TIDF Policy (TARENA Identity Federation Policy)

Contents

1. Document Control 3
1.1. Document Status 3
1.2. Document History 3
2. Definitions and Terminology 4
3. Introduction 6
4. Governance and Roles 7
4.1. Governance 7
4.2. Obligations and Rights of Federation Operator 7
4.3. Obligations and Rights of Federation Members 8
5. Eligibility 10
6. Procedures 11
6.1. How to Join 11
6.2. How to Withdraw 11
7. End-user support 11
8. Legal conditions of use 13

1. Document Control

1.1. Document Status

Document Name	TIDF Federation Policy
Authors	Nabiev Sirojiddin, Alisher Davlatov
Version Number	2
Document Status	Final (Approved)
Date Approved	18.10.2019
Date of Next Review	N/A

1.2. Document History

First release created by Alisher Davlatov in Aug 26, 2019
Second release created by Alisher Davlatov Nov10 2019 by using GEANT's Identity Federation Template

2. Definitions and Terminology

Attribute	A piece of information describing the End User, his/her properties or roles in an Organization
Attribute Authority	An organization responsible for managing additional Attributes for an End User of a Home 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
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 and zero or more Attribute Authorities on the basis of the identification of the End User
End User	Any natural person affiliated to a Home Organization, e.g. as an employee, researcher or student making use of the service of a Service Provider
Federation	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 and/or an Attribute Authority
Federation Operator	Organization providing Infrastructure for Authentication and Authorization to Federation Members
Federation Technology Profile	The federation technology profile specifies how to use the subsets of the specific federation technology in the context of the TIDF Federation
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 (IdP)	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
Metadata	The Metadata contains technical details and descriptive information about the IdPs and SPs. For interoperability in a specific context, the Metadata format definition is part of a Federation Technology Profile
Service Provider	The system component which offers the desired service to the

(SP)	End User. It evaluates the authentication outcome and attributes that the IdP of the Home Organization and /or Attribute Authority asserts for the End User for controlling access to the protected services /resources
Service Provider Organization	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 and Attribute Authorities assert for its End Users to its SP
Technical Specifications of the Service	Document with a technical description of the service being offered to TIDF Identity Providers

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.

3. Introduction

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

The TIDF Identity Federation (the Federation) is introduced to facilitate and simplify the introduction of shared services across the Federation. This is accomplished by using Federation Technologies to extend the scope of a digital identity issued by one Federation Member to be valid across the whole Federation. The Federation relies on Home Organizations and Attribute Authorities 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 TIDF Identity Federation founded by Tajikistan Research and Education Network Association (TARENA) without the formation of a separate legal entity.

The Federation Policy document defines the Federation by defining 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.

This document, together with its appendices constitutes the Federation Policy. The current list of all appendices is available on the website of the Federation.

4. Governance and Roles

4.1. Governance

The TARENA's Identity Federation (TIDF) is governed by the Tajik Research and Education Network Association, performs the functions of organizing secure authentication for organizations that become Members of the Identity Federation, with access to protected resources and services of scientific and educational networks and the Internet.

In addition to what is stated elsewhere in the Federation Policy the TARENA is responsible for:

- Setting criteria for membership for the Federation.
- Deciding whether to grant or deny an application for membership in the Federation.
- Deciding whether a Federation Member is entitled to act as Home Organization.
- Revoking the membership if a Federation Member is in a breach of the Policy.
- Defining future directions and enhancements for the Federation together with the Federation Operator who prepares the plans.
- Deciding entering into interfederation agreement.
- Maintaining formal ties with relevant national and international organizations.
- Approving changes to the Federation Policy prepared by the Federation Operator.
- Address financing of the Federation.
- Approves the fees to be paid by the Federation Members to cover the operational costs of the Federation, on proposal of Federation Operator.
- Deciding on any other matter referred to it by the Federation Operator.

4.2. Obligations and Rights of Federation Operator

In addition to what is stated elsewhere in the Federation Policy, the Federation Operator is responsible for:

- 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.
- Provides support services for Federation Members' appropriate contact persons to work out operational problems regarding the Federation services.

- Acts as center of competence for Identity Federation: tests software, recommends and documents solutions, provides software deployment and configuration guides for selected software and operating systems for use within the Federation.
- Prepares and presents issues to the TARENA and acts as the secretary of the TARENA's meetings.
  Maintaining relationships with national and international stakeholders in the area of Identity Federations. This especially includes contacts regarding interfederation activities and work with other Identity Federations in the area of harmonization.
- Promoting the idea and concepts implemented in the Federation so prospective Federation Members learn about the possibilities of the Federation.

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

- Temporarily suspend individual Technology Profiles for a Federation Member that is disrupting 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.
- Publish some of the data regarding the Federation Member using specific Technology Profile. Definition of which data may be published is provided in appropriate Technology Profiles.

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 an administrative contact for interactions with the Federation Operator.
- Must cooperate with the Federation Operator and other Members in resolving incidents and should report incidents to the Federation Operator 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. Prices and payment terms are specified at https://tidf.tj
- If a Federation Member processes personal data, Federation Member will be subject to applicable data protection laws and must follow the practice presented in Data Protection Profile.

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

- Is responsible for delivering and managing authentication credentials for its End Users and for authenticating them, as may be further specified in Level of Assurance Profiles.
- Should submit its Identity Management Practice Statement to the Federation Operator, who in turn makes it available to other Federation Members upon their request. The Identity Management Practice Statement is a description of the Identity Management life-cycle including a description of how individual digital identities are enrolled, maintained and removed from the identity management system. The statement must contain descriptions of administrative processes, practices and significant technologies used in the identity management life-cycle, which must be able to support a secure and consistent identity management life-cycle. Specific requirements may be imposed by Level of Assurance Profiles.
- Ensures an End User is committed to the Home Organization's Acceptable Usage Policy.
- 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. Home Organizations must not redirect End User queries directly to the Federation Operator, but must make every effort to ensure that only relevant problems and queries are sent to the Federation Operator by appropriate Home Organization contacts.

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

- Is responsible for assigning Attribute values to the End Users and managing the values in a way, which ensures they are up-to-date.
- Is responsible to releasing the Attributes to Service Providers.

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

- Is responsible for making decision 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.

5. Eligibility

Identity Providers and Service Providers are able to join or leave the Federation by applying to the Federation Operator. Participation to the Federation requires the agreement with this Federation Policy and compliance with the terms and conditions presented herein that arise from it.

In the Federation, **only** TARENA and its members can participate as Identity Providers. Each institution may take part with a single Identity Provider in the TIDF's Infrastructure.

Any organization can participate in the Federation as a Service Provider of one or more services provided that these services promote the academic, research or educational work.

TARENA and its members can act as both Identity and Service Providers at the same time.

In the case, the Service Provider does not also participate as an Identity Provider, it is necessary for at least one Identity Provider to express to the Federation Operator an interest in accessing the particular service.

The minimal technical requirements for being able to be affiliated to the TIDF Infrastructure are described in the Technology Profile. The Federation Operator reserves the right to alter the Technology Profile at any time. The alterations are published on the website of the Federation and come into effect **two months** after their notification via e-mail by the Federation Operator.

6. Procedures

6.1. How to Join

In order to become a Federation Member, an organization applies for membership in the Federation by agreeing to be bound by the Federation Policy in written by an official representative of the organization the Terms of Service Agreement (Appendix 1. of the Federation Policy).

Each applicant for membership shall fill out an Application Form (available at https://tidf.tj), indicating in what role (with what role of the Participant) it joins the Federation.

The applicant at its own expense and on its own computer resources deploys the software under the requirements of the Technology Profile in accordance with the role of the Participant specified in the Application Form.

After deployment of the software, the Applicant Organization undergoes the procedure for verifying the correct functioning of the software by the Federation Operator with the elimination of errors identified by the Federation Operator.

After undergoing of the software verification procedure, the Applicant Organization signs the Terms of Service Agreement together with the Authority as the treaty parties, including this Federation Policy.
If the application is denied, this decision and the reason for denying the application are communicated to the applying organization by the Federation Operator.

6.2. How to Withdraw

A Federation Member may cancel its membership in the Federation at any time by sending a request to the Federation Operator. A cancellation of membership in the Federation implies the cancellation of the use of all federations Technology Profiles for the organization in reasonable time interval.

The Federation Operator may cancel its participation in the Federation by announcing the termination date to the Federation Members. Until termination date, Federation Operator shall run the Federation on best effort basis. After the termination date, Federation Operator shall cancel the use of all Federations Technology Profiles for all Federation Members.

7. End-user support

End-user support is implemented by the Identity Provider's service desk and not by the Service Providers or the Federation Operator. For this purpose, Identity Providers must inform the Federation Operator of the user support contact point (e-mail address and/or telephone number). This contact point may be announced on the website of the Federation as well as be published in any other way.

Both Identity Providers and Service Providers must keep the Federation Operator informed about the technical/administrative contact points. These data are communicated to the Federation members but may not be posted on the website of the Federation.

In the case that a problem resides with a Service Provider, the Identity Providers' administrators may contact the Service Provider directly, without the mediation or assistance of the Federation Operator.

8. Legal conditions of use

8.1. Termination

A Federation Member who fails to comply with the Federation Policy may have its membership in the Federation revoked.

If the Federation Operator is aware of a breach of the Federation Policy by a Federation Member, the Federation Operator may issue a formal notification of concern. If the cause for the notification of concern is not rectified within the time specified by the Federation Operator, the *governing body* may issue a formal notification of impending revocation after which the *governing body* can make a decision to revoke the membership.

Revocation of a membership implies as soon as possible the revocation of the use of all Technology Profiles for the Federation Member.

8.2. Protection of personal data

Members of the Federation are obliged to protect the personal data of the end users and commit themselves to execute the processing of the personal data needed for the functioning of the Federation, in compliance with the Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.01.1981, Additional Protocol to the Convention 108 regarding supervisory authorities and transborder data flows, Strasbourg, 08.11.2001, Law of Republic of Tajikistan “About personal information” and other current legislation.

The Identity Providers must ensure the legitimate and safe personal data transmission to the Service Providers while the Service Providers, in turn, must use and store the minimal personal data that is required for the proper functioning of their services in accordance with the currently existing legal framework.

The Federation Operator assumes no responsibility for the compliance of these obligations because the Federation Operator does not distribute or retain users data through the TIDF Infrastructure: the transmission of data is carried out directly from the Identity Providers to the Service Providers.

8.3. Interfederation

In order to facilitate collaboration across national and organizational borders the Federation may participate in interfederation agreements. How the potential interfederation agreement is administratively and technologically reflected for certain technology is described in appropriate Technology Profiles.

The Member understands and acknowledges that via those interfederation arrangements the Member may interact with organizations which are bound by and committed to foreign laws and federation policies. Those laws and policies may be different from the laws and policies in this Federation.

8.4. Abuse

In the case that the Identity or Service Provider is violating requirements of this Federation Policy and if it is deemed that such a violation may result in a security breach and possibly in a personal data leakage, the Federation Operator may temporarily suspend the provider's access to the Federation.

In case of abuse, the affected party may request compensation by the Identity or Service Provider, which is responsible for the loss of personal data or any other possible damage. Courts of Republic of Tajikistan are responsible for resolving disputes. The affected parties may notify the Federation Operator about the dispute; however, his actions in relation to their participation in the TIDF Infrastructure remain at his/her discretion.

8.5. Amendment

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