OIDC to SAML terminology translation

Keystone connects OpenID Connect to SAML federations. The terms used by one may be strange to those used to the other. For those new to either of them it can be an unexpected learning curve. This table should help.

OpedID Connect	SAML	English
Authentication	Authentication	Checking user credentials. Done by the identity provider / IdP / OP - e.g. library.
Authorisation	Authorisation	Checking user permissions. Done by the service provider / relying party - e.g. Journal.
Authorisation Endpoint	SSO address / endpoint	Where the user should be sent for authentication
Claim	Attribute	A defined bit of data about a user - e.g. a persistent ID
Endpoint	Endpoint	A URI where authentication or authorisation happens
Issuer	EntityID	An identifier for the Identity Provider. In OIDC it is the root URI for the provider and has a practical use in the software. In SAML it is a unique identifier that enables one entity to find another in aggregated metadata. It is usually in the form of a secure URI which may or may not have a real target.
Provider / OP	Identity Provider (IdP)	The party that does the authentication - e.g. the library, university, hospital, legislative assembly
Redirect URI/URL	Association Consumer Service (ACS)	Where at the relying party / service provider the user should be returned after they are authenticated
Relying Party	Service Provider (SP)	The party that does the authorisation and provides the service being accessed
Scope	The closest to this would be the attribute statement in the SAML response.	In OIDC, a scope is a collection of related claims. SAML uses the same term for something else
Signed request / response	Signed request / response	In both OIDC and SAML, requests and responses are signed or not based on whether the parties advertise that signing is supported and required. Keystone supports this in both systems.
UserInfo Endpoint	No current equivalent in SAML. The closest would be the Attribute Authority that was used by older versions of SAML that were superseded in 2005.	Where the relying party can obtain the user's attributes. In SAML2 the attributes are encrypted and sent via the browser.
Well known OpenID configuration	A bit like IdP metadata	A defined path to a JSON document where an OIDC relying party can discover information about the Provider
	Metadata	An XML document that describes an entity (IdP or SP) in a SAML federation. Contains information such as endpoints, signing and encryption certificates. A federation will publish an aggregated set of all IdP and SP metadata.
	SAML	Security Assertion Markup Language. You do not need to worry about the technical parts of this if you are using OpenAthens Keystone, but your customers will be used to the way it works and the terms it uses.
	Scope	In SAML federations, a scope is an organisation identifier, most often in the form of an internet domain owned by the Identity Provider. OIDC uses the same term for something else
Token	Token	In SAML, a token is the encrypted XML that is passed as a parameter in the user's browser. This could be the request or response depending on who is sending it. In OIDC, a token is a time limited key issued by an identity provider to a relying party (content provider) which is then used to authorise the call the relying party makes to the identity provider to read any claims.
	Entity Category	A metadata extension that implies a defined set of conditions such as a code of conduct or set of attributes.