Defining a Standard Mechanism to Signal an Entity’s Support for REFEDS Specifications

Google Doc Working Draft at: https://docs.google.com/document/d/1IXeCpKYl4LVc5RiDH0ZUKsNK-3B RNk_Qt_DkwFkncaE/edit

Introduction

REFEDS publishes standards and specifications deployed by the global research and education community to enable scalable, secure, and seamless federated access. These specifications have been developed by and continue to evolve through community volunteer working groups.

These specifications satisfy a wide range of capabilities and needs. They generally perform one or both of these functions:

- To signal an entity’s qualification or support for a particular performance requirement via declarations in entity metadata (ala configuration time)
- To articulate requirements (and performance of those requirements) during a user sign-in event (ala transaction time)

During the last round of REFEDS specification updates, the working groups received numerous feedback that all specifications should have configuration time signaling components. This need arises from several areas:

1. Better User Experience (primary) - A service provider (or its discovery service) wishes to know whether an identity provider supports a transaction time requirement (e.g., REFEDS MFA Profile) so that it can pre-empt unnecessary “access denied” messages by providing better user instruction before they attempt sign-in.
2. Better Set-Up Time Communication (useful) - Examining the other parties’ REFEDS specification support at metadata exchange (configuration time) allows entity operators to clearly articulate and detect requirements and capabilities, thus potentially avoiding unnecessary testing /troubleshooting at integration time.
3. Better Analytics (bonus) - A consistent and complete metadata vocabulary describing an entity’s REFEDS spec support creates an opportunity for the federation community to analyze specification support trends and help promote adoption.

This document proposes the creation of a REFEDS working group to develop a REFEDS framework to define a generalized catalog and signaling mechanism incorporating all REFEDS published specifications. We anticipate this as a lightweight framework that leverages existing mechanisms wherever possible. As such, we recommend the working group scope its work to deliver the first version by the Winter 2024 (presumably December 2024) REFEDS meeting.

Challenges - why do we need a framework?

Several REFEDS specifications already include configuration time signaling mechanisms. For example, the SIRTFI framework (SIRTFI) expresses it as an Entity Attribute. The Research and Scholarship Entity Category (R&S) defines an Entity Category. What is different about this group’s work?

Varying Specification Scope - Not all REFEDS specifications’ scope lend themselves to describing configuration time capabilities. SIRTFI describes requirements for an entity at large. Its scope naturally leads to the creation of a configuration time signal. The REFEDS Assurance Framework (RAF) describes the login user’s identity trustworthiness at sign-in time. Its vocabulary is meant to be used during a user sign-in transaction (e.g., SAML attribute assertion). Defining a configuration time signal within a transaction time-focused specification has been ruled out of scope by multiple working groups working on this type of specification.

Inconsistent Signaling Mechanics - As it turns out, RAF does define a “conformance” signal to help a service provider understand the IdP’s identity assurance capabilities. It just defines it as an attribute value to be delivered at user sign-in. Similarly, the REFEDS MFA Profile relies on the SAML request/response syntax to transmit “need/support” signals at user sign-in. These inconsistent ways of exchanging entity capability signals create confusion and ultimately impede adoption.

Entity Category vs Entity Attribute - These are concepts foreign to many, even among R&E IAM practitioners. Since these are the likely mechanism(s) we will use to perform configuration time signaling in SAML, the WG should consider a more intuitive/friendly way to clarify these concepts.

Work Group Objectives

- Assess current published REFEDS specifications; identify each specification’s need to signal “conformance” or “support”; document current mechanisms.
- Develop REFEDS framework for a standardized mechanism to record and publish a specification’s configuration time “conformance” or “support” signal -> for this arc, this would presumably be a registry of entity attributes and a mechanism to register entity attributes representing each specification’s needs (conformance, support, etc)

Party of the Willing

These individuals have indicated interest in contributing to this working group:

- Pål Axelsson (Sunet) ← Proposer
- Davide Vaghetti (GARR)
- Wolfgang Pempe (DFN)
- Albert Wu (InCommon) ← Voluntold WG Convener / Chair
- John Scullen (Australian Access Federation)
- Alex Stuart (UK federation)
- Nicole Roy (InCommon)
- Niels van Dijk (SURF and GEANT Incubator)
- Björn Mattsson (Sunet)