scintel

Technology for a Changing World

Architecture Assessment Case Study

Single Sign on Approach Document

PROBLEM:

Existing portal has Sign on Capabilities based on the SQL Server database and it's not having essential features to support both Internal and External user's authentication. Internal users are to be part of the client Active Directory and External Users needs a custom database. Apart from this, current mechanism has the following issues:

- Remembering multiple passwords for deferent applications.
- Administration overheads in terms of maintaining the large number of users (e.g., Provisioning, Deprovisioning, etc,).
- Too many set of applications of with deferent usernames and passwords.

TYPICAL PICTORIAL REPRESENTATION OF TO BE SOLUTION:

SOLUTION:

The objective of SSO is to allow users access to all applications with a single account. It provides a unified mechanism to manage the authentication of users and determine user access to applications and data.

The principal functionalities of an SSO system are as follows:

- A limit of 1 account per user to control access to several applications or websites.
- User logs in once and gains access to all applications / websites without being prompted to log in again at each of them.
- Single Sign-off: a single action of signing out terminates access to multiple applications / websites.
  By default, each application will verify that the session managed by the SSO system is active before giving the user access to the requested pages.

FUNCTIONAL ASPECTS OF THE SYSTEM:

The main functionalities and technical components provided by SSO system are as follows:

The objective of SSO is to allow users access to all applications with a single account. It provides a unified mechanism to manage the authentication of users and determine user access to applications and data.

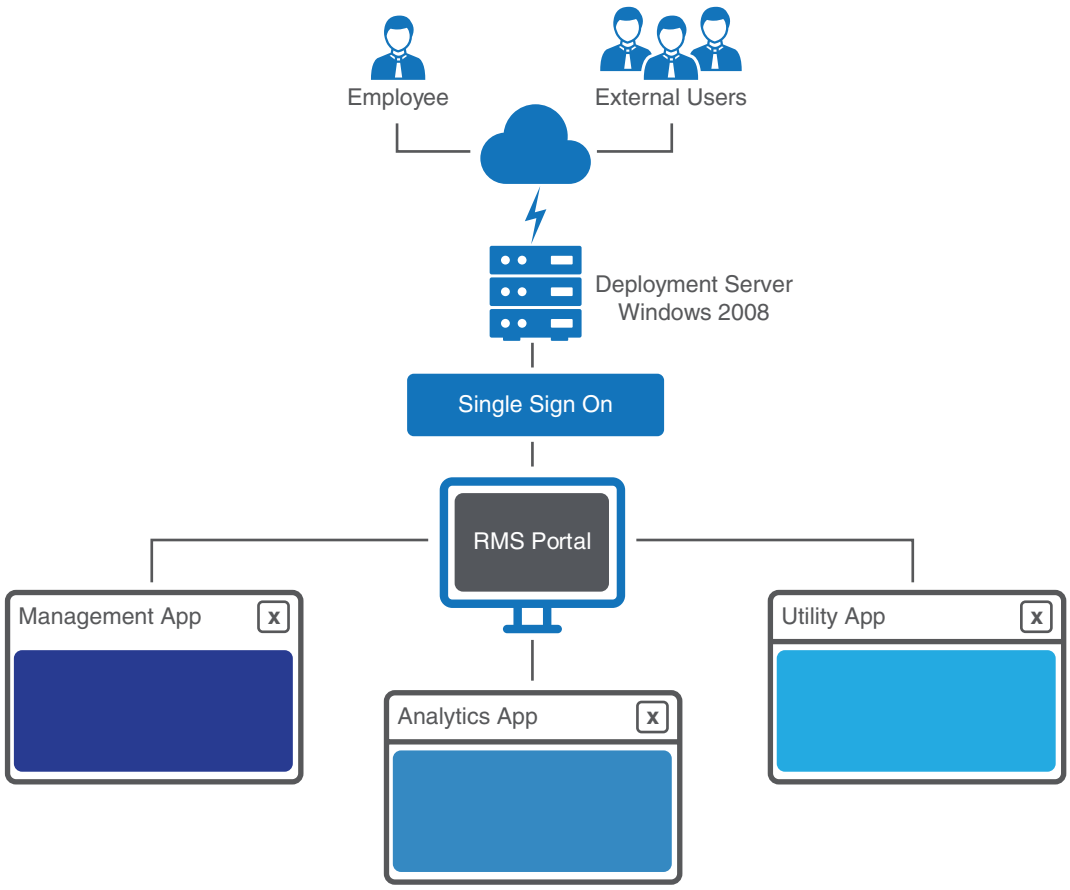
1. A front-end that allows users to.
2. Identify themselves and to memorize all or a part of their credentials via a login window or web portal.
3. For Web SSO, the front-end will automatically redirect users that navigate between federated sites the user will immediately arrive at each new site having been correctly authenticated and secured, transparently and automatically.
4. A back-end that will manage the authentication and the user session.
   - The system provides a centralized authentication server that all applications and websites use for authentication purposes.
   - The user first authenticates to a trusted authentication authority - the SSO system - and is then granted access to all the applications trusting that authority.
   - The SSO system preserves the state of the user for a period of time, so the user may repeatedly access the applications/ websites without needing to authenticate each time.

PILOT INFRASTRUCTURE USED:

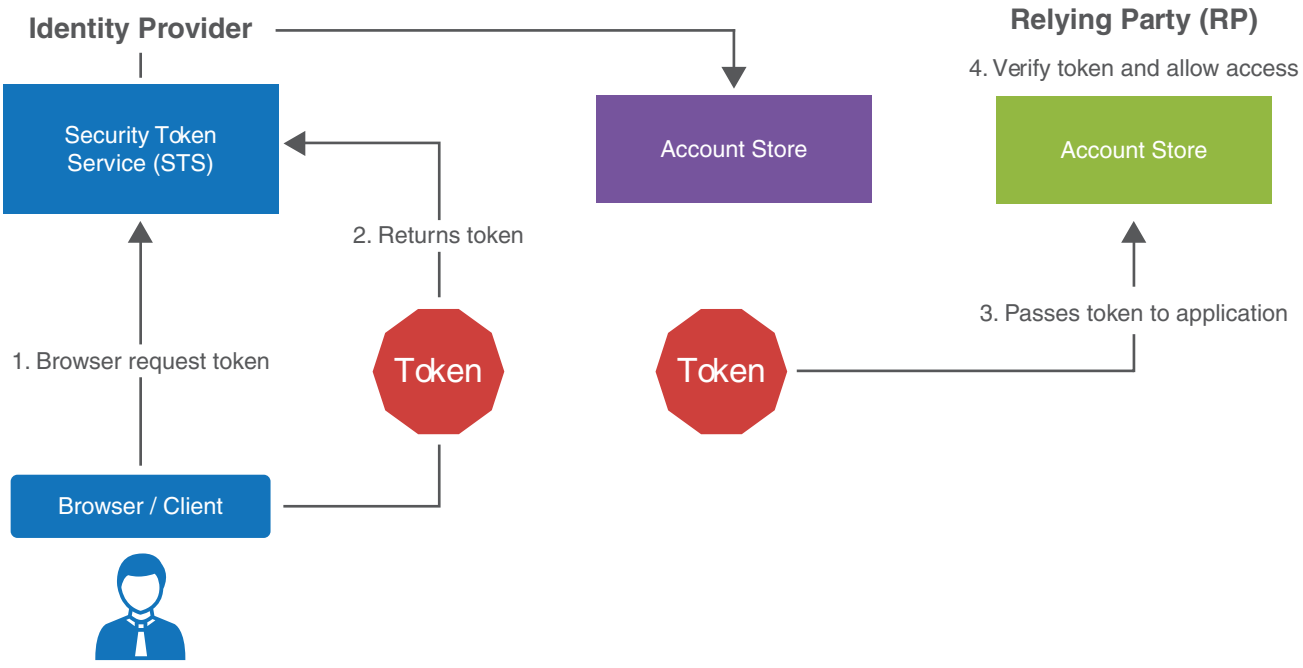
Software:

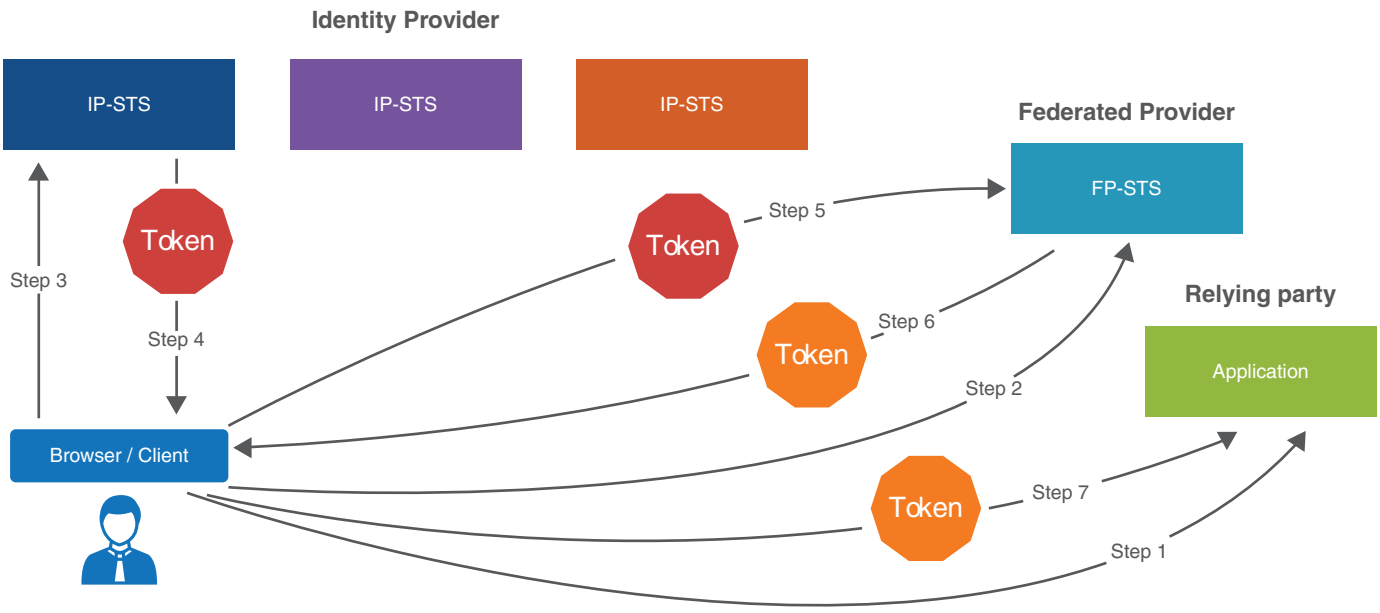
- Windows Server 2008 Enterprise Sp2
- Internet Information Services (IIS) 7.0
- Microsoft .NET Framework 4.0

FLOW DIAGRAM



TYPICAL SCENARIO: STEPS INVOLVED





Step 1: User accesses the Relying Party Application.

Step 2: As user is not authenticated, Relying Party application forwards the user to its trusted Identity provider (here Federated Provider to get authenticated).

Step 3: Now the federated provider, itself is not an Identity Provider It relies on several other Identity Providers. So it gives a list of Identity Providers to the user to get authenticated.

Step 4: Now the user gets a list trusted Identity Provider and it selects an Identity provider (where it has an account) and authenticates itself. Once authenticated, a Token is issued for the user by the selected Identity provider and passed to the Federated Provider.

Step 5: Now as Federation provider trusts the Identity provider, it can understand the token. It first verifies the token and decrypts it if required. It verifies and reads the incoming token and issues a new token and transforms the Claims from Identity provider token using Claim rules (if any) to new token.

Step 6: The new Token (issued by FP) is passed to Application (Relying Party).

Step 7: And this token is forwarded to Relying Party. As relying party trusts the federated provider, it can understand the token and verifies it and once verification gets successful, it allows access to the application.

THE CLIENT:

Our client, a health care major serves more than 50% of American hospitals, 20% of physicians and 100% of health plans, and as the largest pharmaceutical distributor in North America.

INDUSTRY:

Health care.

BUSINESS NEED:

- Remove the complexity in main training and remembering username/password for deferent applications.
- Reduce the administrative over heads in maintaining more number of users.
- Ability to support internal and external user's authentication.

SCINTEL SOLUTION:

- Delivered Single sign-on system (SSO) with a centralized server to handle authentication for all the applications and websites.

BENEFITS:

- Growth and scalability.
- Increased Revenue.
- Simplified Administration.

 | Scintel Technologies Inc. 6340 Sugarloaf Parkway Suite 200, Duluth GA 30097 | 678-775-6874 | info@scintel.com