RUNNetAAI

RUNNetAAI

Technology Profile

Authors	Vasiliy Porhachev Ilya Vasiliyev
Last Modified	17.04.2018
Version	0.0.3

1.Status of the document

1.1. The Technological Profile of the Member of RUNNetAAI Identity Federation (hereinafter - The Technological Profile) is mandatory for signing and implementation by all Members of the RUNNetAAI Identity Federation.

2. Definitions and Terminology

2.1. Besides Definition and Terminology from RUNNetAAI Identity Federation Policy sec.1 applied to this document, here it means:

2.2. SAML (Security Assertion Markup Language) is an open standard describing the interaction of the Service Provider (SP) and the Identity Provider (IdP) (within the framework of the Technology Profile, this role is performed by the Home Organization).

2.3. The SAML V2.0 Web Browser SSO Profile defines a standard that enables Identity Providers and Service Providers interact with Web Single Sign on services using SAML.

2.4. The SAML Entity is managed by the Federation Member and implements the role of SP or IdP.

2.5. Entity Metadata - information about the Entity configuration (SP or IdP) in XML format.

2.6. Federation Metadata - a collection of metadata for all entities of all members of the federation.

2.7. 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. The protocols used

3.1. The RUNNetAAI Identity Federation uses the SAML2 protocol.

3.2. All Identity Providers MUST fulfill the Interoperable SAML 2.0 Profile (stable version)

3.3. All Service Providers SHOULD fulfill the Interoperable SAML 2.0 Profile.

4. SAML metadata

4.1. All RUNNetAAI members' SAML metadata MUST comply with sec. 5 RUNNetAAI Metadata Registration Practice Statement.

4.2. Every SAML entity needs a certificate in order to sign and/or encrypt SAML messages. Usually a self-signed certificate is created during a default install. The certificate is part of the entity metadata, and will have to be published as part of the federation metadata.

4.3. A minimum key requirements: size of 2048 bits and RSA method.

4.4. Members of the Federation MUST inform the Federation Operator about incidents of compromising the certificate. The metadata of the compromised site must be immediately removed from the Federation Metadata. After the release of the new certificate, the metadata of this entity will be included in the federated registry after the node has passed the audit procedure by the Operator (section 5 of The Federation Policy).

5. Attributes

5.1. According to the SAML2.0 protocol, IdP passes to SP information in the form of attributes. All SAML attributes SHOULD be represented using the urn:oasis:names:tc:SAML:2.0:attrname-format:uri Name Format.

5.2. For the functioning of the Federation services, all Identity Providers MUST issue the minimum set of attributes and SP MUST authorize End User or reject by the following minimum set of attributes:

Attribute	**The class in which the attribute is described**	**Comments**
eduPersonPrincipalName	eduPerson	In the framework of the functioning of RUNNetAAI, the ePPN attribute is used as a unique identifier. It is a kind of <user login> @ <FQDN of the organizations> For example, ivan.ivanov@runnet.ru

5.3. All Identity Providers SHOULD issue the attribute:

Attribute	**The class in which the attribute is described**	**Comments**
eduPersonAffiliation	eduPerson	Type of employment in the organization. MUST use of the value from the closed directory in English: • faculty *Teachers and researchers* • student • staff *Workers who are not teachers or scientists* • alum *Graduates and deferred students* • library-walk-in *Visitors to the library* • affiliate *Employees engaged on an interimbasis*

5.4 Service Providers MAY request additional personal attributes from IdP, for example displayName, Mail, sn etc. Each IdP SHOULD decide if SP which is requesting additional attributes is providing enough personal data protection according to the Russian Federation Law 152FZ «Law on Personal Data Protection» and other laws. **To issue or not any set of additional attributes towards certain SP however is under the full responsibility of IdP.**

6. Additional requirements

7.1 Federation members MUST synchronize time scales on their servers. The RUNNetAAI Identity Federation recommends using NTP-servers of VNIIFTRI ntpl.vniiftri.ru, etc.

7. References

[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] https://www.internet2.edu/products-services/trust-identity/eduperson-eduorg/