# A Modeling Approach to Federated Identity and Access Management

Martin Gaedke
University of Karlsruhe
Engesserstr. 4
76128 Karlsruhe, Germany
+49 (721) 608-8076
gaedke@tm.uka.de

Johannes Meinecke
University of Karlsruhe
Engesserstr. 4
76128 Karlsruhe, Germany
+49 (721) 608-8072
meinecke@tm.uka.de

Martin Nussbaumer
University of Karlsruhe
Engesserstr. 4
76128 Karlsruhe, Germany
+49 (721) 608-8073
nussbaumer@tm.uka.de

## ABSTRACT

As the Web is increasingly used as a platform for heterogeneous applications, we are faced with new requirements to authentication, authorization and identity management. Modern architectures have to control access not only to single, isolated systems, but to whole business-spanning federations of applications and services. This task is complicated by the diversity of today's specifications concerning e.g. privacy, system integrity and distribution in the web. As an approach to such problems, in this paper, we introduce a solution catalogue of reusable building blocks for Identity and Access Management (IAM). The concepts of these blocks have been realized in a configurable system that supports IAM solutions for Web-based applications.

## Categories and Subject Descriptors

D.2.13 [**Software Engineering**]: Reusable Software – *Reuse models*; K.6.5 [**Management of computing and information systems**]: Security and Protection – *Authentication*

## General Terms

Management, Design, Security

## Keywords

Security, Identity and Access Management, Federation, Reuse

## 1. INTRODUCTION

The task of constructing Web-based applications and systems is scientifically founded on the discipline *Web Engineering*. Among the many aspects to be considered is the control of accesses to the system as well as the related management of identities. Today we are faced with a large number of heterogeneous, partly Web-based business applications from different companies. Many products implement their own access control mechanisms, leading to the challenge of managing a company's overall security policy and raising unnecessary costs. Even more difficulties have to be overcome when applications under the control of different organizations are involved. These problems have been recognized [2] and resulted in standardization efforts aimed at the construction of systems that are interoperable in terms of security. The principal idea behind such solutions is to make use of Web service technology to separate authentication and authorization mechanisms from the applications themselves. In this context, the Security Assertion Markup Language (SAML) has been specified by OASIS as an XML-based notation for exchanging security-relevant information. Moreover, the Liberty Alliance project is concerned with standardized mechanisms for discovering and offering identity-related services and applications. Furthermore, WS-Federation defines access profiles that describe, how and in which order the messages necessary for a federated authorization process are exchanged between the involved browsers, clients and servers. Because of the high number of different aspects to be concerned, like security technologies, cryptographic algorithms, and communication protocols, solutions based on those standards entail a high degree of complexity, demanding for abstraction. In this paper, we therefore introduce a catalogue of reusable building blocks based on a simple, extendable model. The building blocks provide solutions to common problems using concepts from security and federation specifications. They have also laid the foundation for a configurable system (idFS), which supports the establishment of a uniform Web access control infrastructure.

## 2. FIM – FEDERATED IDENTITY MODEL

In order to provide notations for modeling the IAM infrastructure on an abstract level, we developed the Federated Identity Model (FIM). As an extendable modeling framework based on UML class diagrams, it abstracts from actual technologies in favor of a view that is centered on potential system configurations. The main modeling elements include the resources to be protected (i.e. Web applications and services) and the *security token services* (STS), which act as separate services for issuing security-relevant statements (so-called *security tokens*). These statements relate either to authenticated identities of requesting clients (in the case of *identity providers*) or to access privileges on the resources (in the case of *resource STS*). Between the system elements, trust relationships can be defined to model that one element relies on the digitally signed statements of another element. In particular, this relationship can also span multiple organizations to realize federations of trust. In such scenarios, all services and applications under the control of one federation partner are grouped into a *security realm*. Additional modeling classes represent abstract modules and user interfaces that can be seen as separate system parts, with the configuration specifying the concrete algorithms and mechanisms to be used (like e.g. role-based authorization).

## 3. BUILDING BLOCK CATALOGUE

The outlined modeling framework potentially allows for the description of a wide range of scenarios. In the context of the mentioned identity management problems however, guidelines are required for building solutions in a high-quality and cost-effective way. Therefore, we present a catalogue of building blocks based on FIM. Similar to design patterns in Software Engineering [1], it

WWW 2005, May 10-14, 2005, Chiba, Japan.
ACM 1-59593-051-5/05/0005.

contains a statement of a certain problem together with a description of how to solve this problem as well as a discussion of the solution. In the following, we describe a selection of three building blocks out of our catalogue.

**Single Sign On (SSO)**: An organization runs several Web applications that require access control. Integrating IAM components into the applications would result in high management costs and inconveniences for the users who would have to remember all their credentials.

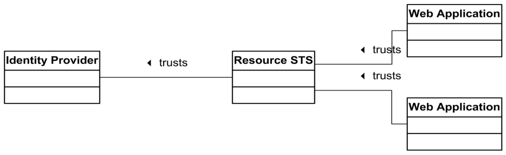

**Figure 1: Single Sign On**

As depicted in Figure 1, an IP and an STS is set up. The Web applications are all configured to send users requesting protected resources to the STS by performing an HTTP redirect. The STS redirects the user again, now to its configured IP that displays a sign-in form. In case valid credentials have been supplied, a security token is generated and passed on to the STS. The STS determines the permissions for the identity stated in the incoming token, generates a new token and redirects to the original application. When the user accesses one of the other federation-enabled applications within the same session, the IP will not have to show the sign-in form again, as it has already authenticated the user and the issued token is still available as session data. The separation of the authentication and authorization processes from the applications allows for reusing accounts and access policies. Any redundancy of identity information is avoided, which lowers the cost of management. A central STS enables the organization to define a uniform role system for all connected applications. Once the infrastructure exists, new applications can easily be integrated by just configuring them for the use of the STS.

**Self-Service Identity Management**: The operation of large, Web-based systems with many different users causes high administration costs. A vast amount of effort is spent on identity-related tasks like creating user accounts for new employees or resetting passwords.

To reduce management expenses, the tasks related to accounts and access policies are delegated to the users themselves as far as possible. Both IP and STS are equipped with management interfaces that are used by the account holders in a self-service manner. For the IP, this means, enabling users to make changes to their own accounts, like resetting passwords and changing contact details. Even the creation of accounts can occur without any dedicated staff involved, e.g. with online registration forms for anonymous users. In case of the STS, a self-service authorization mechanism can allow account holders to enter *activation codes* in order to put themselves in certain roles and, in a way, authorize themselves as foreseen by the business process. An obvious restriction to the self-service concept concerns the security aspect. Anonymously created accounts or role administration by users may not be suitable in high-security zones, but in other areas, close to 100% self-operating solutions can be achieved.

**Identity Federation of Enterprises**: Separate enterprises want to cooperate by the interconnecting of users, applications and systems. This includes problems for the arrangements of transcendental access to distributed processing and data sharing.

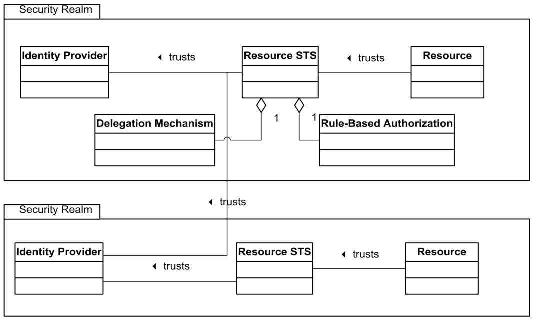

**Figure 2: Identity Federation of Enterprises**

As a solution, the security infrastructures of the partners are linked up by connecting their security realms, for example as depicted in Figure 2. Trust relationships are established between the STS of the realm where resources need to be accessed and the identity providers of the realms where the accessing users have their accounts. When a user accesses a resource, the responsible STS dynamically allocates the proper identity provider based on the rules of a delegation mechanisms. When the security token returns back from the IP to the STS, it is quite possible that the stated foreign identity is unknown in this realm. Therefore, an authorization mechanism should be applied that issues permissions depending on rules. Although the identification process is delegated to an external system, the partners are still in full control of their access policies. External users do not receive permissions unless this has been explicitly stated at the STS. Users of a federation partner do not need an extra account for the external sites and only sign in once at their enterprise. The full potential of this solution relies on the fact that the work of the users transcends organizational borders, as business processes demand.

# 4. SYSTEM SUPPORT BY idFS

In order to support distributed arrangements of Web applications and systems in correspondence with the proposed FIM, we implemented the Identity Federation System (idFS) as the necessary technological infrastructure. Along with security token services and identity providers, idFS also provides binding modules for a seamless integration of arbitrary Web applications and services as well as a Web interface for managing accounts from different sources (e.g. databases or directory services). The building block solutions are put into practice simply by configuring idFS components. An installable version can be downloaded at http://mwrg.tm.uni-karlsruhe.de/downloadcenter/.

# 5. REFERENCES

[1] Gamma, E., et al., Design patterns: elements of reusable object-oriented software. Addison-Wesley professional computing series. 1995, Reading.: Addison-Wesley. xv, 395.

[2] Witty, R.J. and Wagner, R., The Growing Need for Identity and Access Management, Gartner Article Top View AV-21-4512. 2003: Stamford, CT.