safeID SAML WebSSO Technology Profile v1.1

Document	safeID SAML WebSSO Technology Profile
Version	1.1
Last Modified	2019-01-30
Status	FINAL
License	Creative Commons BY-SA 3.0

Copyright

This work is based on the "SWAMID SAML WebSSO Technology Profile v1.0", written by L. Johansson, T. Wiberg, V. Nordh, P. Axelsson, M. Berglund available at https://www.sunet.se/swamid/policy/saml-websso ©2010 SUNET (Swedish University Computer Network) and the "ACOnet Identity Federation SAML WebSSO Technology Profile v0.1" available at https://www.aco.net/technologien.html, used under a Creative Commons Attribution-ShareAlike license: http://creativecommons.org/licenses/by-sa/3.0/.

1 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 RFC2119, see https://www.ietf.org/rfc/rfc2119.txt.

2 Introduction

This document is a safeID Identity Federation Policy Technology Profile which describes how the safeID Identity Federation is realised using the SAML V2.0 Web Browser SSO Profile [1].

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 using SAML.

3 Requirements

- All SAML metadata MUST fulfill the SAML V2.0 Metadata Interoperability Profile Version 1.0 or any later version [2].
- All identity providers (home organizations and attribute authorities) and service providers SHOULD fulfill the SAML V2.0 Interoperability Deployment Profile [3].
- All SAML attributes SHOULD be represented using the urn:oasis:names:ts:SAML:2.0:attrname-format:uri Name Format.
- All SAML attribute names SHOULD be represented using either the urn:oid or http(s) URI scheme namespaces. Usage of MACE-Dir [4] defined attributes MUST conform to the MACE-Dir SAML Attribute Profiles [5] (or any later version).
- All SAML identity providers (home organizations and attribute authorities) MUST implement the Shibboleth Scope Metadata extension as defined in the SAML 2.0 Metadata Extension for Shibboleth [6]. The Scope value MUST be a string equal to a DNS domain owned by the organization that is responsible for a role of the identity provider (in the sense of a data controller as per EU Regulation EC No 45/2001).

- All SAML service providers SHOULD implement checks against the Shibboleth Scope Metadata extension when processing scoped attributes.

4 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] http://middleware.internet2.edu/dir/
[5] http://macedir.org/docs/internet2-mace-dir-saml-attributes-200804a.pdf
[6] https://wiki.shibboleth.net/confluence/display/SC/ShibMetaExt+V1.0