

# Dynamic Identity Federation using Security Assertion Markup Language (SAML)

Md. Sadek Ferdous & Ron Poet

IDMAN 2013

9 April, 2013



University  
of Glasgow

School of  
Computing Science

# Introduction

- Dynamic Federation: Definition
- Trust issues involved
  - formulating novel trust assumptions
- Proof of concept
  - by extending existing works

# Background: Identity Federation

- From ITU-T X.1250: “An association of users, service providers and identity providers”.
  - Vague and sketchy.
- An identity federation:
  - A business model in which a group of two or more trusted (business) parties (legally) bind themselves with a business and technical contract to provide services to users.
- Also known as Federated Identities/Federation of Identities or more commonly Federated Identity Management (FIM).

# Background: Identity Federation

- Three different actors:
  - Identity Provider (IdP),
  - Service Provider (SP) and
  - User (Client)
- FIM offers several advantages:
  - For IdP and SP: improved security and privacy, etc.
  - For Users: Single Sign On (SSO) → less numbers of identity management.
- Two main types:

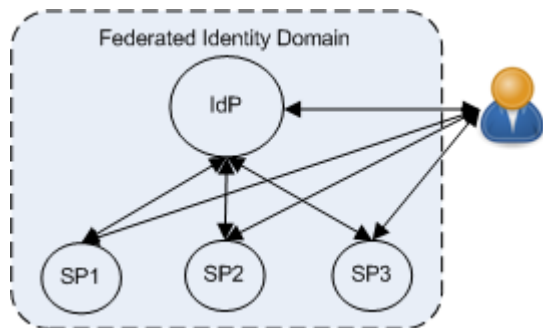


Figure 1: Type 1

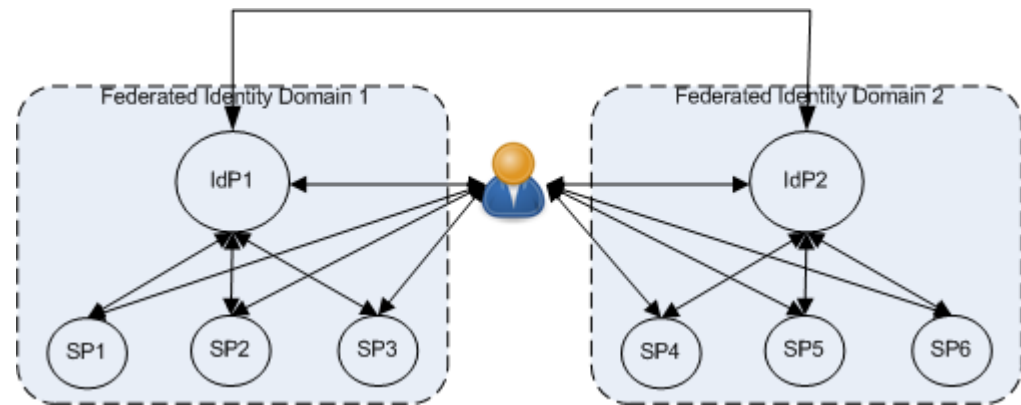


Figure 2: Type 2

# Background: Identity Federation

- The issue of trust is fundamental in FIM.
- The SP trusts the IdP:
  - to authenticate users appropriately and
  - to release attributes to the SP as per the agreement.
- The IdP trusts the SP:
  - not to abuse the released attributes and
  - to use them only for the stated purpose as per the agreement.
- Circle of Trust (CoT).

# Security Assertion Markup Language (SAML)

- SAML is based on:
  - an XML-based standard,
  - the request/response protocol.
- SP → IdP: SAML authentication request.
- IdP → SP: SAML response.
- SAML assertion: essence of the response:
  - containing user's identity information and attributes.

# Establishing Trust in SAML

- Trust in SAML: metadata exchange + Trust Anchor List (TAL).
- The IdP trusts only SPs in TAL and vice versa.
- Metadata is exchanged in out-of-bound fashion
  - Must be done before any interaction takes place.

# Establishing Trust in SAML

- Adding a new entity in a federation needs:
  - to exchange metadata between respective parties and
  - to update the repositories of metadata of each party.
- It becomes extremely difficult when:
  - the number of federations and the number of entities in each federation are large.
- Moreover, pre-configuring trust means:
  - Two prior unknown parties cannot federate.



# Previous Works

- Distributed Dynamic SAML proposal<sup>1</sup>:
  - sign the metadata,
  - include the X.509 certificate and
  - validate the signature using a root certificate and establish the trust.
- SAML Metadata Interoperability Profile: draft of a novel SAML Profile.
- A prototype of Dynamic SAML in the SimpleSAMLphp implementation.
  - Entity ID must be the URL from where metadata can be fetched.

[1]: Patrick Harding, Leif Johansson, Nate Klingenstein, "Dynamic Security Assertion Markup Language: Simplifying Single Sign-On," *IEEE Security & Privacy*, vol. 6, no. 2, pp. 83-85, March-April 2008, doi:10.1109/MSP.2008.31

# Previous Works

- Trust issues not considered:
  - Can the IdP trust SPs?
  - Can the SP trust IdPs?
- Static and Dynamic entities not distinguished.
- SimpleSAMLphp allows SPs to be added dynamically, not the other way around.
  - semi-automatic federation.

# Dynamic Federation

- A Dynamic Federation is a business model in which:
  - a group of two or more previously *unknown parties* federate together dynamically,
  - without any prior business and technical *contract*,
  - to allow users to access services under *certain conditions*.

# Entities in Dynamic Federation

- Fully Trusted Entities:
  - entities in the traditional SAML federation
  - a legal contract between the IdP and the SP.
- Semi-trusted Entities:
  - dynamically added SPs in a dynamic federation under some conditions
  - without the presence of any contract between them and to whom any user(or users) of the IdP has(have) agreed to release a subset of her(their) attributes.
- Untrusted Entities.
  - the dynamically added IdP and SP in a dynamic federation
  - under some conditions without the presence of any contract between them.

# Conditions in Dynamic Federation

- Only a valid user of the IdP can initiate dynamic federation:
  - by exchanging metadata mutually and storing in TALs.
- Such SPs tagged as untrusted entities in the IdP initially.
  - releasing user attributes to the SP promotes it to a semi-trusted entity.
- Such IdPs tagged as untrusted entities in the SP.
- No attributes should be released to an untrusted entity.

# Conditions in Dynamic Federation (contd..)

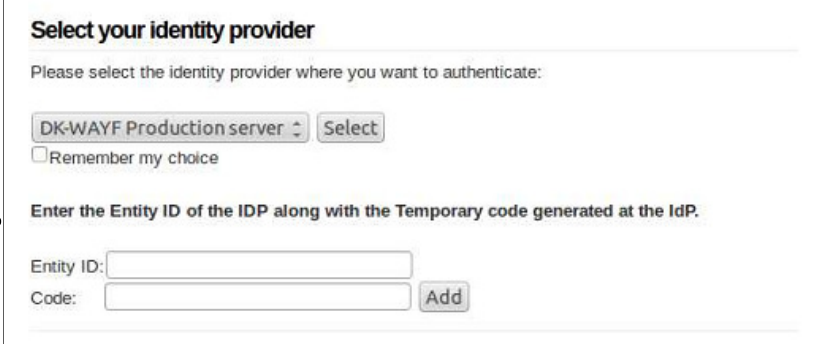
- Crucial and sensitive attributes may not be released to any semi-trusted entity.
  - administrators can configure such attributes.
- SP decides how to treat attributes from an untrusted IdP.
- The NIST LoA (Level of Assurance or Level of Authentication) value of 1 to 4.

# Proof of Concept: IdP-SP Scenario

- Based on the modified SimpleSAMLphp implementation.
- IdP uses a MySQL database at its end:
  - two tables called “semitrusted” and “untrusted” to store the Entity ID of semi-trusted and untrusted SPs respectively.
- SP uses another MySQL database at its end:
  - a table called “untrusted” to store the Entity IDs of untrusted IdPs.
- A configuration parameter called ‘semitrusted.sp’ is used to filter out attributes:
  - ‘semitrusted.sp’=> array (‘username’, ‘name’, ‘telephone’, ‘age’, ‘position’, ‘org’); (email and salaryGrade excluded);

# IdP-SP Scenario: Protocol Flow

- The user visits the SP to access a resource.
- The user is forwarded to the WAYF.
- Since the user's IdP is not listed (Figure 3), she wants to add the IdP dynamically. She needs the Entity ID and a Code.



**Select your identity provider**

Please select the identity provider where you want to authenticate:

DK-WAYF Production server

Remember my choice

Enter the Entity ID of the IDP along with the Temporary code generated at the IdP.

Entity ID:

Code:

Figure 3: Options for Dynamic Federation in WAYF

- The user visits the IdP and logs in there and generates a 4-digit random number and can view the IdP's Entity ID.
- The respective values are added and the user clicks the Add button.
- A request to exchange metadata is sent to the Entity ID of the IdP along with some parameters (e.g. the Entity ID of the SP).



# IdP-SP Scenario: Protocol Flow (contd..)

- The IdP validates the code and fetches the metadata of the SP from the specified location.
- The metadata is added to its TAL and the SP is tagged as the untrusted entity initially.
- Then the IdP returns its metadata to the SP.
- The metadata is added to SP's TAL and the IdP is tagged as the untrusted entity.
- The user is forwarded to the WAYF page (Figure 4).

**Select your identity provider**

Please select the identity provider where you want to authenticate:

Untrusted: <https://192.168.1.115/simplesaml/saml2/idp/metadata.php>

Remember my choice

Enter the Entity ID of the IDP along with the Temporary code generated at the IdP.

Entity ID:

Code:

This is the list of dynamically added IdPs into this SP. While adding another IdP, please make sure that you do not try to add the same IdP into this SP.

- <https://192.168.1.115/simplesaml/saml2/idp/metadata.php>

Figure 4: Added IdP shown in WAYF

# IdP-SP Scenario: Protocol Flow (contd..)

- The user chooses her IdP and the usual SAML authentication phase is initiated.
- Once the user is authenticated, a Consent Page (Figure 5) is shown where she can choose attributes.
- Once she clicks the “Yes, continue” button, the SP is promoted to the “semitrusted” table in database.
- A SAML response with the assertion is sent back to the SP.
- Since the assertion is from untrusted IdP, the SP implicitly considers the assertion has a lower value of 1 and takes authorisation decision.

https://192.168.1.85/simplesaml/module.php/saml/sp/metadata.php/default-sp requires that the information below is transferred.

Since https://192.168.1.85/simplesaml/module.php/saml/sp/metadata.php/default-sp is a semi-trusted SP, some attributes have been excluded. The excluded attribute(s) is/are:email, salarygrade,

**Information that will be sent to https://192.168.1.85/simplesaml/module.php/saml/sp/metadata.php/default-sp**

<input type="checkbox"/> username:ripul
<input type="checkbox"/> name:Ripul Test
<input type="checkbox"/> telephone:01234445566
<input type="checkbox"/> age:34
<input type="checkbox"/> position:Student
<input type="checkbox"/> org:University of Glasgow

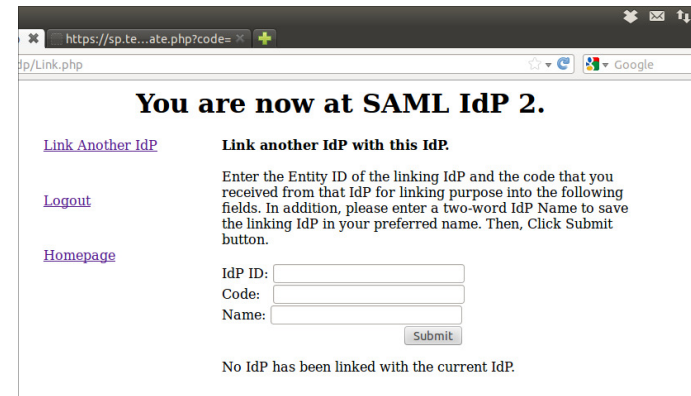
Figure 5: Consent Page at the untrusted IdP

# Proof of Concept: IdP-IdP-SP Scenario

- In the previous setting, the SP may not trust at all the untrusted IdP.
- As a solution, the IdP-IdP-SP scenario.
  - one is a highly trusted IdP and the another is the untrusted IdP, from the SP's perspective.
- The highly trusted IdP: acting as the proxy IdP to the SP and the semi-trusted SP to the untrusted IdP.
- The untrusted IdP: acting as the untrusted IdP to the proxy IdP and an authentication source to the proxy IdP.

# IdP-IdP-SP Scenario: Protocol Flow

- The user visits the untrusted IdP, logs in and generates a 4-digit random code, like before.
- The user visits the proxy IdP, logs in and clicks the “Link Another IdP” option and the user is presented with a form (Figure 6).
- The user provides the Entity ID of the untrusted IdP, the generated code and a Petname for the untrusted IdP.
- Once the submit button is clicked, the previously described flow for Dynamic Federation takes place.
- At the end, metadata of both entities are exchanged and stored in the respective TALs.



The screenshot shows a web browser window with the address bar containing a URL starting with 'https://sp.te...ate.php?code='. The page title is 'You are now at SAML IdP 2.'. On the left side, there are three links: 'Link Another IdP', 'Logout', and 'Homepage'. The main content area is titled 'Link another IdP with this IdP.' and contains the following text: 'Enter the Entity ID of the linking IdP and the code that you received from that IdP for linking purpose into the following fields. In addition, please enter a two-word IdP Name to save the linking IdP in your preferred name. Then, Click Submit button.' Below this text are three input fields labeled 'IdP ID:', 'Code:', and 'Name:'. A 'Submit' button is located to the right of the 'Name:' field. At the bottom of the form, there is a message: 'No IdP has been linked with the current IdP.'

Figure 6: Options to link another IdP

# IdP-IdP-SP Scenario: Protocol Flow (Contd...)

- The user visits the SP to access its resources.
- The user is forwarded to the WAYF.
- The user selects the proxy IdP.
- The user is forwarded to the proxy IdP with a SAML Authentication request.
- The user is presented with available authentication sources (Figure 7). The “My-IdP” in Figure 7 represents the linked untrusted IdP.

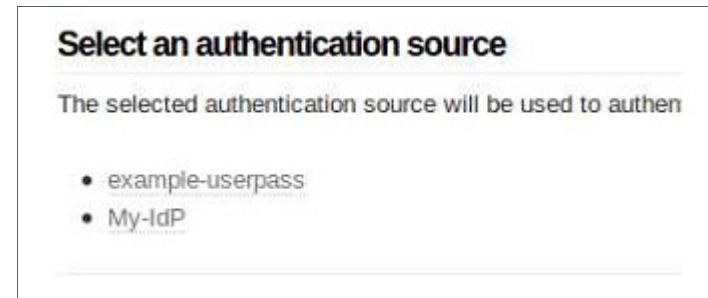


Figure 7: The added IdP as the auth source

## IdP-IdP-SP Scenario: Protocol Flow (Contd...)

- The user chooses the untrusted IdP.
- At this point, the usual SAML protocol flow takes place.
- The proxy IdP receives the user attributes from the untrusted IdP.
- It then Creates a SAML assertion with these attributes with a LoA value of 1 and forwards to the SP.
- The SP takes the authorisation decision.

# Discussions

- Dynamic Federation: federations just in time and whenever required.
- Using separate trust domains inside a federation:
  - a federation can host all types and
  - leverage the advantages of all.
- Allowing users to link two IdPs:
  - Can a Personal IdP (IdP installed in the user's PC) be used to provide some user attributes?
- The possibility of attribute aggregation from different sources.

# Conclusions

- Dynamic Federation – definition.
- Trust issues involved:
  - Trusted, semi-trusted and untrusted entities.
  - Underlying conditions.
- Proof-of-concept:
  - IdP-SP scenario
  - IdP-IdP-SP scenario.
- The end thought:
  - Relaxing trust requirements.
  - But how much? - answer depends on an application scenario.



Thank you!