Enabling SAML for Dynamic Identity Federation Management

Patricia Arias, Florina Almenárez, Andrés Marín and Daniel Díaz-Sánchez

University Carlos III of Madrid

http://pervasive.gast.it.uc3m.es/

WMNC'2009

Second Joint IFIP Wireless and Mobile Networking Conference

September 9-11, 2009 – Gdańsk, Poland

IN THIS TALK

Introduction
- ¿What is Identity Federation?

Background
- Current Id-Federation frameworks

Underlying Trust Models
- Comparison
- Challenges
- Related Work

SAML extension

Conclusions & Future work

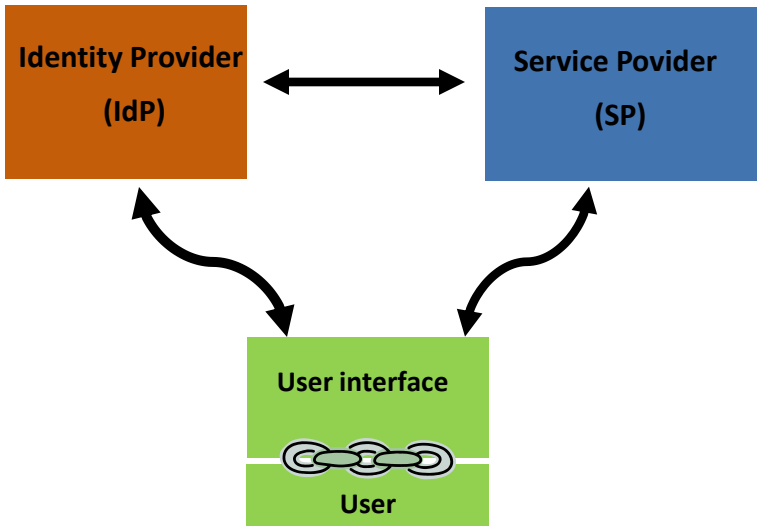
¿What is Identity Federation?

- **Federation:**

Share and distribute attributes and identity information across different administrative domains according to certain established policies

Use Cases: single-sign-on, attribute exchange, account linkage

- **Components:** IdPs, SPs and Users

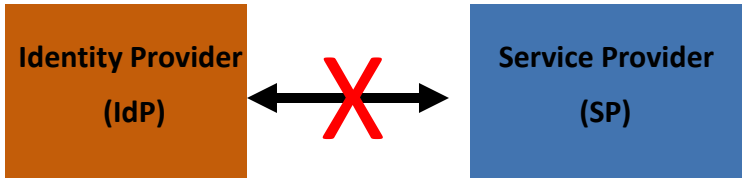


- **Advantages:**
  - User: better user experience
  - Service Providers: personalization, intelligent transactions, complexity and cost reduction

MOTIVATION

Trust models in today identity federation frameworks:

CASE 1: NO trust



Problems NO SECURITY

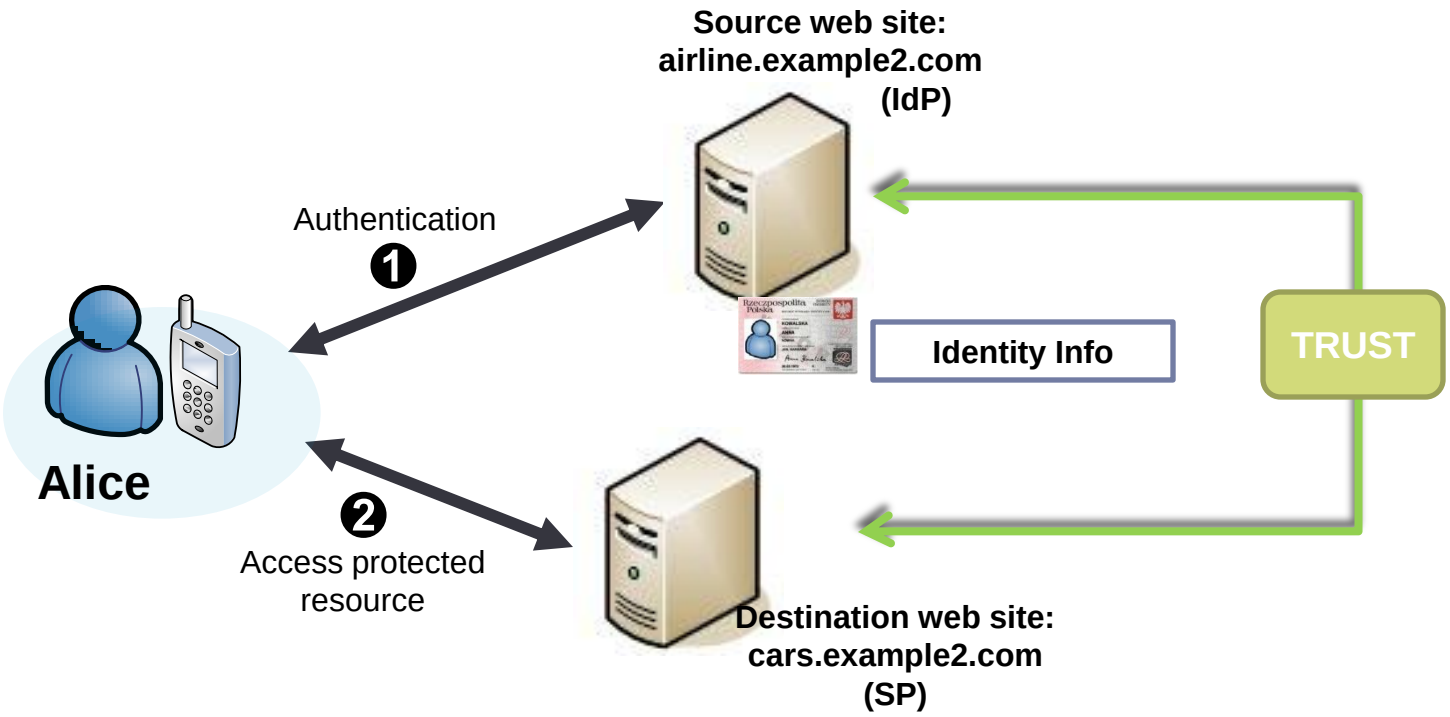
CASE 2: RIGID trust

Problems flexibility, complexity, scalability

An extension is required to allow flexible relationships and facilitate cooperation

Common example: Single-Sign-On

Allows users to authenticate at a single site and gain access to multiple sites in a federation without providing any additional information



OUTLINE

- **Introduction**
  - ¿What is Identity Federation?
- **Background**
  - Current Id-Federation frameworks
- **Underlying Trust Models**
  - Comparison
  - Challenges
  - Related Work
- **SAML extension**
- **Conclusions & Future work**

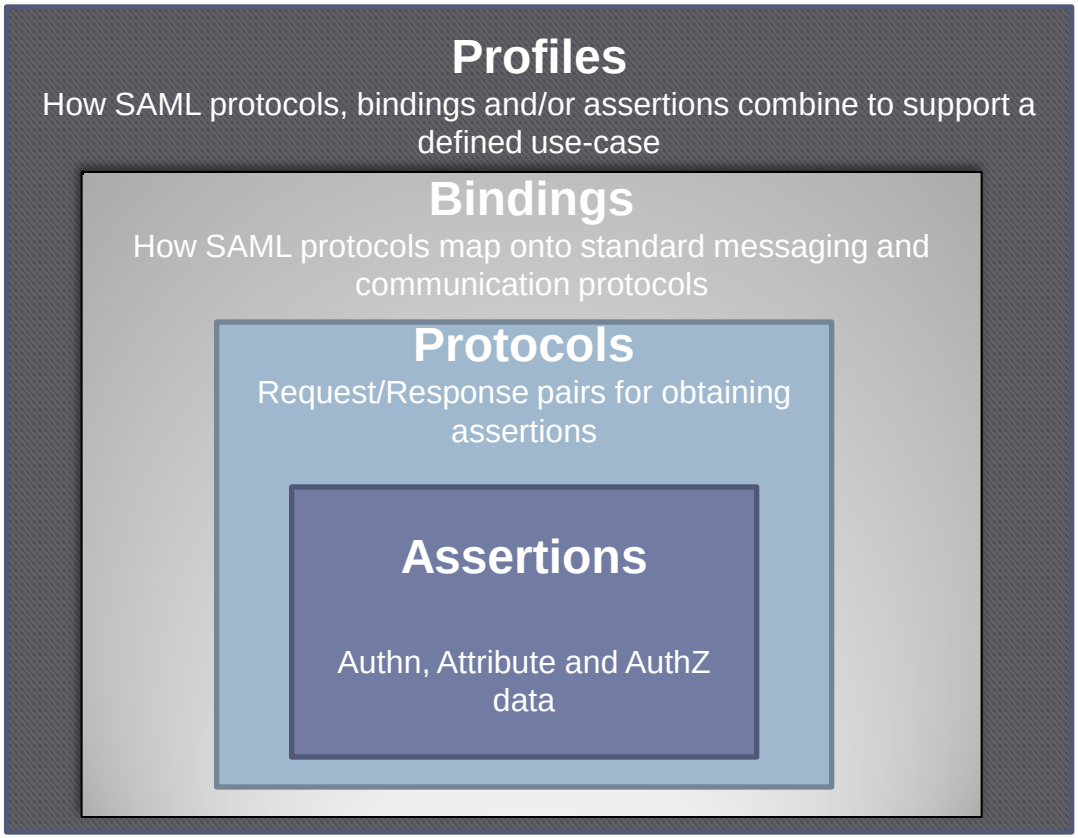
Federation Frameworks

- Identity federation can be accomplished by different means:
  - **SAML** (Security Assertion Markup Language), OASIS 2005 (v2.0)
  - **OpenID**, OpenID Foundation 2005
  - **Identity Federation Framework (ID-FF)**, Liberty Alliance, 2003
  - **WS-Federation**, Alliance of companies 2006

SAML

According to the specs., SAML:

defines an XML based framework to allow the exchange of security assertions between entities



Four main components

❶ **Assertions**
❷ **Protocols**
❸ **Bindings**
❹ **Profiles**

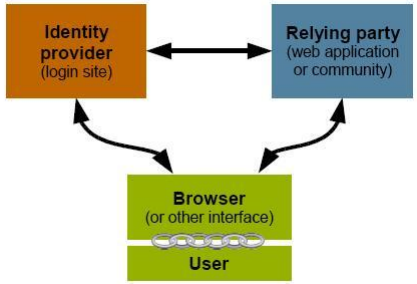
And also:

- **Metadata:** to specify configuration information
- **Authentication context:** to provide extra info about the auth. process

OUTLINE

- **Introduction**
  - ¿What is Identity Federation?
- **Background**
  - Current Id-Federation frameworks
- **Underlying Trust Models**
  - Comparison
  - Challenges
  - Related Work
- **SAML extension**
- **Conclusions & Future work**

COMPARISON



IdM technology	Trust Model
SAML	PKI recommended. Typically implemented with trust lists
OpenID	**No trust model** *trust-all-comers philosophy,* no preconfiguration required
Liberty Alliance	Trust architecture based on CoTs. Follows SAML recommendation (PKI). Typically implemented with trust lists.
WS-Federation	Trust arch. based on WS-Trust. Typically implemented with trust lists

Limitations

Current frameworks are not suitable for dynamic environments:

- trust model poorly defined or out of the specifications scope
- tipically rely on PKI (implementations with trust lists)
- dependence on preconfiguration

Challenges: Dynamic Federation

We need to **modify the underlying trust models** to:

- make trust establishment more agile
- minimize dependences on central admin. or preconfiguration
- Take advantage of common knowledge
- Model trust evolution over time (risk management)

RELATED WORK

- 2008: Internet2, PingIdentity, Stockholm University

  Distributed and Dynamic SAML. Centered around discovery and easiness of configuration. Ligther federation process, but only considers certificate based trust, and is oriented to web SSO

- 2008: L.Boursas, Munich University of Technology

  Dynamic management and expansion of CoTs. Does not address the exchange of trust information over federation protocols

- 2009: U.Kylau, Hasso Plattner Institute

  Identify possible trust patterns in identity federation topologies

Problems: lack of general solution, not all aspects of trust are covered

Requirements

- Extend SAML:
  - In a generic way
  - Maintaining backwards compatibility
  - Allowing Dynamic Federation

- Design and incorporate dynamic trust models in order to facilitate the interaction between different actors involved in an IdM system.

OUTLINE

- **Introduction**
  - ¿What is Identity Federation?
- **Background**
  - Current Id-Federation frameworks
- **Underlying Trust Models**
  - Comparison
  - Challenges
  - Related Work
- **SAML extension**
- **Conclusions & Future work**

SAML EXTENSION FOR DYNAMIC FEDERATION

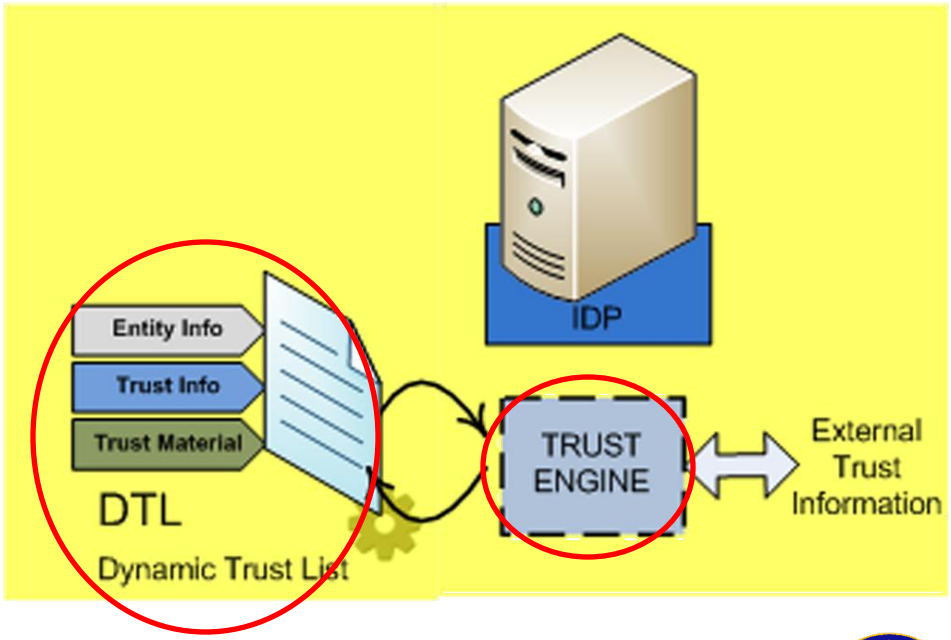
Idea: enrich trust mechanisms, allow the collection of external information, maintain an automatic and dynamic store

Trust engine:

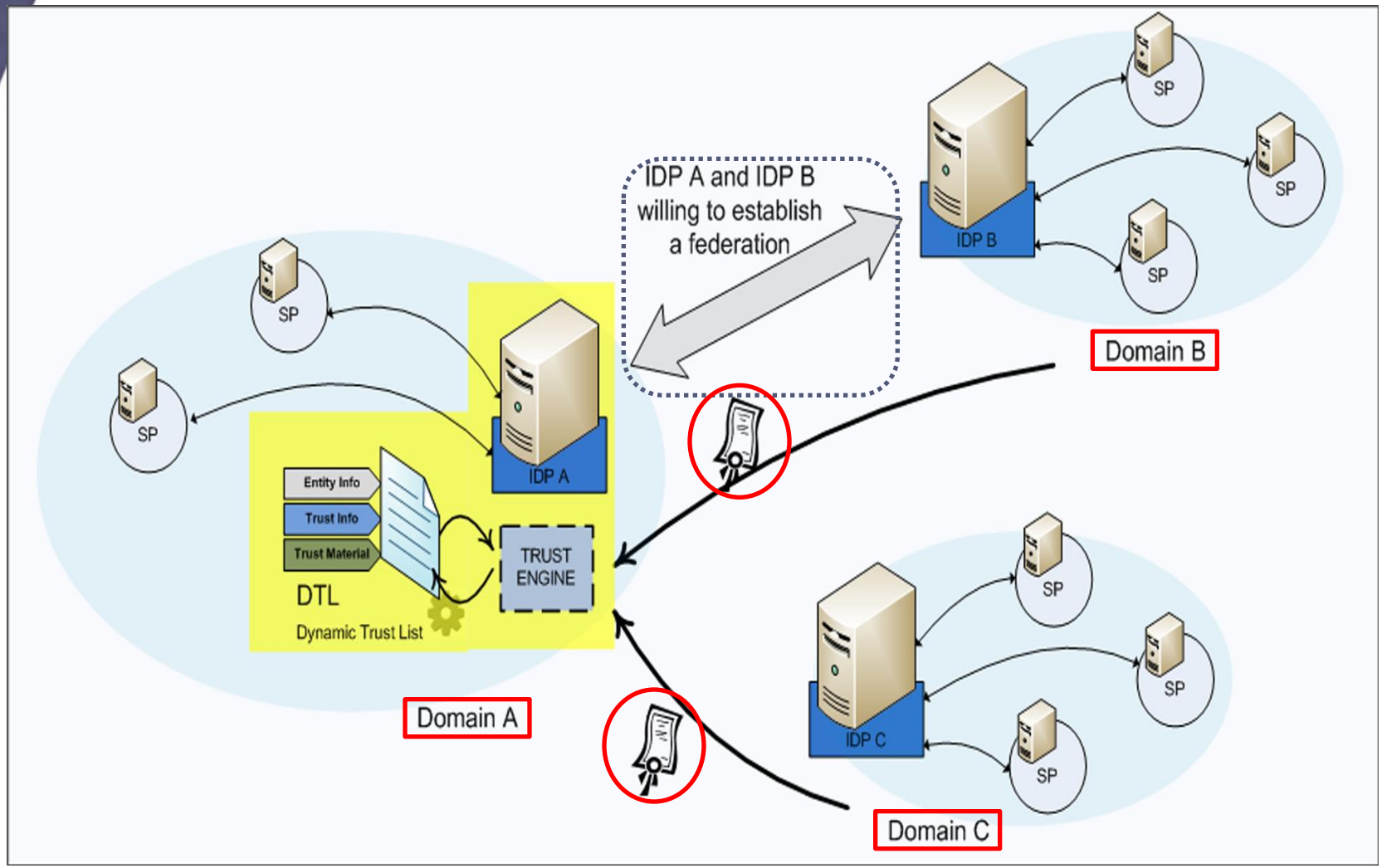
- processes external and internal trust information
- performs DTL updating
- makes decision to trust

Dynamic Trust List (DTL):

is automatically updated according to the establishment and **evolution** of trust relationships



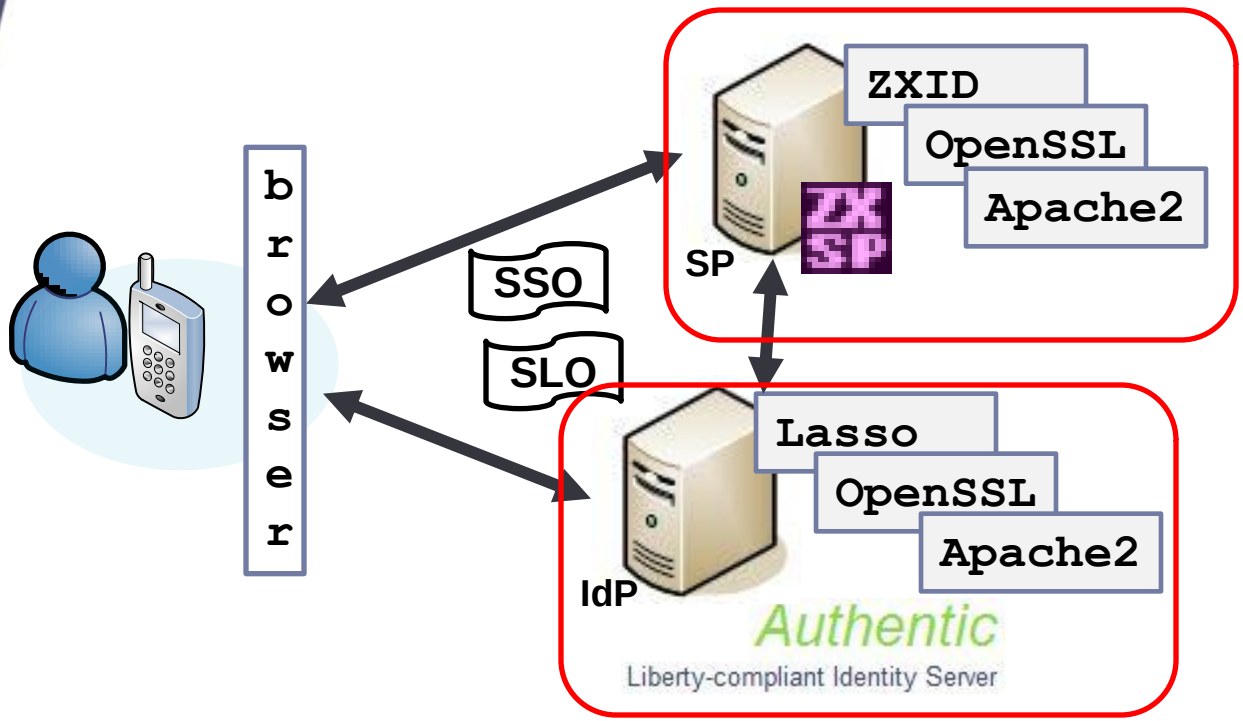
SAML extension: use case



IMPLEMENTATION ISSUES

- **SP** → ZXID: light open C library, implements full SAML 2.0 stack
- **IdP** → Authentic, based on the `lasso` library, supports SAML 2.0 specs

Test Scenario Architecture



Results so far:

- Single Sign-On
- Single Log Out
- LDAP
- WSP-API

Work in Progress:

- Trust engine
- DTLs
- Reputation Protocol

OUTLINE

Introduction

- ¿What is Identity Federation?

Background

- Current Id-Federation frameworks

Underlying Trust Models

- Comparison
- Challenges
- Related Work

SAML extension

Conclusions & Future work

CONCLUSIONS

- We have:
  - Analyzed the main current frameworks to achieve identity federation
  - Identified trust management requirements in dynamic environments
  - Proposed a SAML extension to overcome challenges and to enrich trust decisions
  - Deploy an Identity Management infraestructure
- SAML is the only standard, and offers flexibility, abstraction and modularity. Also, it is the more popular and deployed.

FUTURE WORK

- We are implementing the proposed extension by completing these tasks:
  - Adding Trust Engine and DTLs
  - Defining messages and protocols to exchange reputation data
- As future work we aim to:
  - perform evaluation experiments
  - model trust evolution
  - add risk analysis functionality

Dziękuję!

(Thanks!)

Questions?