CARSI:
CERNET (China Education and Research NETwork) Authentication and Resource Sharing Infrastructure

Identity Federation Policy

Version 1.3

Author	PING CHEN, BO WANG
Version	1.3
Status	Draft
Revised Date	Sep. 1, 2021

Table of Contents:

Document Revised History

Version	Revised Date	Summary of Changes	Authored By	Approved By
1.0	May. 6, 2019	First draft	PING CHEN, LI WAN, JIE LV	
1.1	Sep. 12, 2019	To add eduPersonPrincipalName in *4.2 Recommended Attributes* of *Appendix 2: Attribute Profile*. To correct several errors to be more consistent with Chinese expression.	BO WANG	PING CHEN, QINGNAN LAI
1.2	Dec. 12, 2019	To add eduPersonTargetedId and eduPersonEntitlement and to remove eduPersonPrincipalName in *4.2 Recommended Attributes* of *Appendix 2: Attribute Profile*. To modify the "Amendment" of *Identity Federation Policy, Appendix 2: Attribute Profile, Appendix 3: Data Protection Profile, Appendix 4: Service Provider Management Standard.*	PING CHEN	QINGNAN LAI, BO WANG
1.3	Sep. 1st, 2021	To add pairwise-id and modify the comments about eduPersonTargetedId in *4.2 Recommended Attributes* of *Appendix 2: Attribute Profile*. To correct some English expression.	BO WANG	PING CHEN

1 Definitions and Terminology

Attribute	A piece of information describing the End User, his/her properties or roles in an Organization.
Authentication	Process of proving the identity of a previously registered End User.
Authorization	Process of granting or denying access rights to a service for an authenticated End User.
CARSI Identity Federation	CERNET Authentication and Resource Sharing Infrastructure.
CARSI Operator Team	The group consisting of representatives from Peking University and CERNET Corporation, taking up the role of the Federation Operator.
Digital Identity	A set of information that is attributable to an End User. Digital identity consists of Attributes. It is issued and managed by a Home Organization on the basis of the identification of the End User.
End User	Any natural person affiliated to a Home Organization, e.g. an employee, researcher or student making use of the service of a Service Provider.
Federation	Identity federation. An association of organizations that come together to exchange information as appropriate about their users and resources to enable collaborations and transactions.
Federation Operator	Organization providing Infrastructure for Authentication and Authorization to Federation Members.
Federation Member	An organization that has joined the Federation by agreeing to be bound by the Federation Policy in writing. Within the federation framework, a Federation Member can act as a Home Organization and/or a Service Provider.
Home Organization	The organization with which an End User is affiliated. It is responsible for authenticating the End User and managing End Users' digital identity data.
Identity Management	Process of issuing and managing end users' digital identities.
Identity Provider	The system component that issues Attribute assertions on behalf of End Users who use them to access the services of Service Providers.
Interfederation	Voluntary collaboration of two or more Identity Federations to enable End Users in one Identity Federation to access Service Providers in another Identity Federation.
Resource Sharing	A service based on CARSI Identity Federation to share campus-wide user identity resources and application resources.
Service Provider	An organization that is responsible for offering the End User the service he or she desires to use. Service Providers may rely on the authentication outcome and attributes that Home Organizations assert for their End Users.

2 Introduction

An Identity Federation is an association of organizations that come together to exchange information, as appropriate, about their users in order to enable collaborations and transactions.

CERNET Authentication and Resource Sharing Infrastructure (CARSI) is the Identity Federation and resource sharing service of CERNET – China Education and Research Network. CARSI is introduced to facilitate and simplify the process of shared services among the Federation members in CERNET. It is a multi-organization association effected by using Identity Federation Technologies to extend the scope of a digital identity issued by one Federation Member to be valid across the whole Federation to promote the user identity resources and application resources sharing among members. The Federation relies on Home Organizations to correctly and accurately assert information about the identity of End Users to Service Providers, that may use that information to grant (or deny) access to the services and resources they offer to End Users.

The Federation Policy document defines the fundamental regulation, the Federation Members' obligations and rights to be able to use available Federation Technologies for electronic identification and for access to attribute and authorization information about End Users in the Federation.

The Federation Technology Profiles describe concrete realizations in terms of specific technologies (e.g. SAML). By employing specific choices of technologies for identification and authorization this Policy may be used to support federated identity for a wide range of applications. The use of federation technology (e.g. SAML, 802.1x, WS-Federation, OpenID) is governed by a Federation Technology Profile

This document, together with its appendices constitutes the Federation Policy. The current list of all appendices is available on the website of the Federation https://www.carsi.edu.cn/docs/join_en.htm.

Appendix	Document Type	Document	Purpose
1	Federation Technology Profile	SAML WebSSO Technology Profile	Describes concrete realizations of the Policy and Assurance Profiles in terms of a specific technology - SAML
2	Attribute Management	Attribute Profile	Defines the sets of Core and Recommended Attributes with detailed information and guidance on their values and uses that the deployment of Identity Providers and Service Providers MUST follow
3	Service Provider Management	Data Protection Profile	Defines the attribute processing principles that the deployment of Service Provider MUST follow
4		Service Provider Management Standard	Defines the rules that the deployment of Service Provider MUST follow
5	Identity Provider Management	Identity Provider Management Standard	Defines the rules that the deployment of Identity Provider MUST follow

3 Purpose and Scope

Based on the widely deployed campus-wide unified user identity management systems, the purpose of CARSI Identity Federation is to extend the user's digital identity from Chinese higher education, levels of educational institutions and research institutions to CERNET and the global in order to support users to visit more applications and resources about teaching, researching, management and living with his/her unique and authentic campus digital identity. CARSI identity federation supports users to access educational and commercial resources inside and outside China.

The scope of the CARSI Identity Federation Policy is limited to those technologies which are capable of supporting federated secure authentication and authorization of users as described by the Federation Technology Profiles. Compliance with the Federation Policy for a Federation Member also implies its compliance with all the applicable profiles and standards. Based on the principle of hierarchical management, the Federation Members supervise its organizational IdP and/or SPs to execute the Federation Policy.

In order to facilitate collaboration across national and organizational borders CARSI Identity Federation MAY participate in interfederation agreements.

4 Governance and Roles

CERNET Authentication and Resource Sharing Infrastructure (CARSI) Identity Federation is owned by CERNET (China Education and Research NETwork), aiming to promote services of Higher Education, schools, levels of education administrative agencies and research institutions. The governance of the Federation is undertaken by CARSI Identity Federation Steering Committee and CARSI Identity Federation Operator Team jointly. CARSI Identity Federation Steering Committee owns the final decision rights of the Federation affairs. The development, operation and maintenance of the Federation is delegated to the CARSI Operator Team.

4.1 Governance

In addition to what is stated elsewhere, the Steering Committee is responsible for:

- Approve the Federation Constitution, Policies, Documents and their amendments.
- Setting criteria for membership for the Federation, such as, deciding whether a Federation Member is entitled to act as Home Organization, deciding whether to grant or deny an application for membership in the Federation, revoking the membership if a Federation Member is in a breach of the Policy.
- Deciding on future directions and enhancements for the Federation together with the Federation Operator Team who prepares the plans.
- Entering into interfederation agreement.
- Providing financial support to the Federation; approving the yearly budget plan of the Federation Operator Team and auditing the finance report.
- Approving the fees to be paid by the Federation Members to cover the operational costs of the Federation, on the proposal of Federation Operator Team.
- Deciding on Federation Policy modification and any other matter referred to it by the Federation Operator Team.

4.2 Obligations and Rights of Federation Operator Team

CARSI Identity Federation Operator Team, composed of technical persons from Peking University and CERNET Corporation, is responsible for the Federation technical development and the daily operation and maintenance of related systems. In addition to what is stated elsewhere, the Operator Team is responsible for:

- Following the standards and rules ratified by CARSI Identity Federation Steering Committee.
- Secure and trustworthy operational management of the Federation and providing central services following the procedures and technical descriptions specified in this document and its appendices.
- Providing support services for Federation Members' appropriate contact persons to work out operational problems regarding the Federation services.
- Acting as the center of competence for Identity Federation: testing software, recommending and documenting solutions, providing software deployment and configuration guides for selected software and operating systems for use within the Federation.
- Preparing the yearly budget plan and submitting it to the Steering Committee for approval. Submitting a financial report to the Steering Committee for auditing.

- Maintaining relationships with national and international stakeholders in the area of Identity Federations. This especially includes contacting regarding interfederation activities and working with other Identity Federations in the area of harmonization.
- Promoting the idea and concepts implemented in the Federation so prospective Federation Members can learn about the possibilities of the Federation.
- Marketing the service and promoting the federation development.

In addition to what is stated elsewhere in the Federation Policy, the Federation Operator Team reserves the right to:

- Temporarily suspend individual Technology Profiles for a Federation Member that is disrupting the secure and trustworthy operation of the Federation.
- Publish a list of Federation Members along with information about which profiles each Federation Member fulfills or implements, for the purpose of promoting the Federation with no risk of the privacy breach.

4.3 Obligations and Rights of Federation Members

In addition to what is stated elsewhere in the Federation Policy all Federation Members:

- Shall appoint and name a project manager and a technical contact for interactions with the Federation Operator Team.
- Must cooperate with the Federation Operator Team and other Members in resolving incidents and should report incidents to the Federation Operator Team in cases where these incidents could negatively affect the security, trustworthiness or reputation of the Federation or any of its Members.
- Must comply with the obligations of the Technology Profiles which it implements.
- Must ensure its IT systems that are used in implemented Technology Profiles are operated securely.
- Must pay the fees according to the Fees and Payment Terms specified in Section 6 of this Policy document.
- If a Federation Member processes personal data, Federation Member will be subject to applicable data protection laws and must follow the practice presented in Appendix 3: CARSI Data Protection Profile at https://www.carsi.edu.cn/docs/data_protection_profile_en.pdf.

If a Federation Member is acting as a Home Organization, it:

- Is responsible for End Users' credential management, from the digital identities enrollment, to the information maintenance and removal from the identity management system, and to the other parts of identity life-cycle management, to ensure the correctness and accuracy of credential information.
- Authenticates the End Users and provides the authentication result to Service Providers.
- Operates a helpdesk for its End Users regarding Federation services related issues. Home Organizations are encouraged to maintain a helpdesk for user queries at least during normal office-hours in the local time zone.
- Is responsible for assigning Attribute values to the End Users and managing the values in a way that ensures their correctness, up-to-date and reliability.
- Is responsible for releasing the Attributes to Service Providers.
- Cannot provide IdP services to non CARSI Federation members.
- Must follow the practice presented in Appendix 5: CARSI Identity Provider Management Standard at https://www.carsi.edu.cn/docs/idp_management_standard_en.pdf.
- Uses downloaded software and resources reasonably without infringing on the legitimate rights and interests of third parties.

If a Federation Member is acting as a Service Provider, it:

- Is responsible for making decisions on which End Users can access the services they operate and which access rights are granted to an End User. It is Service Providers responsibility to implement those decisions.

- MUST ensure the proper use of the acquired user information and ensure the safety of user information.
- MUST ensure that the deployment of each of its Service Providers complies with all the attribute processing principles defined in Appendix 3: CARSI Data Protection Profile at https://www.carsi.edu.cn/docs/data_protection_profile_en.pdf.
- MUST ensure that the deployment of each of its Service Providers complies with all the rules defined in Appendix 4: CARSI Service Provider Management Standard at https://www.carsi.edu.cn/docs/sp_management_standard_en.pdf.
- Uses downloaded software and resources reasonably without infringing on the legitimate rights and interests of third parties.

5 Procedures

5.1 How to Join

In order to become a Federation Member, an organization applies for membership (Full Member or Service Provider Member) through CARSI Online Registration https://mgmt.carsi.edu.cn/reg and agrees to be bound by the Federation Policy in written form by an official representative of the organization.

Each application for membership is evaluated by the Federation Operator Team who makes the decision on whether to grant or deny the application in 10 working days. If denied, the reason for denying the application should be provided.

5.2 How to Withdraw

A Federation Member may send a written request to the Federation Operator Team at least one month before it cancels its membership in the Federation. Cancellation of membership implies the Federation will not publish its metadata to other federation members after the requested cancellation date and the canceled Federation member cannot communicate with other federation members through the Federation anymore.

5.3 Suspension or Termination of Services

A Federation Member (Full Member or Service Provider Member) should send a written request to the Federation Operator Team at least one month before it asks to suspend or terminate one or multiple Services it provides to the Federation members. If there are separate agreements or contracts signed between other Federation members and the Service Provider, the Service Provider has to negotiate and deal with its counterparts to either suspend or terminate the agreements or contracts. The Federation Operator Team will notify other Federation members of such suspension or termination of services, however, the Federation Operator Team has no liabilities to any damages it might cause to other Federation members.

The Federation Operator Team reserves the right to suspend any Services which has no access records in the past 6 months. Notice of such suspension should be given to the Service Provider and all Federation members one month prior to the actual suspension.

If all the Services provided by a Service Provider Member are terminated, the membership of the SP Member will be terminated too.

5.4 Revoking of Membership

A Federation Member who fails to comply with the federation policy may have its membership in the Federation revoked. If the Federation Operator Team is aware of a breach of the following regulations by a Federation Member, the Federation Operator Team may issue a formal notification of concern and order to correct it within a specified time.

- Chinese Internet Security Law and relevant Internet Management laws and regulations.
- CARSI Federation Policy.
- Committing acts that affect Internet security, such as launching network attacks and spreading viruses, etc.
- Failed to pay on time.

In case the notification of concern is not rectified within the specified time or no justification is proposed to extend the date, the Operator Team can make a decision to revoke the membership. The Operator Team will notify the cancellation to all federation members. As a result of the disqualification and the loss to other federation members, the Operator Team will not bear the consequences and will not be responsible for compensation.
Revocation of membership implies the revocation of the use of all Technology Profiles for the Federation Member.

6 Fees and Payment Terms

Federation Members should pay the membership fee to the CARSI Federation Operator Team to support the operation of the Federation. The fee structure and payment terms are proved by the Federation Steering Committee and published to all Federation members. The latest Fees and Payment Terms are published on the Federation website at: http://www.carsi.edu.cn/docs/fee_policy_en.pdf.
The membership fees are not refundable. Any changes to the Fees and Payment Terms should be given at least one month notice to all Federation members. Failing to pay membership fees may result in a revoking of membership.

7 Liability and indemnification

The Federation Operator Team offers this service on an “as is” basis, that is, without liability for Federation Operator Team for any faults and defects meaning amongst others that the Federation Member cannot demand that Federation Operator Team amend defects, refund payments or pay damages. Federation Operator Team will nevertheless strive to ensure that any faults and defects of significance are corrected within a reasonable period.
The Federation Operator Team may not be held liable for any loss, damage or cost that arises as a result of the Federation Member connection to or use of Federation services, or other systems to which the Federation Member obtains access in accordance with the agreement. This limitation of liability does not however apply in the case of gross negligence or intent shown by Federation Operator Team personnel.
The Federation Operator Team shall not be liable for damage caused to the Federation Member or its End Users. The Federation Member shall not be liable for damage caused to the Federation Operator Team due to the use of the Federation services, service downtime or other issues relating to the use of the Federation services.
Unless agreed otherwise in writing between Federation Members, the Federation Member will have no liability to any other Federation Member solely by virtue of the Federation Member’s membership of the Federation. In particular, membership of the Federation alone does not create any enforceable rights or obligations directly between Federation Members. Federation Operator Team and the Federation Member shall refrain from claiming damages from other Federation Members for damages caused by the use of the Federation services, service downtime or other issues relating to the use of Federation services. The Federation Member may, in its absolute discretion, agree on variations with any other Federation Member to the exclusions of liability. Such variations will only apply between those Federation Members.
The Federation Member is required to ensure compliance with applicable laws. The Federation Operator Team shall not be liable for damages caused by failure to comply with any such laws on behalf of the Federation Member or its End Users relating to the use of the Federation services.
Neither party shall be liable for any consequential or indirect damage.
Neither the existence of interfederation agreements, nor the exchange of information enabled by it, shall create any new legal obligations or rights between Members or operators of any federation. Federation Operator Team and Federation Members remain bound only by their own respective laws and jurisdictions.
The Federation Member and Federation Operator Team shall refrain from claiming damages from entities in other federations involved in an interfederation agreement.

8 Jurisdiction and dispute resolution

Disputes concerning the Federation Policy shall be settled primarily through negotiation. If the issue cannot be resolved through negotiation, any disputes shall be submitted to the court of law under the jurisdiction.

If such negotiations do not succeed within four weeks of the date on which the claim for negotiations was made in writing by one party, each of the parties may bring the dispute before the court of law under the jurisdiction.

If any provision of the Federation Policy is held to be unenforceable by any court of competent jurisdiction, all other provisions will nevertheless continue in full force and effect.

In case of conflict, the Chinese version of the Federation Policy and its appendix, the agreement and other related documents shall prevail, while the English version is for reference.

9 Interfederation

eduGAIN (https://edugain.org), initiated by GEANT, is a global Identity Federation of Federations, also called Inter Federation. It provides an efficient and resilient technology framework for national federations and their users and services to collaborate.

In order to facilitate collaboration across national and organizational borders, the CARSI Federation may participate in interfederation agreements. How the potential interfederation agreement is administratively and technologically reflected for a certain technology is described in appropriate Technology Profiles: “eduGAIN – Declaration” and “eduGAIN – Constitution”.

CARSI members can choose to opt in joining Inter-Federation (eduGAIN) when they submit the application. The Member understands and acknowledges that via those interfederation arrangements the Member may interact with organizations that are bound by and committed to foreign laws and federation policies. Those laws and policies may be different from the laws and policies in CARSI Federation.

10 Amendment

The Federation Operator Team has the right to amend the Federation Policy from time to time. Any such changes need to be approved by CARSI Identity Federation Steering Committee and shall be communicated to all Federation Members in written form at least 90 days before they are to take effect.