Appendix 1: SAML WebSSO Technology Profile

1. Definitions and Terminology

Section 1 - 'Definitions and Terminology' of the latest CARSI Identity Federation Policy [0] 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 document is a CARSI Identity Federation Technology Profile that describes how the CARSI Identity Federation is realized using the SAML V2.0 Web Browser SSO Profile [1].
The SAML V2.0 Web Browser SSO Profile defines a standard that enables Identity Providers and Relying Parties (Service Providers) to create and use Web Single Sign on services using SAML.

3. Requirements

- All SAML metadata MUST fulfill the SAML V2.0 Metadata Interoperability Profile Version 1.0 or any later version [2].
- All Identity Providers MUST fulfill the Interoperable SAML 2.0 Profile (stable version) [3].
- All Service Providers SHOULD fulfill the Interoperable SAML 2.0 Profile [3].
- All SAML attributes SHOULD be represented using the urn:oasis:names:tc:SAML:2.0:attrname-format:uri Name Format.
- All SAML attribute names SHOULD be represented using either the urn:oid or http(s) URI scheme name spaces. Usage of MACE-Dir [4] defined attributes MUST conform to the MACE-Dir SAML Attribute Profiles [5] (or any later version).
- All SAML Identity Providers MUST implement the Shibboleth Scope Metadata extension as defined in the Shibboleth Metadata Schema [6]. The Scope value MUST be a string equal to a DNS domain owned by the organization that is consistent with the user identity.
- All SAML Service Providers SHOULD implement checks against the Shibboleth Scope Metadata extension when processing scoped attributes.

4. References

[0] https://www.carsi.edu.cn/docs/identity_federation_policy_en.pdf
[1] http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf
[2] http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf
[3] http://saml2int.org/
[4] http://middleware.internet2.edu/dir/
[5] http://macedir.org/docs/internet2-mace-dir-saml-attributes-200804a.pdf
[6] https://wiki.shibboleth.net/confluence/display/SC/ShibMetaExt+V1.0

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 SAML WebSSO Technology Profile will become binding upon the Federation members. The latest version of this document is made available on the CARSI Identity Federation website at https://www.carsi.edu.cn/docs/identity_federation_policy_en.pdf.