeduShare), and "Moonshot".

Site Administrator: A site administrator may create, update, or delete any type of metadata, either IdP or SP metadata. Provisioned by RA Administrators. See also the public wiki page on various FM users.

SP: Service Provider - a piece of SAML "middleware" and its associated SAML role, which acts as the recipient of SAML assertions from an IdP.

Steward Metadata Submitter: Steward Organization staff authorized to act as a metadata submitter, aka "Site Administrator" on behalf of other non-InCommon-Participant organizations as part of the InCommon Steward Program. Metadata submitted by Steward Metadata Submitters enters a metadata approval queue for their Organization's Steward Registration Authority Administrator. Once approved by the Steward RAA, the metadata is published in the InCommon federation, bypassing the InCommon RAA staff metadata approval queue. The Steward Metadata Submitter is implemented in the Federation Manager as a Site Administrator (inc_admin) role in a Sub-Organization marked as a "Steward" organization by the InCommon RA Administrator staff.

Steward Program: A program of the InCommon Federation designed to allow staff at partner Organizations to take on some of the responsibility of the InCommon Registration Authority Administrator (RAA) staff. This program allows a set of people from a Steward Organization to submit metadata on behalf of their Represented Constituents (RCs), and then for a distinct set of people to approve this submitted metadata, bypassing InCommon RAA staff approval. Steward staff are required to have their own set of organizational registration and management practices which meet InCommon requirements for organizational onboarding and metadata registration.

Steward Registration Authority Administrator: Steward Organization staff trained and authorized to act as a Registration Authority Administrator (RAA) for the purposes of approving metadata submitted by their Steward Metadata Submitters. Once approved by the Steward RAA, the metadata is published in the InCommon federation, bypassing the InCommon RAA staff metadata approval queue. The Steward RAA is implemented in the Federation Manager as a Site Administrator (inc_admin) role in a parent Organization which contains at least one sub-Organization marked as a "Steward" by the InCommon RA Administrator staff.

TLS: Transport Layer Security.

eXtensible Markup Language (XML): A specific type of markup language which defines a document format that is both human-readable and machine-readable, for the purposes of structured information representation.