GARNET
Ghanaian Academic and Research Network

GARNET Identity Federation (GIF)
SAML WebSSO Technology Profile

Terminology

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 [1].

Introduction

This Technology Profile describes how the GARNET Identity Federation (GIF) is realized using the SAML V2.0 Web Browser SSO Profile [2]. The SAML V2.0 Web Browser SSO Profile defines a standard that enables Identity Providers and relying parties to create and use web Single Sign On services using SAML Requirements.

Requirements

- All SAML metadata MUST fulfill the SAML V2.0 Metadata Interoperability Profile Version 1.0 or any later version [3].
- All identity providers MUST fulfill the Interoperable SAML 2.0 Profile (stable version) [4] and MAY optionally support the Shibboleth SAML 1.1 Profile [5] for interoperability with legacy systems.
- All service providers SHOULD fulfill the Interoperable SAML 2.0 Profile [4] and MAY optionally support the Shibboleth SAML 1.1 Profile [5] for interoperability with legacy systems.
- Identity Providers and Service Providers are strongly recommended to conform with the interoperable Shibboleth 2.x version [6].
- All SAML attributes SHOULD be represented using the urn:oasis:names:tc:SAML:2.0:attrnameformat:uri Name Format.
- All SAML attribute names SHOULD be represented using either the urn:oid or http(s) URI scheme namespaces.
- All SAML Identity Providers MUST implement the Shibboleth Scope Metadata extension as defined in the Shibboleth Metadata Schema [7]. The Scope value MUST be a string equal to a DNS domain owned by the organization that is responsible for the Identity Provider.
- All SAML Service Providers SHOULD implement checks against the Shibboleth Scope Metadata extension when processing scoped attributes.

References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
[2] http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf
[3] http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf
[4] https://saml2int.org/
[5] https://wiki.shibboleth.net/confluence/display/SHIB
[6] https://wiki.shibboleth.net/confluence/display/SHIB2/Home
[7] https://wiki.shibboleth.net/confluence/display/SC/ShibMetaExt+V1.0