SimpleSAMLphp

making things simple

Victoriano Giralt

Central Computing Facility
University of Málaga

Melbourne
October 3rd 2008

Outline

Outline

Outline

Outline

Outline

SimpleSAMLphp
a definition (sort of)

What is SimpeSAMLphp?

SimpleSAMLphp
a definition (sort of)

What is SimpeSAMLphp?

It is a **simple** application

SimpleSAMLphp
a definition (sort of)

What is SimpeSAMLphp?

It is a **simple** application
that implements **SAML**

SimpleSAMLphp
a definition (sort of)

What is SimpeSAMLphp?

It is a **simple** application
that implements **SAML**
in **PHP**

SimpleSAMLphp
simple means easy

SimpleSAMLphp is easy to

SimpleSAMLphp
simple means easy

SimpleSAMLphp is easy to

- install

SimpleSAMLphp is easy to

- install:
  just drop a folder into an Apache 2 server with PHP 5.2

SimpleSAMLphp is easy to

- install:
  just drop a folder into an Apache 2 server with PHP 5.2
- integrate

SimpleSAMLphp is easy to

- install:
  just drop a folder into an Apache 2 server with PHP 5.2
- integrate
- maintain

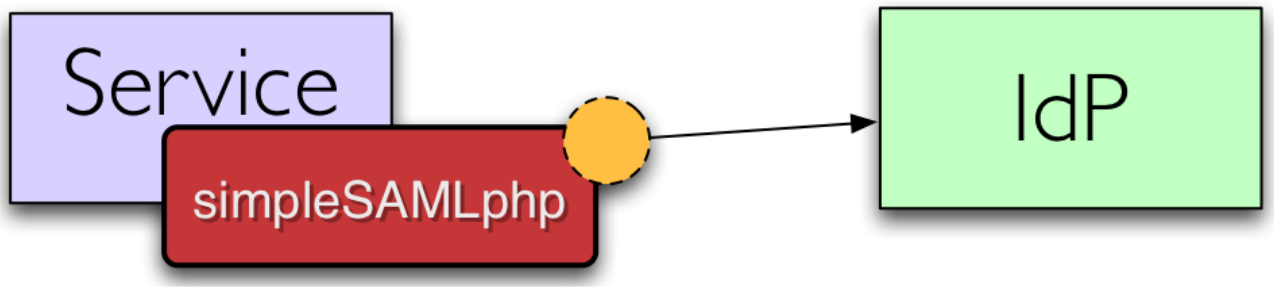
SimpleSAMLphp is easy to

- install:
  just drop a folder into an Apache 2 server with PHP 5.2
- integrate
- maintain
- develop for

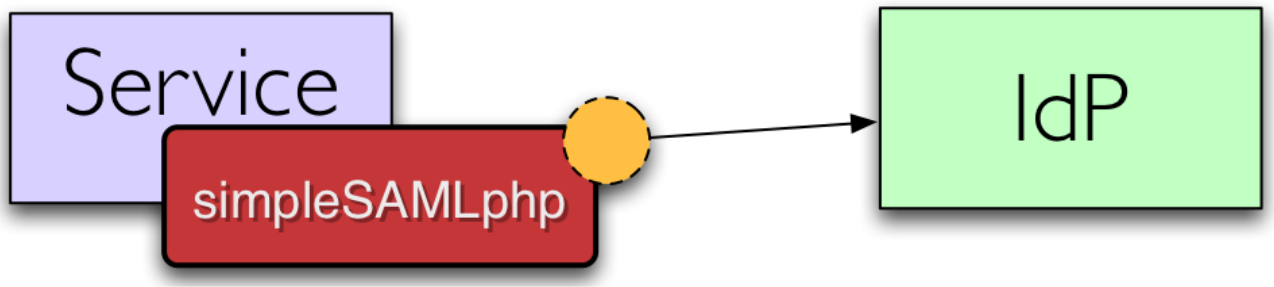
Use cases
Federating an application

SimpeSAMLphp for integrating applications into a federation

SimpeSAMLphp for integrating applications into a federation



SimpeSAMLphp for integrating applications into a federation

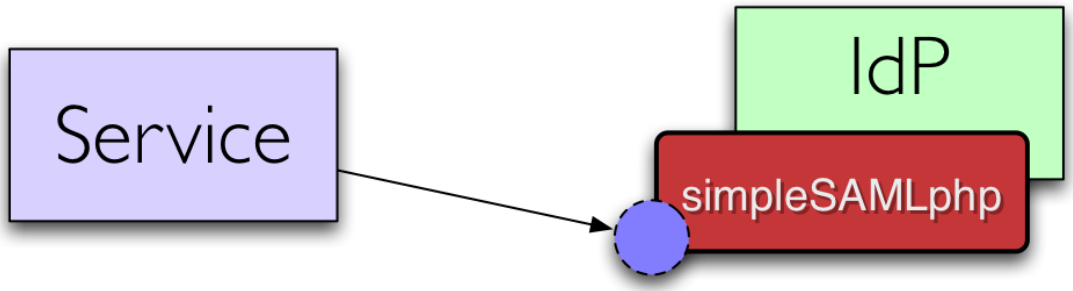


Example: conecting a wiki to the federation

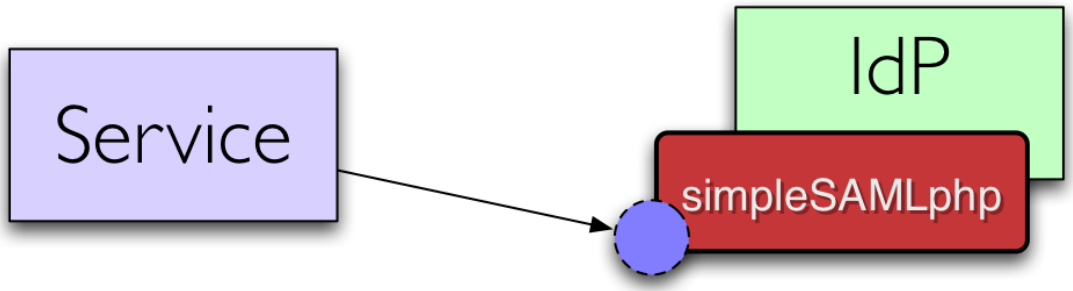
Use cases
Setting up an Identity Provider

SimpeSAMLphp as the federation Identity Provider

SimpeSAMLphp as the federation Identity Provider

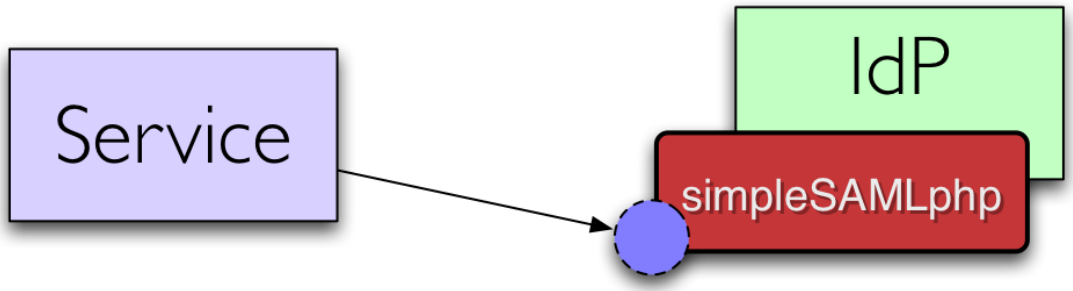


SimpeSAMLphp as the federation Identity Provider



For example:

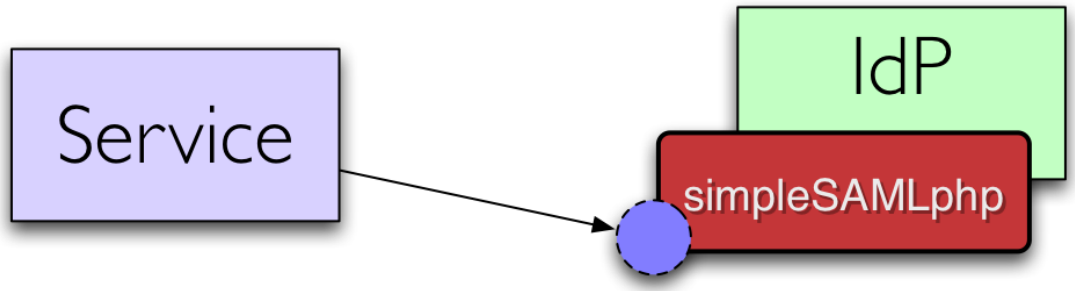
SimpeSAMLphp as the federation Identity Provider



For example:

+ The University of Málaga IdP

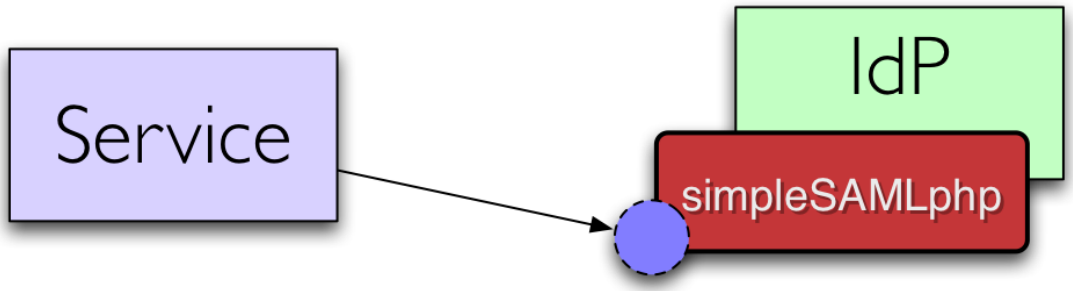
SimpeSAMLphp as the federation Identity Provider



For example:

- The University of Málaga IdP
- The wayf.dk danish federation

SimpeSAMLphp as the federation Identity Provider



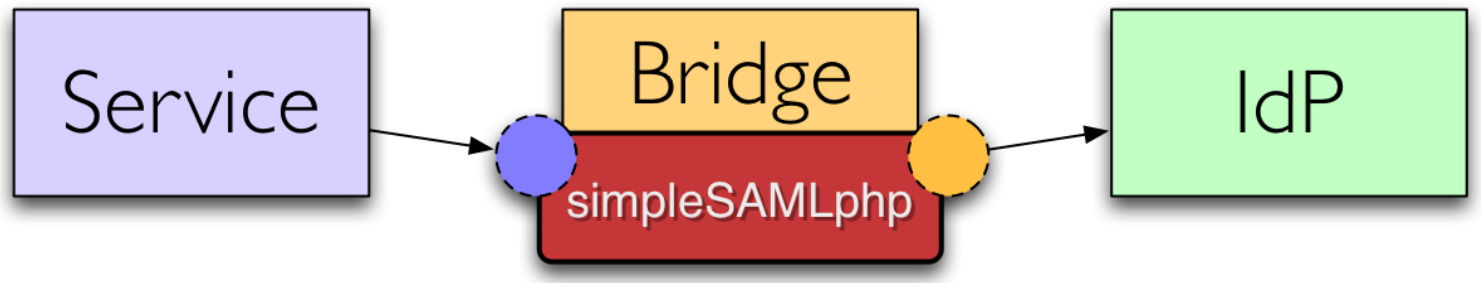
For example:

- The University of Málaga IdP
- The wayf.dk danish federation
- An American University connecting to Google Apps

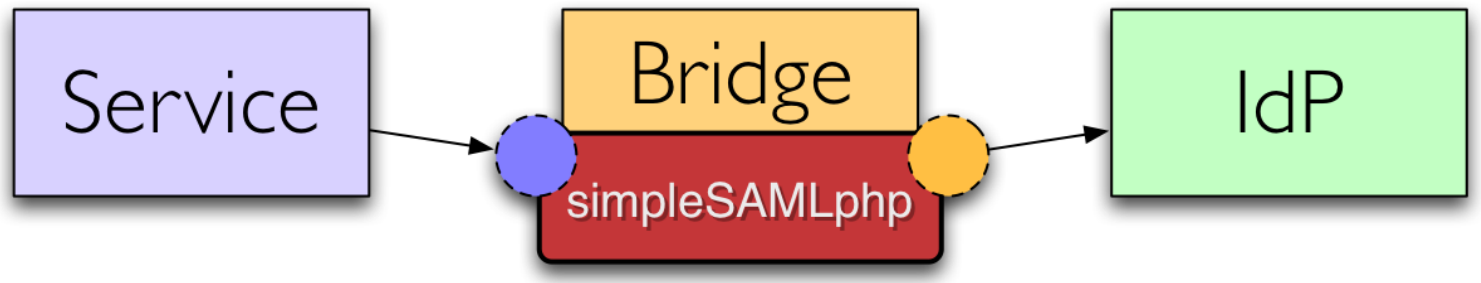
Use cases
Bridging protocols

SimpeSAMLphp can bridge disparate protocols

SimpeSAMLphp can bridge disparate protocols

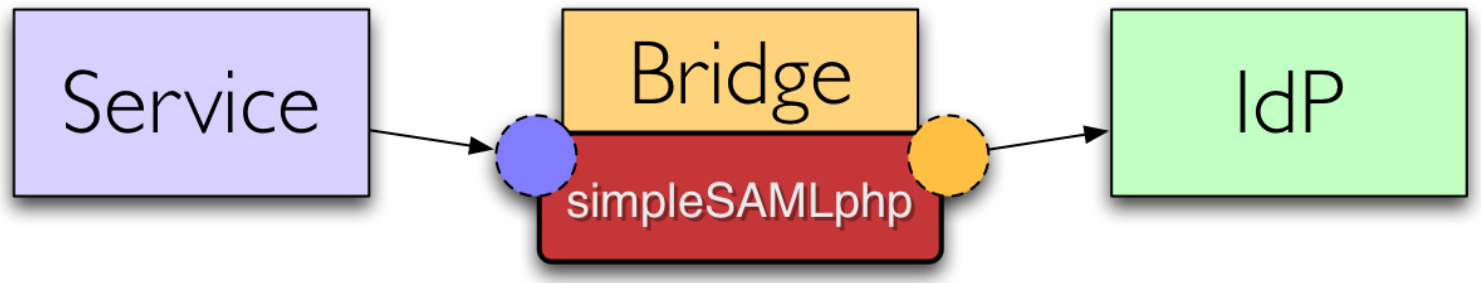


SimpeSAMLphp can bridge disparate protocols



For example:

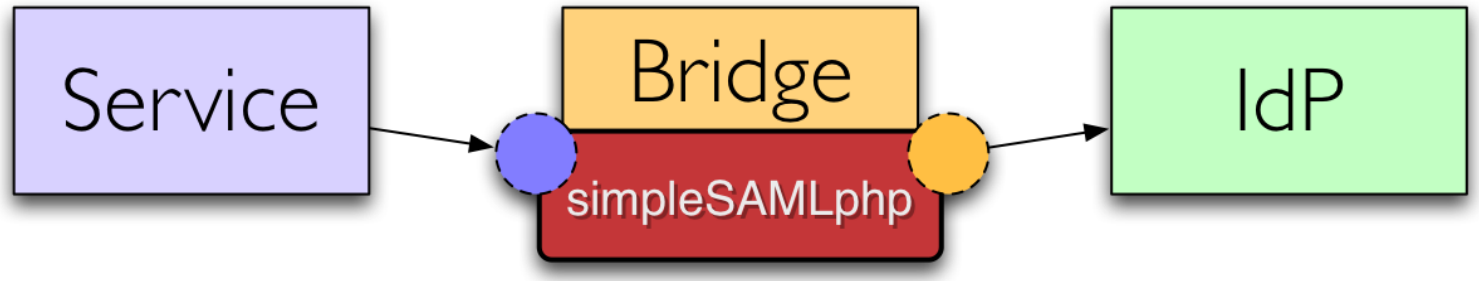
SimpeSAMLphp can bridge disparate protocols



For example:

Shibboleth $\longleftrightarrow$ SAML 2.0

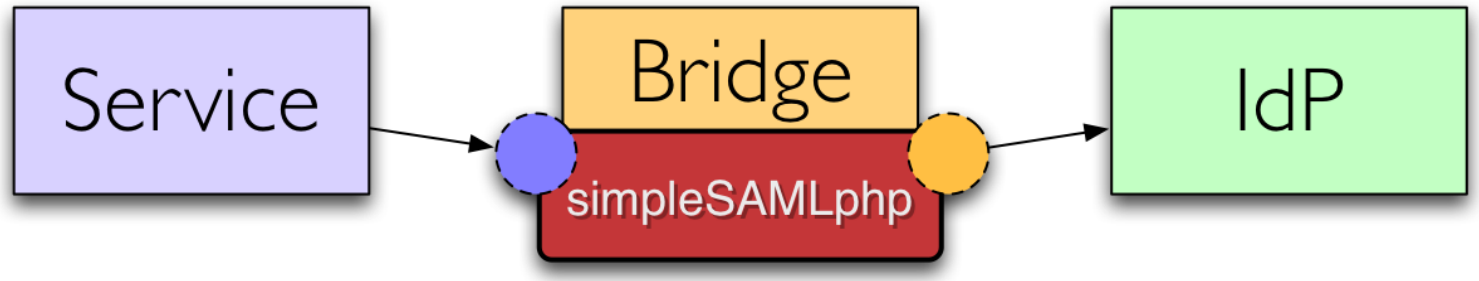
SimpeSAMLphp can bridge disparate protocols



For example:

$$\text{Shibboleth} \longleftrightarrow \text{SAML 2.0}$$
$$\text{OpenID} \longrightarrow \text{SAML 2.0}$$

SimpeSAMLphp can bridge disparate protocols



For example:

Shibboleth	$\longleftrightarrow$	SAML 2.0
OpenID	$\longrightarrow$	SAML 2.0
PAPI	$\longleftrightarrow$	SAML 2.0

Lotsa protocols

simpleSAMLphp *is* multiprotocol

Lotsa protocols
simpleSAMLphp *is* multiprotocol

SimpleSAMLphp version 1.2 can communicate with

Lotsa protocols
simpleSAMLphp *is* multiprotocol

SimpleSAMLphp version 1.2 can communicate with

Now (version 1.2):

Lotsa protocols
simpleSAMLphp *is* multiprotocol

SimpleSAMLphp version 1.2 can communicate with

Now (version 1.2):

- SAML 2.0 SP

Lotsa protocols
simpleSAMLphp *is* multiprotocol

SimpleSAMLphp version 1.2 can communicate with

Now (version 1.2):

- SAML 2.0 SP
- SAML 2.0 IdP

Lotsa protocols
simpleSAMLphp *is* multiprotocol

SimpleSAMLphp version 1.2 can communicate with

Now (version 1.2):

- SAML 2.0 SP
- SAML 2.0 IdP
- Shibboleth 1.3 SP

Lotsa protocols
simpleSAMLphp *is* multiprotocol

SimpleSAMLphp version 1.2 can communicate with

Now (version 1.2):

- SAML 2.0 SP
- SAML 2.0 IdP
- Shibboleth 1.3 SP
- Shibboleth 1.3 IdP

Lotsa protocols
simpleSAMLphp *is* multiprotocol

SimpleSAMLphp version 1.2 can communicate with

Now (version 1.2):

- SAML 2.0 SP
- SAML 2.0 IdP
- Shibboleth 1.3 SP
- Shibboleth 1.3 IdP
- A-Select

Lotsa protocols
simpleSAMLphp *is* multiprotocol

SimpleSAMLphp version 1.2 can communicate with

Now (version 1.2):

- SAML 2.0 SP
- SAML 2.0 IdP
- Shibboleth 1.3 SP
- Shibboleth 1.3 IdP
- A-Select

In the not so distant future:

Lotsa protocols
simpleSAMLphp *is* multiprotocol

SimpleSAMLphp version 1.2 can communicate with

Now (version 1.2):

- SAML 2.0 SP
- SAML 2.0 IdP
- Shibboleth 1.3 SP
- Shibboleth 1.3 IdP
- A-Select

In the not so distant future:

- OpenID as provider (beta)

Lotsa protocols
simpleSAMLphp *is* multiprotocol

SimpleSAMLphp version 1.2 can communicate with

Now (version 1.2):

- SAML 2.0 SP
- SAML 2.0 IdP
- Shibboleth 1.3 SP
- Shibboleth 1.3 IdP
- A-Select

In the not so distant future:

- OpenID as provider (beta)
- OpenID as consumer (experimental)

Lotsa protocols
simpleSAMLphp *is* multiprotocol

SimpleSAMLphp version 1.2 can communicate with

Now (version 1.2):

- SAML 2.0 SP
- SAML 2.0 IdP
- Shibboleth 1.3 SP
- Shibboleth 1.3 IdP
- A-Select

In the not so distant future:

- OpenID as provider (beta)
- OpenID as consumer (experimental)
- PAPI (beta)

Lotsa protocols
simpleSAMLphp *is* multiprotocol

SimpleSAMLphp version 1.2 can communicate with

Now (version 1.2):

- SAML 2.0 SP
- SAML 2.0 IdP
- Shibboleth 1.3 SP
- Shibboleth 1.3 IdP
- A-Select

In the not so distant future:

- OpenID as provider (beta)
- OpenID as consumer (experimental)
- PAPI (beta)
- WS-federation

Lotsa protocols
simpleSAMLphp *is* multiprotocol

SimpleSAMLphp version 1.2 can communicate with

Now (version 1.2):

- SAML 2.0 SP
- SAML 2.0 IdP
- Shibboleth 1.3 SP
- Shibboleth 1.3 IdP
- A-Select

In the not so distant future:

- OpenID as provider (beta)
- OpenID as consumer (experimental)
- PAPI (beta)
- WS-federation
- OAuth

Lotsa protocols
simpleSAMLphp *is* multiprotocol

SimpleSAMLphp version 1.2 can communicate with

Now (version 1.2):

- SAML 2.0 SP
- SAML 2.0 IdP
- Shibboleth 1.3 SP
- Shibboleth 1.3 IdP
- A-Select

In the not so distant future:

- OpenID as provider (beta)
- OpenID as consumer (experimental)
- PAPI (beta)
- WS-federation
- OAuth
- CAS

Lotsa protocols
simpleSAMLphp *is* multiprotocol

SimpleSAMLphp version 1.2 can communicate with

Now (version 1.2):

- SAML 2.0 SP
- SAML 2.0 IdP
- Shibboleth 1.3 SP
- Shibboleth 1.3 IdP
- A-Select

In the not so distant future:

- OpenID as provider (beta)
- OpenID as consumer (experimental)
- PAPI (beta)
- WS-federation
- OAuth
- CAS
- Kerberos?

Lotsa protocols
simpleSAMLphp *is* multiprotocol

SimpleSAMLphp version 1.2 can communicate with

Now (version 1.2):

- SAML 2.0 SP
- SAML 2.0 IdP
- Shibboleth 1.3 SP
- Shibboleth 1.3 IdP
- A-Select

In the not so distant future:

- OpenID as provider (beta)
- OpenID as consumer (experimental)
- PAPI (beta)
- WS-federation
- OAuth
- CAS
- Kerberos?
- ...

Abstraction layers
Abstraction is good, but moderately

Abstraction layers
Abstraction is good, but moderately

Abstraction layers have pros

Abstraction layers
Abstraction is good, but moderately

Abstraction layers have pros

+ system pieces can be easily extended

Abstraction layers
Abstraction is good, but moderately

Abstraction layers have pros

+ system pieces can be easily extended

but they also have cons

Abstraction layers
Abstraction is good, but moderately

Abstraction layers have pros

+ system pieces can be easily extended

but they also have cons

- code becomes more complex, therefore, more difficult to read and trace

Abstraction layers
Abstraction is good, but moderately

Abstraction layers have pros

+ system pieces can be easily extended

but they also have cons

- code becomes more complex, therefore, more difficult to read and trace

So, SimpleSAMLphp has a few carefully selected layers

Authentication mechanisms

you know were your people is

Authentication mechanisms
you know were your people is

SimpleSAML provides an extension mechanism that allows it to authenticate from

Authentication mechanisms
you know were your people is

SimpleSAML provides an extension mechanism that allows it to authenticate from

- LDAP, various flavours

Authentication mechanisms
you know were your people is

SimpleSAML provides an extension mechanism that allows it to authenticate from

- LDAP, various flavours
- CAS

Authentication mechanisms
you know were your people is

SimpleSAML provides an extension mechanism that allows it to authenticate from

- LDAP, various flavours
- CAS
- PostgreSQL

Authentication mechanisms
you know were your people is

SimpleSAML provides an extension mechanism that allows it to authenticate from

- LDAP, various flavours
- CAS
- PostgreSQL
- RADIUS

Authentication mechanisms
you know were your people is

SimpleSAML provides an extension mechanism that allows it to authenticate from

- LDAP, various flavours
- CAS
- PostgreSQL
- RADIUS
- PKI

Authentication mechanisms
you know were your people is

SimpleSAML provides an extension mechanism that allows it to authenticate from

- LDAP, various flavours
- CAS
- PostgreSQL
- RADIUS
- PKI
- self registration

Session management

SimpleSAMLphp inherits sessions from PHP

Session management
SimpleSAMLphp inherits sessions from PHP

Session storage is also extensible:

Session management
SimpleSAMLphp inherits sessions from PHP

Session storage is also extensible:

- PHP sessions

Session management
SimpleSAMLphp inherits sessions from PHP

Session storage is also extensible:

- PHP sessions
- memcache

Session management
SimpleSAMLphp inherits sessions from PHP

Session storage is also extensible:

- PHP sessions
- memcache

and allows for:

Session management
SimpleSAMLphp inherits sessions from PHP

Session storage is also extensible:

- PHP sessions
- memcache

and allows for:

- Single Sign On

Session management
SimpleSAMLphp inherits sessions from PHP

Session storage is also extensible:

- PHP sessions
- memcache

and allows for:

- Single Sign On
- Single Log Out

Session management
SimpleSAMLphp inherits sessions from PHP

Session storage is also extensible:

- PHP sessions
- memcache

and allows for:

- Single Sign On
- Single Log Out
- attribute caching

Shall we use a framework?
or we better have more developers

Shall we use a framework?
or we better have more developers

Why doesn't SimpleSAMLphp use a framework?

Shall we use a framework?
or we better have more developers

Why doesn't SimpleSAMLphp use a framework?

+ There are many good PHP frameworks

Shall we use a framework?
or we better have more developers

Why doesn't SimpleSAMLphp use a framework?

+ There are many good PHP frameworks
- None of them is the best one

Shall we use a framework?
or we better have more developers

Why doesn't SimpleSAMLphp use a framework?

+ There are many good PHP frameworks
- None of them is the best one
- It increases developers learning curve

Shall we use a framework?
or we better have more developers

Why doesn't SimpleSAMLphp use a framework?

+ There are many good PHP frameworks
- None of them is the best one
- It increases developers learning curve
- They increase the installation

Shall we use a framework?
or we better have more developers

Why doesn't SimpleSAMLphp use a framework?

+ There are many good PHP frameworks
- None of them is the best one
- It increases developers learning curve
- They increase the installation

Therefore SimpleSAMLphp does not use frameworks so it is simple to deploy and develop for

Can it grow?
SimpleSAML can cover almost any need

Can it grow?
SimpleSAML can cover almost any need

Scaling is *simpler* for simple products

Can it grow?
SimpleSAML can cover almost any need

Scaling is *simpler* for simple products

from simple

Can it grow?
SimpleSAML can cover almost any need

Scaling is *simpler* for simple products

from simple

Can it grow?
SimpleSAML can cover almost any need

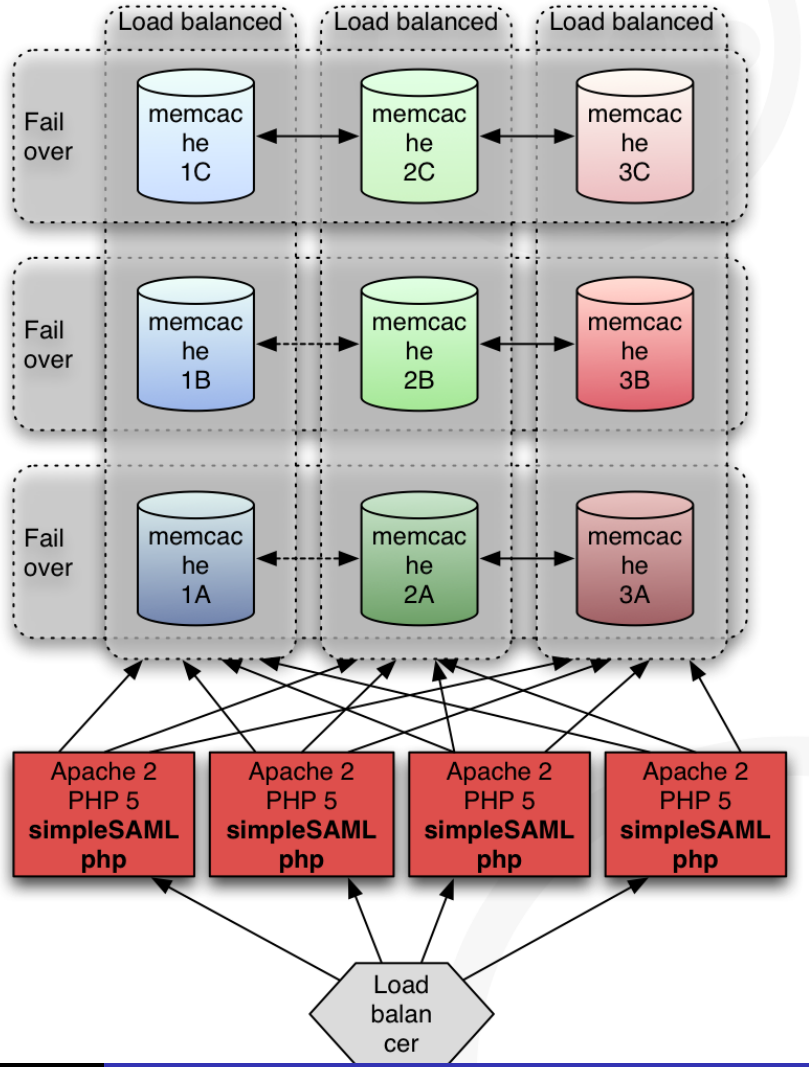
Scaling is *simpler* for simple products

to not so simple

Can it grow?
SimpleSAML can cover almost any need

Scaling is *simpler* for simple products

to not so simple



XML Protocols
simplifying complexity

SimpleSAMLphp handles XML with its usual simplicity

XML Protocols
simplifying complexity

SimpleSAMLphp handles XML with its usual simplicity

- Text templates for sending

XML Protocols
simplifying complexity

SimpleSAMLphp handles XML with its usual simplicity

- Text templates for sending
  simple to fill with attributes and parameters

XML Protocols
simplifying complexity

SimpleSAMLphp handles XML with its usual simplicity

- Text templates for sending
  simple to fill with attributes and parameters
- XPath for receiving

SimpleSAMLphp handles XML with its usual simplicity

- Text templates for sending
  simple to fill with attributes and parameters
- XPath for receiving
  flexible and effective, take what you need, ignore the rest

Metadata management

SimpleSAMLphp simplifies metadata management

SimpleSAMLphp metadata management is really modern

Metadata management
SimpleSAMLphp simplifies metadata management

SimpleSAMLphp metadata management is really modern

- IdPs and SPs produce their metadata *on the fly*

Metadata management
SimpleSAMLphp simplifies metadata management

SimpleSAMLphp metadata management is really modern

- IdPs and SPs produce their metadata *on the fly*
- Pre-installed metadata for some federations

Metadata management
SimpleSAMLphp simplifies metadata management

SimpleSAMLphp metadata management is really modern

- IdPs and SPs produce their metadata *on the fly*
- Pre-installed metadata for some federations
- Dynamic metadata are in the pipeline

Community
users are developers

Community
users are developers

SimpleSAMLphp is an OpenSource project, thus

Community
users are developers

SimpleSAMLphp is an OpenSource project, thus

- Everybody can participate

Community
users are developers

SimpleSAMLphp is an OpenSource project, thus

- Everybody can participate
- Users help other users

Community
users are developers

SimpleSAMLphp is an OpenSource project, thus

- Everybody can participate
- Users help other users
- Users can influence development

Community
users are developers

SimpleSAMLphp is an OpenSource project, thus

- Everybody can participate
- Users help other users
- Users can influence development
- Many of us have contributed to some extent

Who is using it?
SimpleSAMLphp extends like a bush fire

Who is using it?
SimpleSAMLphp extends like a bush fire

SimpleSAMLphp users number grows daily

Who is using it?
SimpleSAMLphp extends like a bush fire

SimpleSAMLphp users number grows daily

- FEIDE(.no)

Who is using it?
SimpleSAMLphp extends like a bush fire

SimpleSAMLphp users number grows daily

- FEIDE(.no)
- WAYF.dk

Who is using it?
SimpleSAMLphp extends like a bush fire

SimpleSAMLphp users number grows daily

- FEIDE(.no)
- WAYF.dk
- SWAMI(.se)

Who is using it?
SimpleSAMLphp extends like a bush fire

SimpleSAMLphp users number grows daily

- FEIDE(.no)
- WAYF.dk
- SWAMI(.se)
- Kalmar(.dk+.fi+.no+.se)

Who is using it?
SimpleSAMLphp extends like a bush fire

SimpleSAMLphp users number grows daily

- FEIDE(.no)
- WAYF.dk
- SWAMI(.se)
- Kalmar(.dk+.fi+.no+.se)
- DFN-AAI(.de)

Who is using it?
SimpleSAMLphp extends like a bush fire

SimpleSAMLphp users number grows daily

- FEIDE(.no)
- WAYF.dk
- SWAMI(.se)
- Kalmar(.dk+.fi+.no+.se)
- DFN-AAI(.de)
- CONFIA(.es)

Who is using it?
SimpleSAMLphp extends like a bush fire

SimpleSAMLphp users number grows daily

- FEIDE(.no)
- WAYF.dk
- SWAMI(.se)
- Kalmar(.dk+.fi+.no+.se)
- DFN-AAI(.de)
- CONFIA(.es)
- A bunch of americans

Who is using it?
SimpleSAMLphp extends like a bush fire

SimpleSAMLphp users number grows daily

- FEIDE(.no)
- WAYF.dk
- SWAMI(.se)
- Kalmar(.dk+.fi+.no+.se)
- DFN-AAI(.de)
- CONFIA(.es)
- A bunch of americans
- ...

Summary

SimpleSAMLphp

- is simple to use and deploy

Summary

SimpleSAMLphp

- is simple to use and deploy
- allows for fast federation building

Summary

SimpleSAMLphp

- is simple to use and deploy
- allows for fast federation building
- multiprotocol

Summary

SimpleSAMLphp

- is simple to use and deploy
- allows for fast federation building
- multiprotocol
- multilingual

Summary

SimpleSAMLphp

- is simple to use and deploy
- allows for fast federation building
- multiprotocol
- multilingual
- http://rnd.feide.no/simplesamlphp

Hard work
let's get our hands dirty

Hard work
let's get our hands dirty

What will we try to achieve today?

Hard work
let's get our hands dirty

What will we try to achieve today?

- Install simpleSAMLphp

Hard work
let's get our hands dirty

What will we try to achieve today?

- Install simpleSAMLphp
- Get an IdP running

Hard work
let's get our hands dirty

What will we try to achieve today?

- Install simpleSAMLphp
- Get an IdP (or many) running

Hard work
let's get our hands dirty

What will we try to achieve today?

- Install simpleSAMLphp
- Get an IdP (or many) running
- Write an authentication module

Hard work
let's get our hands dirty

What will we try to achieve today?

- Install simpleSAMLphp
- Get an IdP (or many) running
- Write an authentication module
- Set up some simple services

Hard work
let's get our hands dirty

What will we try to achieve today?

- Install simpleSAMLphp
- Get an IdP (or many) running
- Write an authentication module
- Set up some simple services
- Build one federation

Hard work
let's get our hands dirty

What will we try to achieve today?

- Install simpleSAMLphp
- Get an IdP (or many) running
- Write an authentication module
- Set up some simple services
- Build, at least, one federation

Hard work
let's get our hands dirty

What will we try to achieve today?

- Install simpleSAMLphp
- Get an IdP (or many) running
- Write an authentication module
- Set up some simple services
- Build, at least, one federation
- Set up a more complex service

Hard work
let's get our hands dirty

What will we try to achieve today?

- Install simpleSAMLphp
- Get an IdP (or many) running
- Write an authentication module
- Set up some simple services
- Build, at least, one federation
- Set up a more complex service
- Modify attributes on the fly

Hard work
let's get our hands dirty

What will we try to achieve today?

- Install simpleSAMLphp
- Get an IdP (or many) running
- Write an authentication module
- Set up some simple services
- Build, at least, one federation
- Set up a more complex service
- Modify attributes on the fly
- Manage user consent

Hard work
let's get our hands dirty

What will we try to achieve today?

- Install simpleSAMLphp
- Get an IdP (or many) running
- Write an authentication module
- Set up some simple services
- Build, at least, one federation
- Set up a more complex service
- Modify attributes on the fly
- Manage user consent
- Protect a non PHP app

Hard work
let's get our hands dirty

What will we try to achieve today?

- Install simpleSAMLphp
- Get an IdP (or many) running
- Write an authentication module
- Set up some simple services
- Build, at least, one federation
- Set up a more complex service
- Modify attributes on the fly
- Manage user consent
- Protect a non PHP app
- ...