

# Identity Dashboard System and Architecture

Jonathan Scudder  
Department of Informatics  
University of Oslo, Norway

Audun Jøsang  
UNIK Graduate Center  
University of Oslo, Norway

E-mail: josang@unik.no

## Abstract

Current SSO identity management solutions for open networks do not solve the scalability problems for users despite their promises. In some cases it might even increase the identity management complexity that users need to handle. This paper describes the identity dashboard architecture which is a user-centric architecture for identity management.

## Categories and Subject Descriptors

H.4 [Information Systems Applications]: Miscellaneous; D.2.8 [Software Engineering]: Metrics—complexity measures, performance measures

## Keywords

Identity management, federation, SSO, single sign on, usability, security, authentication, SAML

## 1. Introduction

Digital identities represent who we are when engaging in online activities and transactions. The rapid growth in the number of online services leads to an increasing number of different identities that each user needs to manage. As a result, many people feel overloaded with identities and suffer from password fatigue. This is a serious problem and makes people unable properly control and protect their digital identities against identity theft. This paper introduces the identity dashboard system. Sec.2.1 describes the federated identity management model.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

IdTrust 2009 Gaithersburg MD, USA

Copyright 200X ACM X-XXXXX-XX-X/XX/XX ...\$5.00.

## 2. Existing User Identity Management Models

### 2.1 The Federated SSO Identity Model

Federated identity models are based on groups of SPs that enter into a mutual security and authentication agreement in order to allow user SSO to their services. In the terminology of the Liberty Alliance, these groups are called *circles of trust* [1].

Identity federation can thus be defined as a set of agreements, standards and technologies that enable SPs to recognise user identities and entitlements from other SPs.

As in the silo identity model, each SP manages the name space of all its users. Various silo identity domains are then linked together to form a federated domain. In practice, the different domain specific identifiers of each user are mapped, as illustrated in Fig.1. This makes it possible for different SPs to refer to the same user with different identifiers. For authentication purposes, an SP will accept a *security assertion* [2] from another SP claiming that a given user has already been authenticated.

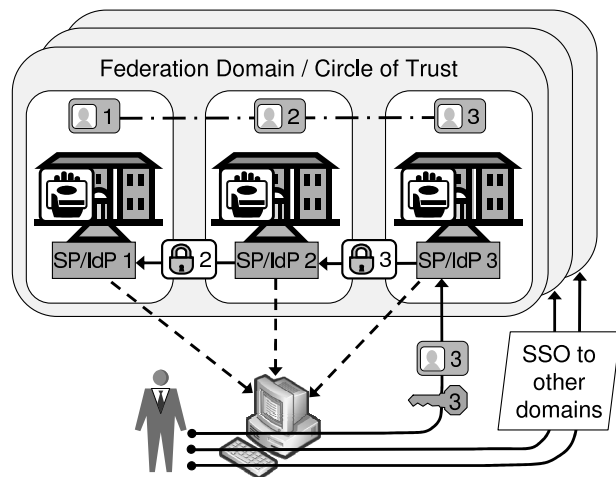


Figure 1. Federated user identity domains

The main advantage of the federated identity model is that it

provides SSO in open environments. The federated model is compatible with, and can be retrofitted to the traditional silo model. SPs can thus keep existing name spaces and authentication systems.

The main disadvantage is that it creates legal and technical complexity. For example, SPs are technically speaking not able to distinguish between a security assertion that reflects a genuine user service request, or one that represents a SP masquerading as a user. SPs must therefore trust security assertions from each other. In addition, the mapping between identifiers will technically speaking allow SPs to correlate information about the same user, which could represent a privacy threat. Users must therefore trust SPs to protect their privacy in this respect.

From a privacy perspective, a federated model can be both an advantage and a disadvantage. Different SPs within the same federation domain are technically able to match personal information of the same user because of the mapping between identifiers. The privacy protection thus depends on the privacy policy and the adherence to the policy, which can pose a threat. On the other hand, a user's identity within a specific SP's silo domain can be anonymous, and only the "home" SP needs to know the real world identity of the user. This can provide additional privacy protection.

Federated identity domains can not solve the scalability problem for the users. By assuming that multiple federated identity domains will exist, a user will most likely access SPs from different domains, and will therefore have to authenticate with the respective IdPs from each domain. The problem of password fatigue will thus remain, illustrated by the multiple login requests originating from the user in Fig.1, and this violates security usability principles. This is thus a model that can provide SSO within each federated identity domain, but not across multiple federated domains.

### 3. Conclusion

### 4. References

- [1] Liberty-Alliance. *Liberty ID-FF Architecture Overview*. Version: 1.2-errata-v1.0. <http://www.projectliberty.org/specs/liberty-idff-arch-overview-v1.2.pdf>, 2003.
- [2] OASIS. *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. Organization for the Advancement of Structured Information Standards, OASIS Standard, 15 March 2005.