

## Case Study:

# UNINETT's simpleSAMLphp: Doing IDM the "Simple" Way

## The Organization

The UNINETT Group supplies network and network services for colleges, universities, and research institutions. It also handles national ICT tasks. The Group is owned by the Norwegian Ministry of Education and Research, and consists of a parent company and four subsidiaries. The parent company, UNINETT, develops and operates the Norwegian Research Network, which links together Norwegian educational and research institutions and connects them to an international network.

## The Challenges

Through the GÉANT project, a European research program, UNINETT wanted to find a way to make its Norwegian identity management system work with systems and solutions from other countries. But the problem UNINETT faced was considerable: When it comes to identity management, different countries in Europe use widely different technology and protocols.

In order to promote interoperability, UNINETT first tried implementing protocol translators using commercial software. They quickly discovered, that these products were not suited to such deployment scenarios.

"We were a bit stuck because we were working with big complex software and we found that we were actually fighting more with the software than we were doing real work," said Andreas Åkre Solberg, the head developer and project leader of the simpleSAMLphp project at UNINETT. "The commercial products were simply not flexible enough to be able to do the kind of protocol translation UNINETT needed."



"It is an honor to present this award to such an innovative, pragmatic deployment. The community UNINETT has built so quickly—and the wonderful open source success that they've lead—is commendable. It shows what can be done with excellent base code, SAML 2.0, some clear education, from Sun and Liberty Alliance, and very smart, committed developers from the UNINETT community. What a brilliant example of the power of community!"

**-Britta Glade  
Director of Marketing  
Liberty Alliance**

## The Inspiration

In November of 2006, the team from UNINETT watched a Liberty Alliance Web cast featuring Pat Patterson, an engineer from Sun Microsystems. When he demonstrated a proof of concept implementation using SAML and the programming language PHP, the UNINETT team found itself paying extra close attention.

“Pat Patterson from Sun showed that it was possible to do the same thing as big commercial software did in a real simple way,” said Solberg. “This was inspiring to us.”

Solberg and his team set to work building simpleSAMLphp, an open source lightweight implementation of several federation protocols. Free to download and available in 15 languages, simpleSAMLphp is a platform for quick implementation of emerging standards or identity-enabled proof-of concept (POC) applications. The software implements Web SSO, and can be applied in any deployment where users need to be authenticated to a World Wide Web Service.

simpleSAMLphp is now used extensively across Europe, both in production and as an experimentation platform. In the educational sector in Eastern Europe, identity federations have been difficult to develop due to the high cost of installation and deployment of federation software. simpleSAMLphp has changed this for some countries, including Croatia and Slovenia.

In the United States, the institutions that have shown greatest interest in simpleSAMLphp are universities that want to hook Google Apps into their own identity systems using the SAML protocol.

UNINETT received a 2008 Emerging Application IDDY Award for this innovative deployment.

“It is an honor to present this award to such an innovative, pragmatic deployment, ” said Britta Glade, the director of marketing at Liberty Alliance. “The community UNINETT has built so quickly—and the wonderful open source success that they’ve lead—is commendable. It shows what can be done with excellent base code, SAML 2.0, some clear education from Sun and Liberty Alliance, along with very smart, committed developers from the UNINETT community. What a brilliant example of the power of community!”

## simpleSAMLphp

For most of the protocols simpleSAMLphp can act as both an SP and an IdP. The protocols that are supported include:

- SAML 2.0 SP
- SAML 2.0 IdP
- Shibboleth 1.3 SP
- Shibboleth 1.3 IdP
- OpenID Provider

In addition, external contributors added these protocols:

- A-Select IdP
- A-Select SP
- PAPI IdP
- PAPI SP
- WS-Federation IdP

simpleSAMLphp has built-in support for bridging any combinations of the protocols above. Solberg reports that he does not know of any other product on the market that has such extensive built-in functionality for bridging identity protocols.

“Simply said, simpleSAMLphp supports most, if not all, of the necessary components necessary in building multi-national identity federations,” says Solberg.

## simpleSAMLphp as a Service Provider

simpleSAMLphp is ideal for organizations that need to authenticate users to Web applications. In addition to providing support for local authentication, it also offers service provider functionality. simpleSAMLphp as a service provider, for example, communicates and delegates authentication with an Identity Provider. And simpleSAMLphp may connect to both a Shibboleth and a SAML 2.0 Identity Provider.

As simpleSAMLphp is written in PHP, it is the most convenient and simple choice for integrating Web-based PHP applications into a federation. That said, simpleSAMLphp now also supports non-PHP environments by using the Auth Memcookie approach. Solberg says this setup is supported in version 1.0, and it will be fully documented very soon.

Basically simpleSAMLphp adds a special cookie in Memcache that is understood by the well-known Apache module Auth MemCookie. It passes authentication information in header variables, and allows setup authorization in Apache.

For those that want to connect the same SP to multiple IdPs, and want to let the user select between the IdPs, a built-in SAML 2.0 Identity Provider Discovery Service may be used.

simpleSAMLphp is also on the leading edge involving new initiatives around SAML 2.0 metadata distribution which is necessary to build large confederations.

“Ways of letting the user select his home identity institution becomes a very important component of a large-scale identity federation,” said Solberg.

## Top three benefits for users:

- simpleSAMLphp provides all the security benefits generally provided by more traditional federated SSO systems.
- The user interface follows Web standards and is easy to use. It has been translated into 11 different languages.
- Features like the user consent module give users more control over personal data.

## simpleSAMLphp as an Identity Provider

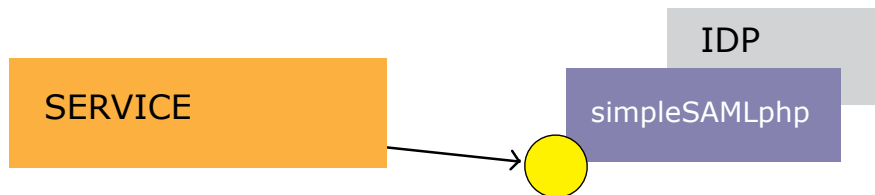
For those that have a user repository, a database, an LDAP or a radius interface, a simpleSAMLphp installation of a federated single sign-on environment can be easily set up. “Also, writing new plug-ins to new user storage systems is really simple,” said Solberg. “Where simpleSAMLphp runs as an Identity Provider both Shibboleth and SAML 2.0 services can connect to it.”

## FEDERATION ENABLING AND APPLICATION



Example:  
Connecting Moodle to a federation

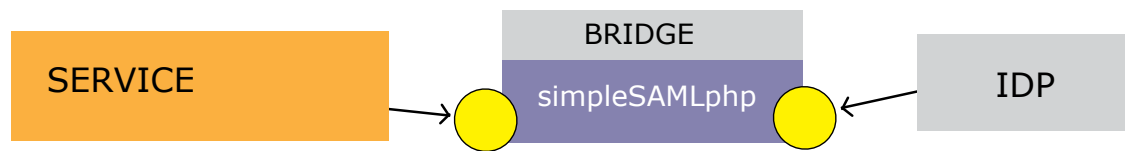
## RUNNING ONE OR MANY IDPS



Examples:

- The Danish educational federation Wayf.dk
- A university in the U.S. federating Google Apps
- A school or university in a federation

## BRIDGING PROTOCOLS



Examples:

- Shibboleth <-> SAML2.0
- OpenID to SAML 2.0
- A-Select to SAML 2.0
- PAPI to SAML 2.0

**PROJECTS:**  
eduGAIN, Kalmar

## The Beauty of simpleSAMLphp

When Andreas Åkre Solberg gives presentations about simpleSAMLphp, he talks about it in terms of “doing things the simple way.”

Simplicity brings with it a range of advantages:

- It provides SAML 2.0, Shibboleth 1.3, WS-Federation support and lets organizations “bake” identity management into the application itself instead of relying on a separate server.
- simpleSAMLphp is horizontal software that implements SSO and can be applied to any deployment where users need to connect to a Web service.
- It can be easily used in a wide range of companies. Both commercial organizations and non-profits can benefit from simpleSAMLphp.
- It makes identity management affordable by essentially providing it for free—keeping the setup and maintenance costs low.
- The current roadmap provides enhanced functionality and support for ID-WSF and/or OAuth (Open Authentication) as well as functionality for ad-hoc groups or virtual organizations.
- The lack of requirements around third-party libraries make it easy to fit into existing deployments, regardless of operating systems or infrastructure.

### Connect to the simpleSAMLphp Blog

For more information about simpleSAMLphp developments, go to Andreas Åkre Solberg’s blog at <http://rnd.feide.no>

## UNINETT Wins a 2008 IDDY Award

The deployment demonstrates both the power of technology and collaboration by showing that open source communities are solving important identity management problems. By bridging the gap among multiple identity standard protocols, it promotes interoperability and makes it easier for different organizations to work with one another.

Additionally, the deployment demonstrates that users, when given the chance, will leave behind the complexity of traditional commercial products and gravitate to solutions that are simple to deploy and maintain.

“We are thrilled to have been awarded the IDDY by the Liberty Alliance,” said Solberg. “Interoperability across institutions and also across countries is so important. There needs to be forums where people can meet and exchange ideas. In that respect, Liberty Alliance is tremendously valuable.”

## About Liberty Alliance

Liberty Alliance is the only global identity community with a membership base that includes technology vendors, consumer service providers and educational and government organizations working together to build a more trust-worthy Internet by addressing the technology, policy and privacy aspects of digital identity management. Liberty Alliance is also the only identity organization with a history of testing vendor products for true interoperability of identity specifications. Nearly 80 products and identity solutions from vendors around the world have now passed Liberty Interoperable™ testing. Liberty Alliance works with identity organizations worldwide to ensure all voices are included in the global identity discussion and regularly holds and participates in public events designed to advance the harmonization and interoperability of CardSpace, Liberty SAML 2.0 Federation, Liberty Web Services, OpenID and WS-\* specifications. More information about Liberty Alliance as well as information about how to join many of its public groups and mail lists is available at [www.projectliberty.org](http://www.projectliberty.org).