08-12-2016

Deliverable DSA1.1:
Pilots to support guest users solutions

Deliverable DSA1.1

Contractual Date:	31-07-2016
Actual Date:	01-08-2016
Grant Agreement No.:	653965
Work Package:	SA1
Task Item:	SA1.1 Pilot on Guest Identities
Lead Partner:	GARR
Document Code:	DSA1.1
Authors:	Mario Reale, Nicolas Liampotis, Christos Kanellopoulos, Barbara Monticini, Pete Birkinshaw, Martin Haase, Maria Laura Mantovani, Peter Gietz, Petr Zabicka, Jiri Pavlik, Jens Jensen, Stefan Paetow, Niels Van Dijk and Paul van Dijk

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

Abstract

This document describes the pilots executed by the Service Activity 1 as part of Task1 (Pilot solutions for guests' users). The aims of this group of pilots were to demonstrate possible approaches to improve the adoption of federated identity management in the libraries community and solutions to support guest user access.

Executive Summary

The main aim of the task "Pilot solutions for guests' users" (SA1-T1) is to support the inclusion of guest identities in the provisioning of federated services. As part of this task, the team explored three solutions to ease the deployment of federated access for the library community.

The team initially focused on the implementation of three pilots that targeted the library community, to supporting them in the authentication and to facilitate moving away from their current IP-based authentication approach.

The pilots executed are:

- Support access to federated and non-federated library resources – **bridging SAML and IP-address based access methods with EZproxy**. The demonstrator and details are available here: wiki.geant.org/x/a4qSAw ;
- **Support authorised access for citizen scientists to library resources (walk-in users)**. The demonstrator and details are available here: https://wiki.geant.org/x/0IqSAw ;
- **Showcase a model for library consortia to reduce the number of interactions between IdPs and SPs (simpleSAMLphp proxy for library consortia)** from a technical and trust point of view while preserving the privacy of users. The demonstrator and details are available here: wiki.geant.org/x/6oCuAw ;

Subsequently, the task has implemented a pilot aimed at demonstrating the possibility of including social identities (i.e. Facebook, Google, LinkedIn, etc.) to authenticate guest users. The goal of this pilot is to demonstrate mechanisms to enhance the assurance associated with social identities, that is the level of trust a service or a resource provider can have in the credentials issued by social identity provider. With this approach, social identities can be used to authenticate guest users and can be trusted by service or resource provides to grant access to their resources.

The demonstrator and a detailed description for this pilot are available here: wiki.geant.org/x/ZIqSAw

This chapter below provides a high-level overview of the rationale of the pilots executed by the SA1-T1 team, the use-cases they solve, the main community they targeted and it offers pointers to the demonstrators.

1 Pilots features

The tables below summarise the scope, benefits and the results of each the pilots executed as part of this task.

Task 1, Pilot 1	SAML / IP bridge
Goal	Support access to federated and non-federated library resources – bridging SAML and IP-address based access methods (SAML to SAML + SAML to IP)
Approach/AARC identified solution	Establish a proxy to bridge SAML and IP address access methods, a so called access mode switch
Components piloted	EZ-Proxy for SAML-IP bridge
Gain for end-users/administrators	• Same entry point for users regardless of the type of Authentication technology required by the service provider • A better user experience • An easy way for technical administrators at the libraries to introduce federated access without disrupting access to services that only support IP-based authentication
Demo/video	Demo Flow Video
Detailed technical description	See wiki
Documentation of components	documentation for EZproxy access mode switch
Software Prerequisite(s)	EZproxy - EZproxy is a commercial software, widely used in the library environment. Its wider adoption made it a suitable candidate for this pilot.
Lead	GARR
Community partners	IT: GARR, Library NL: UKB library consortium
Status	Pilot implementation completed. The pilot has been presented to several libraries. Feedback from the communities will be included in the final SA1 deliverable.

Table 1 - SAML/IP Bridge Pilot

Task1, Pilot 2	Walk in users
Goal	Support authorised access for citizen scientists to library resources (SAML+IP to SAML with authZ)
Approach/AARC identified solution	Establish a guest SAML IdP which adds attributes that can be consumed by services and resources providers to authorise non-institutional users. In addition, explore exploitation models: per library or per national library consortium deployment.
Components piloted	Shibboleth v3 for IdP with IP-based AuthZ attribute
Gain for end-users/administrators	• Users without an institutional account but visiting a research library will have access to library resources using this component. • More consistent authentication interface no matter which resource is being requested by the users. • Ability to use this access method and at the same time maintain full privacy • Admin interface for librarians to scope/configure valid IP ranges
Demo/video	Flow Demo admin portal Demo user portal
Detailed technical description	AARC wiki
Documentation of components	Documentation for walk by user access component, access control wiki
Software source(s)	Shibboleth v3 for walk by user access
Lead	GARR/DAASI
Community partners	IT: GARR, Library NL: UKB library consortium
Status	Pilot implementation completed. Awaiting final phase of feedback from communities

Table 2 - Walk in users PIlot

Task 1, Pilot 3	simpleSAMLphp proxy
Focus	Showcase a model for library consortia to reduce the number of interactions between IdPs and SPs from a technical and trust point of view while preserving the privacy of users
Approach/AARC identified solution	Establish a proxy as a single point for interaction between IdPs and SPs, branded as a HEAL-Link initiative
Components piloted	SimpleSAMLphp as IdP/SP proxy
Gain for end-users/administrators	• More consistent interface no matter which resource is being requested by the users • Better service to end-users, standardised access method • Less effort to maintain and administer access for library administrators • Support publisher contracts to be managed centrally by the consortium • Easier to implement and manage trust relationships among IdPs and SPs Library consortium will retain control on branding and policies • More precise and easier to produce statistics
Demo/video	Flow Demo
Detailed technical description	AARC wiki
Documentation of components	documentation for the HEAL-Link proxy
Software source(s)	SimpleSAMLphp for the IdP/SP proxy Memcached Shibboleth
Lead	GARR/GRNET
Community partners	GR: HEAL-Link consortium GR: Aristotle University of Thessaloniki (Identity Provider) US: Wiley Online Library (Service Provider)
Status	The IdP/SP proxy has joined the GRNET federation and the login workflow has been tested using the production IdP of one of the participating academic organizations, namely the Aristotle University of Thessaloniki. The interconnection of the proxy with the (pre-production) SP of Wiley Online Library (partners with HEAL-Link) is close to finalization

Table 3 - Task1, Pilot 3 - IdP/SP Proxy for library consortia