Appendix 2: Attribute Profile

1. Definitions and Terminology

Section 1 - 'Definitions and Terminology' of the latest CARSI Identity Federation Policy published on the CARSI Identity Federation website at https://www.carsi.edu.cn/docs/identity_federation_policy_en.pdf applies to this document.
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119, see http://tools.ietf.org/html/rfc2119.

2. Introduction

This Attribute Profile is the required profile for End Users' attributes exchanged throughout the CARSI Identity Federation service. It covers the scenario under the SAML WebSSO Technology Profile. The profile may be amended later by adding scenarios with different requirements.
This profile summarizes the details about the attributes of End Users, their handling and exchange in the Federation.

3. Attribute Standard

CARSI Identity Federation supports attributes defined in various sources. These include:
a. [eduPerson]
- eduPerson object class specification (202001)
- https://wiki.refeds.org/display/STAN/eduPerson+2020-01

b. [SAML Core]
- Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, 15 March 2005
- https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

The syntax for expressing all CARSI Identity Federation attributes SHALL follow the MACE-Dir SAML Attribute Profiles [MACEDir] (http://macedir.org/docs/internet2-mace-dir-saml-attributes-200804a.pdf).

c. [SAML-SubjectID-v1.0]
- OASIS SAML V2.0 Subject Identifier Attributes Profile Version 1.0
- https://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/cs01/saml-subject-id-attr-v1.0-cs01.pdf.

4. Attributes for SAML Web Single Sign-On

The CARSI Identity Federation Policy requires that, when acting as a Service Provider Organization, Federation Member MUST ensure that the deployment of each of its Service Providers follows all the attribute processing principles defined in the Appendix 3: CARSI Identity Federation Data Protection Profile for providing access to the protected resources or services.
The technical representation of an attribute during the transfer in the Federation is presented in the CARSI Identity Federation SAML WebSSO Technology Profile.

4.1. Core Attributes

A Core Attribute means that it is available, in general, for most End Users. However, it can be left empty for those End Users who do not qualify for any of the values in the vocabulary.
The CARSI Identity Federation Policy requires that Federation Member MUST collect or generate the Core Attributes regarding their qualified End Users for their Identity Providers.

The set of Core Attributes supported in the Federation are summarized in the table below:

Attribute	Defining Schema	Meaning	Example Value
eduPersonScopedAffiliation	[eduPerson]	Specifies the person's affiliation within a particular security domain in broad categories such as student, faculty, staff, alum, etc.	staff@pku.edu.cn

Table 1: CARSI Identity Federation Core Attributes

The set of Core Attributes may evolve over time in response to the needs of the Federation Members.

4.2. Recommended Attributes

It is RECOMMENDED that Federation Identity Providers support the Recommended Attributes in the following table. They can assist in interacting with some federation services.

Attribute name	Defining Schema	Meaning	Example
Pairwise Subject Identifier (pairwise-id)	[SAML-SubjectID-v1.0]	A substitute to eduPersonTargetedID. This is a long-lived, non-reassignable, uni-directional identifier suitable for use as a unique external key specific to a particular relying party. Its value for a given subject depends upon the relying party to whom it is given, thus preventing unrelated systems from using it as a basis for correlation.	HA2TKNZZGE2TOZDCGMZWKOLDHBQWIMBSGM4TGZBYGUYGINRQHAYTINBZGYZDOZBZMZRGKNZTME3TMNBXGYYTIOBYGMYWKNLFMYYDAYY=@osu.edu
SAML2 Persistent NameID (eduPersonTargetedID)	[SAMLCore, eduPerson]	Deprecated. A persistent, non-reassigned, privacy-preserving identifier for a principal shared between a pair of coordinating entities.	7eak0QQIEhygtPXtpgmu5l5hRnY
eduPersonEntitlement	[eduPerson]	A simple example would be a URL for a contract between an idp and a licensed resource provider. The trust between the two parties must be established out of band.	urn:mace:dir:entitlement:common-lib-terms

Table 2: CARSI Identity Federation Recommended Attributes

The list of Recommended Attributes may evolve over time in response to the needs of the Federation Members.

4.3. Controlled Vocabularies

4.3.1. eduPersonScopedAffiliation

eduPersonScopedAffiliation is defined in [eduPerson]. CARSI Identity Federation Members SHOULD limit their Identity Providers to use the following attribute values:

- faculty
- student
- staff
- alum
- member
- affiliate
- employee
- other

4.3.2. eduPersonEntitlement

eduPersonEntitlement is defined in [eduPerson]. CARSI Identity Federation Members SHOULD limit their Identity Providers to use the following attribute values:

- urn:mace:dir:entitlement:common-lib-terms

4.4. Scoped Attributes

If a Federation Member makes use of a scoped attribute (such as eduPersonScopedAffiliation) in its Service Provider, it is encouraged to use available mechanisms to ensure the “scope” value of the attribute asserted by an Identity Provider matches one permitted to the associated Home Organization.

5. Amendment

The Federation Operator Team has the right to amend this document from time to time. Any such amendments need to be approved by the CARSI Identity Federation Steering Committee. The amended Attribute Profile will become binding upon the Federation members. All Federation Members MUST support the latest set of Core Attributes in their Identity Providers. The latest version of the Attribute Profile is made available on the CARSI Identity Federation website at https://www.carsi.edu.cn/docs/attribute_profile_en.pdf. The amended Data Protection Profile will become binding upon the Federation Members. The Federation Members MUST follow the latest version of this document which is made available on the CARSI Identity Federation website at https://www.carsi.edu.cn/docs/data_protection_profile_en.pdf.