Especificações Técnicas da Comunidade Acadêmica Federada (CAFe)

Protocolo

O protocolo utilizado pela Federação CAFe para a troca de informação entre os membros é o SAML na versão 2.0 [1].

Software

A Federação CAFe oferece suporte para o sistema Shibboleth [2], nas versões 2.x. Outros softwares compatíveis com o protocolo indicado pela Federação podem ser utilizados. Porém, não haverá suporte por parte da RNP.

Sistema Operacional

A Federação CAFe oferece suporte para o sistema operacional Linux na distribuição Ubuntu 14.04 LTS.Outros sistemas operacionais podem ser utilizados. Porém, não haverá suporte por parte da RNP.

Metadados

Os metadados da Federação CAFe são disponibilizados no formato SAML 2.0 Metadata [1, 3].

Certificados

Os certificados gerados para os provedores devem respeitar as seguintes restrições:

- Nome distinto: o campo common name deve ser preenchido com o nome completo de domínio (FQDN) do servidor.
- Validade: o certificado deve ser válido, ou seja, deve estar dentro do período de validade, não estar revogado, e ter sua política do caminho de certificação correta.
- Algoritmo de assinatura: deve ser utilizado o algoritmo RSA ou ECDSA com hash SHA-2. Admite-se o uso de hash SHA-1 para sistemas e certificados legados.
- Tamanho da chave: recomendam-se chaves de RSA de 2048 ou 4096 bits, devendo ser de, no mínimo, 1024 bits e de, no mínimo, 256 bits para ECDSA.
- Campo de Uso da Chave: os bits digitalSignature e keyEncipherment devem ser iguais a 1 (verdadeiros).
- Uso estendido da chave: deve incluir o identificador serverAuth para provedores de identidades e clientAuth para provedores de serviço.
- Extensão de restrições básicas: O bit cA da extensão de restrições básicas deve ser igual a 0 (falso).

Atributos

Recomenda-se que os Provedores de Identidade sejam capazes de liberar os seguintes atributos:

Atributo	Descrição	Fonte
Cn	Nome do usuário	inetOrgPerson [4]
Sn	Sobrenome do usuário	inetOrgPerson [4]
Mail	Endereço de e-mail do usuário	inetOrgPerson [4]
eduPersonPrincipalName	Identificador único do usuário dentro da federação. Formato: identificador@domínio	eduPerson [5]
brEduAffiliationType	Tipo de vínculo do usuário com a instituição. Vocabulário: faculty, student, staff, position, scholarshipawardee, other	brEduPerson [6]

Existindo atributos disponíveis, os Provedores de Identidade devem disponibilizá-los no seguinte formato:

Fonte	SAML 1.1	SAML 2.0
inetOrgPerson	urn:mace:dir:attribute-def:	urn:oid:
eduPerson	urn:mace:dir:attribute-def:	urn:oid:
brEduPerson	urn:mace:rnp.br:attribute-def:	urn:oid:

[1] Security Assertion Markup Language (SAML) v2.0: https://www.oasisopen.org/standards#samlv2.0

[2] Shibboleth web page: http://www.internet2.edu/products-services/trustidentitymiddleware/shibboleth/

[3] SAML V2.0 Metadata Interoperability Profile: https://wiki.oasisopen.org/security/SAML2MetadataIOP

[4] Definition of the inetOrgPerson LDAP Object Class (RFC2798): http://tools.ietf.org/html/rfc2798

[5] eduPerson Object Class Specification (200806): https://www.internet2.edu/en/products-services/trust-identity-middleware/edupersoneduorg/docs/internet2-mace-dir-eduperson-200806.html/

[6] Esquema brEduPerson: https://wiki.rnp.br/display/cafewebsite/brEduPerson