Introducing A-select, a Web Initial Sign-On System

Maarten Koopmans
Surfnet BV
maarten.koopmans@surfnet.nl

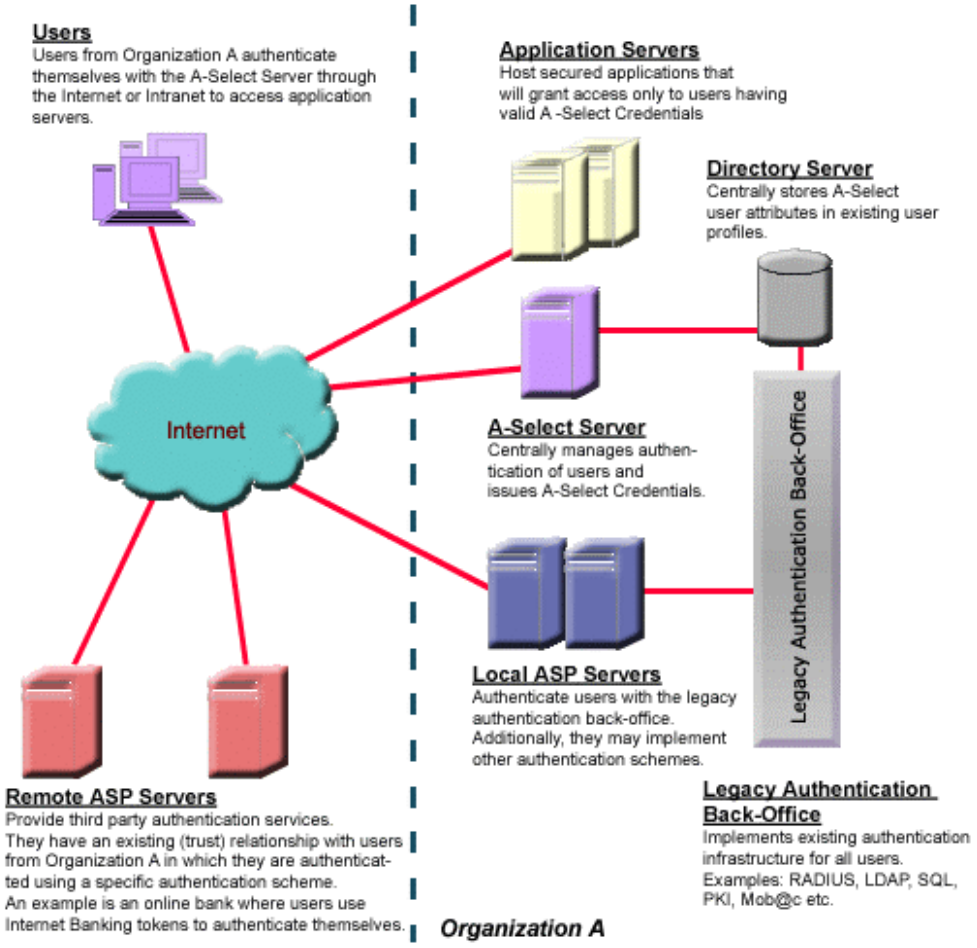
Ali Odaci
Alfa&Ariss
Ali.Odaci@alfa-ariss.com

Introduction

In higher education and research being flexible with authentication means and web single sign-on is becoming more and more important. Different user groups using different application sets require different authentication strengths and this typically implies adapting applications on a case-by-case basis. When collaboration - and thus cross-domain authorization- is required as well, web single sign-on becomes a complex issue. In this paper we present A-select, our authentication middleware designed to easily enable cross-domain authorization using multiple authentication methods.

Architecture

The A-Select systems consists of several components that communicate with each other in some way. The core components are depicted below.



A-Select Aware Applications

A-Select Aware Applications are Web applications that implement their access control according to the A-Select security and trust model. Applications may communicate directly with the A-Select Server for implementing this but may also use the A-Select Agent that offers convenient functionality for implementing A-Select security. There are also web server filters available for Apache and Microsoft Internet Information Server. Depending on the complexity of the application (e.g. how sophisticated is the level of personalization) some effort may be necessary to integrate an application.

A-Select Agent

The A-Select Agent is software (a lightweight server or daemon) that runs on the application server. The A-Select Agent itself offers an API that applications must use when using the agent. One of the advantages of the A-Select Agent is that it implements session management and generation of application tickets. These features are very convenient because Web applications mostly are not able to do this themselves due to the asynchronous nature of the HTTP protocol.

A-Select Server

The A-Select Server authenticates users in a transparent manner. For that purpose, the A-Select Server has a database in which information is stored about users and how they can be authenticated. Applications that need to authenticate a user will redirect him/her to the A-Select Server. When the user is authenticated, the A-Select Server will issue the user credentials and redirect him/her back to application. The A-Select Server does not authenticate users himself but rather redirects him/her to an A-Select Authentication Service Provider (ASP). The A-Select Server maintains a registry of all ASP servers and also knows which ASP can authenticate which users and for which applications.

A-Select Authentication Service Provider

An A-Select Authentication Service Provider (ASP) is a server that knows how to authenticate a user in some manner. Typically, an ASP offers a Web front-end for traditional authentication systems like RADIUS, LDAP authentication etc. ASPs may be local or remote.

Requirements.

In the design of A-select the following points have been taken into consideration:

- Institutions have their own user-base with their own **local** administration. Trust relations between institutions may exist, e.g. students following courses on different faculties, universities.
- Policies regarding authentication strengths are locally different (very heterogeneous).
- It is very hard to force people to use a certain kind of token. Better let them use what they have/know already.
- Applications should not be aware of authentication methods.
- Smooth integration with existing infrastructure is crucial for success.

Implementation.

A-select has been implemented using common technology. Except for the Apache and IIS web server filters (written in C) all code is written in Java. Configuration information such as authentication means of users can be stored in a relational (JDBC-compliant) database or in an LDAP database.

The following Authentication Service Providers exist:

- RADIUS, also available in our 802.1x implementation for network access.

- LDAP
- IP-based
- Mobile phone (one-time password using SMS), also available in our 802.1x implementation for network access.
- Banking card

All this means that one can deploy all components of A-select on most platforms, integrating it with e.g. a directory service initially. For specific groups of users some applications can then be selected to test new (stronger) authentication means, e.g. using a banking card for somebody from the financial administration accessing an application from home. It is straightforward to implement new ASPs and thus add new authentication means.

Cross-organizational A-select is realized by exchanging certificates out-of-band to establish a trust relationship between two A-select servers. Users can then be referred to their "home" A-select server to authenticate when accessing a remote site. In the long run (2003/2004) SAML support will provide bridging to authorization and federated administration frameworks such as PERMIS, SPOCP and Shibboleth that will provide more sophisticated cross-domain authorization.

Use cases

Right now A-Select is being used as middleware for the following end-user applications:

- Blackboard, an Electronic Learning Environment. Used with LDAP authentication
- Citrix, a remote desktop solution with banking card authentication or the mobile phone.
- A web shop for campus licensed software with the banking card
- An application that allows students to see their grades with their banking card
- Reading Outlook web mail form home or elsewhere (off-campus) using RADIUS authentication.

In the next few months support will be added for Oracle web portal as well.

As A-Select is free for not-for-profit organizations we expect a good adoption outside the research and academic community as well. We are already experiencing a growing interest for A-Select from other organizations outside research and higher education, such as governmental agencies.